

# Wearing Many Hats

**DATA &  
SOCIETY**

The Rise of the Professional Security Hacker

---

Matt Goerzen  
Gabriella Coleman



# Executive Summary

Today, the global computer security industry is booming, with thousands of well-compensated and well-respected jobs. And in many cases, these jobs are being done by those who self-identify as “hackers”—a term now openly embraced by many high-profile security researchers. This was not always the case, however, and the professionalization of the hacker figure was far from a foregone conclusion. At the end of the 1980s, many in the computer security establishment considered hackers to be talented but disreputable criminals—the people they were trying to secure their systems against. How, then, did the term “hacker” (and the hackers them selves) make the transition from security risk to security professional?

*Wearing Many Hats* presents one series of answers to that question, by collecting a previously un-told history of the 1990s. It was during that period that the figure of the hacker underwent a transformation, moving from the “underground” of the 1980s subculture, into the domain of respected employment, favorable media coverage, and cultural status—all of this best symbolized by the 1998 testimony of the L0pht before the US Senate. That is, a notorious “hacker crew” dressed in suits and broadcast on TV as various senators applauded their good works of citizenship. While the contestation over the hacker identity was far from resolved, the work of creating a legitimate professional role for the hacker had been accomplished.

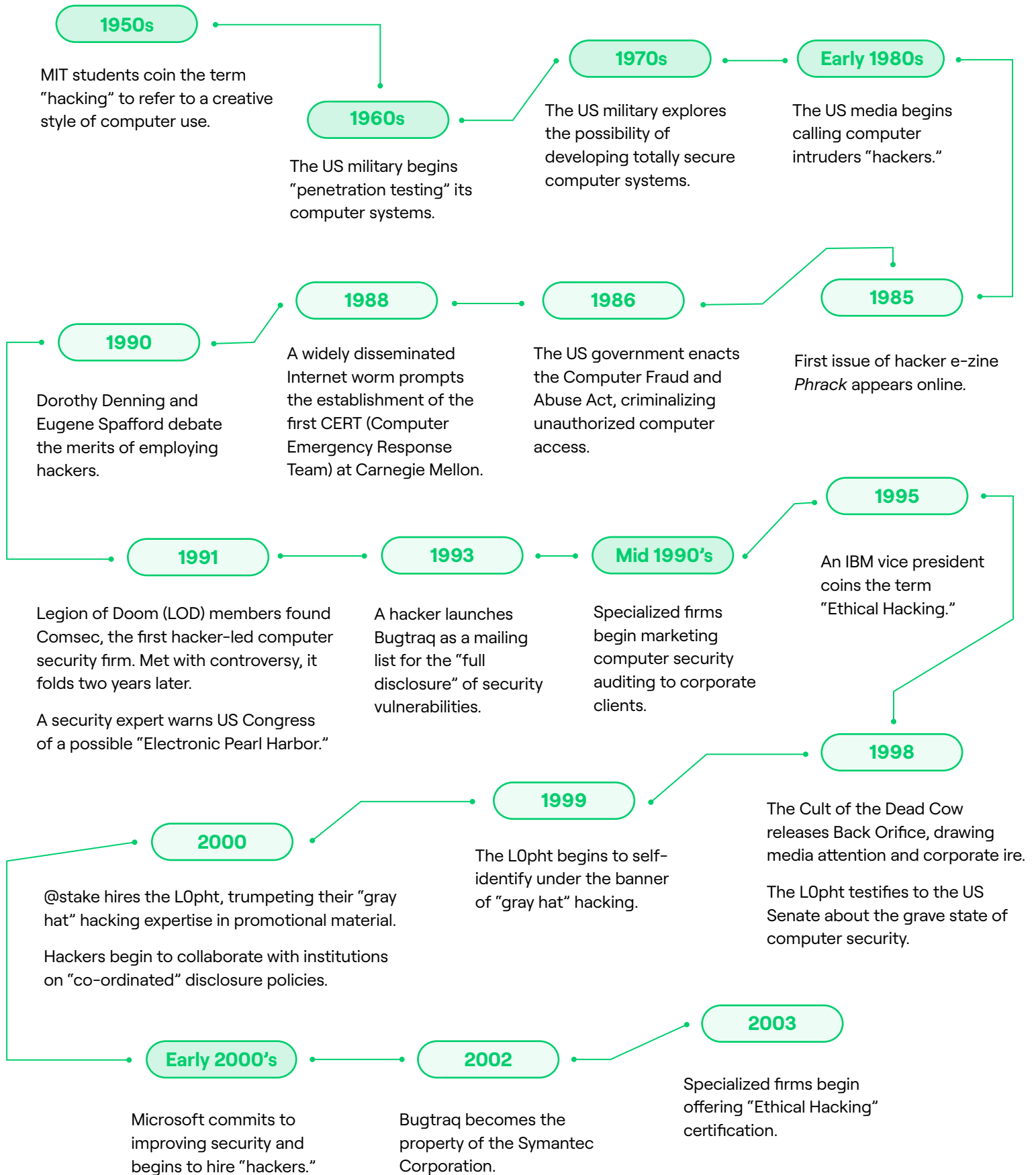
But it had been *work*. During the decade of the 1990s, two primary (and parallel) struggles defined the process by which hackers went from underground to professionals. The first of these was the negotiation of *full disclosure*, a controversial security procedure, in which independent hackers and technologists openly published full accounts of any vulnerabilities they discovered. Rather than exploiting these vulnerabilities, or chastely reporting them to the companies, hackers used full disclosure to simultaneously develop the technical state of their craft and to pressure software companies into what they saw as more responsible security practices, ultimately shifting the

public perception of computer insecurity.

The second major effort was largely non-technical, and was the broad reconfiguration of the hacker image through PR stunts, media collaborations, and rhetorical inventions. It was during that period that many hackers began to evoke imaginary hats. “Black hat” hackers were those who disregarded the law, “white hat” hackers tried to work inside of it, and “gray hat” hackers (like those that testified in 1998), lived somewhere in between: touting the technical skills of the hacker underground, but willing to sign contracts and work “above” ground.

The literal white-and-black morality of these hats, however, can mask ongoing negotiations around ethical commitments in computer security. By the early 2000s, the role of the hacker had been successfully professionalized, but the question of just what counted as security—security for whom, security from what—remained a point of open debate. The 1990s professionalization of the hacker class had set the stage for the next period of struggle over the concept of security in the modern world.

# Timeline



# Table of Contents

Executive Summary	02
<b>1.0</b> Introduction	06
<b>2.0</b> The Emergence of the Underground (1980s)	12
<b>3.0</b> Interlude: Safecrackers or Security Guards? (1991–1994)	25
<b>4.0</b> Full Disclosure (1991–2001)	28
<b>5.0</b> Interlude: Arsonists or Firefighters? (1990–2000)	41
<b>6.0</b> Public Legitimacy Through Media Work and Corporate Engagement (1995–2000)	43
<b>7.0</b> Conclusion: Security by Spectacle and the Limits of Legitimacy	63
Acknowledgments	68
Bibliography	69

# 1.0 Introduction

- 1 Steve Morgan, “Cybersecurity Talent Crunch To Create 3.5 Million Unfilled Jobs Globally By 2021,” *Cybercrime Magazine* (blog), October 24, 2019, <https://cybersecurityventures.com/jobs/>.
- 2 Steve Morgan, “Global Cybersecurity Spending Predicted To Exceed \$1 Trillion From 2017-2021,” *Cybercrime Magazine* (blog), June 10, 2019, <https://cybersecurityventures.com/cybersecurity-market-report/>.
- 3 For a similar trend in cryptography, whereby the monopoly on encryption held by the state was broken by another group of hackers, notably the cypherpunks, see Levy, *Crypto* and Greenberg, *This Machine Kills Secrets*.
- 4 See Nissenbaum, “Hackers and the Contested Ontology of Cyberspace” and Sterling, *The Hacker Crackdown*.
- 5 Also known as the “digital underground” or “computer underground.” This term seems to have been emic to the hacker subculture from its creation sometime in the 1980s. “Underground” served as the go-to term in the hallowed hacker zine *Phrack* to describe both particular hackers and the scene in which they participated. The following description is typical of how the term was used: “Taran King is back for a special *Phrack* Pro-Phile with Lex Luthor, the founder of the Legion of Doom and perhaps the most legendary underground hacker ever,” See: Dispat, “*Phrack* #40 File 1 of 14,” *Phrack*, August 1, 1992, <http://www.phrack.org/issues/40/1.html>.
- 6 Rosalie Steier, “News Track: Just Say No,” *Communications of the ACM*, May 1990.

## <change log [a.k.a., corrections]>

On page 20, in footnote 51, an earlier version of this report incorrectly referred to the Chaos Communications Congress as the Chaos Computer Congress.

On page 54, an earlier version of this document incorrectly cited Reid Fleming as the legal name of cDc member “Oxblood Ruffin.” Reid Fleming is in fact a different cDc member. “Oxblood Ruffin” is a pseudonym of Laird Brown.

On page 55, an earlier version of this report attributed a quotation to an unnamed cDc member. This has been updated to directly attribute the quotation to Sam Anthony (“Tweety Fish”).

The computer security industry is booming. Jobs are bountiful and profits are high. Security companies in the United States, Australia, Israel, and elsewhere are desperate to hire talent. Between 2019 and 2020, 715,000 people held cybersecurity positions in the United States alone, and another 314,000 positions were unfilled.<sup>1</sup> Industry analysts describe growth in the cybersecurity market as “stratospheric,” estimating its worth will reach US\$170.4 billion in 2022.<sup>2</sup> One of the premier professional security conferences, Black Hat, declared another record-setting year in 2019, with more than 20,000 attendees. Its community-driven counterpart, DEF CON, attracted an estimated 30,000 participants.

While “security researcher” is a common title for those working in this industry, many of these technologists also openly call themselves “hackers.”<sup>3</sup> But a few decades ago, very few firms, government agencies, or companies offering services in computer security were willing to openly hire hackers—or admit to hiring them. Indeed, in the 1980s and for much of the 1990s, while many in the “underground” hacking scene proudly embraced the hacker label, the hacker figure was nothing if not controversial. In the mainstream media, popular culture, and even government circles, “hacker” designated a particular type of computer criminal who broke into systems, stole data, and caused serious damage.<sup>4</sup>

The 1980s and 1990s generations of these underground hackers frequently communed in exclusive and secretive associations, digitally picking every lock they could find to roam the internet’s nooks and crannies. They treated computer infiltration like a sport, identifying vulnerabilities, honing new techniques, and writing up the exploits necessary to come and go as they pleased, frequently sharing information with their peers. They contributed to a growing body of knowledge, a decentralized but collective culture replete with local customs, de facto norms, and reputational appraisals: the hacker underground,<sup>5</sup> or simply “the scene,” as insiders often called it.

Even if potential employers believed these hackers held advantageous technical skills—and many did—their outlaw status raised serious questions about their trustworthiness. Indeed, in the early 1990s, esteemed academic critics even advised the fledgling computer security industry to steer clear of hiring any technologist willing to break into systems.<sup>6</sup> How, then, did perceptions of that class of hacker go from untrustworthy and suspicious to valued computer security experts, not only entering the computer security industry as prized workers, but also having fundamentally shaped contemporary cybersecurity norms and protocols? When did hackers become a



source of security, rather than its (perceived) enemy? In other words, how did hackers legitimize their craft?

The answers to these questions are tied up in a history that not only involves computer networks and software security, but also rhetorical flourishes, public stunts, and clever PR. In some ways, these efforts are symbolized by a struggle over the color of imaginary hats; during the 1990s, many of those interested in the security of computer networks began to signal their relationships to laws and norms with a new set of jargon that channeled, at first, an ethical binary: “white hat” hackers tried to work with companies and governments to legitimate themselves as security experts whose skills could help improve systems and keep users safe, while “black hat” hackers were proud to flout legal protections, to hack for their own ends, and to keep underground knowledge about security vulnerabilities within their community. And while the imagery of white and black hats channels a stark morality of good and bad, the reality is far more complicated. In fact, by the end of the 1990s, a subset of hackers claimed a third shade; “gray hat” hackers claimed to offer the best of both worlds—their associations with the hacker underground maintained their subcultural credibility and access to exclusive security knowledge, but they were also willing to leave the shadows, sign contracts, and work with companies and governments.

This report is foremost concerned with what underground hackers did—technically, linguistically, and culturally—to establish their legitimacy as employable, trustworthy security experts.<sup>7</sup> There was no single coordinated plan of legitimization—and indeed, many hackers did not understand their activity in this conceptual frame—but countless individuals and influential hacker “crews” worked in parallel, demonstrating skill by developing novel attack and auditing methodologies, refining processes of disclosure, and reforming their collective image. They educated journalists about their technical craft and virtuous intentions, launched media campaigns, engaged in linguistic re-engineering, or deployed linguistic code switching to obfuscate their past deeds. A few even sought to cultivate sympathetic pop cultural representations.<sup>8</sup> Looking back, we can see two significant interventions as exemplary of these legitimization efforts.

The first key intervention centered on the advocacy and practice of an informal security protocol called “full disclosure.” Full disclosure rebuked the popular practice, then prevalent among both establishment tech organizations and the hacker underground, of keeping information about computer insecurity carefully siloed and out of the public view. The most pointed engagement in full disclosure occurred on a mailing list called Bugtraq, started in 1993 as a platform for hackers and researchers operating outside of institutional confines to publicly document and publicize newly discovered technical vulnerabilities. In doing so, Bugtraq created a space for hackers interested in courting legitimacy as security researchers to dialogue and commune with institutionally aligned technologists and others convinced that

7 The question of expertise and professional legitimacy form a touchstone in the anthropology and sociology of science and technology studies (see Ballesterio, *A Future History of Water*; Boyer, “Thinking through the Anthropology of Experts”; Folch, *Hydropolitics*; Merry, *The Seductions of Quantification*; Hull, *Government of Paper*; Hetherington, *Guerrilla Auditors*; Riles, *Financial Citizenship*; Ho, “Disciplining Investment Bankers”). One of the canonical texts in this corpus is Steven Epstein’s work on “lay expertise.” (Epstein, *Impure Science* and Epstein; “The Construction of Lay Expertise”). His work examines not only how ACT UP activists and HIV+ patients acquired the knowledge necessary to contribute to the science around medical treatment, but credibility as legitimate and trustworthy participants. This report is indebted to Epstein’s framing, even as it provides a counter-example to aspects of his study; unlike the lay-experts he examines, the hackers profiled here often held equal or even greater knowledge about some aspects of security as established experts. But like Epstein’s lay-experts, hackers still faced the need to establish their professional legitimacy given lack of credentials and often engagement in legally fraught activities. Like the lay-experts, those hackers interested in engaging with the field of computer security had to walk a fine line: simultaneously antagonizing the establishment (to contest their characterization) and exhibiting a willingness to work in a professional setting.

8 For instance, Dave Buchwald (“Bill From RNOC”), a member of the Legion of Doom (LOD), served as a technical consultant on the 1995 movie *Hackers*. The movie portrays a diverse group of New York City-based underground hackers, who come together through various hacking exploits. They struggle to foil a computer security officer’s plans to defraud his employer and frame the protagonists for the deed.

public discussion was conducive to the improvement of security.

The second key intervention was rehabilitating the public image of the hacker, in order to undo the criminal associations of the 1980s underground. Hackers rebuilt their moral credibility through a range of linguistic, rhetorical, and mediatic labor. That involved coining terms like “gray hats,” but also strategically interfacing with journalists, developing controversial software tools, and launching sophisticated campaigns designed to vilify software vendors, most notably Microsoft. These efforts were assisted by allies, inside and outside of the US government, who saw some of these hackers as noble security experts advocating for the public interest—and sometimes underscoring concerns of growing import to the national security establishment.

Owing in part to these interventions, hackers ultimately became respected, frequent fixtures in conversations about computer security. That legitimacy became nearly incontrovertible in 1998, when the United States Senate invited seven hackers—part of a group called the L0pht—to testify to the pressing need for greater attention to computer security. Not long after, in 2000, the same group joined a freshly minted computer security firm called @stake. The company boasted in PR material of their merger with a “renowned hacker think-tank.” As they put it, “This strategic move reflects the firm’s commitment to build a world-class team of professionals offering non-traditional, e-commerce-age security solutions for clients.”<sup>9</sup>

By the turn of the millennium, formerly vilified hackers gained the potential to occupy legitimate—even privileged—roles in security companies and institutions.<sup>10</sup> Against the backdrop of the late-’90s dotcom boom, then the specter of the Y2K problem, and subsequently a post-9/11 security obsession and the steady rise of e-commerce, many hackers found a welcome home in a booming security sector shaped, in part, by their earlier interventions. Many joined companies, while others started their own, or served as consultants in both the public and private sector.

This report details how hackers were able to redeem their image sufficiently for many of them to be deemed trustworthy experts and employees of governments and corporations. Still, even if they were able to help define and participate in the public-interested pursuit of securing technology, the security methods and imperatives that consolidated in the 2000s were also narrow in scope; their focus was overwhelmingly on technical matters, like finding and patching vulnerabilities. Other types of social insecurity and risk stemming from the use of networking technologies—such as harassment, surveillance, and the targeting of civil society activists—were only substantially addressed later by different types of communities and actors. The lack of diversity in the underground scene and the early security industry—both populated overwhelmingly by white men—might have also precluded a more expansive vision of what technological security entails, an issue we raise in our conclusion and will engage with more

<sup>9</sup> “The L0pht, Renowned ‘hacker Think-Tank,’ to Join @stake: Receives \$10 Million in Initial Backing from Battery Ventures,” *@stake Events & News* (archive.org capture), January 6, 2000, [https://web.archive.org/web/20000819004156/http://www.atstake.com/events\\_news/press\\_releases/launch.html](https://web.archive.org/web/20000819004156/http://www.atstake.com/events_news/press_releases/launch.html).

<sup>10</sup> For more on the varying ways hackers approached the prospect of professionalization, see: Nicolas Auray and Danielle Kaminsky, “The Professionalisation Paths of Hackers in IT Security: The Sociology of a Divided Identity,” *Annales Des Télécommunications*, 62 (2007): 1312–26.



substantially in a subsequent report.

This report is based on 23 formal ethnographic interviews, dozens of informal interviews, and analysis of archival data (Usenet and mailing list posts, reportage, recorded conference talks, advisories, text files, books, technical journal articles, and other documentation), and concentrates on the period between 1991 and 2001.<sup>11</sup> While we focus on hacking in the US context, some of our interview subjects came of age in European hacker communities, interfacing increasingly with US hackers as the internet expanded. The dynamics at play in other Western countries were often similar, but different in notable ways that we leave outside the scope of this study. Likewise, the question of how hacking in what Anita Say Chan has called “peripheries” relates to the story of visibility and legitimization told here is a subject worthy of more attention.<sup>12</sup>

The body of this report is divided into three sections with two interludes. Following this introduction and a brief discussion of key terminology section 2, “The Emergence of the Underground,” sets the stage for the rest of the report by summarizing some foundational aspects of the 1980s and early 1990s hacker scene, such as hacker motivations, demographic attributes, and subcultural dynamics. Section 3 serves as a brief interlude describing the resistance that two professionally minded hackers met in the early 1990s, providing context for the hacker-led interventions discussed in the remainder of the report. In section 4, we explore the significance of the controversial full disclosure approach to security research, focusing on the history of the Bugtraq mailing list, launched in 1993. Section 5, our second interlude, showcases the polarized tenor of the debate regarding hacker motivations and trustworthiness in the early 1990s. Section 6 covers how hackers built moral credibility by castigating the negligence of big corporations and courting media attention, as well as the role played by hacker allies in government, the academy, and the nonprofit sectors, who worked alongside hackers to help refashion their image.

The history of legitimization explored in this report is not the full story. Some participants in the computer underground were less than thrilled by the incorporation of hackers into the computer security establishment. Some fought back, maligning those deemed as white hats, and even hacking some of them to cast aspersions on their capabilities. Many already-professionalized security researchers remained suspicious of the hacker newcomers and their methods. And offshoots of the 1990s hacker underground, including hacktivists and political activists, would challenge the very notion that technical improvements to security necessarily served the interests of the public.

Nevertheless, this account offers some insights into the ways hackers gained public legitimacy, and also helps us ask larger questions about security. How are issues nominated as matters of concern? Whose perspectives mattered and why? How might those left outside the security establishment continue to influence the security agenda?

<sup>11</sup> Other studies have laid out dynamics in the hacker scene of the 1980s and early 1990s: See for instance Sterling, *The Hacker Crackdown*; Thomas, *Hacker Culture*; Jordan, *Cyberpower*.

<sup>12</sup> Chan, Anita Say. *Networking Peripheries: Technological Futures and the Myth of Digital Universalism*. MIT Press, 2013.

What does it mean that a domain so consistently equated with technical matters relied on social processes, such as media spectacle and extra-institutional collaboration?

We briefly take on these questions in our concluding remarks, as they stem from the history we now turn to.

## 1.1 < Hacker Terminology >

First, it is worth establishing some core terminology. As will shortly become clear, nearly every term used in computer security discourse—not only hacker—is contested and polysemic, marked by a distinct valence tied to a given community of use. As such, in our report, we spend considerable time on linguistic politics, examining how and why different actors deployed terms like “hacker,” “white hat,” and “gray hat,” among others, to make claims about skills, disposition, and moral worth. Alongside analyzing such terminology, we also default, at times, to using the term “hacker” in a more descriptive register, as it was so commonly used by our interview subjects.

Indeed, we typically use the term “hacker” in its broadest sense: referring to those technologists who self-identified as such and were involved in various specific hacker subcultures of the 1980s and 1990s, and also those technologists interested in learning about computer security in a hands-on manner, typically outside of any institutional remit.

That said, it is useful to offer a bit of context about the term’s specificity for different communities of use. Many technologists working with computers in the 1980s modeled themselves as “hackers” in the mold of those Massachusetts Institute of Technology (MIT) students who first adopted the label in the 1950s to characterize their brand of creative, explorative computer use.<sup>13</sup> But those 1980s computer users focused on breaking into systems also saw themselves as “hackers.” As journalists latched on to the term to describe these digital rapsallions, the more high-minded technologists began referring to them as “crackers.”<sup>14</sup>

For their part, those hackers interested in breaking into systems often further qualified themselves as “underground hackers” or participants in the “hacker scene,” “computer underground,” “digital underground,” “hacker underground,” or perhaps most commonly, simply “the scene.” Some of these hackers were even more specific, referring to their subculture as the “H/P (Hack/Phreak) Scene,” the “HPAVC (Hack/Phreak/Anarchy/Virus/Carding) Scene,” or a related variant. The term “Phreak,” common in hacker publications like *Phrack*, was inherited from the 1970s “phone phreaks,” who spent time discovering ways to exploit pre-digital phone systems.<sup>15</sup> The addition of “Anarchy/Virus/Carding” signifies the overlap with subculturally adjacent activities with their own histories: the writing and distribution of anti-establishment text files, the exploration of computer viruses,

<sup>13</sup> Levy, *Hackers*.

<sup>14</sup> The term was coined circa 1985 “by hackers in defense against journalistic misuse of hacker,” according to the Jargon File—a vast compendium of hacker terminology. “Though crackers often like to describe themselves as hackers, most true hackers consider them a separate and lower form of life. An easy way for outsiders to spot the difference is that crackers use grandiose screen names that conceal their identities.” Eric Raymond, “Cracker,” *The Jargon File* (version 4.4.7), December 2003, <http://www.catb.org/jargon/html/C/cracker.html>. Suitably, the term “cracker” was also adapted by subcultural technologists, as a label for hackers focused on copy protection circumvention, a foundational aspect of software piracy (also known as “warez”).

<sup>15</sup> Phil Lapsley, *Exploding the Phone: The Untold Story of the Teenagers and Outlaws Who Hacked Ma Bell* (New York: Grove Press, 2013).

and the exploitation of long-distance calling cards.

Adding to the complexity of the term “hacker” was the emergence of technologists outside “the scene”—computer scientists, programmers, and systems administrators, among others—who were also invested in learning about computer insecurity. Some of these figures identified as hackers, while others did not; for those outside “the scene,” the term “hacker” was often treated as a marker of above-average technical ability, and had nothing to do with computer (in)security.

Where possible, we have also attempted to clarify any ambiguities by using terms like “underground hackers,” “institutional security researchers,” and “technologists.” But even these distinctions are unsatisfying for a variety of reasons, not the least of which is the dynamic we are most interested in here: the legitimization, and ultimately professionalization, of the underground hacker. That transition often witnessed underground hackers identifying as security researchers while still maintaining their hacker identity and underground status. For the above reasons, we sometimes use the term “security hackers” to characterize those figures for whom an interest and involvement in hacking served as an entry route to the broader computer security field.

It is tempting to see the subsequent typology of “hats” as further clarifying these complexities; in the 1990s, the labels “white hat hacker” and “black hat hacker” became popular as a way to distinguish between those hackers interested in using hacking-derived knowledge and techniques to enhance the security of digital infrastructure, and those hackers interested in hacking for dubious, malicious, or self-interested reasons. But in many instances, these qualifications only muddied the water further: was the application of hacker knowledge to enhance a client’s security not also a type of self-interest? And what about those cases in which “black hat” methods were essential for revealing the insecurity in the first place? Some treated “white hat” as a term for establishment-aligned professional security workers. Others treated it as a label for any hacker perceived to be operating in the public interest. Others still leaned into the term “black hat,” embracing it to signal dissatisfaction with the commodification of underground knowledge—using “white hat” as a pejorative shorthand for “sellouts.” Moreover, many hackers who would be identified as “black hat” in one aspect of their lives had quietly gone to work as “white hats” for early computer security companies, keeping their pseudonymous nonprofessional lives secret, even as they drew on the knowledge gleaned in one context to inform the other. And as we discuss in depth in section 6, some hackers advanced the term “gray hat” to recognize these ambiguities. For these reasons and more, we analyze these hacker-hat terms as historically important rhetorical material, but do not ourselves draw on them as a useful tool for qualifying particular types of hacker activity.<sup>16</sup>

<sup>16</sup> Other distinctions became salient after our period of study, mostly tied to professional areas of expertise (as in “offensive security” and “defensive security”), scene status (as in “active”) or political orientation (as in “hacktivist”), and will not be addressed in depth in this report.

## 2.0 The Emergence of the Underground (1980s)

See: Sterling, *The Hacker Crackdown*;  
 17 Meyer, “The Social Organization of the Computer Underground”; Assange and Dreyfus, *Underground*.

18 Lapsley, *Exploding the Phone*.

See Sterling, *The Hacker Crackdown*;  
 19 Driscoll, “Social Media’s Dial-Up Ancestor”; Driscoll, “Demography and Decentralization.”

The hacker “underground” community of the 1990s and early 2000s owed a tremendous amount to what has been variously called the “digital underground,” “computer underground,” or “H/P (hack/phreak)” scene of the 1980s.<sup>17</sup> Made up of hackers and phone phreaks, the underground consisted of technologists who banded together into small and secret associations of various kinds, focused on gaining access to phone or computer systems. In the 1980s, long before the advent of the publicly accessible internet, the phone network was king—whether as a direct object of exploration, as for the phone phreaks,<sup>18</sup> or as a means to connect to Bulletin Board Systems (BBSes) or Private Branch Exchanges (PBX).<sup>19</sup>

Indeed, in the 1980s (and well into the 1990s), much of the underground’s activity relied on BBSes. Often maintained by just one person, BBSes were frequently run off home computers equipped with software that allowed participants, using the triad of a phone, modem, and computer, to connect to file troves, messaging systems, and even chat rooms. Largely using pseudonyms (in part because most BBS software limited usernames to eight characters), hackers and phreaks flocked to BBSes to post and share various informational goods, like software, documentation, or their own literature of text files and electronic zines.

The hacker underground of that period included a motley set of participants: self-directed technology enthusiasts, moonlighting computer science students, writers publishing in digital zines like *Phrack* and hard-copy subcultural magazines like *2600: The Hacker Quarterly*, software crackers, and various scene hangers-on. A few hacker groups achieved real notoriety (both inside and outside the scene) during that period. These tended to be small groups, composed of anywhere from 3 to 15 members who collaborated and shared information with each other, and who increasingly advertised their exploits with obscure, edgy, acronym-heavy group names. Famous examples include the Legion of Doom (LOD), the Masters of Deception (MOD), and the Cult of the Dead Cow (cDc).

Taken together, these publications, crews, boards, and distributed social networks constituted a complex subcultural “scene”<sup>20</sup>—one that far exceeded any single micro-culture, crew, or BBS. In the growing number of publications churned out, these technologists etched out expectations and boundaries of various kinds, especially around technical skills, ethical and aesthetic sensibilities, and cultural knowledge.

It is also helpful to understand the identity of that scene in relation to its foils. Most significant in the 1980s were the “telcos”—the

20 See Straw, “Some Things a Scene Might Be” and Hebdige, *Subculture*.

- 21** Nicolas Auray and Danielle Kaminsky, “The Professionalisation Paths of Hackers in IT Security: The Sociology of a Divided Identity,” *Annales Des Télécommunications*, 62 (2007): 1312–26.
- 22** “Most hackers regard credit-card theft as ‘poison’ to the underground, a sleazy and immoral effort that, worse yet, is hard to get away with.” (Sterling, *The Hacker Crackdown*). Carding for financial gain also rammed against a dominant justification for illicit access: to learn about the systems. To card as an end, instead of a means for access in the pursuit of intellectual edification or solving puzzles, was further considered intellectually lazy and beneath them. This points also to the unrelenting intellectual elitism common to the H/P scene in the 1980s—an elitism that continued to manifest, often with little push back, in the 1990s.
- 23** That said, the more general enterprise of “carding”—using calling cards or credit cards to acquire stuff or services for free, beyond need—was typically snubbed. In this way, we can understand the early hacker allowance of illegality in service of need as exemplary of what Chris Kelty calls a “recursive public”—a public devoted to the maintenance of a condition which their existence depends upon. See Christopher Kelty, *Two Bits: The Cultural Significance of Free Software* (Durham: Duke University Press, 2008).
- 24** Morris was also the son of then-NSA chief scientist Robert Morris Sr. By most accounts, Morris Jr. created the worm as a hands-on academic exercise to see what was possible. More information on the virus-writing underground, which flourished in the early 1990s, and its complex relationship with the nascent antivirus industry can be found in: George Smith, *The Virus Creation Labs: A Journey into the Underground* (Tucson, Arizona: American Eagle Publications, 1994). See also: Christopher Kelty, “The Morris Worm,” *Limn* Issue 1: Systemic Risk, January 2011, <https://limn.it/articles/the-morris-worm/>.
- 25** For more, see: Rebecca Slayton and Brian Clarke, “Trusting Infrastructure: The Emergence of Computer Security Incident Response, 1989–2005,” *Technology and Culture* 61, no. 1 (2020): 173–206.
- 26** CERT, as a private-public intermediary, sought to juggle the trust of big companies, the trust of government, and the trust of private and academic systems administrators. Often this meant not publicly disclosing vulnerabilities, or disclosing months after a report (once a patch had been developed), or disclosing in vague ways, to avoid losing the trust of big organizations. This disclosure avoidance even seems, in many instances, to have

telecommunications phone companies who controlled the connective infrastructure which both enabled and resisted the activities of the early hackers and phreaks. And indeed, while one of the most pronounced taboos of the underground hacker scene was profit-seeking behavior,<sup>21</sup> particularly “carding” or credit card theft,<sup>22</sup> early scene participants had no qualms about stealing and using phone cards to avoid paying for phone access.<sup>23</sup> At the tail end of the 1980s, two other foils became prominent, in the form of law enforcement and institutional gatekeeping. Both arrived in the wake of a high-profile incident: the Internet Worm of 1988. Written by Robert Tappan Morris, a graduate student at Cornell University, the worm (a piece of self-replicating code) spread far and wide on the early internet, prompting a costly clean-up process.<sup>24</sup> As a result, in 1990, Morris was subject to the first conviction under the Computer Fraud and Abuse Act (CFAA), a vague piece of legislation enacted in 1986 to prohibit unauthorized access to computer systems. Between the Morris conviction and “Operation Sundevil,” a US Secret Service-led operation launched in 1990 to crack down on “illegal computer hacking activities,” members of the hacker underground felt under attack, reinforcing a culture of secrecy, pseudonymity, and anti-establishment sentiment.

The Internet Worm also prompted the creation of the first Computer Emergency Response Team (CERT) at Carnegie Mellon University.<sup>25</sup> Designed to increase collaboration between academic researchers, government, law enforcement, and industry, CERT was widely regarded by hackers—and by many computer scientists and systems administrators—as a “black box.” Information reported to CERT would go in but would rarely come out, or so it seemed to them.<sup>26</sup> While CERT published public-facing advisories on the subject of newly discovered vulnerabilities, detractors found the time between vulnerability discovery and disclosure to be unduly long, and the advisories—if they appeared at all—to be scant on technical details. Moreover, some hackers felt they did not receive proper credit when their reports informed CERT activity, hampering their public recognition as legitimate experts. The desire for public information and discussion was often cited by technologists we spoke with as a major factor in the growth of open-access mailing lists devoted to non-academic security research in the 1990s. It was also a contributor to the hacker underground’s evolving role as a repository—if at times also a gatekeeper—of public security research.

## 2.1 < The Hands-On Imperative and Other Motivations >

The hackers we spoke with expressed a range of motivations for their interest in computer intrusion and the hacking scene. Most salient was the characterization of hacking as a sort of intellectually stimulating game. That could mean the satisfaction of discovering a vulnerability or figuring out how to exploit it—what multiple subjects described as akin to solving an intellectual puzzle. It could also mean



precluded information sharing with law enforcement. For more on this point, see: Charles C. Mann and David H. Freedman, *At Large: The Strange Case of the World's Biggest Internet Invasion* (Simon and Schuster, 1998).

**27** As our subjects explained, this could be as simple as the desire to play around on a different or rare operating system, at a time when dozens of operating system variants were in use. Emulation was impossible, legitimate access was often not an option, and the cost of setting up a personal computer network was prohibitively expensive.

**28** Eliteness, or the goal of being “1337,” as an emic form of often self-parodic speech would have it, was subject to countless avid and satirical diatribes in the text files that proliferated throughout the decade.

**29** The dynamic between humility and elitism in various hacker communities, especially free software development, has been unpacked in Coleman, *Coding Freedom*. Not all hackers embrace elitism and even in the underground, a domain of hacking where elitism is more pronounced than in free software, some checks on its expression exist. Nevertheless, in this period and among underground hackers, discourses and posturing around elitism ran rampant. Indeed, such elitism was partly an outgrowth of an unquestioned commitment to meritocracy; displays of technical prowess were expected and it was fully acceptable to denigrate those deemed technically inferior. For a discussion on how meritocracy in engineering and technical circles works to reinscribe structural inequities see Slaton, “Meritocracy, Technocracy, Democracy” and Subramanian, *The Caste of Merit*.

**30** The exceptions were a couple hackers who believed their parallel computer science or software development careers would benefit from an engagement with hacker-produced knowledge, and one who saw hacking as an entry route to professional security work.

the satisfaction of hacking into, learning about, and “owning” a variety of different systems. Others described the thrill of discovery that came from accessing new systems and, in particular, encountering operating systems otherwise unavailable to them.<sup>27</sup> “It was a challenge to me, and I think to most others, just to see who is the smartest, who can access the most systems,” said one hacker we spoke with.

Some enjoyed the accrual of status and peer recognition that came from demonstrations of “elite” skills.<sup>28</sup> These demonstrations could be intellectual, as in the development of reproducible and reliable methods for exploiting vulnerabilities. They could also be performative, such as through the act of logging into an Internet Relay Chat (IRC) channel from a secure web server—an act that would demonstrate to everyone in the channel the feat of accessing the server.

Others rejected such performative status seeking, instead treating vulnerability discovery and exploitation as a near-scientific pursuit—sharing those discoveries that would advance the state of the art. “Every vulnerability is different and every one has a different challenge,” as one subject put it. “We wanted to just get the information out there and have other people to build on that [sic].” Otherwise, he continued, “There was almost a challenge of who can keep the lowest profile out there. What was expected was to participate in research and just come up with smarter ideas.” Importantly, that did not preclude the elitist and meritocratic disposition that was nearly ubiquitous in security hacking; rather, it favored recognition by a small group of elite figures over more general fame.<sup>29</sup>

Finally, there were those—technically proficient hackers in their own right—who were attracted to the scene as an end in itself, by a sense of camaraderie and desire for sociality. “I don’t think it had anything to do with technical anything, they’re just my people. Just smart outcasts, you know?” relayed one hacker. “To be honest, all of the hacker conferences I’ve gone to, I spend very little time at anything technical. It’s just about socializing for me. At DEF CON 3 [1995] we went out into the desert and fired guns, and launched fireworks, and fired guns at fireworks, with a bunch of people I had never met before. Many of whom went on to be friends, who are still friends.” Friendships, like the ones this hacker describes here, undergirded many of the most consequential hacker interventions discussed in this report.

Few of the hackers we spoke to expressed any recollection of being motivated by profit, careerism, social or political power, or even the desire to improve the state of security—at least not initially.<sup>30</sup> Rather, interviews indicate that most hackers during that period used their expertise to accrue knowledge and status, rather than accomplish more material personal or political goals. For instance, one respondent expressed regret about failing to take political action. His group had achieved access to the email servers of several powerful people, but never seriously considered scanning these for evidence of malfeasance—a “hack and leak” tactic that would become common among

<sup>31</sup> Coleman, E. Gabriella. “The Public Interest Hack.” *Limn*, 2017. <https://limn.it/articles/the-public-interest-hack/>.

<sup>32</sup> Levy, *Hackers*, 28.

<sup>33</sup> This latter practice involved sifting through the trash stored in large, often unlocked bins, outside of companies, and could become quite elaborate: mapping exactly where they were located, when they were locked, and when the best times to go were. Garbage contained a treasure trove of documentation, manuals, and print outs that included passwords—all helpful aids to facilitate computer intrusion or to fortify their knowledge of a system. Slatalla and Quittner, *Masters of Deception* contains a detailed description of a dumpster diving excursion in New York City by the founding members of the Masters of Deception.

hacktivists after 2011s.<sup>31</sup> Seen from that angle, then, it’s clear that even if power was not a significant initial motivator, these hackers possessed a form of “latent power”—the capacity to utilize their knowledge, access, and techniques to direct effect, even as most hackers held that power in reserve. Ultimately, that power would be drawn upon in later efforts to legitimize hackers as security professionals.

Whatever their motivations, hackers frequently sought to learn by doing. That reflects a commitment to what Steven Levy, in his book *Hackers: Heroes of the Computer Revolution*, identified as a core aspect of hacking since its beginnings: the “hands-on imperative.” Levy describes how the early hackers toiling away in labs at elite institutions like MIT during the 1960s were essentially experimenters and tinkerers. “Hackers believe that essential lessons can be learned about the systems—about the world—from taking things apart, seeing how they work, and using that knowledge to create new and even more interesting things. They resent any person, physical barrier, or law that tries to keep them from doing this.”<sup>32</sup> In the course of doing so, the early hackers learned how to build and improve systems, and indeed were integral to creating knowledge, theory, tools, and products that shaped both computers and computer science for decades.

For those hackers interested in security in the 1980s and early 1990s, the hands-on imperative was often the only way to learn about the subject of their intense interests, for two main reasons: First, security knowledge was carefully controlled by the academics, governments, and companies that possessed it. Disclosure of computer security issues and techniques to the public was not, at the time, seen as conducive to the project of enhancing computer security in a global sense. Second, while some computer science students managed to learn about security through extracurricular contact with research-involved professors or organizations like CERT, it was rare to find formalized academic courses, syllabuses, and textbooks devoted to security until the late 1990s or even early 2000s.

One hacker explained it thus:

Well, back then if you wanted to learn a system, you had two options. You can go to Barnes and Noble and hope that someone wrote a book on it, and then you probably couldn’t afford it because they’re probably 50 to 80 bucks. Or you could get manuals or information about it in the trash.<sup>33</sup> And actually, the third way is: you hack the thing. So back in ‘92 to ‘96 when I was really active, there was no Google, Yahoo! had next to nothing [...] There were sites on the internet by that point, FTP sites, and [they] had tfiles [text files written by hackers] [...] but hey, SunOS, HP-UX, AIX, [...] UNICOS on a Cray, you just don’t find many books on that shit.

Two of our subjects went so far as to break into physical buildings to acquire information. In one case, a 16-year-old skater-hacker with a rebellious personality flew to another state to hang out

with hacker friends he had met online. Once there, the small group gained access to a fenced-in Bell Telephone Company office parking lot and broke into company trucks. “Cause at the time that’s what everybody wanted was the gear and the documentation that you could only get if you worked there,” he explained. “And as kids, you can’t work there.” Materials obtained in that way functioned as both trophies and practical pedagogical tools.

Even an interview subject who pursued an academic computer science degree, and was thrilled to find a rare security-related job with CERT, expressed dissatisfaction about the anemic state of knowledge production. “I read everything I could get my hands on, on the net and otherwise. And there was a stack of papers about maybe an inch thick, inch-and-a-half thick, of everything I could find on computer security anywhere.” Eventually, he explains, he wanted to work more proactively to find vulnerabilities, write exploits, and develop automated methods for probing systems. “I left CERT in part because I wanted to do more work on programs and such, and I said to [my superior], ‘I’d like to write worm stuff and do some experimentation and write some stuff down,’ and he said, ‘There’s no way our sponsors will let that happen.’”

34 In fact, a few of our interviewees morally justified break-ins by explaining how they would fortify a system once in control, for instance by patching vulnerabilities. This wasn’t entirely altruistic, however; in part, they were motivated by a belief that this would help secure their own ongoing access. “In many cases we would actually fix broken stuff on those systems,” explained one hacker, “because we didn’t want an admin poking around any more than they needed.” Not only could their efforts prevent less careful hackers from gaining access and drawing admin attention, but by going above and beyond the hacker could pre-empt regular administrative attention.

35 The L0pht gathered old computer gear together into a shared workspace where they could legally simulate intrusions of networking environments. Other Boston-area hackers benefited similarly from the combined negligence and good will of MIT admins, who failed or benignly neglected to change passwords that were common knowledge in the local hacker scene—ensuring they would remain secretly available for any curious youngster who might want to try a new operating system, take a spin around the MIT network, or use it as a jumping off point to the internet. As one L0pht member recounted: “The Athena clusters were basically these rooms with like, one of those five push button locks on the door. And there would be like, you know, 15 Sun[OS] 2 and Sun[OS] 3 terminals in there. And they were on the internet. And the root password was ‘mrroot.’ So we got the code and we got the password, probably from [a hacker from cDc], I think. And so, like, we would, we would go there and have free access to those resources to explore.”

The hands-on imperative, then, was often the only way to go. And since being hands-on often implied illegally accessing things, the independent security hacker was almost by default defined by a willingness to break laws—though not necessarily with any ill will or nefarious intent.<sup>34</sup>

Some hacker groups, like the Boston-based L0pht, managed to cobble together the space and resources needed to build their own computer labs, or gain access to academic labs from sympathetic insiders.<sup>35</sup> But that was reportedly rare, especially at a time when many of our subjects considered themselves privileged just to have a PC connected to the internet in their home.

The knowledge attained by hackers in that morally flexible manner eventually underwrote their ability to publicly contest common institutional norms and practices for securing systems. By possessing that knowledge and drawing attention to the issues they identified as the sources of security problems, they were able to demonstrate ongoing insecurity and legitimize their expertise in the doing—topics we take up later in this report.

## 2.2 < Demographics and the Conditions of Accessing the Scene >

While the hacker underground of the 1980s and ‘90s was broadly shaped by anti-establishment cultural tenets and the push for access to information, it’s important not to divorce these from the embodied and demographic reality of the scene. The way these values

<sup>36</sup> Douglas Thomas went so far as to theorize hacker culture as a type of “boy culture” in his book *Hacker Culture* (see 75-76).

<sup>37</sup> Up until the early 1960s in the United Kingdom and the United States, women programmers and code breakers, initially hired as part of WWII war time labor efforts, had played prominent roles in these technical crafts (see Light, “When Computers Were Women”; Hicks, *Programmed Inequality*; Mundy, *Code Girls*). As a profitable industry around software took off, female workers were not only systematically sidelined and excluded, but the activity of programming, once seen as feminine, became re-coded as masculine (Ensmenger, *The Computer Boys Take Over*). Nascent hacking and phreaking communities established in the 1960s never attracted a sizable number of women (Levy, *Hackers*; Sterling, *The Hacker Crackdown*). As various hacking subcultures expanded and attracted different types of participants in the 1980s, hackers tended to uncritically embrace the ideal of meritocracy, mirroring the industry of the time (Coleman, *Coding Freedom*; Kelty, *Two Bits*). Many of these hackers downplayed or ignored cultural and structural barriers of exclusion, as they insisted judgement of others was based solely on assessing the technical worth of contributions. In the last decade, hacker communities across North American and Europe became less homogenous and, as documented by Christina Dunbar Hester’s ethnography of open content and hacker communities, by 2010 the ideal of meritocracy came under vigorous critique as feminist and diversity advocates attempted to encourage more inclusive spaces (Dunbar-Hester, *Hacking Diversity*). Even as the industry and many hacker communities have instituted laudable changes as a result of these changes and critiques, many problems around racism and sexism still plague these domains (Dunbar-Hester, *Hacking Diversity*; Amrute, *Encoding Race, Encoding Class*; Mullaney et al., *Your Computer Is on Fire*).

<sup>38</sup> Eric “Emmanuel Goldstein” Corley, the founder of *2600*, explained in an email correspondence with Gabriella Coleman that the “first meeting was in NYC on June 5th, 1987 at Citicorp Center. They were modeled after the old TAP meetings, which had also been held on Fridays in New York City as part of TAP Magazine, which ceased publishing in 1983. Our meetings remained weekly for 1987 and were changed to monthly after that in order to make them more of an event to look forward to.”

<sup>39</sup> Remarks by Eric “Emmanuel Goldstein” Corley, to Gabriella Coleman’s Class on

developed was inextricable from class status and the gendered and racialized identities of scene participants.

With a few exceptions, our interview subjects were overwhelmingly white men, which is representative of the hacker underground in our period of study.<sup>36</sup> Hacker subcultures have mirrored broader demographic trends in computing sectors since the 1980s, and our research echoes more general sociological and cultural explanations for disparate representation in technological cultures.<sup>37</sup> For instance, many of our interview subjects recount having computers in their household early on, thanks to parents who worked in nascent technology industries or adjacent academic fields like mathematics. Other parents had the foresight and resources to purchase computers for their children. For these subjects, an interest in hacking emerged as a natural outgrowth of their ability to explore these machines in intimate settings with parental encouragement. For those whose parents did not have the connections, wherewithal, or financial means to have a computer in the household, initial computing interest and skill was often contingent on other structural dynamics. For instance, one African American hacker we spoke with was thrilled to first encounter a computer owned by his parent’s colleague, gleaning time at the keyboard whenever possible before later gaining access to a computer lab made available to gifted students at his public school. Ultimately, he relays that his mother saved up for months to buy him a Commodore 64 as a birthday present, when the line of computers first hit the market at a more affordable price point compared to machines like the Apple 2 or Atari 600. After that, he recounts entering into the hacker scene through a mixture of natural curiosity and network exploration that mirrored the entry route of more privileged subjects.

Some hacker subcultural institutions made efforts to facilitate entry into the scene. For instance, those associated with *2600: The Hacker Quarterly*—a print magazine founded in 1984 and named after the frequency used to exert control over the pre-digital telephone network—promoted the creation of open, regional hacker meetups beginning in 1987.<sup>38</sup> Staff actively worked to prevent the publication, its meetups, and associated conference (HOPE, or Hackers on Planet Earth, founded in 1994) from evolving into hardcore technical affairs that could only be comprehended by the already technically proficient, making sure to include material accessible to newcomers and those curious to learn.<sup>39</sup> Yet that very push toward inclusivity was sometimes treated with scorn. In an illustrative dynamic, *2600*’s eschewal of technical elitism made it the subject of derision for a number of hackers we interviewed. These hackers expressed preference for those publications and conferences (like Black Hat, founded in 1997) that emphasized increasingly niche technical discussion, suggesting that cultural outlets like *2600* became fixated on activism and other political issues over the 1990s, while also serving to facilitate the entry of unskilled newbies into the scene.



Hacker Culture and Politics, January 21, 2020.

<sup>40</sup> The Mentor, “The Conscience of a Hacker.” *Phrack* 1 (7), 3 of 10, 1986. <http://phrack.org/issues/7/3.html>

<sup>41</sup> CITRIS, *Fireside Chat*, Dean Tsu-Jae King Liu and Window Snyder, Square, Inc., 2020, <https://www.youtube.com/watch?v=x65Nyy77-Hc>.

<sup>42</sup> Segan, Sasha. “Facing a Man’s World: Female Hackers Battle Sexism to Get Ahead.” *abc News* (archive.org), June 9, 2001. <https://web.archive.org/web/20010603002603/https://abcnews.go.com/sections/tech/DailyNews/hackerwomen00609.html>

While some hackers have argued that the anonymity afforded by the digital environment precluded discrimination (for instance, an influential *Phrack* article often referred to as the “Hacker Manifesto” includes the line, “We exist without skin color, without nationality, without religious bias... and you call us criminals”<sup>40</sup>), online discourse often assumed a white male subject. Hacker sociality was increasingly grounded in conferences and in-person meetups as the 1990s wore on. Interview subjects who fell outside of the default subject position report a mixed bag of discouraging and supportive encounters with other hackers.

Indeed, women were notably absent in much of the underground hacker scene and the public channels—mailing lists, conferences, or the industry—where security matters were being hashed out and eventually adopted. Those few women who participated sometimes felt unwelcome or were subject to harassment, leading to forms of discrimination that could be subtle or overt. “It was... a kind of space where there weren’t a whole lot of women, and it was not a friendly place. So a lot of folks who had something significant to contribute did not stick around,” explained Window Snyder—herself one of the most prominent security hackers in the field—during a 2020 fireside chat.<sup>41</sup>

A female hacker we interviewed told us that, while she connected with several supportive male hackers, some of whom became lifelong friends, she had to work hard to open certain doors that swung wide open for her male counterparts. As a teenager attending in-person hacker meetups in the Boston area, she was routinely ignored or treated as if her interlocutors incorrectly assumed she was the romantic sidekick of another attendee, and not someone there of her own volition and with her own ambitions. Online spaces did not offer refuge; she “quit IRC in 2000 because of the harassment.” A number of other hackers we interviewed noted the prevalence of derogatory epithets on IRC and hacker subcultural publications, and a quick scan of zines, tfiles, and IRC logs, particularly from the late ’90s, easily substantiates these assertions. As contemporaneous reporting makes clear, our interviewee was not alone in experiencing these practices as a barrier to participation.<sup>42</sup>

Women were also conspicuously absent from many of the crews that rose to prominence in the 1990s. One interview subject relayed that, while she and a few other female hackers had been in the same social circles as members of named hacker associations throughout the 1990s, “They never deputized us. They never invited us to be official members of the crew.” Discrimination hardly waned as she entered the nascent security profession—even as she helped to define and pioneer core security protocols, like bug bounty programs, for dealing with vulnerabilities. She faced pay discrimination at well-established firms, and many of her contributions—whether large or small—have been routinely overlooked or minimized.



Indisputably, some skilled non-white male subjects also faced barriers to inclusion in the hacker community. While regions like New York City were home to ethnically diverse, all-male hacker groups like the MOD, encounters with hackers in other regions could present difficulties. In one famous example documented in a book about the “war” between the LOD and the MOD, the myth of a “color blind” digital sociality was challenged when a Black MOD member called in to a phone bridge hosted by Texan hackers and was treated to a racist polemic about New York hackers.<sup>43</sup> More recently, some have brought critical scrutiny to the terms “white hat” and “black hat,” suggesting their perceived racial connotations could function as a barrier to participation.<sup>44</sup> While hackers have typically downplayed these particular concerns<sup>45</sup>—citing the terms’ historical origins and the pride with which some hackers owned the “black hat” label—there is growing acknowledgment that other terminology contributes to exclusionary dynamics and should be changed.<sup>46</sup>

<sup>43</sup> Slatalla and Quittner, *Masters of Deception*. See also Thomas, *Hacker Culture*, for a discussion of how some quarters of the hacker community reacted to this story’s publication and diminished its significance.

<sup>44</sup> Patricia Hswe et al., “Toward Anti-Racist Technical Terminology,” *The Association for Computers and the Humanities*, n. d., <https://ach.org/toward-anti-racist-technical-terminology/>.

<sup>45</sup> See Cimpanu, “Infosec Community Disagrees with Changing ‘black Hat’ Term Due to Racial Stereotyping.”; Carey, “If you think that ‘black hat’...”; Rosenblatt, “Block/Allow: The Changing Face of Hacker Linguistics.” *MalwareTech*, “Little confused by...”

<sup>46</sup> Marcus J. Carey, “Black hat and white hat terms have nothing to do with race...,” *Twitter*, June 12, 2020, <https://twitter.com/marcusjcarey/status/1271624977805185024>.

<sup>47</sup> Carey and Jin, *Tribe of Hackers* throughout, especially Carey’s own account on page 8.

<sup>48</sup> Our account builds on contemporaneous documentation of the 1990s hacker scene by observers like Bruce Sterling (*The Hacker Crackdown*) and scholars including Paul Taylor (*Hackers*), Douglas Thomas (*Hacker Culture*), and Tim Jordan (*Cyberpower*). We also benefit from a hindsight not available to these authors at the time: a concrete sense of the significance these hackers’ actions would have on later institutionalized computer security.

<sup>49</sup> We pay particular attention to the period after that documented by Bruce Sterling in *The Hacker Crackdown*. Our account benefits from a hindsight not available to sociologists like Paul Taylor, Douglas Thomas, and Tim Jordan as they wrote contemporaneous accounts of the scene—particularly, a sense of the significance these hackers’ actions would have on later institutionalized computer security.

Despite these dynamics and barriers, a number of hackers who defied the demographic stereotype rose to influential positions in the world of professional computer security. Others took less visible pathways into the hacker community, such as by emerging into the professional hacking field at the conclusion of military service.<sup>47</sup>

## 2.3 < The 1990s Scene Develops (1990s) >

Many describe the 1990s as a golden age for hackers, as they reigned and roamed as they pleased on the early internet—even if there was the occasional major bust.<sup>48</sup> In that period, the hacker scene developed from a collection of hobbyists sharing information of mutual interest and pushing the limits of access into a cultural enterprise with a sense of purpose: discovering, exploiting, and documenting vulnerabilities to advance the state of the art. For some, the pursuit of that state of the art remained an end in its own right. For others, it became a ticket to legitimacy and lucrative employment, a means of discovering profitable vulnerabilities, or part of the higher order pursuit of advancing security... or insecurity. All of those ends were made possible by the emergence of a robust cultural infrastructure that enabled the interchange of knowledge and the definition of a unique identity, most notably hacker conferences, in-person meetups, zines, IRC, and mailing lists. In the subsequent section, we will consider the significance of one exemplary mailing list, Bugtraq, in depth. But first, it’s worth surveying some of the other cultural dynamics that were crucial to the development of the hacker identity and subject position.<sup>49</sup>

With the growth of the internet, the prominence of BBSes gave way to IRC, email-based mailing lists, and ultimately websites where hackers and hacker groups could offer tools and advisories to broader publics. Electronic zines like *Phrack* became more readily accessible. All the while, hacker conferences appeared and grew in

**50** Said one, “To some degree, I think DEF CON is responsible for the security community existing.” Continuing, “I went home [from my first DEF CON and] started reading about security all the time that I could, started taking this open access to information, which is what revolutionized the industry. We used to keep these things secret ... and as soon as someone made a place for people to talk openly about it, where they weren’t going to get arrested, everything changed.”

**51** European hackers had the leg up—as with so many other hackerish pursuits, including hacktivism; Germany’s Chaos Computer Club launched an annual conference called the Chaos Communication Congress in 1984.

**52** For the latest figures, see defcon.org, “DEF CON Conference Transparency Report,” accessed January 25, 2021, <https://www.defcon.org/html/links/dc-transparency.html>. The estimate of 100 attendees for DEF CON 1 comes from a 1999 ZDNet article by Annaliza Savage. See: Annaliza Savage, “Remembering the First DEF CON,” ZDNet (defcon.org archive), July 5, 1999, [https://www.defcon.org/html/links/dc\\_press/archives/7/zdnet\\_remembering.htm](https://www.defcon.org/html/links/dc_press/archives/7/zdnet_remembering.htm).

**53** Maxigas and Guillaume Latzko-Toth, “Trusted Commons: Why ‘Old’ Social Media Matter,” *Internet Policy Review* 9, no. 4 (2020), <https://policyreview.info/articles/analysis/trusted-commons-why-old-social-media-matter>. See also: Maxigas, “Keeping Technological Sovereignty: The Case of Internet Relay Chat,” *Git-Book, Technological Sovereignty*, 2018, <https://sobtec.gitbooks.io/sobtec2/en/content/05irc.html>.

**54** The dynamics of this time are memorialized in many of the tfiles produced by these groups. One edition of *~EL8*, for instance, sees the writer giving tips for how to avoid having to answer tough technical questions—by quitting IRC suddenly with a spurious disconnect message, for instance. The ironic instructionals lampoon scene dynamics, even as they re-instantiate the ingroup and reaffirm the negative connotations attached to non-technical scenesters. Other tfiles give hints about new exploits, often by reproducing the actual logs generated by hackers as they go about their business.

**55** For a first-hand account by a participant in the cracker scene, see Anonymous, “So You Want to Be a Pirate?” 109–12. For scholarly discussion, see Rehn, “The Politics of Contraband,” Goode and Cruise, “What Motivates Software Crackers?” and Wasiak, “‘Illegal Guys’. A History of Digital Subcultures in Europe during the 1980s.”

popularity, alongside more frequent, locally organized, in-person meetups. Each of these sites offered ways for individuals newly interested in hacking to gain the basic skills and mindset, share knowledge, compete for membership in elite groups, and also come into contact with a broader scene—replete with particular ways of talking, doing, and being.

Some hackers we spoke with cited meetups and conferences as the main drivers of innovative, hacker-led security research.<sup>50</sup> Beginning with Summercon in 1991, a wave of hacker conferences proliferated across the United States.<sup>51</sup> The most famous of these was and remains DEF CON, which began in 1993 with around 100 attendees and now sees an annual attendance estimated to be over 30,000.<sup>52</sup> Many of our interview subjects attribute some of the most infamous hacker relationships of the 1990s to the local meetups listed in *2600*. By the early 1990s, *2600* had secured national distribution in popular stores like Barnes & Noble, and thus became accessible to many who may not have otherwise stumbled upon hacker cultural material.

For others, IRC was king. Invented in 1989 as a simple protocol for chat rooms, the technology became far more accessible during the mid-1990s as internet access proliferated. IRC offered numerous advantages over email or BBSing: it was easy to set up and any user could host their own channel on one of the networked servers, as long as the name wasn’t already in use. Moreover, on hacker-preferred servers like EFNnet, communications were shared only between those participants present on a given channel, with no intermediary storing the logs.<sup>53</sup> Channel operators (“ops”) could be vested with privileges to kick out or ban users and configure things like a “message of the day” that would appear to users as they logged in. Hackers chatted under pseudonyms, self-organizing into channels defined by subject of interest or group affiliation. IRC made it easy for hackers from around the world to be in real-time communication with one another. Participants could be periodically active and idle for years on end in channels like #phrack and #hack, waging endless flame wars, competing to log in from the most interesting servers, feuding with rival crews, surreptitiously attempting to gain channel operator status under false pretexts in order to kick out rivals, and hocking their latest exploits in bids to gain status or membership in the most elite groups.<sup>54</sup> Groups sometimes formed alliances, shared members, and probed one another for information about exploits they could trade. Other times, exchanges between groups or individuals devolved into intense rivalry and conflict.

On IRC, the hack scene also dovetailed with the increasingly popular “warez” scene, where a different class of hacker (who self-identified as “crackers,” in the sense of “software cracking”) would produce and dispense pirated programs—sometimes embedded with malware.<sup>55</sup> That community could function as a feeder for the hacking scene, with some of our interviewees noting that curious and often

<sup>56</sup> The varying statuses of these different pursuits can be difficult to neatly sort out. High-level security hacking, like the discovery of complex vulnerabilities and development of exploits, seems to have been unquestionably of higher status than warez cracking. But the sorts of reverse engineering and programming skills involved in high-level cracking were greatly respected across the board, earning the best practitioners there more regard than lower status security hackers, with “script kiddies” being the lowest status alongside those involved in less technical aspects of warez (distributing, packaging, user interface design, etc.)

<sup>57</sup> For another example of a contemporary security hacker who credits the game cracking scene for acting as the gateway to security work, see Ryan Naraine, “Matt Suiche, Comae Technologies,” MP3, Security Conversations, accessed January 25, 2021, <http://securityconversations.fireside.fm/matt-suiche-comae>.

<sup>58</sup> While not exclusively rooted in the warez scene, Joseph Menn has tracked a similar dynamic related to the IRC-focused w00w00 security group. See: “WhatsApp And Napster Were Spawned From An Elite Security Posse Called ‘Woowoo.’” *Business Insider*, March 7, 2014. <https://www.businessinsider.com/r-elite-security-posse-fostered-founders-of-whatsapp-napster-2014-07>

<sup>59</sup> In one amusing anecdote, a subject relayed how his group was amicably granted editorial control over *Phrack* by its acting editor after they hacked the site and took over registration of the domain name.

<sup>60</sup> Most famously: the so-called gang war in cyberspace between the Masters of Deception and the Legion of Doom in the late 1980s and early 1990s. See Slatalla and Quittner, *Masters of Deception*.

<sup>61</sup> While the name derives from the first letters of the founding members’ names, the crew was never referred to as anything but TESO.

<sup>62</sup> Various, “Phrack #64 File 15: International Scenes,” *Phrack*, May 27, 2007, <http://phrack.org/archives/issues/64/17.txt>.

talented warez acolytes were drawn to what was considered a higher status and often more challenging form of illicit puzzle solving.<sup>56</sup> “You would be surprised to see the number of important people in computer security today that trace their origins to the ‘90s cracking scene,” said one of our respondents, who credits the warez scene with teaching him the reverse engineering skills that would prove invaluable to his later professional security work.<sup>57</sup> He compared the “copy protection community” to the collegial sports clubs that act as social preening mechanisms for lawyers and other professionals. “It was like a very medieval bizarre thing, [but] it turned out the 1990s cracking scene ended up being essentially the global fraternity for tech.”<sup>58</sup>

Nearly every hacker we spoke with noted the importance of a digital magazine called *Phrack*. It served as both a repository of knowledge and a crucial site where fame and eliteness could be negotiated—whether through the publishing of new vulnerabilities, reports on local scenes, “pro-photos” of notable hackers, or maneuverings into editorial control (we spoke to no fewer than four hackers who had assumed that role).<sup>59</sup> And by all accounts, *Phrack* deserved its reputation. As one hacker put it, “*Phrack* was almost a Bible to everyone because of the quality of the articles.” Another explained, “If you look at the citation counts that *Phrack* racks up, there’s a few important *Phrack* articles that have a much higher impact rating than almost every academic computer security [article].” Even those subjects we spoke to involved in institutional security research, including one employed with the National Security Agency during the 1990s, noted that *Phrack* was required reading, both for adversarial research and as a source of novel knowledge.

Nevertheless, as one researcher who worked for CERT in the early 1990s made clear, *Phrack* was not initially recognized as a legitimate source of knowledge within the institutional computer security world. “I was a believer that if you understood the mindset and the techniques that were used, you’d have a much better chance of protecting yourself. [...] It was not unprecedented, but it was not a common thought [among the establishment security community] at the time. [There was] not a lot of great stuff [in *Phrack*], but once in a while there was a really important bit in there.”

As they assembled more original research, hackers began to make decisions about how such privileged knowledge should be shared and with whom. That contributed to complex social hierarchies, constituted most notably by the creation of hacker crews—intellectual secret societies whose boundaries and circles of trust were constantly being renegotiated in often dramatic and exciting ways.<sup>60</sup> Against that cultural infrastructural backdrop, groups with names like TESO,<sup>61</sup> ADM (Association De Malfaiteurs—roughly translated as the Association of Evildoers or Criminals<sup>62</sup>), w00w00, THC (The Hacker’s Choice), and h4gis (Hackers and Geeks in Snowsuits) sprung up, while older crews like LOD and MOD floundered or, as in the case of the cDc, adapted and flourished.

While most hackers we interviewed were members of one or more named hacker associations (the exception was a female hacker, which is quite telling of the gender dynamics of the time), the configuration of these groups varied significantly. Some hacker affiliations of the era were composed of people who also spent most of their offline time together—they sometimes lived in the same apartment and spent weekends alternating between clubbing, or other forms of revelry, and hacking. Other groups emerged from what were essentially online watering holes, full of participants who bonded but did not meet in person, except perhaps at conferences or, later, industry functions. Some groups were nationally bounded in scope, like the highly respected<sup>63</sup> and predominantly French contingent ADM, who were also known as an “active” group, which is to say they not only developed exploits but also used them to gain unauthorized access to computers.<sup>64</sup> Others were resolutely international, like the research-oriented group w00w00, whose members spanned both sides of the Atlantic and were sometimes affiliated with other groups, including ADM. And yet another type emphasized in-person activity and maintained collective spaces to work, like Boston/Cambridge-based L0pht and the Seattle-based Ghetto Hackers. The maintenance of a computer lab could facilitate security research without strictly necessitating the penetration of networks “in the wild.”

<sup>63</sup> This respect was ranging; a former NSA hacker told us that in the early 2000s he and his colleagues “saw them as our peers.”

<sup>64</sup> As one hacker we spoke with put it, “Not only was ADM writing more sophisticated code, they were also using it. Because they actually hacked.” This hacker went so far as to argue that only those “active” in illegal forms of hacking deserve the mantle of “hacker” at all. This distinction was common in the “black hat” discourse that emerged in the late 1990s—and will be a major subject of a subsequent report.

<sup>65</sup> We will address this issue more substantially in a subsequent report.

<sup>66</sup> Most infamously, in order to draw public attention to internet censorship in China, cDc invented or greatly exaggerated their connection to an ostensible Chinese dissident hacking organization called the Hong Kong Blondes. See Oxblood Ruffin, “Blondie Wong And The Hong Kong Blondes” and Menn, *Cult of the Dead Cow*.

<sup>67</sup> As Joseph Menn describes in *All the Rave* (2003), w00w00 started as an invite-only IRC channel which drew in independent security researchers and also members of existing hacker groups.

cDc was one of the more public groups, and unusual insofar as it had both a security focus and a hacktivist bent. While some members were highly technical, originating in groups like the L0pht, others were more focused on writing text files of a political nature or provoking companies (or “vendors,” in subcultural parlance) like Microsoft. It’s notable that the great majority of hackers we looked at for this report steered clear of hacktivist activities, and the hacktivism of the time was quite separate from the security underground.<sup>65</sup> As we explore later in this report, cDc’s contributions lay more in their capacity to make noise over human rights abuses or embarrass Microsoft for its dubious security practices. Often that involved media stunts, always spectacular in nature and sometimes fueled by outright disinformation, rather than advances to the craft of technical security research.<sup>66</sup> Those priorities meant opinions about cDc were polarized among technically oriented members of the scene.

While each of these group types had different micro-cultures and approaches to hacking, aspects of their social dynamics tended to be more uniform. Membership was exceedingly controlled and exclusive. The L0pht, for example, had a few roster changes in the first half of the 1990s but otherwise remained fixed until it became incorporated into the @stake computer security firm in 2000. By comparison, w00w00 was in some ways more open, with membership sometimes ascribed to whoever happened to appear in its password-protected IRC channel, though gaining access was no trivial feat.<sup>67</sup> Pecking orders between groups and even between members within groups were constantly being negotiated. Intergroup



<sup>68</sup> One hacker, for instance, told us he welcomed this competitiveness for the way it incentivized more research.

rivalries, sometimes gentle and playful, other times much harsher, were common.<sup>68</sup> Intense camaraderie and friendships (and so, too, betrayals) were typical within groups. The processes to vet new members varied, but as is the norm across the hacking spectrum, candidates had to prove themselves in one manner or another—by tests of knowledge on IRC, vetting by peers, or demonstrations of valuable exploits.

Hackers and groups also began to create websites in the mid-1990s. These were used to host tools, vulnerability documentation, exploit code, and text files. Massive troves of knowledge formerly sequestered on private BBSes were suddenly more accessible. And websites disseminated new “advisories” and press releases to alert the public about discovered vulnerabilities or cutting-edge tools, usually imitating or parodying the institutional forms used by organizations like CERT. Hackers used websites to cultivate visual identities and foster associations with other groups and figures through links and access to shell accounts and email addresses.

These public materials enabled interested hackers to develop a broad base of knowledge simply by reading, limiting the need for the hands-on imperative and illegal exploration. But it also marked the rise of the “script kiddie,” an unskilled hacker who, as the name implied, knew just enough to run a script that would allow them to access a system, but not enough to ensure they did so responsibly. Being condemned as a “skiddie” was the opposite of being praised as elite. For some, the existence of those figures fueled a growing desire for the improvement of security. Others were infuriated by the way skiddies advanced negative stereotypes of hacking or drew unwanted attention to the methods they relied on to access systems.<sup>69</sup>

<sup>69</sup> Hopper, Ian, and Richard Stenger. “Large-Scale Phone Invasion Goes Unnoticed by All but FBI.” *CNN.com*, December 14, 1999. <http://archives.cnn.com/1999/TECH/computing/12/14/phone.hacking/index.html>

Those trends meant that as the 1990s progressed, the hacker underground simply wasn’t so underground any more—hacker crews were gaining notoriety, companies and governments were increasingly interested in security, and hacking materials were more and more available. That prompted security-minded hackers to make significant decisions about where and how to position themselves in the emerging security field.

In what follows, we document that process through two efforts that were central in transforming a fringe, underground subculture into a security-minded public whose participants were increasingly recognized as trustworthy, legitimate experts in computer security. First was the advancement of the full-disclosure philosophy of vulnerability disclosure, which advocated the public release of information to enhance knowledge, empower independent systems administrators, and pressure companies and institutions to increase their security. Primarily sited on hacker-led mailing lists, the approach triggered polarizing debates, even as it ultimately facilitated exchange between hackers, institutionally aligned security researchers, and even company representatives. The second effort, which resulted in a transformation of the popular perception of hackers, entailed linguistic



and journalistic interventions used to signal hackers' sound intentions as they publicly flogged vendors like Microsoft for their shoddy security. The two efforts helped ensure that professional security hackers would come to occupy positions of prominence in security circles at the turn of the millennium, just as fears of a "Cyber Pearl Harbor" attack on critical infrastructure, the Y2K bug scare, and the 9/11 attacks were fueling computer security pushes in both the public and private sector.

## 3.0 Interlude: Safecrackers or Security Guards? (1991–1994)

*“Would I hire a safecracker to be a security guy at my bank?”*

After a wave of governmental crackdowns in the late 1980s and early 1990s, some hackers began exploring other avenues for their interests. Whether motivated to push companies to confront the insecurity they knew so intimately, or by a sense that it might be possible to turn their passions into careers, a number of underground figures started to reprioritize—beginning with some early attempts to create hacker-led private security companies. In many ways, the story of how that became possible—and what it took to make that possible—is the story of this report.

The experiences of Scott “Doc Holiday” Chasin and Chris “Erik Bloodaxe” Goggans are instructive. Against a backdrop of hacker arrests and an escalating feud with a rival crew, these two LOD hackers decided to found a security company in 1991, alongside fellow LOD member Jake “Malefactor” Kenyon Shulman.

According to our interviewees, Comsec Data Security, Inc. was almost definitely the first hacker-led security company.<sup>70</sup> Yet, as this report will show, it was also established fully ten years before the hacker scene can be recognized to have gained the legitimacy it needed to interface unfettered with the corporate and computer security establishment.

Nevertheless, Comsec in many ways provided a template for what was to come: offering “systems penetration testing, auditing, and training services as well as security products.”<sup>71</sup> And in the short term, it would demonstrate the many impediments that stood in the way of hacker professionalization.

At the time, a *Computerworld* reporter captured the significant reputational challenge facing Comsec:

The announcement was met with skepticism, “Would I hire a safecracker to be a security guy at my bank?” asked John Blackley, information security administrator at Capitol Holding Corporation in Louisville, Kentucky. “If they stayed straight for 5 to 10 years, I might reconsider, but 12 to 18 months ago, they were hackers, and now they have to prove themselves.”<sup>72</sup>

Comsec was dogged with suspicions from both the underground, where it was accused both of selling out fellow hackers to gain legitimacy and leveraging their ostensible legitimacy to

<sup>70</sup> Two other LOD members would also found a pathbreaking company called MindVox in 1991, one of the first Internet Service Providers.

<sup>71</sup> Michael Alexander, “Hackers Promote Better Image,” *Computerworld*, June 24, 1991. See also: David Ellis, “After You’ve Beat ‘Em – Join ‘Em,” *Time*, June 24, 1991, <http://content.time.com/time/magazine/article/0,9171,973222,00.html>.

<sup>72</sup> Ibid.

<sup>73</sup> Slatalla and Quittner, *Masters of Deception*.

<sup>74</sup> Michael Alexander, "Group Dupes Security Experts," *Computerworld*, July 29, 1991.

<sup>75</sup> Message titled "Wanted: hackers for tiger team (New England area)." Sent by Brad.Powell@ebay.sun.com to the Firewalls and Bugtraq mailing lists on October 3, 1994. Archived at: <https://seclists.org/bugtraq/1994/Oct/35>. And indeed, these sorts of suspicions—that hackers invited to audit source code would leak vulnerabilities to the underground—were a major source of distrust. According to our sources, the concern was not always hypothetical.

<sup>76</sup> Palmer, C. C. "Ethical Hacking." *IBM Systems Journal* 40, no. 3 (March 1, 2001): 769–80. <https://doi.org/10.1147/sj.403.0769>.

<sup>77</sup> Anthes, Gary H. "Safety First." *ComputerWorld*, June 19, 1995.

<sup>78</sup> Palmer, "Ethical Hacking."

undermine rival underground groups.<sup>73</sup> The mainstream business world accused it of conducting espionage of other businesses, exploiting its company status as a false pretense.<sup>74</sup>

By the end of 1993, Comsec had folded. But by the end of the decade, Goggans and Chasin were both respected security researchers. That outcome was not inevitable; it was the product of a slow, sometimes calculating and sometimes incidental process of legitimization.

Some in the computer industry saw the appeal of hiring hackers from the beginning. But anxieties were front and center. As put in a 1994 message from a Sun Microsystems security analyst, cross-posted to multiple mailing lists in response to a request for trustworthy hackers willing to perform penetration tests:

We don't want to pay someone to bang on the doors and then tell us ½ of our bugs and then tell the cracker community [*sic*] the other half :-):-( :-([...] Its a matter of integrity [*sic*], a trait that is not commonly associated with crackers too often :-\ . Too bad \_some\_ of them show some real promise. [...] trust is something to be earned not assumed.<sup>75</sup>

By the mid-'90s, the US computer industry was coming around to the value of the "techniques of the hacker"<sup>76</sup>—if not to the value of the hackers themselves; notably, the IBM vice president for internet applications is credited with coining a now-common industry buzzword, telling *Computerworld* in 1995 that the company would start offering "ethical hacking" services like penetration testing for clients.<sup>77</sup> He stopped short of suggesting that anyone from the hacker scene would conduct the work. As one of the architects of the initiative later elaborated, that was intentional:

One rule that IBM's ethical hacking effort had from the very beginning was that we would not hire ex-hackers. While some will argue that only a "real hacker" would have the skill to actually do the work, we feel that the requirement for absolute trust eliminated such candidates. We likened the decision to that of hiring a fire marshal for a school district: while a gifted ex-arsonist might indeed know everything about setting and putting out fires, would the parents of the students really feel comfortable with such a choice? This decision was further justified when the service was initially offered: the customers themselves asked that such a restriction be observed. Since IBM's ethical hacking group was formed, there have been numerous ex-hackers who have become security consultants and spokespersons for the news media. While they may very well have turned away from the "dark side," there will always be a doubt.<sup>78</sup>

One early computer security consultant describes encouraging colleagues in federal law enforcement to hire Goggans

<sup>79</sup> M. E. Kabay, “An Interview with Jerry Harding,” *Ubiquity* 2004, no. May, accessed January 26, 2021, <https://ubiquity.acm.org/article.cfm?id=1008529>.

<sup>80</sup> Ibid.

<sup>81</sup> Pleon, “Security Design International and Trust Factory Announce Security Vulnerability in Lotus Notes,” ResponseSource Press Release Wire, August 2, 2000, <https://pressreleases.responsesource.com/news/8397/security-design-international-and-trust-factory-announce-security-vulnerability-in/>.

<sup>82</sup> Mark Abene, *Hack in the Box 2007: Mark Abene Keynote Address (Complete)*, 2012, <https://www.youtube.com/watch?v=bdr0-iF4k6Y>.

in 1991, after the hacker announced that “He would work for anyone who would not force him to cut his hair.”<sup>79</sup> Policies against employing people engaged in illegal activities served as stumbling blocks to that course of action. So, after the consultant expanded his own firm’s remit in 1994 to deal with security issues, he hired Goggans himself. Nevertheless, he was concerned that customers would be wary of giving hackers access to their systems during penetration tests. “To address the risks of hiring former criminal hackers, I used Chris only in education while we were building that trust relationship.”<sup>80</sup> He also amusingly notes that despite Goggans’ earlier pronouncements, he had “cut his hair down to almost military standards” by the time he landed full employment at WheelGroup, a security consultancy founded by ex-Air Force technologists in 1995 and later acquired by Cisco Systems. Goggans would subsequently found a security consortium called SDI (Security Design International), a company which offered “expertise in infrastructure vulnerability assessment, security network architecture, and the application of enabling technology such as PKI [Public Key Infrastructure] security solutions,”<sup>81</sup> and serve as CTO of a vulnerability assessment company called PatchAdvisor.

Chasin was also in it for the long haul, chartering a series of companies in the years that would follow—not all of them security related; in 1995, he established USA.NET, for which some credit him with inventing web-based email, before delving into the professional side of the computer security industry once again, as CTO of McAfee, and later co-founder and CEO of Protectwise.

These hackers were not alone in quietly joining the burgeoning mid-’90s cyber security workforce—moving from underground association with outlaw peers into collegial professional relations with ex-military computer experts and insurance company wonks. Among others, Mark “Phiber Optik” Abene—one of the most visible members of LOD’s archival MOD—quietly went to work in the early auditing and penetration testing field after serving out a hacking-related prison sentence between 1992 and 1994.<sup>82</sup> Undoubtedly, the professional attitude with which these figures comported themselves behind the scenes did much to recuperate opinions about hackers in the corporate world. But the employment of hackers was not something companies would begin to acknowledge or advertise until the turn of the millennium, when their public image had been revamped.

The question remains: what changed in that decade to allow the hacker scene to be treated not only as a security threat, but also as a resource—an expert labor pool that could be tapped in service of computer security?

## 4.0 Full Disclosure (1991–2001)

Shortly after the failure of Comsec in 1993, Scott Chasin founded the Bugtraq mailing list as an informal, publicly accessible venue where anyone interested in security could share computer security vulnerabilities and discuss protocols for their redress. Quickly becoming popular among a gamut of technologists, it served as a major node of what came to be known as the full disclosure movement. It also laid much of the groundwork for the future professional success of Chasin and his hacker peers.

In essence, those who supported full disclosure believed that vulnerabilities in computer hardware, software, and networks were best addressed not by keeping them secret, but by publicly disclosing and discussing them. Focusing on Bugtraq, we will argue that it and other outlets of full disclosure functioned as what scholar Peter Galison has called a trading zone,<sup>83</sup> with a variety of outcomes. First, it opened up knowledge about vulnerabilities to a wider audience. Second, it served as an intermediary space for security researchers, computer scientists, vendors, and hackers to engage, share information, and develop new vocabularies and methods for security research. Third, it grounded debates about the ownership of vulnerabilities and exploit code—and the question of credit in security research more generally. Fourth, it enabled hackers to compete for accolades and accrue reputation—effectively gamifying the process of vulnerability discovery and enabling a form of CV building. Fifth, it provided a showcase for hacker knowledge and tools to demonstrate utility in service of the computer security project. Finally, it grounded debates about the process of disclosure itself—with full disclosure ultimately serving as a foil to later, more measured, proposals of “coordinated” or “selective” disclosure,<sup>84</sup> in which hackers would provide information about the vulnerability to the vendor, offering them a grace period to address the issue before publicly releasing the information.

In addition to bringing together different types of technologists and enabling experimentation and debate about modes of vulnerability disclosure, the full disclosure movement also served a crucial role in creating public pressure on software vendors to fix security issues, with two major consequences. First, it helped hackers to rebrand themselves as skilled “good guys” discovering vulnerabilities not for illicit purposes, but to advance the interests of the user community and, in doing so, contribute to a broader project of computer security—a subject that will be covered in the next section. Second, it pushed companies to try to stay ahead of the vulnerabilities, in part leading to early experiments with bug bounty programs.<sup>85</sup>

<sup>83</sup> Peter Galison, “Trading Zone: Coordinating Action and Belief (1998 Abridgment),” in *The Science Studies Reader*, ed. Mario Biagioli (Routledge, 1999), 137–60. Galison examined how experimental and theoretical physicists, who held different epistemologies, collaborated by forging new modes of reasoning and linguistic vernaculars. While his study covers only credentialed scientists, we find the concept generative for the case at hand. His metaphor encourages one to examine how those with different training, skills, outlooks, and moral standings came together in a dedicated place to enable new methods for dealing with the problem of computer security. More so, some of the barriers to such exchange did not simply stem from different styles of reasoning and work among those on full disclosure—but contentions over publicity. For a compendium that applies Galison’s metaphor to multiple distinct areas in and outside of academia, with a more sustained look at expertise and the role of boundary objects, see Gorman, Michael E., ed. *Trading Zones and Interactional Expertise: Creating New Kinds of Collaboration*. MIT Press. <https://mitpress-universitypressscholarship-com-proxy3.library.mcgill.ca/view/10.7551/mitpress/9780262014724.001.0001/upso-9780262014724>.

<sup>84</sup> Sometimes these involved a moralism that many hackers found insufferable, as in the framing of “responsible disclosure.” More on this in a next report.

<sup>85</sup> This subject is covered in depth by Ryan Ellis and Yuan Stevens in a complementary Data & Society report, “Bounty Everything: Hackers and the Making of the Global Bug Marketplace,” 2021.



## 4.1 < The Roots of Full Disclosure (1988) >

At the dawn of the 1990s, information about computer vulnerabilities could be found in two primary places: with hackers, and with computer security researchers working in academic or military environments.

As described above, hacker knowledge was available to those able to find their way into the underground—but in the days before Google or even the World Wide Web, an interested party had to know where to look. Detailed knowledge about computer insecurity held by computer scientists and government technologists was no more readily available; the dominant orthodoxy was for vulnerability discussion to be conducted on private mailing lists, with response coordinated between vendors, government agencies, and academic computer scientists through institutions like CERT—the previously mentioned Computer Emergency Response Team formed at Carnegie Mellon in the wake of the 1988 Internet Worm.

A swath of technologists sat in between those two poles of the establishment and the underground: developers, sysadmins, hobbyist technologists, academics operating outside of the security establishment, and more. Many disliked the status quo arrangement, believing that the goal of advancing computer security could best be achieved by sharing knowledge openly, proactively discovering vulnerabilities through hands-on research, and perhaps even learning from those hackers already getting their hands dirty.

But early attempts to act on those convictions served as cautionary tales. Consider the case of the US Department of the Treasury Security Branch BBS, put online in 1991. Maintained by Kim Clancy, a network security expert with a military background, the publicly accessible BBS drew controversy when she made *2600* magazine and a collection of hacking tools available to her users. Many, it seemed, felt that methods of exploitation should be hidden from public view. But Clancy had initiated correspondence with a *Phrack* contributor called “The Butler,” and ultimately determined his insights were as valuable as those held by the security experts of the day. (Her opinion was only hardened after one security contractor inadvertently introduced a destructive virus onto the Security Branch network while installing antivirus software.) Documenting those events, writer George C. Smith relays Clancy’s assertion that “The Butler told me everything I know about network hacking.”<sup>86</sup>

The controversy only intensified when Clancy began to publish archived computer viruses to the BBS, with the rationale of facilitating defensive research. The antivirus research community was scandalized, and Clancy’s actions drew scathing critiques on respected, above-the-boards security mailing lists like *RISKS*.<sup>87</sup> While countered by opinions from the editors of the *Computer underground Digest* (CuD),<sup>88</sup> a mailing list sympathetic to the digital underground,

<sup>86</sup> George Smith, *The Virus Creation Labs: A Journey into the Underground* (Tucson, Arizona: American Eagle Publications, 1994), p. 74.

<sup>87</sup> “I am dismayed that this type of activity is being condoned by an American Governmental Agency. I can only hope that this operation is shut down and the responsible parties are reprimanded. I am extremely disturbed by the thought that my tax money is being used for, what I consider, unethical, immoral and possibly illegal activities.” Anonymous, “This Text Was Forwarded to Me...,” *The RISKS Digest*, Volume 14 Issue 58, May 7, 1993, <https://catless.ncl.ac.uk/Risks/14/58#subj7>.

<sup>88</sup> CuD was created by two professors of criminal justice to track and discuss social and legal issues related to hacking and internet culture more generally. See: “Computer Underground Digest Volume 5 : Issue 51,” *Computer Underground Digest*, July 11, 1993, <http://computer-underground-digest.org/CUD5/cud551.txt>.

the accusations led to scrutiny from the US House of Representatives' Committee on Space, Technology, & Science. Smith relays the events that followed:

Calling a meeting to discuss the future of [the US Department of the Treasury Security Branch] BBS, managers thrust aside arguments from Clancy that removing the hacker files and code from the BBS would only shoot security workers in the foot, depriving the less-experienced among them of a source of information and techniques already widely available throughout the U.S. to any 15-year-old with a modem and a minimal understanding of the word 'BBSing.'

The offending code was removed from the BBS, and *The Washington Post* picked up the story in a salacious June 19, 1993, front page article, complete with quotes likening Clancy's actions to "leaving a loaded gun around."<sup>89</sup> In her defense, Clancy stated simply, "Until you understand how penetration is done, you can't secure your system."<sup>90</sup>

A flurry of condemnations, accusations, defenses, and clarifications ensued on security mailing lists and electronic magazines, fueling a controversy that would frame the announcement of the Bugtraq mailing list later that year.

## 4.2 < The Bugtraq Mailing List and Early Disclosure Debates (1993–1994) >

Fresh on the heels of both Clancy's BBS debacle and Comsec's dissolution, Scott Chasin launched Bugtraq on November 5, 1993. The welcome message made the mailing list's purpose clear:

Welcome to bugtraq!

What is this list about?

This list is for \*detailed\* discussion of UNIX security holes: what they are, how to exploit, and what to do to fix them.

This list is not intended to be about cracking systems or exploiting their vulnerabilities. It is about defining, recognizing, and preventing use of security holes and risks.

Everything submitted to the list is archived and is available to the public. Simply send a message to bugtraq-request@crimelab.com with the subject of "archive".

Remember: YOYOW.

You own your own words. This means that you are responsible for the words that you post on this list and that reproduction of those words without your permission in any medium outside the distribution of this list may be challenged by you, the author.<sup>91</sup> [sic]

<sup>89</sup> Quoted from Smith, Ibid. Original article is archived here: [https://totseans.com/totse/en/hack/legalities\\_of\\_hacking/aisbbs.html](https://totseans.com/totse/en/hack/legalities_of_hacking/aisbbs.html)

The article was also re-printed in *Phrack* Volume Four, Issue Forty-Three.

<sup>90</sup> Ibid.

<sup>91</sup> "Welcome to Bugtraq!" comp.security.unix, November 8, 1993, <https://groups.google.com/forum/message/raw?msg=comp.security.unix/cSiLU04BgIlg/mg8yp-YbKxcJ>.

Mailing lists devoted to the discussion of security issues were nothing new. But Bugtraq did it differently; the list quickly attracted participants dissatisfied with the advisories put out by CERT—at that time, still the US institution tasked with coordinating responses to computer security threats. One of CERT’s main activities in the early 1990s was the disclosure of new vulnerabilities to stakeholders through periodically published advisories. Bugtraq advocates’ main charge against CERT was that of vagueness; CERT advisories stopped short of fully documenting the exploit or vulnerability in question. But participants also resented the “legal noise”<sup>92</sup> and “opinions”<sup>93</sup> found in the attendant mailing lists; long lag times between a vulnerability’s discovery, its submission to CERT, and its ultimate publication in incomplete form; and the omission of any mechanism for providing credit to the reporting source.

<sup>92</sup> Brian Bartholomew, “Re: CERT Advisory CA-93:17,” Seclist.org: Bugtraq mailing list archives, November 16, 1993, <https://seclists.org/bugtraq/1993/Nov/2>.

<sup>93</sup> MIke, “CERT Advisories Wanted,” Seclist.org: Bugtraq mailing list archives, November 17, 1993, <https://seclists.org/bugtraq/1993/Nov/6>.

<sup>94</sup> MITRE Corporation was and remains a significant government defense and technology contractor.

<sup>95</sup> “Bugtraq Mailing List Archives: 4th Quarter (Oct-Dec) 1993,” Geek-girl.com (archive.org capture), January 1, 1997, [https://web.archive.org/web/19970101080345/http://geek-girl.com/bugtraq/1993\\_4/](https://web.archive.org/web/19970101080345/http://geek-girl.com/bugtraq/1993_4/).

Bugtraq, conversely, was devoted to full disclosure.

Along with describing or identifying the weakness of a system—its vulnerability—list members also frequently published the exploits—code or programs that demonstrated how the weakness could be taken advantage of. Moreover, Bugtraq, at first, was unmoderated. That meant those submitting a vulnerability didn’t have to wait for it to be viewed by an intermediary and processed (potentially with some information removed) into a vague advisory. The appeal of that approach was immediate and ranging. From the beginning, emails from institutional domains like @nasa.gov., @mitre.org,<sup>94</sup> and @ufl.edu were in dialogue with emails originating from private individuals—hackers and independent security researchers—with edgily named domains like @crimelab.com, @panix.com, and @dis.org.<sup>95</sup>

The first archived post to Bugtraq, from a hacker named Peter Shipley, set the tenor of the site. With the subject line **CERT Advisory CA-93:17** (the name of an advisory recently issued by CERT), Shipley writes simply:

CERT Advisory CA-93:17 can be exploited with:

```
% cat >! /tmp/fofo
```

```
newroot::0:0:The New Superuser on the block:./bin/csh
```

```
^D
```

```
% xterm -l -lf /etc/passwd -e cat /tmp/fofo
```

```
% su newroot
```

```
# whoami
```

```
root
```

```
# id
```

```
uid=0(root) gid=0(wheel)
```

The first response, from University of Florida mathematician Brian Bartholomew, approved. “Thank you, Peter, for your posting. It was crystal clear, to the point, and contained exactly the information I wanted to see without a bunch of legal noise.”<sup>96</sup>

Also clear was the implication: unlike CERT and other mailing lists, Bugtraq would not tiptoe around the “dangerous” elements of disclosure.

By contrast, the referenced CERT advisory was vague: “A vulnerability in the logging function of xterm exists in many versions of xterm that operate as a setuid or setgid process. The vulnerability allows local users to create files or modify any existing files.”<sup>97</sup> A set of steps a sysadmin could take to see if the problem affected them followed that brief write-up—and encouragement to install a “vendor supplied patch if available.” There is also the assurance that “CERT is working with the vendor community to address this vulnerability,” an acknowledgment of a researcher who helped address the issue,<sup>98</sup> and a statement of copyright.

The vagueness bothered figures like Shipley; he had contributed his store of vulnerabilities to the initial stock of CERT and was now treated to scant information about new vulnerabilities, barring membership of a trusted inner circle.<sup>99</sup> That black-boxed approach was anathema to both hackers and researchers who craved details, and also systems and network administrators who wanted to better understand how to deal with such issues in the absence of a patch—without waiting for a vendor to act. The defense of that secrecy was that it prevented exploitable knowledge from falling into the hands of malicious hackers. But many, echoing Kim Clancy, insisted the hackers already had that knowledge.

And of course, while the goal of Bugtraq was explicitly, at least in part, about “preventing use of security holes and risks,” not every reader or contributor took that ostensibly noble mission to heart. In the years that followed, a searing, running debate raged between hackers, software company employees, and academic security researchers about the ethics, practicality, and logical validity of full disclosure.<sup>100</sup> While somewhat resolved around the year 2000 with the introduction and uptake of “coordinated” disclosure policies that specified a time-lag between selective disclosure to vendors and public disclosure, debates about disclosure exist to this day.<sup>101</sup>

But in 1994, the practice of full disclosure was far from settled. And Bugtraq became host to an extended debate on the nature of security which spawned several distinct positions. As mentioned above, supporters of full disclosure often justified the practice by pointing to the failings of CERT. An exchange on the comp.security.unix Usenet group exemplified that assessment. One researcher described a recent attempt to disclose to the organization: “Christ, we sent email to CERT over a week ago advising them that there was a <serious> problem with RDIST being exploited by these

<sup>96</sup> Bartholomew, “Re: CERT Advisory CA-93:17.”

<sup>97</sup> CERT Division, “1993 CERT Advisories” (Carnegie Mellon University, 2017), <https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=496246>.

<sup>98</sup> It is unclear, in this instance, whether the named researcher submitted the vulnerability or contributed to a patch. Typically, these acknowledgements were directed at institutional bodies who responded to address the vulnerability, and many hackers asserted that CERT did not provide credit to the researchers who submitted the vulnerability.

<sup>99</sup> Peter Shipley, “About Pete Shipley,” dis.org (archive.org capture), April 20, 2019, <https://web.archive.org/web/20190420173146/http://www.dis.org/shipley/>.

<sup>100</sup> For an illustrative example, consider the heated debates that occupied Bugtraq at the tail end of November 1994, prompted by an advisory posted by reformed hacker group 8LGM. Drawing comments from hackers, sysadmins, researchers, and even establishment voices like Eugene Spafford, participants debated not only the limits and efficacy of full disclosure but also what, exactly, full disclosure even was. See: Seclist.org. “Bugtraq: By Date,” November 29, 1994. <https://seclists.org/bugtraq/1994/Nov/date.html#136>.

<sup>101</sup> See Sylvain Besençon and David Bozzini, “The Ethnography of a Digital Object,” *TSANTSA—Journal of the Swiss Anthropological Association* 25 (2020): 153–60. For an example of contemporary debates around disclosure, consider the controversy surrounding the policies of Google’s Project Zero. See: Willis, Tim. “Policy and Disclosure: 2021 Edition.” *Project Zero* (blog), April 15, 2021. <https://googleprojectzero.blogspot.com/2021/04/policy-and-disclosure-2021-edition.html>.

**102** Exchange between John Hawkinson and Rob J. Nauta between February 2 and February 5, 1994.

**103** Ibid.

**104** Klaus, Christopher. "Full Disclosure Works, Here's Proof." Seclist.org: Bugtraq mailing list archives, December 1, 1994. <https://seclists.org/bugtraq/1994/Dec/1>.

**105** A representative version of this argument appears here: That Whispering Wolf. "Security through Obscurity, Etc." Seclist.org: Bugtraq mailing list archives, November 29, 1994. <https://seclists.org/bugtraq/1994/Nov/127>.

**106** Spafford, Gene. "Re: [8lgm]-Advisory-14. UNIX.SCO-Prwarn.12-Nov-1994." Seclist.org: Bugtraq mailing list archives, November 29, 1994. <https://seclists.org/bugtraq/1994/Nov/126>.

**107** 8LGM's legal troubles are briefly discussed in Slatalla and Quittner, *Masters of Deception*.

**108** Message titled "Immediate full disclosure (was Re: [8lgm]-Advisory-Introduction)" from John DiMarco to comp.security.unix, March 9, 1994.

folks, and how to get around it in the short term, and NEVER EVEN GOT BACK A REPLY."<sup>102</sup>

Another researcher responded:

Did you ever expect anything else? CERT is like a secret police, they gather data but don't really give any information to the public. You can mail whatever you want, and that info will enter their big databases on security, and suspects, and maybe eventually get mutated into an advisory, but if you ever expected CERT to warn the public when someone warns them of a break-in, you're wrong. If you spot crackers attacking other machines, you got to warn them yourself.

[...]

Maybe not 100% right for this, but try the bugtraq mailing list.<sup>103</sup>

Relatedly, advocates argued that full disclosure empowered systems administrators to defend themselves against attack methods already known in the underground, enabling them to proactively audit their own systems for the disclosed vulnerabilities.<sup>104</sup> Proponents often further asserted that full disclosure motivated rapid vendor response to issues, countering a practice characterized as "security through obscurity" (i.e., hoping potential attackers would never discover the vulnerabilities in the first place).<sup>105</sup> Moreover, many interested in learning more about computer security saw full disclosure as a pedagogical tool.

Others were outright hostile to full disclosure, arguing that it enabled attackers, and that any incentive it gave vendors to address security issues was a form of "extortion."<sup>106</sup> Often, criticism came in response to the presence of hacker advisories on computer security mailing lists other than Bugtraq. For example, after a brush with the law, members of a UK-based group named 8LGM (The Eight-Legged Groove Machine) seemingly decided to go straight and began posting their own advisories on lists and Usenet groups less supportive of full disclosure.<sup>107</sup> Some participants were less than pleased:

Gee, thanks. :-( Some of us have labs full of students, many of whom would succumb to the temptation of breaking into our system were the means handed to them on a platter. The result: disruption for everybody, tons of work for the admins, and a ruined career for the student involved. Face the facts: immediate full disclosure RUINS LIVES.<sup>108</sup>

All told, the responses to Bugtraq, and full disclosure more generally, varied widely. Many believed vulnerabilities should be shared only with vendors, others that "time-lapsed" full disclosure should occur only after a fix had been implemented, or when it became clear the vendor was ignoring the issue. Some thought full disclosure was reasonable, but argued that exploit code fell outside of the remit,



**109** These “idiots” would later be designated as “script kiddies” and associated with a rash of website defacements in the late 1990s. \*Hobbit\*. “Just What Is Full Disclosure...?” Seclist.org: Bugtraq mailing list archives, November 30, 1994. <https://seclists.org/bugtraq/1994/Nov/136>.

**110** This view has been shared by black hats, state-backed offensive users, and participants (both sellers and purchasers) in the shadowy market for “zero day vulnerabilities.” See: Nicole Perlroth, *This Is How They Tell Me the World Ends: The Cyberweapons Arms Race* (New York: Bloomsbury Publishing, 2021).

**111** In particular, many resolutely underground hackers began to self-identify as “black hats” at the turn of the millennium in response to the professionalization or “selling out” of other underground hackers. From this perspective, which will be addressed in a subsequent report, vulnerability research and the power it enabled was best maintained as the preserve of an elite group of underground hackers. This could be rationalized through activist, anti-establishment, or criminal logics.

preferring information that would enable a technically skilled user to understand the bug.

“Publishing the canned script is an interesting approach, but has the disadvantages that a> any idiot can run it and b> alone, it doesn’t really explain the problem,” as hacker Al “Hobbit” Walker put it.<sup>109</sup> On the flip side, there were those who believed vulnerabilities shouldn’t be disclosed at all—not out of fear that bad actors would use them, but because they wanted the vulnerabilities to persist so they could exploit them themselves.<sup>110</sup>

### 4.3 < Full Disclosure as a Trading Zone (1994–1996) >

Bugtraq attracted posts not only from institutionally aligned security researchers but also hackers “active” in the development and use of exploit code. While some of those figures were clearly interested in improving the general state of computer security by discovering vulnerabilities, disclosing them, and advocating for their redress, the motivations of others were more suspect. And indeed, our interview subjects detailed some of the alternative reasons why someone might share or publicly disclose a novel exploitation technique. As one explained,

You got your bragging rights on Bugtraq. You know, you could prove to somebody that you’d figured out this cool hack. So you might use it for a while until people began to see that they were being hacked using this technique. And then you do what they call ‘tossing it over the wall.’ You’d post to Bugtraq, or maybe wouldn’t post to Bugtraq—you’d share with a few friends who weren’t as skilled. Now, they were using the same thing, but they weren’t as good. They would be messier. So when they break into a machine, they might do it from their school network and they could be tracked back. Whereas the person who created the hack in the first place, now they’ve diffused the trail. Other people are using the same tools and so they’re [the ones who are] going to get caught.

As time went on, these “active” hackers would be increasingly identified as “black hats.” And they were increasingly distinguished from an emerging professional class of technologists engaged in penetration testing and other types of so-called ethical hacking, and also from those erstwhile underground (“white hat”) hackers who embraced full disclosure alongside close dialogue with vendors and the security establishment in the interest of improving the general state of computer security.<sup>111</sup>

Thus, hackers of varied motivation could find reasons to use Bugtraq. Vulnerabilities not attached to identifiable illegal activity might be published under real names to accrue reputation. Others might be published using pseudonyms. Or, as some informants suggested, a hacker might publish an illicit vulnerability under their real name but

use a method of “parallel construction” to suggest they discovered it on their own network while performing sysadmin duties. Still others, like Julian “Proff” Assange and members of the L0pht, published research under their hacker handles—communicating the message that pseudonymous hackers resolutely attached to the underground could still contribute to the broader project of improving the state of computer security.

In that way, Bugtraq also attracted knowledge that would not be directly submitted to CERT (or wouldn’t be published by CERT—some of those we spoke with said they tried submitting vulnerabilities to the organization, only to see them disappear into a void). Regardless of whether these posts were motivated by fame, a concern for security, or the desire to diffuse attribution attempts linked to a particular exploit, many defense-oriented technologists appreciated having access to that knowledge.

Bugtraq, then, functioned as a trading zone<sup>112</sup> between underground and aboveground researchers and between different types of practitioners: computer scientists, hackers, system administrators, programmers, and vendor representatives. Figures emerged who were happy to draw from both worlds and discuss issues with all comers—blurring the divide between elements of the hacker underground and the CERT-adjacent security establishment. As one interviewee told us: “Bugtraq was a great resource for me. So was Brent Chapman’s Firewalls mailing list. So then again you have that typical split. You have the hacker types on Bugtraq, and then in firewalls mailing list you had the defender types. Studying those two, that’s how I learned internet security.”

In effect, those figures willing to draw on both domains created the mold of the contemporary “security researcher.” Whether entering into that discourse through the hacker scene, academia, system administration, or something else, they were willing to accept knowledge from any source. For many, “hacking” increasingly just became shorthand for techniques used to jeopardize security, and “hackers” a label for those with expertise in such techniques. In that way, the term began to partly shed connotations of underground criminality.

Sites like Bugtraq thus troubled the neat distinction between underground hacker and security establishment, and provided a platform from which hackers could interface with other technologists and earn their trust. While participants may have had a variety of motivations for posting, Bugtraq was a place where technical matters could be discussed without assertions of the potential criminality of participants. On Bugtraq, hacking was framed as the pursuit of detailed, complete knowledge of security vulnerabilities. Hackers could be recast as “security researchers” or members of a “security community” and also understand themselves as contributing to a more universal practice of advancing detailed technical knowledge about computer insecurity.

<sup>112</sup> Galison, “Trading Zone: Coordinating Action and Belief (1998 Abridgment).”

For many, “hacking” increasingly just became shorthand for techniques used to jeopardize security, and “hackers” a label for those with expertise in such techniques. In that way, the term began to partly shed connotations of underground criminality.

**113** Chasin, Scott. "MESSAGE FROM MODERATOR - Please Read." Seclists.org: Bugtraq mailing list archives, June 5, 1995. <https://seclists.org/bugtraq/1995/Jun/24>.

**114** See: Aleph One, "Administrivia (Jul 28)" on the subject of discussion; See: Aleph One, "Administrivia (Dec 30)" on the subject of marketing material.

**115** As the subsequent moderator, Elias Levy, explained later in 1998: "I attempt to review any such software or patches posted to the list but make no guarantees that the software does not contain trojans or that I even reviewed it at all." Aleph One, "Administrivia (Nov 14)," Seclists.org: Bugtraq mailing list archives, November 14, 1998, <https://seclists.org/bugtraq/1998/Nov/206>.

**116** Wietse Venema and Eugene Spafford; respectively, an esteemed Dutch programmer/security researcher and an influential computer scientist who documented the Internet Worm in 1998 and was involved in the establishment of CERT.

**117** Message from Rob J. Nauta titled "Re: [8lgm]-Advisory-Introduction" to comp.security.unix, March 7, 1994.

**118** This reality also seems to have contributed to the early formation of normative limits around the practice of full disclosure. Some of our interview subjects told us how publishing an exploit on a Friday, thus forcing vendors to respond over the weekend, was increasingly seen as impudent behavior.

That said, not everything was permitted. Chasin introduced moderation on June 5, 1995, stating, "As of today, Bugtraq will now be a moderated mailing list. This is due to the ridiculous amount of noise being floated through the list. If the list traffic continues on a path that is acceptable with Bugtraq's charter then I will remove the moderation."<sup>113</sup> By noise, it seems Chasin mostly meant off-topic discussion, discussion that lacked any novel technical discussion of vulnerabilities themselves, and also promotional or marketing-oriented posts.<sup>114</sup> But in the years that followed, it became clear that moderation was also being used to mitigate the dissemination of questionable material, like credit card numbers, that had previously concerned some participants, and the occasional incidence of exploit code containing Trojan horses.<sup>115</sup>

Thus, while framed as a simple mechanism for eliminating "noise," it seems clear the moderation practices were also aimed at enhancing the legitimacy of the list—a perception that could not be taken for granted.

Pushing back on charges in the large comp.security.unix newsgroup that Bugtraq harbored malicious hackers, one participant drove home the importance of the list as a third space between the underground and the security establishment. "So this just boils down to the discussion who's 'legit' and who's not. A bit like the childish discussions in the hacker underground on who's 'eleet' and who's not." He continued:

Don't underestimate the current amount of people interested in security. Many of those are not as famous as Wietse or Spaf<sup>116</sup> and thus are regarded as potential crackers fishing for holes to abuse when posting a normal question to a security newsgroup. Mailing lists like bugtraq and the IRC channel #hack are active communities of people sharing information, not groups of anarchists or KGB spies trying to cause maximum damage to all UNIX systems.<sup>117</sup>

Full disclosure brought other figures into the trading zone, too. By presenting the possibility that a vulnerability could be disclosed at any time, the cadence of software patching changed. Vendors had to be ready to address issues whenever they might appear on Bugtraq. As such, representatives from major software companies increasingly participated in the mailing list, demonstrating a willingness to learn from and engage with hackers.<sup>118</sup>

#### 4.4 < Expertise, Legitimacy, Credit, and Laments (1996–2001) >

As time went on, the boundary work being done on Bugtraq contributed to changing perceptions about the hacker scene. The growing embrace of full disclosure meant that knowledge from a variety of underground publications was of interest to security

researchers. Individual hackers could use Bugtraq to demonstrate the skills and knowledge they possessed and, by extension, the value of the community they came from.

*Phrack*, for example, had long been a proponent of the open and avid discussion of exploits and vulnerabilities. But it was also firmly associated with the hacker underground, and had a questionable reputation stemming from early guides to calling card fraud and a widely publicized trial in which editor Craig “Knight Lightning” Neidorf was prosecuted for disseminating sensitive information derived from stolen telecom documents. (Neidorf was not convicted, after it was pointed out that Bellcore itself made the supposedly sensitive information available to the public through mail-order. But the hacker who provided the documents to *Phrack* was ultimately sentenced to 21 months in prison).<sup>119</sup> Nevertheless, many Bugtraq participants viewed *Phrack* in a positive light—and Chasin himself had written for the publication.<sup>120</sup> The associations would only deepen in the years to follow.

On May 14, 1996, Chasin handed over the reins of Bugtraq to Elias “Aleph One” Levy.<sup>121</sup> Shortly after, Levy published the article “Smashing the stack for fun and profit” in *Phrack*.<sup>122</sup> The article is a practical documentation of a buffer overflow attack which many of our subjects cited as a seminal, revolutionary piece—a watershed moment in full disclosure and hacker-led security research that helped establish the expertise of non-institutional actors. Some well-known contemporary security researchers even credit the article with crystallizing their commitment to the field.<sup>123</sup>

Suddenly, a significant technical paper that advanced the craft of vulnerability exploitation was linked to a hacker periodical, while also identifiable with the moderator of an increasingly respectable security mailing list. These public associations were not possible through intermediaries like CERT, which did not name or credit the reporting source of a vulnerability in its advisories.

At the same time, as the World Wide Web became more established, advisories and hacking tools increasingly became available on aggregating websites. Indeed, Levy’s own website, “underground.org,” was considered by some to be ironically named, given its role in making hacker knowledge public to new audiences. Full disclosure platforms like Bugtraq became foundational resources as both institutional and independent researchers began combing mailing lists and websites for vulnerabilities, assembling them into inventories often called vulnerability databases (VDBs). One subject told us that, at one point in the late ’90s, he was combing through hundreds of sources a day to feed the database he maintained.

As vulnerability research became valued, and professional opportunities in computer security appeared, the question of credit gained new pertinence. With disclosures in Bugtraq and other venues increasingly regarded as line items on a CV, some hackers began to shed their handles. As one explained, “I knew early on that I wanted

<sup>119</sup> Denning, “The United States vs. Craig Neidorf”; Sterling, “Hacker Crackdown,” pp. 276 - 283. The trial was a major factor in the creation of the Electronic Frontier Foundation (EFF).

<sup>120</sup> Reputedly, Chasin also edited and released a couple editions of *Phrack* during the lull in publication that followed Operation Sundevil. Their status as official *Phrack* publications was later contested. See: Various, “Phrack #33,” September 15, 1991, <http://phrack.org/issues/33/1.html>.

<sup>121</sup> “Bugtraq,” SecurityFocus.com, accessed January 25, 2021, <https://www.securityfocus.com/archive/1/description>.

<sup>122</sup> Aleph One, “Phrack #49 File 14 of 16: Smashing The Stack For Fun And Profit,” *Phrack*, November 8, 1996, <http://phrack.org/issues/49/14.html#article>.

<sup>123</sup> In this way, it also serves to illustrate how lists like Bugtraq and the increasing visibility of publications like *Phrack* on the web were opening up security research to broader audiences. Source: Interview data, and the positive response to this post by Peiter Zatkó: Mudge @ dotMudge, “The Paper That Moved the Needle...,” Twitter, accessed May 26, 2020, <https://twitter.com/dotmudge/status/1186117644472213505>.

With disclosures in Bugtraq and other venues increasingly regarded as line items on a CV, some hackers began to shed their handles

<sup>124</sup> See: Ryan Ellis and Yuan Stevens, “Bug Bounties” (Data & Society Research Institute, forthcoming 2021). See also: Andreas Kuehn and Ryan Ellis, “Bug Bounty Programs: Institutional Variation and the Different Meanings of Security,” in *Rewired: Cybersecurity Governance*, ed. Ryan Ellis and Vivek Mohan, 2019, 175–94.

<sup>125</sup> Perlroth, *This Is How They Tell Me the World Ends*.

<sup>126</sup> F0RMiCA, “How to Exploit AlephOne by JP of AntiOnline,” Seclists.org: Bugtraq mailing list archives, April 24, 1998, <https://seclists.org/bugtraq/1998/Apr/152>.

<sup>127</sup> Dr. Mudge, “How to Exploit Mudge by AlephOne by JP AntiOnline,” Seclists.org: Bugtraq mailing list archives, April 24, 1998, <https://seclists.org/bugtraq/1998/Apr/155>.

<sup>128</sup> Aleph One, “Re: How to Exploit Mudge by AlephOne by JP AntiOnline,” Seclists.org: Bugtraq mailing list archives, April 24, 1998, <https://seclists.org/bugtraq/1998/Apr/158>.

to be in this industry, and I wanted to be able to laud the things I had done and attribute them to me. So while I always had my handles and such, I also started identifying via my given name.” Others told us with bitterness about private exploits that were plucked from the underground community and published by hackers seeking to professionalize. One resolutely underground hacker told us:

People grew up, they realized that food doesn’t cook themselves and they need to pay for it [*sic*]. Looking back it was obvious this was going to happen [...but] I think what I felt back then, and what a large portion of these people I was with felt—not all of them, but probably 80%—was that the people that are starting to commercialize these ideas, they would take our secrets away, the things we found, and get them secretly fixed with the vendors, or making money from our ideas, and using these exploits in the wild. And the exploits would stop working for us, and we wouldn’t be able to have fun any more.

Moreover, with exploits and vulnerabilities increasingly understood as commodities with reference to nascent bug bounty programs<sup>124</sup> and the rise of the offensive “zero day” market,<sup>125</sup> questions of ownership rights were becoming a major concern.

Bugtraq served as a forum for normalizing new practices around credit. For example, in one 1998 exchange, a contributor accused a much-maligned security advocacy group called AntiOnline of violating Levy’s “intellectual property.” Allegedly, the site had published buffer overflow attack documentation that included code lifted from Levy’s aforementioned “Smashing the stack...” article in *Phrack*. “Hello, I am bringing to your attention a very serious offense to Aleph One’s First Amendment Rights and to Copyright Violation,” it begins, before showcasing the near-identical snippets of code side by side and concluding, “it is a serious illegal offense, not to mention highly immoral, to steal the works of other colleagues in this field.”<sup>126</sup> Judging from the tone, the accuser was likely “trolling” other mailing list participants—satirizing the language of intellectual property to make a point. Indeed, it is likely the post was designed to critique the very sensibility that saw issues of copyright as more important than the pursuit of knowledge. But serious or not, the post sparked discussion on an issue of newfound import.

Peiter “Mudge” Zatko—the most outspoken member of the L0pht—quickly responded to downplay the allegations, pointing out that Levy had also borrowed code from earlier work Zatko himself had published in 1995.<sup>127</sup> He hadn’t been cited, but there were no hard feelings. Levy then chimed in to note that buffer overflows had been documented nearly a decade earlier in the work of a hacker called “Red Dragon.” “Nothing is new, everything is recycled,” he said.<sup>128</sup> And indeed, since then, it has become public knowledge that contractors working with the US military had been cognizant of buffer overflow-



type attacks since at least the 1970s.<sup>129</sup>

That particular exchange affirmed an emerging norm of permissibility and open knowledge.<sup>130</sup> But the manner of discussion also signaled the importance of giving credit where it was due, and identifying innovation with particular individuals. That was similar, in some ways, to practices in the underground, wherein hackers embedded references to their handles and group affiliations in tools and exploit code. But in other ways, it was radically different: assigning credit to recognizable individuals who stood to profit in an emerging professional sphere through the accrual of reputation and expertise. It also meant that research shared anonymously, in an informal, collectivist spirit, could be co-opted by those interested and positioned to convert it into professional capital. As one of our interviews made clear, that could mean that women and others—like hackers who had served time in prison—who did not fit the typical professional mold, or were not present on platforms like Bugtraq,<sup>131</sup> could have their work exploited.

#### 4.5 < New Disclosure Paradigms, Institutionalization, and Imminent Backlash (1999–2002) >

By the end of the 1990s, full disclosure was strongly associated with a professionalizing current in hacking and independent security research. Hackers and security researchers were finding work in auditing, penetration testing, and consulting, and even getting hired for in-house security teams, addressing the flaws they had made visible.

A number of projects, such as the free software operating system OpenBSD, welcomed full disclosure into their development cycles, creating public listservs devoted to the activity. These were intended to enhance transparency, performatively embrace the challenge to rapidly fix issues, and alert users who would potentially be affected by the vulnerability for as long as it remained viable.<sup>132</sup>

But increasingly, full disclosure was also becoming recognized less as a principled approach to advancing transparency and accountability, or enabling self-motivated systems administrators to proactively address problems in the absence of a CERT- or vendor-led response, and more as a form of advertising and CV building. A few developments contributed to that change in perception. First, Bugtraq was consolidated under Levy's company, SecurityFocus in 1999<sup>133</sup> and, in turn, acquired by Symantec in 2002.<sup>134</sup> In effect, some came to believe that Bugtraq, and the entirety of its contents, had become one big commodity. Second, Bugtraq was perceived to have become stricter in the enforcement of the moderation policy it had put in place in 1995,<sup>135</sup> with some arguing that Bugtraq was abandoning its full disclosure values by filtering out certain types of discussion.<sup>136</sup> (Despite that perception, it seems a major motivation for filtering posts was to remove advisory notices that required readers to click through to third-party corporate websites, or were otherwise interpreted by Levy

<sup>129</sup> Karger, Paul A., and Roger R. Schell. "Thirty Years Later: Lessons from the Multics Security Evaluation." In *18th Annual Computer Security Applications Conference, 2002. Proceedings.*, 119–26. IEEE, 2002. Shostack, Adam. "Buffer Overflows and History: A Request." Adam Shostack & friends, October 20, 2018. <https://adam.shostack.org/blog/2008/10/buffer-overflows-and-history-a-request/>.

<sup>130</sup> For two likely reasons: first, the documentation referred only to the general class of buffer overflows, and not the discovery of a particular buffer overflow attack that could exploit an unknown vulnerability in a niche system. Second, both Levy and Zatzko were on career paths that did not rely on the litigation of particular pieces of code in a scarcity-driven commodity market, but were instead reputation driven. The L0pht was on the verge of acquisition by a well-funded security start-up, and Levy's SecurityFocus company was poised to benefit from the continued popularity of Bugtraq and, by extension, full disclosure—ultimately, Bugtraq would come under the ownership of Symantec following the company's purchase of SecurityFocus in 2002. Indeed, both Levy and Zatzko stood to benefit more generally from the continued open and public disclosure and discussion of vulnerabilities and exploits. The case further illustrates a peculiarity of early security research: in the pre-web days, information could easily remain siloed in a way that is now hard to imagine. This situation could make credit difficult and rediscovery common.

<sup>131</sup> Indeed, absent the possibility of direct remuneration for this type of security research, those who did not have the luxury of time (read: financial security) to participate in this discourse were structurally excluded ex-ante.

<sup>132</sup> See, for example, OpenBSD's offered rationale: "OpenBSD: Security," [www.openbsd.org](http://www.openbsd.org), accessed January 25, 2021, <https://www.openbsd.org/security.html>.

<sup>133</sup> Aleph One, "Administrivia (Jul 05)," [Seclists.org](http://seclists.org): Bugtraq mailing list archives, July 5, 1999, <https://seclists.org/bugtraq/1999/Jul/28>.

<sup>134</sup> Masnick, Mike. "Symantec Buys SecurityFocus/BugTraq." [Techdirt](http://www.techdirt.com), July 17, 2002. <https://www.techdirt.com/articles/20020717/1825218.shtml>.

<sup>135</sup> See, for example, comments in this article: Masnick, Mike. "Symantec Buys SecurityFocus/BugTraq." [Techdirt](http://www.techdirt.com), July 17, 2002. <https://www.techdirt.com/articles/20020717/1825218.shtml>.

<sup>136</sup> The message accompanying the 2002 creation of a competing mailing list

unambiguously named Full Disclosure reads: “We are pleased to announce the creation of a new security mailing list dedicated to FULL DISCLOSURE. When Scott Chasin handed over the bugtraq mailing list, it was clearly dedicated to the immediate and full dissemination of security issues. The current bugtraq mailing list has changed over the years, and some of us feel it has changed for the worse.” Simon Richter, “Announcing New Security Mailing List,” Full Disclosure mailing list archives, Seclists.org, accessed May 27, 2020, <https://seclists.org/fulldisclosure/2002/Jul/7>.

- 137** Most pointedly, at least two “summits” were held in late 2000, bringing hackers and industry figures together to discuss new approaches to vulnerability disclosure. On November 3, eWEEK Labs hosted an event called The Vulnerability Summit in Foster City, California. Elias Levy, Jeff Forristal, Chris Wysopal from the L0pht, and other hackers were joined by representatives from MITRE, Guardent, and a variety of industry representatives. From December 6 - 8, Microsoft hosted the first “Safenet” summit (later renamed the Trusted Computing Forum), featuring a similar assortment of characters.
- 138** RFP stands for Rain Forest Puppy, the pseudonym of Jeff Forristal, the hacker who developed the original policy.
- 139** Rain Forest Puppy, “Full Disclosure Policy (RFPolicy) v2.0,” Wiretrip.net (archive.org capture), October 17, 2000, <https://web.archive.org/web/20001017192112/http://www.wiretrip.net/rfp/policy.html>.
- 140** Chris Wysopal and Steve Christey, “Responsible Vulnerability Disclosure Process,” IETF.org, February 2002, <https://tools.ietf.org/html/draft-christey-wysopal-vuln-disclosure-00>. See also: John T. Chambers and John W. Thomson, “Vulnerability Disclosure Framework: Final Report and Recommendations by the Council” (National Infrastructure Advisory Council, January 13, 2004), <http://nob.cs.ucdavis.edu/bishop/notes/2004-niacvtf/index.html>.
- 141** Ellis and Stevens, “Bounty Everything.”

as a type of advertisement.) Third, Levy and others began to engage in direct dialogue with vendors like Microsoft and institutions like CERT to develop new disclosure paradigms.<sup>137</sup> The first significant proposed version, released in 2000 and dubbed “RFPolicy,”<sup>138</sup> specified that security researchers and hackers would first disclose vulnerabilities directly to vendors, granting them a grace period to patch or otherwise address the issue before the hackers made any public disclosure.<sup>139</sup> The policy would prove foundational to later advocacy for “selective,” “coordinated,” or “responsible” disclosure frameworks by the US National Infrastructure Advisory Council, among others.<sup>140</sup> It would also lay important groundwork for policies related to bug bounty programs.

While selective forms of disclosure, including bug bounty programs, would eclipse full disclosure in popularity in coming years, the philosophy behind full disclosure would retain a following of devotees—and also lurk in the background as a reminder to vendors that their inactivity to address privately disclosed issues could always result in public attention.<sup>141</sup> Ultimately, full disclosure left an indelible mark, not only as a philosophy which underwrote many of the public maneuvers that helped reconfigure perceptions of hackers and increase pressure on companies to take security seriously (the subject of our next section), but also as a practical tool, still deployed at times today, which many credit with improving the state of security, one vulnerability at a time.

And, as if it was Chasin’s goal all along, full disclosure ultimately facilitated the integration of hackers into institutional processes and professional roles in a variety of ways: by allowing them to demonstrate capability, to advertise themselves, to accrue reputation, to cultivate new identities, and to collaboratively dialogue with vendors and establishment figures. It also helped to provide the fodder needed to make visible a threat—that insecurity is real.

Of course, a backlash was imminent, spurred by the professional and institutional successes of full disclosure’s most ardent supporters. It would come from both principled “white hat” security researchers upset with forms of disclosure they interpreted as snake oil salesmanship, and also from those hackers who proudly owned the “black hat” label, angry at the professionalizing current and the lost effectiveness of their most prized exploits. These reactions were of significant consequence, revealing profound disagreements not only about preferred methods for improving security, but also what improving “security” even meant. But these are stories for another time.

For now, we will step back to the onset of the 1990s, to consider a process that ran parallel to full disclosure and proved equally crucial in the project to legitimize hackers in the face of skepticism about their moral integrity.

## 5.0 Interlude: Arsonists or Firefighters? (1990–2000)

One of the core issues hackers had to address and redress were public doubts about their trustworthiness. At issue was not simply the merits of their technical proposals, but also their trustworthiness as individuals. Could hackers, some of whom had openly admitted to breaking into computer systems, be trusted to do the “right thing” in a professional setting? Would they respect non-disclosure agreements?

In the early 1990s, two academics—Gene Spafford and Dorothy Denning—helped set the terms of the debate around that question, largely by disagreeing with each other. Spafford, a computer science professor at Purdue University; and Denning, a former Purdue professor employed by the Digital Equipment Corporation to research information security; publicly sparred over the role of hackers in the nascent field of computer security.<sup>142</sup> Their perspectives, which could not be more different, provide a window into the polarized and heated nature of the questions surrounding hackers’ moral legitimacy.

The debate took off soon after Spafford was quoted in an Association of Computing Machinery (ACM) news brief, addressing firms who might want to hire Robert T. Morris, the aforementioned author of the infamous Internet Worm of 1988. Published in May 1990 under the ACM’s “News Track” section, we’re informed Spafford has been urging his “colleagues to refuse to do business with any firm that would employ a known hacker.” In case any part of his position was unclear, a short extract relays Spafford’s opinion on the prospect of hackers as security professionals. “This is like having a known arsonist install a fire alarm [...] Just because he knows how to set a fire doesn’t mean he knows how to extinguish one.”<sup>143</sup>

<sup>142</sup> Such questions had been posed in public before. One of the earliest and most famous journalistic pieces on phone phreaking, the precursor to hacking, even raised this issue when it featured a phone phreak and hacker, Mark Bernays. He had been fired from his day job after cracking the password manager on a “huge time sharing computer,” but explained to the journalist that while “[a]t first the security people advised the company to hire me full-time to search out other flaws and discover other computer freaks,” (Rosenbaum, “Secrets of the Little Blue Box”) they ultimately decided not to move forward with hiring him. Nevertheless, this ongoing and multi-year conversation between two cybersecurity academics represented a decisive turning point due to the visibility and prominence of the debaters, the depth of their positions, and the venues of their arguments.

<sup>143</sup> Rosalie Steier, “News Track: Just Say No,” *Communications of the ACM*, May 1990.

### NEWS TRACK

**JUST SAY NO...**Eugene Spafford says one way the computing community can rid the headlines of hackers is by applying some consumer pressure. The Purdue University professor is urging colleagues to refuse to do business with any firm that would employ a known hacker. Spafford, an outspoken security expert, is betting many firms will offer Robert T. Morris a high-paying security consulting job once his legal problems subside. “This is like having a known arsonist install a fire alarm,” Spafford insists. “Just because he knows how to set a fire doesn’t mean he knows how to extinguish one.”

Not long after, in July 1990, Spafford published a lengthy article entitled “Are Computer Hacker Break-ins Ethical?” While Spafford fleshes out his position in more detail, he still reaches the same conclusion: hiring hackers is a bad idea.

144 Dorothy E. Denning, "Concerning Hackers Who Break into Computer Systems," in *Proc. 13th National Computer Security Conference* (Washington, D.C., 1990), 653-64, <http://cpsr.org/prevsite/cpsr/privacy/crime/denning.hackers.html/>. Republished, in "High Noon on the Electronic Frontier: Conceptual Issues in Cyberspace"

145 Denning, "Concerning Hackers Who Break into Computer Systems."

Dorothy Denning responded in October 1990 with a substantive counterpoint, advocating cautiously on behalf of hackers in a talk at the National Computer Security Conference in Washington, DC, titled, "Concerning Hackers Who Break Into Computer Systems."<sup>144</sup> Denning directly addresses Spafford's position, arguing that in some cases hackers have both the skills *and* the integrity needed to improve security. It is worth quoting her assessment, to show just how carefully she had to tread given her heretical stance:

My initial findings suggest that hackers are learners and explorers who want to help rather than cause damage, and who often have very high standards of behavior. Several hackers said that they would like to be able to pursue their activities legally and for income. They like breaking into systems, doing research on computer security, and figuring out how to protect against vulnerabilities. They say they would like to be in a position where they have permission to hack systems. Goodfellow suggests hiring hackers to work on tiger teams that are commissioned to locate vulnerabilities in systems through penetration testing. Baird Info-Systems Safeguards, Inc., a security consulting firm, reports that they have employed hackers on several assignments. They say the hackers did not violate their trust or the trust of their clients, and performed in an outstanding manner.<sup>145</sup>

Denning goes on to note that employers should evaluate individual hackers on "his or her own competency and character." But she nevertheless shreds the argument that a hacker—solely by virtue of breaking into systems—is unprincipled. Although she recognizes that some hacker activity resides in a "gray" area, presaging the future term "gray hat" by nearly a decade, she also provides an alternative to Spafford's binary, entertaining the possibility that some of these hackers held even higher ethical standards and had superior technical talents than academically trained engineers.

Denning's unorthodox position, ahead of its time, eventually prevailed. Ultimately, many companies openly sought out hacker talent, and nascent hacker firms were able to leverage the cachet of the term "hacker" in marketing efforts. But when she first delivered her speech, it was truly uncertain whether the hacker "who broke into systems" would be embraced as a curious maverick pedagogue with the mindset and skills needed to improve security, as Denning saw it; or dismissed as a dangerous, anarchist, felon-arsonist, as Spafford had it figured.

Hackers, for their part, were not content to leave it to outsiders like Denning and Spafford to settle the question. Through the 1990s, they repeated and reiterated versions of Denning's argument, while engaging in other types of linguistic and mediatic labor, much of it adversarial, that would ensure some hackers would be taken seriously as a force for good.



## 6.0 Public Legitimacy Through Media Work and Corporate Engagement (1995–2000)

We now turn to the pointed interventions hackers used to enhance perceptions of their legitimacy as security researchers in the 1990s, concentrating on a few dynamics.

First, we provide some background to the moralistic distinction between “white hat” and “black hat” hacking that grew in popularity during the 1990s. We subsequently examine the ways specific individuals and groups, particularly the Boston-based L0pht, worked with journalists to ensure more nuanced, or at least more favorable, portrayals of hackers, especially of their own group. During the course of that media work, they eventually invented and adopted the “gray hat” label as part of a branding strategy. By using that term, they were able to convey their trustworthiness to would-be employers while simultaneously connoting an ongoing connection to the hacker underground.

Next, we examine how and why hackers sought to shame software vendors for purportedly lax approaches to security. Microsoft often served as a poster child for the problems plaguing the software vendor industry at large. Whether it was Microsoft or other vendors being targeted, these campaigns had the effect of diverting some of the blame away from hackers, and onto the makers of the software in question, creating space for legitimacy-seeking hackers like the L0pht. These engagements have been described as “media hacking,”<sup>146</sup> and we could further understand them as an early form of what danah boyd has called “hacking the attention economy.”<sup>147</sup>

Finally, we explore how the success of these interventions was bolstered by the work of powerful and prestigious allies, including lawyers, government officials, and academics who supported select underground and gray hat hackers and advocated for the full disclosure practices they championed. The most visibly impactful of these allies was Richard Clarke (at the time the National Coordinator for Security, Infrastructure Protection, and Counter-Terrorism for the US government) who, in 1998, invited the L0pht to testify in the US Senate.<sup>148</sup> Their testimony coincided with a growing concern among some US government and military officials to identify and prepare for a catastrophic cyberattack, rhetorically formulated as a “Cyber Pearl Harbor.”<sup>149</sup> After that watershed event, senators and the press alike showered the L0pht with accolades, and the subsequent media boost helped them disseminate and cement their vision of hacking in service of the public interest (or the government’s interests)—even as the specter of hacking’s danger was never fully eliminated.

<sup>146</sup> See, for instance, comments by Peiter “Mudge” Zatko in a 2015 interview for the Silver Bullet Security Podcast. <https://www.garymcgraw.com/technology/silver-bullet-podcast/>. The concept is more generally referenced in Gareth Branwyn, *Jamming the Media*. Chronicle Books, October 1, 1997.

<sup>147</sup> danah boyd, “Hacking the Attention Economy” *Points*, Jan 5, 2017, <https://points.datasociety.net/hacking-the-attention-economy-9fa1daca7a37>

<sup>148</sup> Dennis Fisher, “Thirty Minutes Or Less: An Oral History of the L0pht, Part Three,” *Decipher*, March 8, 2018, <https://duo.com/decipher/thirty-minutes-or-less-an-oral-history-of-the-l0pht-part-three>.

<sup>149</sup> Sean Lawson and Michael K. Middleton, “Cyber Pearl Harbor: Analogy, Fear, and the Framing of Cyber Security Threats in the United States, 1991–2016,” *First Monday*, March 1, 2019, <https://doi.org/10.5210/fm.v24i3.9623>.



## 6.1 < Redefining Hackers by Way of White and Black Hats (1980–1999) >

During the 1990s, as the hacker underground splintered and became entangled with the growing computer security industry, the terms “white hat” and “black hat” (and eventually “gray hat”) became common parlance to describe the range of hacker motivations and reputations. The precise origins of the terms are murky, even to experienced hackers, but some suggested a likely source as the visual conventions of Hollywood Westerns, where the intruders wore black hats and the heroic defenders wore white hats.

Even if the exact origin of the terms “white hat” and “black hat” are difficult to pinpoint, we found several instances of their use in the security mailing lists in the 1980s.<sup>150</sup> While “black hat” later came to refer to a very particular type of subcultural hacker, it was more diffuse in early uses—referring to any class of “bad actor” intruding into systems. The terms also appeared briefly in a blockbuster 1989 non-fiction account, *The Cuckoo’s Egg*, authored by university system administrator Clifford Stoll. The book chronicles his year-long (ultimately successful) struggle to locate and snuff out a West German hacker who had sold to the KGB secrets pilfered from dozens of university and military systems, including the one Stoll tended at the Lawrence Berkeley National Lab.<sup>151</sup> The book’s acknowledgments section opens in caps with a reference to black hats and a prefiguration of forthcoming debates about vulnerability disclosure:

HOW DO YOU SPREAD THE WORD WHEN A COMPUTER HAS A SECURITY HOLE? SOME SAY nothing, fearing that telling people how to mix explosives will encourage them to make bombs. In this book I’ve explicitly described some of these security problems, realizing that people in black hats are already aware of them.<sup>152</sup>

Despite the book’s popularity—it was a *The New York Times* bestseller for over a year, re-enacted in an episode of PBS’s *Nova* series, and translated into over a dozen languages—the terms “white hat” and “black hat” did not immediately take hold, only appearing intermittently in publications or other discourse about those technologists in the subsequent decade.<sup>153</sup>

“Black hat” came into common usage during the last few years of the 1990s. Its popularity was likely triggered by a 1997 offshoot of the DEF CON hacker conference called Black Hat Briefings. Still held annually, the event, most often referred to simply as “Black Hat,” was intended to brief members of the computer security industry about threats from the underground.<sup>154</sup> Despite the negative connotations (or perhaps because of them), by 2000, some members of the underground had latched onto the “black hat” label as a mark of prestige. Many embraced it specifically to define themselves as distinct from the security industry, as they lashed out against the “sellout”

<sup>150</sup> See, for instance: Various, “The Risks Digest: Volume 2 Issue 50,” *The Risks Digest: The Virtual Memorial Garden*, May 8, 1986, <http://catless.ncl.ac.uk/Risks/2/50>.

<sup>151</sup> Clifford Stoll, *The Cuckoo’s Egg: Tracking a Spy through the Maze of Computer Espionage* (New York: Doubleday, 1989).

<sup>152</sup> The terminology appears in another passage, too. “Somewhere, somehow, something was wrong here. The guys in black hats knew the combinations to our vaults. But the white hats were silent.” Ibid.

<sup>153</sup> See, “BEST SELLERS: February 4, 1990,” *The New York Times*, February 4, 1990, <https://www.nytimes.com/1990/02/04/books/best-sellers-february-4-1990.html>.

<sup>154</sup> “While many conferences focus on information and network security, only the Black Hat Briefings will put your engineers and software programmers face-to-face with today’s cutting edge computer security experts and ‘hackers,’” as the initial promotional copy put it. (“The Black Hat Briefings: July 9–10, 1997,” Blackhat.com, July 1997, <https://www.blackhat.com/html/bh-usa-97/info.html>.) Blackhat has become the premier corporate hacker conference, known for the quality of its technical discussion—and promotional opportunities. It is also much pricier than DEF CON, which remains a community-driven security hacker conference even as it has grown to be the largest hacker conference in the world.

<sup>155</sup> We will address this backlash in our companion report with particular reference to the “anti-security” movement and its outgrowths.

<sup>156</sup> Rebecca Slayton, “The Paradoxical Authority of the Certified Ethical Hacker,” *Limn* Issue 8: Hacks, Leaks, and Breaches, February 14, 2017, <https://limn.it/articles/the-paradoxical-authority-of-the-certified-ethical-hacker/>.

<sup>157</sup> Ibid.

“white hats” who they deemed to be destroying their way of life, their cultural scene, and their exclusive access to exploits.<sup>155</sup> Still, the dominant meaning of “black hat” among security professionals was negative; it functioned as a clear pejorative.

Similarly, the “white hat” label only appeared sporadically for most of the 1980s and 1990s, referring to a broad class of figures defending computer systems against attacks, malicious software, or (“bad”) hackers. It was only in the late 1990s that the term acquired its contemporary meaning, referring to a class of security-focused hackers who (ostensibly, at least) relied exclusively on legal, permissioned, or simulated processes to accomplish their work—and who also demonstrated marked professional aspirations. When it came to disclosure, these hackers favored reporting vulnerabilities directly to vendors, only subsequently sharing information with the public when a patch was in place (if at all). White hats might also have supported full disclosure—when it could be rationalized as motivating vendor commitments to security improvement (and, in so doing, perhaps also growing the market for professional hacking). Some companies began to offer professional training focused on those attributes in the 1990s, formalizing them as “ethical hacking” certifications in the early 2000s.<sup>156</sup> Like the term “ethical hacking,” “white hat” did not *automatically* summon any association with an underground scene, as “gray hat” and “black hat” did, but still evoked a cultural connection to the hacker identity.<sup>157</sup>

“Gray hat,” for its part, was a more pointed linguistic intervention introduced by the LOpht into mainstream discourse in 1999. One member explained their motivations in this way:

It was confusing to the press when we would find a vulnerability in, say, Microsoft software. There were news stories that would say “LOpht broke into Microsoft” and leave out the software part. There was this assumption that if you had a vulnerability and an exploit you must be using it [to access] other people’s systems, so you are a criminal. We would say, no that’s a black hat. But then there was a rising use of white hat to mean a security person who used hacker techniques to secure their organization. People started labeling us white hats. But we didn’t want to be associated with that. We didn’t work for corporations. We were doing research, releasing vulnerability information and building tools and we knew it would be used by both white hats and black hats. Ideally, we didn’t want to be labeled because that puts you in a box. We were pioneering independent security research and doing new things.

As we will see in the next subsection, the LOpht’s coinage of “gray hat hacker” was, in some respects, the culmination of years of diligent media work that allowed them to clarify their style of hacking and moral outlook to various publics, while still retaining connections to the

underground scene from which they originally hailed. We now turn to the mid-1990s, when the L0pht aspired to become a self-sustaining enterprise and establish their legitimacy as formidable and employable security researchers and practitioners.

## 6.2 < A New Hat Is Worn: Media Work and a Plan for Business (1992–2000) >

The origins of the L0pht can be traced to a South Boston loft where, in 1992, two founding members began stashing their electronic goods and working on their computers in a space originally secured by their wives for making hats. Within a few years, they acquired a larger loft, added additional members (it hovered between seven and eight), and scrounged the MIT electronics flea market (FLEA at MIT) to add to their growing collection of equipment. In the process, they also solidified their identity as a hobbyist shop for cutting-edge security and computer research, establishing the l0pht.com website in 1994.<sup>158</sup>

In 1995, they formally incorporated as L0pht Heavy Industries (LHI). A year later, as a side enterprise, they launched the website, “LHI Technologies,”<sup>159</sup> which quietly ran parallel to their l0pht.com domain. That partner site was not linked to or announced on their highly trafficked and prominent L0pht website, and separate business cards were even printed for the two entities—L0pht cards with handles and LHI cards with real names. Presented as a “communications technology research and development center,” the new site listed LHI’s research projects and offered a suite of services, including “security analysis” as well as “tiger team”<sup>160</sup> services which involved probing the client firm’s networks and computers. LHI sought to offer something similar to (but more comprehensive than) what was then offered by insurance companies and banks, who by the mid-’90s had begun to partner with security firms like WheelGroup and hire security professionals to provide pentesting and auditing for their customers.<sup>161</sup>

At the time, members held day jobs and paid dues to cover rent and utilities, but they aspired to transform the L0pht into an economically self-sustaining enterprise. At minimum, they sought to generate enough revenue to cover rent and utilities and, ideally, to secure more funds to cover salaries for those members who wanted to work full time on projects that already consumed so much free time.

In 1995, they also coined their famous motto, “Making the theoretical practical.”<sup>162</sup> That tagline functioned as a response to Microsoft, after the company publicly dismissed a vulnerability as merely “theoretical.”<sup>163</sup> It also embodied the L0pht’s working philosophy for years to come. While it would be another few years before the L0pht would more aggressively antagonize Microsoft over the company’s handling of vulnerabilities, the group was already explicit in its mission to ensure that dangerous vulnerabilities were taken seriously. They wanted to make security issues “practical,” which is to say: unignorable. And they did so in any number of ways, at first through the full disclosure

<sup>158</sup> See Menn, *Cult of the Dead Cow* and Fisher, “An Oral History of the L0pht.”

<sup>159</sup> “LHI Technologies,” LHI.com (archive.org capture), December 19, 1996, <https://web.archive.org/web/19961219062445/http://lhi.com:80/>.

<sup>160</sup> “LHI Technologies: Tiger Team,” LHI.com (archive.org capture), February 21, 1997, <https://web.archive.org/web/19970221194423/http://lhi.com/tiger/>.

<sup>161</sup> According to one of our interviewees, firms including Price Waterhouse and Coopers & Lybrand were doing security audits that involved penetration testing from at least the mid 1990s. Our subject says they “hired former blackhats [sic] while advertising loudly that they did no such thing.” A *Fortune* magazine article from that time relays that WheelGroup, a security firm made up of both ex-military and ex-underground hackers, offered penetration testing (what they then called “external auditing”) that would be complemented by the supervision of accounting firms like Coopers & Lybrand. Richard Behar, Amy Cover, and Melanie Warner, “WHO’S READING YOUR E-MAIL? AS THE WORLD GETS NETWORKED, SPIES, ROGUE EMPLOYEES, AND BORED TEENS ARE INVADING COMPANIES’ COMPUTERS TO MAKE MISCHIEF, STEAL TRADE SECRETS—EVEN SABOTAGE CAREERS,” February 3, 1997, [https://money.cnn.com/magazines/fortune/fortune\\_archive/1997/02/03/221526/index.htm](https://money.cnn.com/magazines/fortune/fortune_archive/1997/02/03/221526/index.htm).

<sup>162</sup> The full motto, “Making the Theoretical Practical Since 1992,” still appears on the banner of the l0pht.com website. As the next footnote explains, the phrase was invented in 1995.

<sup>163</sup> For a blog post covering the details of Microsoft’s dismissal of this particular vulnerability as merely theoretical, see: jerichoattrition. “That Vulnerability Is ‘Theoretical!’” OSVDB (blog), August 13, 2017. <https://vulndb.wordpress.com/2017/08/13/that-vulnerability-is-theoretical>

practice of documenting vulnerabilities, writing exploit code, developing proofs of concept, and publishing public advisories. Later, they would make those theoretical issues even more practical, releasing software tools with user-friendly graphical interfaces.

Practicality also meant advertising the issues in popular media, attracting public attention to what they considered matters of public security, and promoting themselves, too, as noble hackers. For that strategy of advancing the global state of security to be successful, it meant the hackers bringing the vulnerabilities to public attention would have to be perceived as legitimate.

Thus, the L0pht also sought to re-educate journalists about hackers' roles in securing systems, and they found ample opportunities to do so. Their first media appearances in 1995 tended to be in niche outlets. But starting in 1996, they landed higher-profile spots in print (such as *Wired*) and TV segments in the evening news.<sup>164</sup> As they armed themselves with talking points, the L0pht was picky about who they spoke with and discerning about their message, seeking to avoid being pegged as malicious miscreants in order to frame themselves as righteous and skilled security hackers.

As a result, the question of morality—and thus legitimacy—came up frequently in their media work. One representative example can be found in a March 1997 *New England Cable News* feature. A news anchor relays to the audience how “software that we think is secure, they [the L0pht] find flaws with.” A second anchor then asks: “Are they the bad guy or the good guy?” Without skipping a beat, the first anchor confirms: “Good guy.” She then turns to a desktop computer displaying L0pht advisories and explains why publishing that material is in the public interest.<sup>165</sup>

The L0pht sought to convey both sound moral intentions and hacker “cred” to the technical and hacker community. Take, for instance, the 1997 talk delivered by Peiter “Mudge” Zatko, one of the group’s best-known members, at the first Black Hat Briefings conference. Titled “Secure Coding Practices and Source Code Analysis,” Zatko opens by complicating the distinction between white and black hats. “I like to think we’re good guys. I like to think we’re both white and black hat. I don’t think the black hats are bad. Sure, you have some people that break things. You choose who you want to associate with and what you do.”<sup>166</sup>

By 1998, even as the L0pht scored favorable press mentions and further clarified its philosophy of work, the group struggled to meet its financial goals. Members laid out a more ambitious plan in a document titled “PLAN FOR BUSINESS.”<sup>167</sup> In a passage diagnosing the failures of COMSEC—almost certainly the first security company founded by underground hackers—half a decade earlier, two things become clear: first, even as the L0pht was comfortable with going pro, they were anxious to retain their hacker identities and credibility

<sup>164</sup> Their TV and film appearances are collated in the following video: Joe Grand. *L0pht Heavy Industries Video Press Kit (1994-1999)*. From original VHS tape release, 2021. <https://www.youtube.com/watch?v=P5j7chCzzPA>. We were also provided a list of print media citations.

<sup>165</sup> Ibid.

<sup>166</sup> Mudge. *Secure Coding Practices and Source Code Analysis - Black Hat USA 1997 Audio*. InfoCon Collection: Hacking Conference Archive, 1997. <https://infocon.org/cons/Black%20Hat/Black%20Hat%20USA/Black%20Hat%20USA%201997/audio/>.

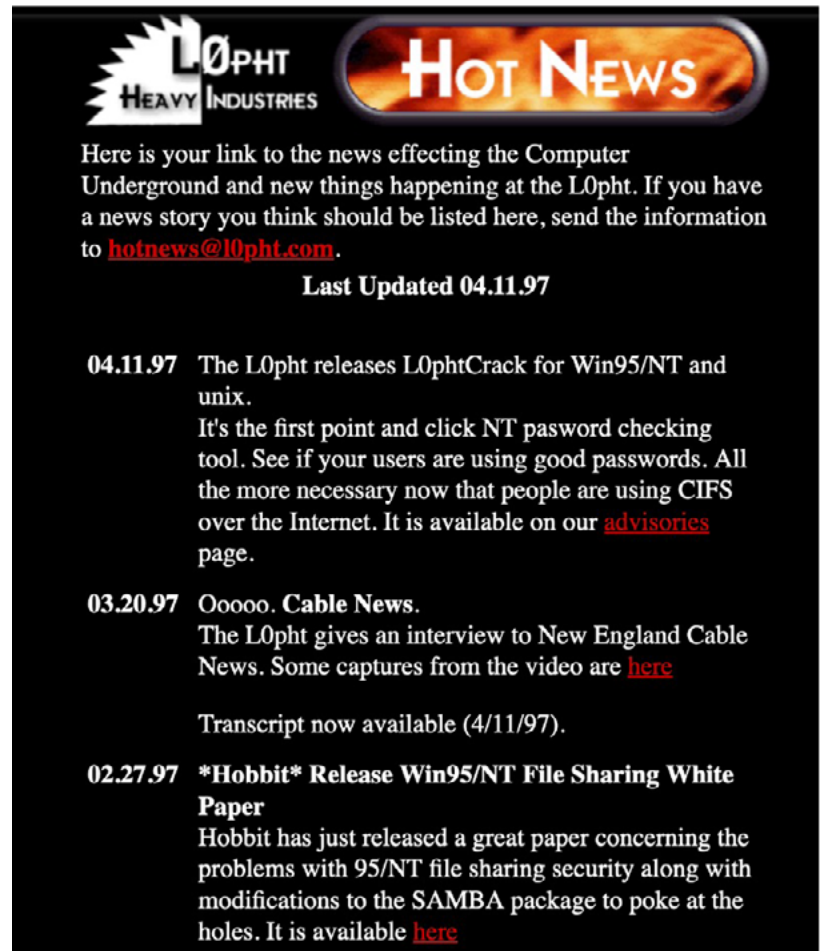
<sup>167</sup> During an interview, a member of the L0pht provided us with this document in addition to L0pht media material.

in the scene and, second, they were already considering the work they had done engaging with media as a victory for hackers, laying the groundwork for their further success:

COMSEC lost respect both in the hacker community as well as the industry. COMSEC was the first “hackers turned consultants” company. The industry was not ready to trust hackers enough to hire them though and the group hadn’t cleaned up their image enough to change that perception. *L0pht has primed the media to accept hackers.* Hackers now work in all the large companies who are potential customers for computer security software and represent L0pht’s most valued network of contacts. L0pht has not and will not turn its back on the hacker community and will continue to contribute to it as well as use that community to L0pht’s advantage. [Emphasis added]

And indeed, the media had been primed. The L0pht garnered scores of glowing accounts in both boutique and mainstream press—all carefully curated on the group’s website under a “Hot News” category, alongside notifications of new technical advisories.<sup>168</sup>

<sup>168</sup> “L0pht Heavy Industries: Hot News,” L0pht.com (archive.org capture), April 15, 1997, <https://web.archive.org/web/19970415132515/http://www2.l0pht.com/hotnews.html>.



**L0PHT HEAVY INDUSTRIES** **HOT NEWS**

Here is your link to the news effecting the Computer Underground and new things happening at the L0pht. If you have a news story you think should be listed here, send the information to [hotnews@l0pht.com](mailto:hotnews@l0pht.com).

**Last Updated 04.11.97**

**04.11.97** The L0pht releases L0phtCrack for Win95/NT and unix.  
It's the first point and click NT password checking tool. See if your users are using good passwords. All the more necessary now that people are using CIFS over the Internet. It is available on our [advisories](#) page.

**03.20.97** Ooooo. Cable News.  
The L0pht gives an interview to New England Cable News. Some captures from the video are [here](#)  
Transcript now available (4/11/97).

**02.27.97** \*Hobbit\* Release Win95/NT File Sharing White Paper  
Hobbit has just released a great paper concerning the problems with 95/NT file sharing security along with modifications to the SAMBA package to poke at the holes. It is available [here](#)

<sup>169</sup> We were unable to locate any reference to gray hat prior to this period and independent of the L0pht. However, we recognize others might have also started to riff and respond to the proliferation of the white and black hat terminology by using the phrase “gray hat” prior to 1999. Whatever the provenance, the L0pht certainly popularized the term. Asked about the term in an email correspondence, Wysopal relayed that he and Zatko were not able to remember if they coined the term in 1998 or 1999.

In 1999, L0pht began to replace the language of white and black hat all together, favoring a third term of their invention: “gray hat.”<sup>169</sup> In response to an email query, L0pht members recalled that



the term was first hit upon during an impassioned discussion between Zatzko and another L0pht member, Chris “Weld Pond” Wysopal. The subject was one of the biggest players in the corporate technology world—IBM. As we addressed earlier, IBM started to adopt the term “hacking” to describe some of its security services, but in a fashion that disavowed any association with the underground or black hat hacking. L0pht members relayed that Zatzko was incensed at Big Blue’s marketing of such services as “ethical hacking,” with all the moral implications implied. During his “rant,” he told Wysopal that they were not black or white hats but *gray*. As they both saw it, IBM was also adding insult to injury by profiting from underground methods. In a subsequent email exchange for this report, Wysopal explained the tenor of the conversation as follows:

The commercial world was trying to adopt the techniques and capabilities of the underground but wanting to draw clear lines. We didn’t want to do that. They wanted to learn from us and take the information and commercialize it, leaving the tainted researcher behind. We were non-white hat. We wanted the researcher to be accepted as the authority and get them the job.

The term “gray hat” thus allowed the L0pht to continue its quest to rehabilitate and legitimize hackers in a way that bypassed the stark binary of white and black hat increasingly adopted by corporations, the press, and even some hackers.

And the timing could not have been better. Coming off the heels of the L0pht’s testimony to the US Senate on the subject of internet security (addressed in the next section), they were profiled in a lengthy 1999 *The New York Times Magazine* article. The journalist gave the group ample room to flesh out the meaning of “gray hat”: “‘We are all extremely ethical and moral,’ one member allowed, ‘but we’re not white-hat hackers. We have our own moral and ethical standards’—the term is gray-hat.” Their “moral standards” referred to their willingness to publicly disclose vulnerabilities and release controversial cracking tools, which they maintained, contra Microsoft, was not malicious but a politically expedient mechanism to pressure negligent companies into writing more secure software from the get-go or force them to patch any bugs quickly. Crucially, in the same piece, Zatzko also elaborated on what the morally flexible “gray” position entailed. “Mudge frankly admits that he’ll answer anyone’s technical questions about hacking. ‘If a black hat approaches us and says, Hey, this is the project or problem I’m looking at... we’ll talk to them, no problem. And if a government agency approaches us and says, How do you do this, or, How does this work, we’ll talk to them.’”<sup>170</sup> In doing so, the L0pht announced itself as a potential bridge between the underground and the establishment.

By the time L0pht was acquired in 2000 by a nascent security firm called @stake, the “hacker” label had largely been made into a professional selling point. The company even printed T-shirts emblazoned

<sup>170</sup> Bruce Gottlieb, “Hack, CouNterHaCk,” *The New York Times*, October 3, 1999, <https://archive.nytimes.com/www.nytimes.com/library/magazine/home/19991003mag-hackers.html>.

- 171** “The L0pht, Renowned ‘hacker Think-Tank,’ to Join @stake: Receives \$10 Million in Initial Backing from Battery Ventures,” @stake Events & News (archive.org capture), January 6, 2000, [https://web.archive.org/web/20000819004156/http://www.atstake.com/events\\_news/press\\_releases/launch.html](https://web.archive.org/web/20000819004156/http://www.atstake.com/events_news/press_releases/launch.html).
- 172** Ted Bridis, “Hackers Becoming Consultants,” *ABC News*, January 6, 2000, <https://abcnews.go.com/Technology/story?id=99325&page=1>. (Date is wrong on website).
- 173** Space Rogue, “Hackers Need Not Apply,” *SPACE ROGUE: L0pht, Whacked Mac, HNN, CSI* (blog), December 11, 2009, <https://www.spacerogue.net/wordpress/?p=191>.
- 174** Consider, for instance, the case of Mark Abene, whose job offer from @stake was retracted when management learned of his hacking-related legal troubles. Poulsen, Kevin. “AtStake Jilts PhiberOptik.” *SecurityFocus*, September 1, 2000. <https://www.securityfocus.com/news/79>.

with the term across the back in large letters for employees to wear as they manned an @stake booth during the 2000 RSA conference. The January 6, 2000, @stake press release announcing the group’s acquisition renders the “grey-hat,” “unorthodox, extreme technical sophistication” of these hackers into a marketing pitch,<sup>171</sup> and it features prominently in related PR. Consider the *ABC News* article reporting on the event, “Hackers Becoming Consultants.” Zatkan, speaking then as @stake’s VP of Research and Development, reaffirmed the “gray hat hacker” label, prompting the journalist to inform readers about the length of the newly employed hacker’s hair: “‘We wear it with pride,’ Mudge explained, whose long hair flows past his shoulders. ‘We will look at any angle that we can. We’re not over there breaking into systems. We’ll let our record speak for itself.’”<sup>172</sup>

@stake, benefiting from the attentional work of hackers like the L0pht, reaped fantastic PR for that move. Prior to that moment, companies had been reluctant to publicize their employment of these types of hackers—if they even knew that they had hackers on staff. @stake’s public position was understood by some as opening a door to acknowledging that hacker workforce, and even inviting more hackers into the profession.<sup>173</sup>

Still, in that transitory moment, the stigma attached to the hacker underground continued to serve as a stumbling block to would-be professional researchers. Many firms, even @stake, were unwilling to hire hackers with felony convictions.<sup>174</sup> If they were able to get jobs, hackers faced, or at least feared, the prospect of legal troubles and termination given their association with that illicit craft and scene. Hackers hired in that period at other firms described feeling pressured to obscure or sever their ties to underground hacking communities—barring them from attending conferences like DEF CON, for instance. At least some of the hackers we interviewed report having felt the heat and complying through small acts of obfuscation; they would attend events, but steer clear of any photographers, ensuring no record of their presence existed for their bosses to find. One researcher told us about his experience being hired by Hewlett Packard, specifically due to his hacker status. “At this point in time, the only people to hire with any existing knowledge and ability were hackers. So companies (like HP) wanted to hire hackers, but they also couldn’t hire hackers from a PR perspective. This caused some weird company announcements where they would celebrate hiring a well known set of hackers, but also deny hiring hackers.” That meant hackers had to maneuver carefully within their new workplaces. “We were all told we couldn’t go to DEF CON. ‘We’re not hackers.’” He recounted another story from his first year at Microsoft. Encountering a hacker he knew from the scene, he relays that “The person hauled me out of the room and was like, ‘Do not tell anyone my handle.’” Much of that reputational work occurred informally and quietly, as both hackers and management sought to negotiate what everyone recognized as a potentially delicate HR situation

## 6.3 < Blaming the Vendor, and Vendor Engagement (1995–2002) >

As hackers managed their reputations, they also contributed to a parallel effort that boosted their public legitimacy. Many hackers featured in this report were central players in an informal but aggressive shaming endeavor against software vendors. While various firms took the heat, one company was singled out above all others, becoming the whipping boy of a multi-year bashing campaign: Microsoft. In an effort starting in the mid-1990s and peaking at the end of the decade, hackers, academics, security professionals, and sympathetic journalists were united in the conviction that Microsoft was particularly egregious, even reckless, in its disregard for security.

The push against Microsoft began in the mid-'90s as a then-routine critique: multiple hackers documented and lamented various Microsoft flaws in mailing lists and other venues. But, as the decade wore on and public scrutiny grew, these critiques morphed into adversarial screeds, and many made sport of publicly shaming the company. That process reached its zenith in 1998, when hacker group Cult of the Dead Cow (cDc), released their "Back Orifice" software package—a collection of readily abusable tools aimed at Microsoft's operating system. These tools demonstrated Microsoft's role in producing insecure software and also presaged the use of spectacle in hacker activism in the following decades.<sup>175</sup>

Nevertheless, the broader shaming campaign proceeded with little coordination between the different individuals, hacker groups, and other aligned technologists who all, in distinct but often complementary registers, managed to credibly demonstrate Microsoft's negligence.<sup>176</sup> In diverting the blame for software insecurity away from the hacker class, and placing responsibility fully on Microsoft's poor security choices and engineering, they also inverted the usual associations between good and bad actors. Even as many technologists had endeavored to call out Microsoft's shoddy projects as an end in itself, they nevertheless succeeded in elevating themselves in the public eye, gaining esteem as security experts operating in the public interest.

While initial criticism of Microsoft on platforms like Bugtraq was rooted in technical details, commentators also peppered their analysis with a light confection of grumbling at Microsoft's irresponsibility. "The whole encryption scheme used by Microsoft in Windows95 is a Bad Joke," propounds the author of a 1995 Bugtraq post otherwise focused on password issues stemming from mounting Unix disks on Windows. "I find this kind of 'security' shocking. I think this should go to the mass media."<sup>177</sup> Over the next couple years, the problems identified with Microsoft products piled up, the posts to mailing lists increasingly expressed dissatisfaction with the company, and the levy of patience started to crack. By 1997, Microsoft's premier operating system Windows NT housed so many flaws, and commanded

<sup>175</sup> As sociologist Douglas Thomas recounted in 2002, the "corporation has been under the skin of hackers since [Bill] Gates's initial confrontation with hackers over pirated software in the 1970s." He argues "mounting antagonism towards Microsoft in the 90s marked a self-reflexive politicization of the hacker community. See Thomas, *Hacker Culture*, p. 93.

<sup>176</sup> Incidentally, it was also a period when free software hackers were critical of Microsoft for how the company sought to discredit the Linux operating system. (See Coleman, *Coding Freedom*, especially, Chapter Two).

<sup>177</sup> Michael S. Fischer, "Cracked: WINDOWS. PWL," Seclist.org: Bugtraq mailing list archives, December 5, 1995, <https://seclists.org/bugtraq/1995/Dec/4>.

- 178** Russ Cooper, “Announcing the NTBugtraq Mailing List,” Seclists.org: Bugtraq mailing list archives, February 1, 1997, <https://seclists.org/bugtraq/1997/Feb/0>. The list, which proved popular, would be sold in 2000 (Bob Sullivan, “NTBugtraq Goes Corporate,” ZDNet, September 20, 2000, <https://www.zdnet.com/article/ntbugtraq-goes-corporate/>.)
- 179** Douglas Thomas, “Why Hackers Hate Microsoft,” *Online Journal Review*, April 29, 1998, <http://ojr.org/ojr/technology/1017969479.php>.
- 180** Aleph One, “L0pht Advisory: Release of L0phtCrack for NT,” Seclists.org: Bugtraq mailing list archives, April 11, 1997, <https://seclists.org/bugtraq/1997/Apr/27>. Also: Jeremy Allison, “Windows NT Password Hash Retrieval,” Insecure.org, March 22, 1997, <https://insecure.org/sploits/WinNT.passwordhashes.deobfuscation.html>.
- 181** Larry Lange, “‘Hack’ Punches Hole in Microsoft NT Security,” *EE Times (Archive.Org Capture)*, March 31, 1997, <https://web.archive.org/web/19981201072421/http://techweb.cmp.com/eet/news/97/947news/hack.html>.
- 182** Larry Lange, “Enhancements to Windows NT ‘hack’ Could Cause More Problems,” *EE Times (Archive.Org Capture)*, April 1997, <https://web.archive.org/web/19981206114812/http://pubs.cmpnet.com/eet/news/97/948news/enhance.html>.
- 183** Aleph One, “L0pht Advisory: Release of L0phtCrack for NT,” Seclists.org: Bugtraq mailing list archives, April 11, 1997, <https://seclists.org/bugtraq/1997/Apr/27>.
- 184** “It primarily exploits the poor design of the LanMan algorithm to recover plaintext passwords.” See: odzhan, “How the L0pht (Probably) Optimized Attack against the LanMan Hash.,” Modexp (blog), February 2, 2019, <https://modexp.wordpress.com/2019/02/02/3883/>.
- 185** Larry Lange, “Hackers Keep the Heat on Windows NT Security,” *EE Times (Archive.Org Capture)*, 1997, <https://web.archive.org/web/19981205132055/http://pubs.cmpnet.com:80/eet/news/97/950news/hackers.html>.
- 186** Jonathan Littman, “It Takes a Hacker to Catch a Hacker: Part 2 Beyond the Pranks,” Defcon.org, August 10, 1997, <https://media.defcon.org/DEF%20CON%205/DEF%20CON%205%20articles/DEF%20CON%205%20-%20Johnathan%20Littman%20-%20It%20takes%20a%20hacker%20to%20catch%20a%20hacker%20-4.html>. “The Black Hat Briefings July 9-10, 1997 Speaker List,” Blackhat.com, July 1997, <https://www.blackhat.com/html/bh-usa-97/speakers.html>.

so much attention on Bugtraq, that a security consultant named Russ Cooper created a spin-off list called NTBugtraq.<sup>178</sup>

According to our interview subjects, Microsoft responded to the mounting evidence of its products’ insecurity by stonewalling—failing to substantially address the critiques by fixing the identified flaws. Then, in March 1997, a free software developer named Jeremy Allison helped set the stage for a far more aggressive campaign to put the Blue Chip company on the hot seat by releasing an exploit called pwdump.<sup>179</sup> The tool exploited weaknesses in Microsoft’s password protection scheme, allowing anyone with administrative access to dump a list of hashed user passwords to file.<sup>180</sup> This was a big deal, as Microsoft was marketing NT as a more secure alternative to Unix. As one journalist described it, “The hack is particularly perturbing for Microsoft since it goes directly for the heart of the NT security system: the Security Accounts Manager (SAM), where the passwords reside.”<sup>181</sup> Even as most of the security community agreed the tool exploited a *security flaw*, Microsoft rejected culpability: “The reported problem is not a security flaw in WindowsNT, but highlights the importance of protecting the administrator accounts from unauthorized access.”<sup>182</sup>

The significance of Allison’s tool was only heightened on April 17, when the L0pht released L0phtCrack v 1.0, a program designed to efficiently defeat Microsoft’s proprietary LANMan password encryption algorithm.<sup>183</sup> Combined with the output of pwdump, every user password on an NT system could be quickly rendered into plain text.<sup>184</sup> While that software had the potential for legitimate uses—helping sysadmins recover lost user passwords or audit them for strength—the primary effect was clear: it made Microsoft look very bad indeed.

In case that message was unclear, Zatko made it explicit. As he explained to Larry Lange, a journalist closely covering the beat, “We’re doing this because Microsoft is shoving stuff down people’s throats, and you don’t have the ability to look and see how good it is.”<sup>185</sup> Microsoft officials, given yet another chance to opine, continued to toe the party line—doubling down on rhetoric that positioned the user of their software as ultimately responsible for their own security. As Lange tells us, “Officials insist that if network administrators and users pay adequate attention to security issues, cracking encrypted passwords on any NT network remains inherently difficult.”

As the spring of 1997 gave way to summer, the hacker assault against Microsoft continued to intensify in presentations at Black Hat, DEF CON, and Hackers on Planet Earth. When a hacker known as “Hobbit” (Al Walker) detailed a slew of problems in Microsoft’s products at Black Hat,<sup>186</sup> an audience member, Paul Leach (Microsoft’s director of NT architecture), at one point defied normal conference decorum, interjecting that Walker’s characterization of an encryption mechanism was wrong. After Walker asked him to wait until the question-and-answer period, Leach later interjected again for a number of seconds, prompting Walker to become defensive and skip to a subsequent



Hobbit, "CIFS: Common Insecurities Fail Scrutiny," Wittys.com, January 1997, <http://www.wittys.com/files/cifs.txt>.

**187** Hobbit, *Microsoft LM Authentication, CIFS, and All Kinds of Password Problems* (Bh-Usa-97-Hobbit-Audio.Rm) (InfoCon Collection: Hacking Conference Archive, 1997), <https://infocon.org/cons/Black%20Hat/Black%20Hat%20USA/Black%20Hat%20USA%201997/audio/>.

**188** Larry Lange, "Microsoft Opens Dialogue With NT Hackers," Blackhat.com, July 15, 1997, <https://www.blackhat.com/media/bh-usa-97/black-hat-eetimes-3.html>.

**189** Lange, "The Rise of the Underground Engineer."

**190** mudge, "Windows NT Rantings from the L0pht: Who Cares What the Hell Goes into a Gecos Field Anyway!," Bugtraq (Cliplab.org archive), July 24, 1997, <https://cliplab.org/~alopez/bugs/bugtraq2/0162.html>.

**191** *Beyond HOPE (1997): The L0pht* (Channel2600), accessed May 26, 2020, <https://www.youtube.com/watch?v=QaAS1I6qigc>.

portion of his presentation.<sup>187</sup>

Then, in July, it seemed that Microsoft had suddenly altered their public stance around hacker-critics. "We've opened up a dialogue. The hackers do a service. We're listening and we're learning," said Carl Karanan, Microsoft's NT marketing director, in *Electronic Engineering Times (EE Times)*.<sup>188</sup> However, that admission came on the heels of a quietly organized meeting between Microsoft employees and three of the most vocal critics—Zatko, Walker, and Yobie Benjamin—in the interim between Black Hat and DEF CON. Retroactively dubbed "The Dinner," the Las Vegas meeting inspired mixed results. While Lange's account of the events in the *EE Times* notes that Benjamin was enthused by what he characterized as a "good first effort" that was likely to lead to "more cooperation," he describes Zatko's vigorous disagreement: "'No, no, no. I got the distinct impression that they were forced to come here,' he says, his piercing blue eyes shining with anger. 'About seven minutes into it, I was about to get up and walk out. They were so not getting it.'"<sup>189</sup>

A couple weeks later, the L0pht continued its offensive anew, sending a lengthy missive to various mailing lists, including Bugtraq: "Windows NT rantings from the L0pht."<sup>190</sup> Barbed insults sit side by side with the technical details of a new 1.5 version of L0phtCrack.

#### A L0phtCrack Technical Rant

Date: Thu, 24 Jul 1997 10:24:37 -0400  
From: Who cares what the hell goes into a Gecos field anyway!

To: BUGTRAQ@NETSPACE.ORG  
Subject: Windows NT rantings from the L0pht

I didn't ask to be cc'd into the rantings of the MS Borg Marketing Juggernaut but since I'm here... I find this hilarious. The people at MS should know better. I haven't been following this thread tremendously but I've seen bit's and pieces. Recently there was an atrocious article in WindowsNT magazine, where they stated it would take 5000 or so years to break the passwords; thus put policy in place to have users change their passwords every 2500 years. HELLO? I think these people aren't getting it. Let's shed some light on things shall we?

1. Thank you very little MS for dropping any reference to the l0pht, hobbit, or myself in reference to your recent LM-Hash fix. If this is how you "correspond" with people who point out problems to you it's no wonder that people prefer to release things to the public instead of your "proper" channels.

2. MS agrees that the LM hash is a horrible implementation from a security standpoint. They respond with: "well we didn't write the protocol that was IBM".

3. When MS had the chance to do things a different way (ie Network challenge/response obfuscation on NT boxes) they implemented it based upon LM techniques to break up components (see #2).

4. The LM-hash fix works great if you don't have anything but NT machines on your network. If you want to continue being "productive" with your win95 machines it is my understanding that you "do it insecurely" or you are S.O.L.5. Few places are running "nothing but NT" (ie just about everyone has 95 or WfW boxes if MS has already gotten their foot in the door).(see #4)

5. MS can't swallow their pride enough to say "oops", even in technical circles where they don't have to worry about the general public mis-interpreting things.

6. For the LM hash you only have to break 7 characters, not 14!

Just over two weeks later, the L0pht conveyed a similar message at the New York City-based conference Hackers on Planet Earth. Zatko, who did most of the speaking, mixed jargon-laden technical analysis with florid, and often cocky, rapid-fire remarks defending hackers and chastising Microsoft and other vendors. He went so far as to opine that "hackers are probably the best thing America has going for it,"<sup>191</sup> which given the venue—a hacker con—unsurprisingly earned



a rousing cheer. He reminded the already riled-up audience that the “bad guys” were the big corporations, that hackers were the “good guys,” and that Microsoft had up to that point failed to address and improve their subpar crypto in any substantive way.

A year later, attention shifted to cDc, as they moved to more aggressively put Microsoft under the spotlight. The group’s tagline, “Global domination through media saturation,” made their aim clear: rather than simply hacking together (in)security tools, they were hacking media perceptions.<sup>192</sup> Known primarily for their edgy text files, by the mid-’90s, cDc was hard at work exploiting the media’s preconceived notions about hacking to mostly playful effect. Where the L0pht sought to present an image of the underground hacker as a Renaissance figure, the cDc frequently played into the stereotypes in an ironic manner, laughing at the media’s willingness to play up the hacker menace.<sup>193</sup> Fittingly, another cDc tagline read “cDc. Hyperbole is our business.” In 1998, cDc released a text file titled *The Journalist’s Cookbook* (a clear reference to the notorious *Anarchist Cookbook*, a mainstay of edgy digital libraries and subject of media consternation<sup>194</sup>). In it, author Laird Brown (“Oxblood Ruffin”) mixes genuine information with parodic advice, including ironic suggestions about how to best introduce the common clichés found in formulaic journalistic coverage of hacking.<sup>195</sup>

Shortly after, the media-savvy group released *Back Orifice* (BO) to great media spectacle at DEF CON 6, in 1998. Developed by cDc member Josh “Sir Dystic” Buchbinder, the software’s name was a punny jab at Microsoft’s *BackOffice* product suite. It was described as a “remote administration tool,” and indeed it delivered on that promise: allowing for stealth remote control of Microsoft Windows 9x machines—with or without a user’s knowing consent (Windows 9x refers to MS operating systems rolled out between 1995 and 2000). It was common for hacking groups to maintain forms of plausible respectability with their tools—recall the ability to use *L0phtCrack* to recover lost passwords. But the cDc hedged their position with only the thinnest rhetorical veneer, quoting Buchbinder on the “two main legitimate purposes” for the tool in their initial press release, before taking aim at Microsoft’s “swiss cheese approach to security.”<sup>196</sup>

The existence of that software alone was likely to ruffle feathers, but cDc went the extra mile to court attention, ultimately making it clear that BO was designed and promoted to facilitate mischief with Microsoft systems, plain and simple. Numerous security and antivirus firms went on to explicitly label BO (and its successor *BO2k*) as malicious software (for instance, F-Secure, a respected Finnish company, deemed both BO and *BO2k* as examples of “backdoor Trojans.”<sup>197</sup>).

BO’s technical presentation at DEF CON was preceded by cDc co-founder Kevin “Grandmaster Ratte” Wheeler pacing back and forth on a conference table wearing leather chaps, a thick chain

<sup>192</sup> See Menn, *Cult of the Dead Cow* and Goerzen, “Critical Trolling.” (MA Thesis)

<sup>193</sup> See Menn, *Cult of the Dead Cow* for stories. The exploits of cDc Minister of Propaganda Deth Vegetable are particularly notable, as when he wrote an over-the-top parodic bomb-making guide that drew substantial media attention.

<sup>194</sup> Sankin, Aaron. “‘The Anarchist Cookbook’ and the Rise of DIY Terrorism.” *The Daily Dot* (archive.org), March 22, 2015. <https://web.archive.org/web/20170109183816/http://kernelmag.dailydot.com/issue-sections/headline-story/12210/anarchist-cookbook-history-usenet/>.

<sup>195</sup> Fleming, Reid. “cDc Communications Presents: The Journalist’s Cookbook Version 1.0.” *Textfiles.com*, July 15, 1998. <http://www.textfiles.com/groups/CDC/cDc-0360.html>.

<sup>196</sup> The Deth Vegetable, “RUNNING A MICROSOFT OPERATING SYSTEM ON A NETWORK? OUR CONDOLENCES,” *cultdeadcow.com* (archive.org), July 21, 1998, [https://web.archive.org/web/20000816004036/www.cultdeadcow.com/news/back\\_orifice.txt](https://web.archive.org/web/20000816004036/www.cultdeadcow.com/news/back_orifice.txt).

<sup>197</sup> F-Secure, “BO2K Description,” F-Secure Labs, accessed January 26, 2021, <https://www.f-secure.com/v-descs/bo2k.shtml>. BO2k, “Back Orifice,” BO2k Cyber Security Blog, March 15, 2017, <http://www.bo2k.com/category/back-orifice/>.

necklace, and two holstered (presumably fake) pistols, demanding of the crowd, “When I say dead, you say cow!” Another cDc member, Sam Anthony (“Tweety Fish”), then encouraged members of the audience to use tools like BackOrifice in service of a particular goal. “Hacktivism,” he said. “What we have here is a concept and a series of tools and a whole methodology that takes the slacker ethic out of all you people. We are making it easy enough that an eight-year-old can make a difference, can fuck shit up, a little bit, for the Cult of the Dead Cow.” The audience cheered, and Buchbinder proceeded to demonstrate the software and speculate as to the most covert ways to implant it on a target machine.<sup>198</sup>

**198** Buchbinder, Josh. “DEF CON 6 - the Cult of the Dead Cow (CDc) - The Announcement of Back Orifice.M4b.” InfoCon Collection: Hacking Conference Archive, August 1, 1998. <https://infocon.org/cons/DEF%20CON/DEF%20CON%206/DEF%20CON%206%20audio/>.

**199** BetaFred, “Microsoft Security Bulletin MS98-010 - Critical,” Microsoft Documentation, August 4, 1998, <https://docs.microsoft.com/en-us/security-updates/securitybulletins/1998/ms98-010>.

**200** CULT OF THE DEAD COW, “ST. PAUL, BACK DOOR BOOM BOOM, AND ALL THE TEA IN CHINA,” [cultdeadcow.bnb.it](http://cultdeadcow.bnb.it), accessed January 26, 2021, <https://cultdeadcow.bnb.it/news/response.txt>; see also a line-by-line response to Microsoft’s statement: “Cult of the Dead Cow Responds to Microsoft,” [cultdeadcow.com](http://cultdeadcow.com) (archive.org), <https://web.archive.org/web/19990129060839/http://www.cultdeadcow.com/news/rebuttal.txt>.

**201** Matt Richtel, “Hacker Group Says Program Can Exploit Microsoft Security Hole,” *The New York Times*, August 4, 1998, <https://archive.nytimes.com/www.nytimes.com/library/tech/98/08/cyber/articles/04hacker.html>; Michael J. Martinez, “Windows Faces Hack Attack,” *abc News* (archive.org), August 11, 1998, <https://web.archive.org/web/19990507233331/https://abcnews.go.com/sections/tech/DailyNews/backorifice980811.html>.

**202** Emma Best, “Behind the Scenes with the Hacktivists Who Took on Microsoft and the FBI,” *The Outline*, June 5, 2019, <https://theoutline.com/post/7529/cult-of-the-dead-cow-beto-orourke-hacktivists-bo2k-fbi>.

**203** [cultdeadcow. \*Présentation de B02K Dans Les Coulisses\*. YouTube video, 1999. https://www.youtube.com/watch?v=oHxNEvklKqE](https://www.youtube.com/watch?v=oHxNEvklKqE).

Shortly afterward, Microsoft issued a press release, affirming the security of their products and suggesting that any harms caused by BO were solely due to misguided user practices.<sup>199</sup> And so the cDc responded via their own lengthy press release—a self-styled “morality alert.” It addressed the question of responsibility point blank, opening with the following question: “Was releasing Back Orifice to the public immoral?” and continuing, “Microsoft would love for their customers to believe that we’re the bad guy and that they—as vendors of a digital sieve—bear no responsibility whatsoever. But questions of morality are more relative than absolute. So to make things easier, we’ll frame our culture and actions against theirs and let the public determine which one of us looks better in black.”<sup>200</sup>

A range of journalistic outlets reported on the event, often with quotes from respected security researchers and consultants who affirmed the software as a useful tool for illustrating problems with Microsoft’s lax security.<sup>201</sup>

A year later in 1999, at DEF CON 7, with Microsoft-bashing a more popular activity than ever, L0pht / cDc member Christien “Dildog” Rioux debuted a second edition of Back Orifice, Back Orifice 2000 (BO2K). The event was even more over-the-top and spectacular than the year before, casting cDc and L0pht members as subcultural celebrities.<sup>202</sup> The talk opened in a darkened room, strobe lights flashing alongside music beats, with audience members cheering. Footage of the event captures a woman muttering, “My god this is going to rock so much,” as the members of the collective make their way to the stage.<sup>203</sup> When the lights turn on, the audience erupts into volcanic cheers. Ratte’ riles up an already riled-up crowd, once again having the audience answer back to his call: “When I say dead, you say cow!”

In the short term, tools like L0phtCrack, Back Orifice, and Back Orifice 2000 provided platforms to publicly flip the moral narrative around good and bad guys. Many of our interviewees also acknowledged that these visible stunts and tool releases shifted the conversation around insecurity. One human rights technologist, who otherwise chastised the cDc for failing to provide substantive technical contributions to human rights causes (despite rhetorical commitments), commended BO, going so far as to describe it as “a

genius hack.” He explained further, “I loved it. It was hilarious. I thought it was a great way to show how completely unthinking Microsoft was about these kinds of key security issues. It was a really valuable demonstration for me when I was talking to human rights people in the field about the insecurity of computers.” On the flipside, other hackers we interviewed felt that the cDc was the unthinking party, arguing that their brazen actions erected roadblocks for hackers seeking to professionalize. As one put it: “You could argue the whole BO2K stunt obstructed [that] path,” elaborating that it was because of the way it could be spun to fuel the hysteria around hackers.

Pinpointing the exact effects of BO and BO2k, independent of other trends, may be impossible. cDc courted controversy so successfully, it is likely the release of that software worked at multiple registers: simultaneously demonizing hackers to some observers, valorizing hackers to others, and making Microsoft look bad to most.<sup>204</sup> That could have a good cop / bad cop sort of effect—while some hackers, like the cDc might look bad, legitimacy-seeking groups like the L0pht were made to appear, by contrast, like eminently respectable and reasonable hackers—the sort of hackers you might want working for you to protect against the Cult of the Dead Cow (with whom they shared some members).<sup>205</sup> It also helped establish computer security as a fixture of the media agenda. And, when placed alongside the other trends discussed here, the totality of those interventions had an undeniable, incremental effect on Microsoft.

Over time, those types of campaigns and the growing chorus of critiques tarnished Microsoft’s reputation on security, eventually coaxing change in the company’s Redmond headquarters. Most immediately, that meant consulting with hackers. By 2002, Bill Gates declared “security” (under the guise of a “trustworthy computing” initiative) was now the company’s “highest priority.”<sup>206</sup> They proceeded to hire former enemies—hackers—to help lead the way. Among the new hires was Window Snyder, a former employee of @stake and member of the Boston hacker scene. Alongside other changes, and in keeping with the hacker “hat” fixation, she opened the Microsoft gates to security-minded hackers by hosting a new conference dubbed BlueHat Security.<sup>207</sup> One lawyer we interviewed who had defended hackers in that era noted that bringing Snyder and other hackers on board was “a great exhibit of the [change] from hackers being Microsoft’s mortal enemy in some ways to being its partners and employees.” Or, as a member of the L0pht told us, it was evidence of Microsoft’s new “If you can’t beat them, hire them” policy.

## 6.4 < Allyship and the L0pht’s Testimony (1998 and On) >

As hackers were engaged in diverse efforts of linguistic re-engineering, media hacking, tool building, PR stunting, and vendor blaming, they were also aided by prominent non-hackers convinced of their skills and trustworthiness. Throughout the decade, a small

<sup>204</sup> For the value and limits of using shaming as a political tactic to catalyze social change, see: Jacquet, Jennifer. *Is Shame Necessary? New Uses for an Old Tool*. Vintage Books, 2016.

<sup>205</sup> Menn, *Cult of the Dead Cow*, p.77 provides evidence that the good/bad cop dynamic between cDc and L0pht was concocted as a deliberate strategy.

<sup>206</sup> Robert Lemos, “Gates: Security Is Top Priority,” *CNET*, March 2, 2002, <https://www.cnet.com/news/gates-security-is-top-priority/>.

<sup>207</sup> Menn, *Cult of the Dead Cow*, p. 111.

**208** Bruce Schneier, “Crypto-Gram,” Schneier on Security, August 15, 1999, <https://www.schneier.com/crypto-gram/archives/1999/0815.html>.

**209** Ibid.

**210** Thanks to a Freedom of Information Act (FOIA) request, journalist and former hacker Emma Best revealed the FBI had opened a case against cDc after the release of B02K but eventually dropped it. See: Best, “Behind the Scenes with the Hacktivists Who Took on Microsoft and the FBI.”

**211** A detailed list of such the source, nature and outcome of such threats is kept by a hacker collective, attrition, many members of which were part of the underground and later professionalized. “Legal Threats Against Security Researchers: How Vendors Try to Save Face by Stifling Legitimate Research,” Attrition.org, 2008, [http://attrition.org/errata/legal\\_threats/](http://attrition.org/errata/legal_threats/).

**212** See Sterling, *The Hacker Crackdown*.

**213** She first spoke at DEF CON 6, held in 1998 (Granick, “A Review of Several Major Computer Crime Cases from the Past Year or Two”), and continued to give talks in the subsequent years on legal issues of concern for the hacker community (see: Poulsen and Granick, “The Legalities and Practicalities of Searches and Interrogations”; Granick, “The Law and Hacking”).

**214** “The Lawyer Hackers Call,” *Forbes*, August 4, 2000, <https://www.forbes.com/2000/08/05/feat.html#273825163211>.

but well-resourced supporting cast of characters assessed that class of hacker and their tools in the pages of computer science journals, conferences, blogs, and other venues. In the case of Back Orifice, even as various vendors labeled the software as a cyberweapon, esteemed public figures, such as the cryptographer Bruce Schneier, showered the tool with technical praise. He unraveled the argument that since the tool is written by hackers, it is necessarily “evil.”<sup>208</sup> Indicting such rhetoric as “wrong,” he noted that while the cDc was perhaps better at media “spin” than other aligned technologists, the group’s tool was only one critical method among many others, and the value of BO lay in forcing Microsoft to address the issue: “Explain the threat in an academic paper and Microsoft denies it; release a hacking tool like Back Orifice, and suddenly they take the vulnerability seriously.”<sup>209</sup>

It’s worth noting that even if the Back Orifice, Back Orifice 2000, and L0phtCrack developers never faced legal threats or sanction—at least openly—those risks always loomed over those hackers exposing vulnerabilities in corporate software.<sup>210</sup> Numerous companies went after such technologists, wielding the prospect of prosecution under the CFAA or the Digital Millennium Copyright Act, or putting pressure on researchers or hackers to pull out of talks at conferences like Black Hat that would expose and detail a vulnerability.<sup>211</sup> Those risks were partly mitigated by some of the most important allies from the 1990s: lawyers. While a fuller history of those legal threats has yet to be written (and is beyond the scope of this report), one thing is clear: some American hackers tapped into legal resources. Two of the most important figures in that era were a criminal defense lawyer, Jennifer Granick, and the Electronic Frontier Foundation (EFF), a civil-liberties shop stocked with tech-savvy lawyers unafraid to protect hackers.<sup>212</sup>

Granick first attended DEF CON in the early 1990s, and for largely professional reasons. Working at the time for a small white-collar firm, she was encouraged to develop a specialty and decided to venture into the field of computer crime. But Granick quickly developed personal reasons for supporting the legality of hacking. She “liked that [hackers] were willing to go out on a limb and question everything,” as she explained it during an interview for this study. Many hackers indeed needed legal counsel for exposing vulnerabilities, and she soon became the go-to lawyer for that community, especially after giving numerous talks at DEF CON.<sup>213</sup> Known for her intellectual acumen and approachability, a 2000 *Forbes* profile described her in the headline as “The Lawyer Hackers Call.”<sup>214</sup> She earned that reputation not simply because she was willing to defend hackers, but due to her excellent track record. Most of the cases she took on never went to trial, and were settled favorably for her clients out of court. When asked about the risks around disclosing flaws, she reminisced that “there were a lot of cases around vulnerabilities and disclosing them,” and part of her work entailed conferring with hackers about how they wanted to proceed. Many such cases concerned “Microsoft



- 215** As the conference page puts it, “Industry has tried to develop ‘best practices’ for reporting and repairing vulnerabilities, but major disagreements - over how much information to disclose, to whom, and when - persist.” (“Cyber-Security, Research and Disclosure,” Stanford Law School CENTER FOR INTERNET AND SOCIETY Conference on CyberSecurity, Research, and Disclosure, November 22, 2003, <http://cyberlaw.stanford.edu/security/>.)
- 216** Levy, *Crypto* contains a comprehensive discussion of the debates around cryptography and munitions export laws.
- 217** “Coders’ Rights Project,” Electronic Frontier Foundation, accessed May 26, 2020, <https://www.eff.org/issues/coders>.
- 218** “Coders’ Rights Project,” Electronic Frontier Foundation, accessed May 26, 2020, <https://www.eff.org/issues/coders>.
- 219** “A ‘Grey Hat’ Guide,” Electronic Frontier Foundation, November 19, 2008, <https://www.eff.org/pages/grey-hat-guide>.
- 220** “Coders’ Rights Project Vulnerability Reporting FAQ,” Electronic Frontier Foundation, August 6, 2008, <https://www.eff.org/issues/coders/vulnerability-reporting-faq>.
- 221** See “Legal Threats Against Security Researchers.” (Attrition.org) and see: Sunoo Park and Kendra Albert, “A Researcher’s Guide to Some Legal Risks of Security Research” (The Cyberlaw Clinic at Harvard Law School & The Electronic Frontier Foundation, October 2020), [https://clinic.cyber.harvard.edu/files/2020/10/Security\\_Researchers\\_Guide-2.pdf](https://clinic.cyber.harvard.edu/files/2020/10/Security_Researchers_Guide-2.pdf). More so, legal threats remain an issue in bug bounty work, leading to legal scholar Amit Bar On’s recent push for “safe harbor” for bug bounty workers. See: Amit Elazari, “Hacking the Law: Are Bug Bounties a True Safe Harbor?,” 2018, <https://www.usenix.org/conference/enigma2018/presentation/elazari>.
- 222** Fred Kaplan, *Dark Territory: The Secret History of Cyber War* (New York: Simon & Schuster, 2016). Nicole PerIroth, *This Is How They Tell Me the World Ends: The Cyberweapons Arms Race* (New York: Bloomsbury Publishing, 2021). Slayton, “Framing Computer Security, 1967-1992.” Slayton, Rebecca. “What Is a Cyber Warrior? The Emergence of U.S. Military Cyber Expertise, 1967-2018.” *Texas National Security Review*, January 11, 2021. <http://dx.doi.org/10.26153/tsw/11705>.
- 223** Lawson and Middleton, “Cyber Pearl Harbor.”

because [they] were very aggressive about people disclosing vulnerabilities.” At times, she would even act as liaison between a company and a technologist who sought to inform the firm of the flaw anonymously. In 2003, Granick also co-hosted a day-long Stanford Law School conference intended to bring hackers (“security researchers”) and vendors together to discuss best practices around vulnerability disclosure in the wake of full disclosure.<sup>215</sup>

Similarly, the EFF served as a nonprofit consulted by many hackers (Granick also worked there for a period of time). For instance, another lawyer we interviewed, who’s been at the foundation since 1993, recalled how members of the cDc had visited her for legal advice, given that the encryption included in BO2k could run afoul of munitions laws.<sup>216</sup> For much of its history, the EFF provided extensive legal support to the security hacker community and other technologists. Eventually, in 2008, they compiled lessons learned into a massive online resource called the Coders’ Rights Project.<sup>217</sup> Its introduction conveys just how involved and how important that organization was in protecting hackers:

The Coders’ Rights Project builds on EFF’s longstanding work protecting researchers through education, legal defense, amicus briefs, and involvement in the community with the goal of promoting innovation and safeguarding the rights of curious tinkerers and hackers on the digital frontier. We also provide policy advice to decision-making officials who are considering new computer crime legislation and treaties.<sup>218</sup>

Among many other provisions, it details the risks and rights around “grey hat hacking”<sup>219</sup> and “vulnerability disclosure.”<sup>220</sup>

The legal safety net provided by lawyers like Jennifer Granick and nonprofit organizations like the EFF was instrumental for hackers who were maneuvering in a legal minefield—a set of threats that persisted after hackers were hired in large numbers to work for security firms and has never fully gone away.<sup>221</sup>

Finally, during that period, it was significant that legitimacy-seeking hackers gained the support of powerful allies in the US government. While there would always be detractors, a handful of government officials, policy makers, military personnel, and others came to see computer security as a grave matter of national security. As such, they began to treat domestic hackers as more of a resource than a threat.<sup>222</sup>

That push is perhaps best encapsulated with reference to fears of an “Electronic” or “Cyber Pearl Harbor.” First heralded as a major threat by cyberwarfare proponent Winn Schwartau in a 1991 opinion piece for *Computerworld* and subsequent congressional testimony,<sup>223</sup> the rhetoric would be echoed with increasing consistency toward the end of the decade, as a silent push to securitize information technologies mounted in government.<sup>224</sup> A definitive moment can be



224 Kaplan, *Dark Territory*. Slayton, “Cyber Warrior.”

225 For a hacker cultural take on this securitization rhetoric and the role of the media in amplifying it, see “Guided Perceptions” in the Summer, 1996 edition of *2600*. Collected in *Best of 2600*, p. 256

226 This history is covered in Menn, *Cult of the Dead Cow*, pp. 74-76 and Kaplan, *Dark Territory*, pp. 89-96.

227 Quoted in Menn, *Cult of the Dead Cow*, p. 74.

228 Kaplan, *Dark Territory*, p. 89-95; covered as well in Menn, *Cult of the Dead Cow*, p. 74-77

229 This was not the first time a US governmental committee heard from a hacker. For instance, in 1983, former phone phreak and hacker Susan Headley (“Susy Thunder”) testified to a Congressional Committee entitled “Computer Security in the Federal Government and the Private Sector.” See: US Senate, *Computer Security in the Federal Government and the Private Sector: Hearings before the Subcommittee on Oversight of Government Management of the Committee on Governmental Affairs, United States Senate, Ninety-Eighth Congress, First Session*, S. Hrg.; 98-440 iv, 504 p. (Washington: US G.P.O., 1983), <https://hdl.handle.net/2027/pst.000012047208>. However, the L0pht testimony generated far more press.

230 “Cybersecurity: When Hackers Went to the Hill – Revisiting the L0pht Hearings of 1998,” National Security Archive, January 9, 2019, <https://nsarchive.gwu.edu/briefing-book/cyber-vault/2019-01-09/cybersecurity-when-hackers-went-hill-revisiting-l0pht-hearings-1998>.

seen in then-President Bill Clinton’s executive order that put emphasis on the cybersecurity of critical infrastructure in the wake of the Oklahoma City Bombings in 1995.<sup>225</sup>

One key figure involved in selling the importance of cybersecurity to government and military officials was Richard Clarke, who had been tapped by President Clinton to be the National Coordinator for Security, Infrastructure Protection, and Counter-Terrorism. Lacking a technical background, he first educated himself about computing, security, and cyber threats by reaching out to hackers and corporate executives running technology firms.<sup>226</sup> According to Clarke, both intelligence agencies and computer and software firms downplayed cyber threats. The companies claimed their products were sound from a security perspective, with the CEOs of Microsoft, Oracle, and Cisco Systems telling him, “their shit didn’t stink.”<sup>227</sup> Given that Clarke had also been reading about hacks in the news, he was unconvinced by the corporate party line and set out to get a second opinion from hackers themselves. Through an FBI contact who had received technical help and guidance from the L0pht, Clarke arranged an evening drinking session with these hackers in Boston. As mentioned earlier, the L0pht was willing to provide technical assistance to anyone, including law enforcement, which was a shrewd reputational move given the crackdowns against hackers of the era. Clarke was both impressed and stunned by how they informed him that internet security was essentially a unicorn—a nonexistent magical being—and that a proficient hacker, not just the might of a nation-state, could intrude and disrupt whatever was connected to the system. Clarke also helped secure an invitation from Senator Fred Thomson for L0pht to testify at a hearing held by the Senate Governmental Affairs Committee on Cybersecurity.<sup>228</sup>

And so on May 19, 1998, a congressional hearing on the subject of computer security was held with hackers.<sup>229</sup> In what became hacker legend almost overnight—and a source of endless derision for some black hat purists we spoke with—seven members of the L0pht sat down next to each other at a long, stately desk with Zatzko in the middle.<sup>230</sup> Introduced not by their legal names but their hacker handles, the tone was far more somber and serious compared to their talk the year before at Hackers on Planet Earth. Zatzko—sitting behind a placard bearing his handle, “Mudge”—began by introducing the buffet of skills held by each member of what he described as a “hacker think tank.” After, he moved to a more alarmist exposition about the insecurity of the internet, claiming they could technically take down the internet in thirty minutes. But the more substantial part of the testimony backed away from sounding the alarm. Instead, it concentrated on both the reasons driving insecurity and the many “trivial” changes and fixes that could be made or incentivized through a variety of channels—legislative and technical—to ensure a modicum of security.

The four senators in attendance—Fred Thompson, Susan

Collins, Joe Lieberman, and John Glenn—were smitten with the hackers, who presented as regular and clean-cut young white men, even if Zatzko's hair was an exception (his long golden hair nearly reached the wooden table). Each hacker was soft-spoken, measured, even gentle in their style of talk. Most importantly, they had an assuring, reassuring, and comforting message: even if there were problems, solutions were readily available. After the testimony, the senators showered them with praise, with Lieberman telling them they were good patriots who “are performing an act of very good citizenship.”<sup>231</sup>

<sup>231</sup> Gottlieb, “HacK, CouNterHaCk.”

<sup>232</sup> Peiter Zatzko, *Conan O'Brien Jokes about the L0pht Hacker Group*, 2015, <https://www.youtube.com/watch?v=xmSXkA6Xlr4>.

While the L0pht had scored plenty of headlines before their Capitol Hill visit, the event propelled them into their 15 minutes of mini-stardom. Along with a dedicated *The New York Times Magazine* spread, complete with glossy color pictures, the late-night TV host Conan O'Brien cracked jokes about them in his opening monologue.<sup>232</sup>

*The New York Times* magazine profile is worth revisiting one final time for how it provided the L0pht with a platform to explain—not only on their own terms, but in lay terms—the technical, often esoteric debates around full disclosure, vulnerabilities, vendor shaming, and so on. Those debates had been otherwise unfolding in geekier corners of the internet or the security press throughout the prior decade. The journalist portrayed them as fiercely independent, Ralph Nader-like renegades, willing to call out vendors when necessary. “We were trained by the vendors to go public,” says Mudge, “to give them a black eye.”<sup>233</sup> More so, the L0pht maintained their integrity by claiming their autonomy. They were portrayed as invested in security work, not for money but because it was the right thing to do: “Like Nader, the L0pht members can get a bit preachy on the subject of ethics. ‘Any of us could leave L0pht right now and take six-figure jobs,’ Mudge says. ‘The fact that we don’t and we’re on the ramen-noodle, mac-and-cheese diet, that speaks for our ethics right there. It’s not a job for us; this is what drives us through life.’”<sup>234</sup>

<sup>233</sup> Gottlieb, “HacK, CouNterHaCk.”

<sup>234</sup> Ibid.

A year and half later, the L0pht transitioned to working on those matters as a full-time job when they were acquired by @stake in early January 2000 (whether they continued eating ramen and mac-and-cheese, who knows). Their plan for business, drafted years earlier, clearly panned out—no doubt boosted and enabled by their glorified visit to Capitol Hill.

Once clearly ensconced in the corporate world, did they retain the support of the hacker community at this juncture, as had been their concern? As is to be expected, opinions differ. Some accused the L0pht of being sellouts but, generally, among those working on lists like Bugtraq, this acquisition hardly came as a surprise. It was also applauded by many formerly underground hackers who were themselves seeking and landing employment opportunities.

While the L0pht may have been the most visible as they steered the course of their history, other hackers were also trying to

**235** Brian Fonseca, “Odd Coupling Links Hackers with Security Firm,” *InfoWorld* (archive.org capture), January 7, 2000, <https://web.archive.org/web/20041116162703/http://www.infoworld.com/articles/ic/xml/00/01/07/000107icstake.html>.

**236** See Molotch, *Against Security*, Dyer-Witheford and Matviyenko, *Cyberwar and Revolution*, Masco, *The Theater of Operations*.

**237** Even if professionalization facilitated some forms of diversity, many newcomers to the field still faced rampant discrimination in corporate settings. For example, Katie Moussouris, who sued Microsoft over pay discrimination, continues to lead the fight for addressing this and other inequities plaguing the industry. See: Russell Brandom, “Mind the Gap: After a Bruising Lawsuit with Microsoft, Katie Moussouris Is Fighting for Fair Pay,” *The Verge*, March 16, 2021, <https://www.theverge.com/22331972/pay-equity-now-pledge-katie-moussouris-microsoft-lawsuit>.

**238** Carey and Jin, *Tribe of Hackers*.

**239** By the late 1990s, though less common, some critics still questioned the practice of hiring hackers due to their “ethics.” Emblematic of this attitude is a piece entitled “Hiring Hackers” by Peter Stephenson where he asks: “Hire a hacker? Why not have banks hire bank robbers as guards? Or perhaps we’d hire Jack Kevoorkian to work in the emergency room at the local hospital?” Peter Stephenson, “Hiring Hackers,” *Information Systems Security* 8, no. 2 (June 1, 1999): 10–13, <https://doi.org/10.1201/1086/43305.8.2.19990601/31059.3>, p. 11. A 2002 piece on legal threats facing hackers makes it clear that some companies remained reluctant to admit they hire hackers. Robert Lemos, “The Thin Gray Line,” *CNET*, September 25, 2002, <https://www.cnet.com/news/the-thin-gray-line/>. More so, the term hacker never fully shed its controversial nature, even in the cybersecurity field. See: Leonie Maria Tanczer, “50 Shades of Hacking: How IT and Cybersecurity Industry Actors Perceive Good, Bad, and Former Hackers,” *Contemporary Security Policy* 41, no. 1 (2020): 108–28, <https://doi.org/10.1080/13523260.2019.1669336>.

open up or take advantage of such opportunities. In an article about the acquisition that entertained this very question of legitimacy, airing criticisms of hypocrisy alongside support, Bugtraq’s Elias Levy commented: “I think a lot of people figured that this was going to happen a while ago.” He continued, “Mudge and those guys have a lot to offer. At times it seems they could have been prevented from doing more work because of their interaction with hackers. Having a big company behind them will lend them credibility in some circles [that] they might not have had before.”<sup>235</sup>

## 6.5 < Recuperation or Co-option? >

A couple of things are worth keeping in mind as concluding remarks to this section. At the turn of the century, just when L0pht managed to get acquired by @stake, both the dotcom economic boom and the Y2K crisis were in full swing. And, even though these economic drivers each went bust not long after, the security industry expanded partly due to the events of 9/11. Indeed, those attacks would dramatically accelerate society’s embrace of “securitization” of all sorts, not just of software or the internet, and in both negative and positive ways—as many scholars have documented.<sup>236</sup> Hackers with a history of breaking into systems were well positioned to take advantage of the tremendous financial and government interests in security because they had laid the foundation to do so. Had they not done the work we covered here, it is not clear they would have been treated as legitimate and credible experts at the moment when computer security became so tied to matters of national security. Some were even drawn to work for the government—so often cast as the enemy of the hacker—after the events of 9/11.

Moreover, that opened door likely facilitated the entry into both professional security work and the evolving hacker scene for those hackers who were never quite at home in the 1990s underground. Hackers like Katie Moussouris and Window Snyder found prominent roles institutionalizing hacker processes in corporate and government environments.<sup>237</sup> The institutionalization of hacker conferences like Black Hat and DEF CON meant that security experts who honed their skills outside of the “scene” became participants in what Marcus J. Carey and Jennifer Jin call the “Tribe of Hackers” in their 2019 book surveying members of this new professional community.<sup>238</sup>

Still, even as the 2000s marched on, that vision of the hacker as a morally upright technical citizen was a fragile one, only just starting to take shape, and was always under threat by negative caricatures and legal cases that could be weaponized (and were) against hackers or security research. Indeed, many of the searing debates and controversies we’ve just visited—Should you hire former hackers? Is detailing information about flaws a legitimate method for improving security?—were partially settled, though never closed.<sup>239</sup>

While companies hired hackers (or former hackers), security

firms, and especially vendors, never accepted full disclosure. And just like hackers had done in the late 1990s, various firms, including Microsoft, went on the offensive in the early 2000s, advocating for disclosure mechanisms they framed in moralistic terms as “responsible” disclosure. These were mutual agreements between security researchers and vendors to withhold publication of the flaw for a period of time (if at all) to give the latter time to fix it. As we will detail in subsequent work, that practice became the norm—and those who deviated were frequently cast as “irresponsible” and not only easily demonized, but threatened with legal action.

Indeed, the record here is clear. Vendors have continued to legally threaten security researchers up until the present. The cases, documented in great detail by former members of the underground,<sup>240</sup> showcase the ongoing need for grassroots advocacy and legal allies like the EFF. The Coders’ Rights Project is culled from historical work, but continues to be a living resource. Legal threats are always simmering below the surface ready to boil over and burn those technologists—often hackers, but also academics—who are willing to be adversarial not only by breaking security, but by offering the public all the details.<sup>241</sup>

And so while the LOpht and others did the work of rehabilitation, remodeling, updating, and qualifying around the term “hacker,” they never rid hacking of one of its core linguistic features: moral polyvalence.<sup>242</sup> The term “hacker” is unstable and can be used in ways that seem contradictory. While the LOpht was marketing itself as a cohort of *hackers* that could aid the government (and were convincing on that point), that did not stop US government officials in the 2000s, having whipped up fears of hackers and hacking, from leveraging the “Cyber Pearl Harbor” rhetoric to justify its own particular brand of cybersecurity.

<sup>240</sup> “Legal Threats Against Security Researchers.” (Attrition.org)

<sup>241</sup> See for instance, the case around Russian programmer and security researcher Dmitry Sklyarov. In 2001, he broke and cracked the encryption on the Adobe e-book reader format and presented the details at DEF CON, earning him both accolades from the hacker community and jail time (See Postigo, *The Digital Rights Movement*; Coleman, *Coding Freedom*).

<sup>242</sup> See Tanczer, “50 Shades of Hacking.”

## 7.0 Conclusion: Security by Spectacle and the Limits of Legitimacy

At the dawn of 2000, many security-minded hackers now had the opportunity to enter a growing professional security workforce. Many did. Some went to work for security-focused companies or started their own, others joined technology companies as in-house security staff, and others still began working or consulting for government agencies.

Those opportunities were indebted, in part, to the two processes highlighted in this report. First, was the development of a full-disclosure-oriented trading zone. It was a sociotechnical infrastructure of exchange, where then-marginalized hackers could showcase, develop, and establish expertise; workshop trustworthy protocols for security auditing; and collaborate with a range of other technologists. Second, the slow work of shifting perceptions—among both general audiences and key political and technological stakeholders—that hackers could be part of a project to enhance the technical security of increasingly important computer systems.

In doing so, hackers were foundational to the crystallization of a vision of what “computer security” even meant. Alongside technical processes of vulnerability discovery, system auditing, and security-oriented engineering processes, that vision of computer security involved social mechanisms for information sharing, agenda setting, and policy. Together, those practices informed what is often now known as “cyber security.”

Shifting opportunities aligned with changes in the identity of the hacker figures themselves. As hackers worked with others in public channels, whether on mailing lists or in companies, their motivations for doing security work also changed over the course of the decade. Many hackers came to recognize that the powerful skills they possessed came with a measure of responsibility. One of our interview subjects described the growing possibility of accessing hacker knowledge in the 1990s:

I didn't understand [then] that it was changing me instantly. First by giving me the thing I thought I wanted, which was the techniques and technology for breaking things. But then in a much deeper way, for understanding how vulnerable things are. The wisdom was coming right along with the knowledge.

For many, this wisdom implied a responsibility to address those vulnerabilities: Whether to protect individual users of software like Microsoft Windows, or to support the broader networking



infrastructure increasingly important to society at large. Many felt it was crucial to publicize the insecurity they had come to know so intimately—with the belief that by making such issues visible, in a full-disclosure register, they could inform broad publics and motivate the owners of the technical systems to acknowledge and redress problems.

In this way, we argue the hacker-led advancement of a computer security project entailed what we call “security by spectacle.” In short: security by spectacle is the advancement of security by making both technical instances of insecurity and also negligent practices not only public, but also attentionally unignorable. The cDc’s BO can be seen to epitomize this process, for the way it staged a mediatic encounter between hackers and a powerful corporation, ultimately nominating both technical design decisions and corporate governance questions for public debate. But security by spectacle was also present in the steady release of vulnerabilities and the development of other tools not referenced in this paper: scanners like Security Administrator Tool for Analyzing Networks (SATAN), released in 1995, and Nmap, released in 1997.<sup>243</sup> In many ways, they provided the template for later programs like L0phtCrack and BO. Those efforts were spectacular in the sense that their framing—through provocative names, associations with controversial figures and practices, the use of PR techniques like press releases, and combative dispositions—often made them ripe for uptake in mainstream media and public discourse.<sup>244</sup>

We can also see that the hacker drive to publicize computer vulnerabilities had significant consequences for the broader project of computer security. Perhaps most interestingly, the hacker-led process of disclosure and attention-seeking functions as a case study for a novel mode of what critical security scholars term “securitization.” Securitization is the process by which powerful institutional actors, like the state and massive commercial entities, deem a particular issue to be an extraordinary threat, and thus to warrant extraordinary measures of address through security processes.<sup>245</sup> While governments often engage in securitization in response to events like the 9/11 terrorist attacks, here we can observe that calls for the introduction of security measures often emerged from the bottom up—from figures (hackers) who were often treated in both legal, governmental, and popular discourse as the very agents of insecurity. Thus, we propose that hacker efforts of “security by spectacle” also served as novel instances of “bottom-up securitization.”

Of course, even as hackers played a prominent role in defining the security agenda, computer security practices were influenced by a variety of other factors, many of them originating within established sites of power. By the end of the 1990s, when the L0pht testified to a Senate committee regarding the significance of computer insecurity, bottom-up calls from hackers can be seen to have resonated in perfect harmony with top-down paranoia of an imminent “Cyber Pearl Harbor.” In this way, while it is tempting to cast hackers as the primary

<sup>243</sup> These tools facilitated nascent security auditing practices while simultaneously drawing greater public attention to the issue of computer security. SATAN, developed by Dan Farmer and Wietse Venema, was controversial upon its release and succeeded in drawing some popular attention to issues like full disclosure. Nmap, developed by Gordon Lyon (“Fyodor”), was published as free software in *Phrack*, and quickly became a go-to network scanning tool.

<sup>244</sup> For an account that makes a case for the necessity and vitality of spectacle for political communication, see: Stephen Duncombe, *Dream: Re-Imagining Progressive Politics in an Age of Fantasy* (New Press, 2007).

<sup>245</sup> Buzan, Barry, Ole Wæver, Ole Wæver, and Jaap De Wilde. *Security: A New Framework for Analysis*. Lynne Rienner Publishers, 1998.

agents of change—who recuperated their image in even step as they succeeded in getting powerful actors to take their critique of security seriously—the reality is more complicated. Indeed, the legitimacy-seeking contingent of the hacker scene was perfectly aligned with a burgeoning demand for security expertise and labor to secure technical and financial infrastructure in the interests of national security. **Hacker professionalization occurred precisely as fears of a “Cyber Pearl Harbor” that threatened critical infrastructure came to full prominence.** In other words, what may have begun as a bottom-up process converged neatly with top-down interests by the turn of the millennium.

Whether hackers, then, were involved all along in the admirable work of advocating for security in the name of consumer safety, the distasteful work of “selling out,” or the incidental work of rendering themselves into legible subjects for “co-option,” is a matter of perspective. And certainly, many perspectives exist. And so it happened that even as many hackers were celebrating their recuperation into a mainstream security apparatus, other hackers were mourning the “death of the underground”—and developing strategies to wrest control of technological power out of institutional hands.

Meanwhile, those already employed as computer security experts, including some figures interviewed for this report, began wringing their hands at what they perceived to be hacker snake oil salesmanship, and rallied to police the boundaries of their profession. As one self-identified “security professional,” who was resolutely *not* a hacker, characterized security by spectacle-type initiatives in 1999, “The Congress critters quake, the press salivates, and security professionals think ‘Oh (\*\$^ %\*(#..... here we go again!’”<sup>246</sup> He went on to express resentment that these “hackers” were now getting more business than trusted computer security professionals. “Maybe I’d get more consulting if I adopted a ‘handle’ instead of just being a consultant. To paraphrase some presidential candidate, ‘It’s the HYPE, stupid!’” Before long, the markers of “eliteness” common in the underground were matched by meritocratic markers of employability in the professional space. Some questioned whether hacker skills translated into professional environments.<sup>247</sup> Others acknowledged the skills hacker possessed, but questioned their ethics—laying the groundwork for a move toward certifications,<sup>248</sup> multi-stakeholder disclosure processes, and institutional intermediaries like bug bounty programs.<sup>249</sup>

One final observation bears mention. As hackers contributed to the technical and policy procedures that were increasingly known as “cybersecurity,” both the vision of security on offer and its implementation were relatively narrow in scope. **While social processes like security by spectacle were foundational to the way that hackers drew attention to technological threats, the harms those hackers were concerned about were almost entirely confined to those injuries that could stem from the exploitation of technological vulnerabilities, like data or credential theft.**

<sup>246</sup> Peter Stephjenson, “Hiring Hackers.”

<sup>247</sup> As a former member of the hacking scene who later founded a successful security consultancy told us, “Most of the hackers didn’t know code. They don’t know any code. So if you were going to hire some cool hacker who doesn’t read code to do consulting, they’re going to do black box [penetration testing / auditing without access to source code]. That’s all they can do. And then the thing is, if they can’t talk to a dev[eloper] and tell the dev how to fix it correctly, you lose all credibility.”

<sup>248</sup> Slayton, “The Paradoxical Authority of the Certified Ethical Hacker.”

<sup>249</sup> Even by this time, the trope of undermining hacker legitimation by analogy to other dubious arrangements of trust retained currency. As the same security professional quoted above emphasized: “This is not an argument about hacking skill – it’s about ethics. (...) The real issue is hiring the fox to guard the hen house.” See: Peter Stephjenson, “Hiring Hackers.”

There are a few reasons that might be the case. First, technical issues are often thought of as more tractable than other types of problems. That is to say, a vulnerability in software can be addressed by technologists—but a vulnerability stemming from a misuse of a technology implies other matters: the intended use of the technology, the culture of use that develops around the technology’s social life, the business models that guide technological development, and a vision of what the technology ought to be doing in society. By focusing on narrowly technical issues, higher order social and political implications could be bracketed out. While some of these concerns—such as the relationality between monopolistic business practices and computer security—would emerge as controversial topics in later discussion about computer security (and will be a subject of analysis in our next report), there was a fixation on seemingly apolitical technical matters. That meant security researchers emerging from an anti-establishment subculture could work with new colleagues and frame their professional activity as productive without reference to bigger political questions.

But that also meant that harms produced by other forms of vulnerability—such as harassment, extremist political organizing, child-abuse images, non-consensual pornography, and more—that were equally prevalent, and arguably more destructive in the early days of the internet, did not draw the same level of remedial attention or concern that they may have warranted. For example, in his book *Black Software*, Charlton McIlwain describes how quickly an early Usenet newsgroup devoted to issues of interest to Black users was overrun:

The participants scorched the earth, made it virtually uninhabitable for any black person to survive without their intelligence, morality, political interests, even their very identity being demeaned, called into question, or dismissed. Here these people were building a so-called new society online. They wanted to talk about issues of concern to black people. But almost inevitably they began to regurgitate the stereotypes that had dogged black people since they arrived in America.<sup>250</sup>

McIlwain goes on to detail how Black users and developers innovated a number of ways to mediate those effects—in both technically and socially proficient ways, as through the creation of gated web communities that prefigured the turn to web 2.0. But the issues were never seen as within the scope of computer “security,” nor were they addressed in a substantive global or infrastructural way.

These unaddressed issues, which we could identify as “sociotechnical security” issues, have come to prominent public attention in recent years.<sup>251</sup> And yet, in 2021, they still appear quite stubborn to the types of technical security logics that are at times brought to bear on their redress.<sup>252</sup>

It is possible the vulnerabilities that facilitate those types

<sup>250</sup> Charlton D. McIlwain, *Black Software: The Internet & Racial Justice, from the AfroNet to Black Lives Matter* (New York: Oxford University Press, 2019), page 86.

<sup>251</sup> Law professor Danielle Citron’s work and advocacy has been crucial in transforming perceptions, laws, and policies around harassment online. Her 2014 book helped change the prevailing attitude that little could be done—technically, socially, or legally—around curbing online harassment. Sustained harassment and abuse are now recognized as significant harms that should be remedied through an array of interventions. See Danielle Keats Citron, *Hate Crimes in Cyberspace* (Harvard University Press, 2014).

<sup>252</sup> Matt Goerzen, Elizabeth Anne Watkins, and Gabrielle Lim, “Entanglements and Exploits: Sociotechnical Security as an Analytic Framework,” in *9th {USENIX} Workshop on Free and Open Communications on the Internet*, 2019, <https://www.usenix.org/conference/foci19/presentation/goerzen>.

**253** At times this dismissal of the cultural aspects of hacking was rationalized as a rejection of politicization—an assertion that carries with it the implication that technical engagements are somehow politically neutral, even as decisions about what technologies are engaged with, what constitutes a vulnerability, or who is tasked with addressing a vulnerability thus identified, carry undeniable political consequences.

**254** Nevertheless, it remains vital to recognize the importance of social labor in shaping a security agenda, and the possibility of its use by marginalized figures to shape popular perceptions about what issues should be taken seriously as matters of security. As is frequently observed in Science and Technology Studies discourse, the de-emphasis of social labor and other types of expertise necessary for the production of scientific or “technical” facts has significant implications. Erasing this component can promote technocratic conceptions of governance—and produce paternalistic discourses that radically limit who is recognizable as an expert and prescribe which types of issues and solutions will be entertained and in what mode. The field of Science and Technology Studies (STS) and cognate areas in Anthropology, Sociology, and History have often surfaced invisible or devalued forms of labor and expertise that are central to technological innovation, management, repair, and scientific discovery. Alongside this evergreen and expansive concern, numerous scholars and critics have detailed the harms of technological and scientific paternalism and what Evgeny Morozov has phrased as “technological solutionism,” whereby technical fixes are sought and supported over other organizational, political, or social solutions (Morozov, *To Save Everything, Click Here*. See also: Benjamin, *Race After Technology*; Eubanks, *Automating Inequality*; and Noble, *Algorithms of Oppression*.) For accounts that demonstrate how certain framings or modes of discourse marginalize essential types of perspectives and expertise see Cohn, “Sex and Death in the Rational World of Defense Intellectuals” and Mellström, “Machines and Masculine Subjectivity.”

**255** A subject we will turn to in a follow-up report.

of harms might have been explored more avidly earlier on, if not for the fetishization of a particular type of technical framework. In the hacker community, that prioritization had clear implications. Users who were perceived to be lacking technical expertise were frequently gatekept out of groups and often also maligned. That is to say, they were often derided by more technical participants in IRC chat and zines in a way that structurally normalized their inferiority. Indeed, many of those we interviewed, especially those celebrated for their technical chops, themselves even diminished socially demonstrative acts of security, such as the cDc’s promotion of BO. But perhaps more significantly on that front, some denigrated publications like *2600* and conferences like DEF CON for their sustained focus on cultural and political dynamics of interest to the hacker scene, at a time when other segments of the hacker community increasingly leaned into highly technical discourse.<sup>253</sup>

In that way, the meritocracy, defined solely in terms of technical prowess and achievement, implicit to both the hacker underground and the nascent professional security field, worked wonders for advancing the technical discovery of vulnerabilities and exploits.<sup>254</sup> But it also came at the cost of ignoring or sidelining expertise harbored in other communities, thus precluding attention to other strains of insecurity and risk related to technological use.

Immediately on the heels of the hacker legitimization described in this report, a variety of heterodox visions of security hacking came to prominence. Some envisioned a system in which black hat hackers maintained knowledge of vulnerabilities and exploits among an elite underground cadre of selective peers. Others, operating under the mantle of hacktivism, advocated for the use of hacking skills and techniques in service of human rights, civil liberties, or anti-corporatism. Others still set out to apply proven computer security techniques to areas of civil society underserved by government, military, or private sector security initiatives. As we recognize the importance of computer security practices, and the tremendous work it took to institute them, it is also an occasion to reflect on what issues of security have been left aside, and why.<sup>255</sup>

# Acknowledgments

The authors would like to thank the Data & Society staff members who offered sustained feedback, suggestions, and editorial advice during the development of this report, in particular Patrick Davison and Sareeta Amrute. Special thanks also to danah boyd, who saw the value of this project from the outset and also offered crucial feedback to an early draft of the report. Thanks to Molly Laas for editorial support, and Beth Garrett for help navigating the intricacies of IRB. We gleaned important insights during riffs with the Data & Society DAL initiative team: Charley Johnson, Cristina López G., Will Partin, Emma Margolin, Moira Weigel, Kevin Ackermann, Meredith Clark, Dan Bouk, and danah boyd. Thanks to Chris Redwood and the D&S Communications team for ensuring all the pieces were in place for the design and launch of this report.

Thanks to everyone who read a draft and offered insightful comments: Rebecca Slayton, Benoit Dupont, Walter J. Scheirer, Yuan Stevens, Brian Martin, and Space Rogue. Thanks to Camille François and Josh Kenway from the Algorithmic Justice League, Ryan Ellis, Yuan Stevens, Gabby Lim, and Elizabeth Watkins for vital discussions that shed light on the resonance of this historical material for the contemporary moment. Thank you to all the D&S staff who work to keep the institution functioning at a day-to-day level, and who supported this project in a myriad of ways. Thanks to Janet Haven and Jenna Burrell for crucial last minute guidance. Also, thanks to Brian Stauffer for the cover art and Andrea Carrillo for the layout.

We acknowledge the Ford Foundation, Open Society Foundation, Hewlett Foundation, and the McGill University Wolfe Chair donors for financial support which made this involved research possible. We are grateful for the existence of the Internet Archive's Wayback Machine and Gordon Lyon's seclists.org security mailing list archives; each facilitated access to crucial research material. Thank you to respondents at the 2019 International Communication Association session where some of our core concepts were first workshopped. Thank you to everyone we spoke with at the 2019 edition of The Hacker Conference, and in particular to Frank Heidt for the invite. Finally, thank you to everyone who was open to speak with us and share their stories for hours on end.



# Bibliography

Abene, Mark. *Hack in the Box 2007: Mark Abene Keynote Address (Complete)*, 2012. <https://www.youtube.com/watch?v=bdr0-iF4k6Y>.

Aleph One. "Administrivia (Dec 30)." Seclist.org: Bugtraq mailing list archives, December 30, 1998. <https://seclists.org/bugtraq/1998/Dec/208>.

———. "Administrivia (Jul 05)." Seclist.org: Bugtraq mailing list archives, July 5, 1999. <https://seclists.org/bugtraq/1999/Jul/28>.

———. "Administrivia (Jul 28)." Seclist.org: Bugtraq mailing list archives, July 28, 1998. <https://seclists.org/bugtraq/1998/Jul/297>.

———. "Administrivia (Nov 14)." Seclist.org: Bugtraq mailing list archives, November 14, 1998. <https://seclists.org/bugtraq/1998/Nov/206>.

———. "LOpht Advisory: Release of LOphtCrack for NT." Seclist.org: Bugtraq mailing list archives, April 11, 1997. <https://seclists.org/bugtraq/1997/Apr/27>.

———. "Phrack #49 File 14 of 16: Smashing The Stack For Fun And Profit." *Phrack*, November 8, 1996. <http://phrack.org/issues/49/14.html#article>.

———. "Re: [CVEPRI] Proposal: An Open Letter on Responsible Disclosure." CVE.Mitre.org, September 22, 2000. <https://cve.mitre.org/data/board/archives/2000-09/msg00036.html>.

———. "Re: How to Exploit Mudge by AlephOne by JP AntiOnline." Seclist.org: Bugtraq mailing list archives, April 24, 1998. <https://seclists.org/bugtraq/1998/Apr/158>.

Alexander, Michael. "Group Dupes Security Experts." *Computerworld*, July 29, 1991.

———. "Hackers Promote Better Image." *Computerworld*, June 24, 1991.

Algorithmic Justice League. "Help Prevent, Report, and Redress Algorithmic Harms: Join the CRASH Project." AJL.org, 2020. <https://www.ajl.org/avbp>.

Allison, Jeremy. "Windows NT Password Hash Retrieval." Insecure.org, March 22, 1997. <https://insecure.org/splotts/WinNT.passwordhashes.deobfuscation.html>.

Amrute, Sareeta. *Encoding Race, Encoding Class: Indian IT Workers in Berlin*. Duke University Press, 2016.

Anonymous. "So You Want to Be a Pirate?" In *High Noon on the Electronic Frontier: Conceptual Issues in Cyberspace*, edited by Peter Ludlow, 109–12. MIT Press, 1996.

———. "This Text Was Forwarded to Me..." *The RISKS Digest*, Volume 14 Issue 58, May 7, 1993. <https://catless.ncl.ac.uk/Risks/14/58#subj7>.

Anthes, Gary H. "Safety First." *Computerworld*, June 19, 1995.

"Anti Security: Save a Bug, Save a Life." Internet Archive, March 1, 2001. <https://web.archive.org/web/20010301215117/http://anti.security.is/>.

Assange, Julian, and Suelle Dreyfus. *Underground: Tales of Hacking, Madness and Obsession on the Electronic Frontier*. Edinburgh: Canongate Books, 2012.

Auray, Nicolas, and Danielle Kaminsky. "The Professionalisation Paths of Hackers in IT Security: The Sociology of a Divided Identity" 62 (2007): 1312–26.

F-Secure. "Back Orifice Description | F-Secure Labs," 2019. <https://www.f-secure.com/v-descs/backori.shtml>.

Ballestero, Andrea. *A Future History of Water*. Duke University Press, 2019.

Bartholomew, Brian. "Re: CERT Advisory CA-93:17." Seclist.org: Bugtraq mailing list archives, November 16, 1993. <https://seclists.org/bugtraq/1993/Nov/2>.

Behar, Richard, Amy Cover, and Melanie Warner. "WHO'S READING YOUR E-MAIL? AS THE WORLD GETS NETWORKED, SPIES, ROGUE EMPLOYEES, AND BORED TEENS ARE INVADING COMPANIES' COMPUTERS TO MAKE MISCHIEF, STEAL TRADE SECRETS—EVEN SABOTAGE CAREERS." February 3, 1997. [https://money.cnn.com/magazines/fortune/fortune\\_archive/1997/02/03/221526/index.htm](https://money.cnn.com/magazines/fortune/fortune_archive/1997/02/03/221526/index.htm).

Benjamin, Ruha. *Race After Technology: Abolitionist Tools for the New Jim Code*. Polity, 2019.

Besençon, Sylvain, and David Bozzini. "The Ethnography of a Digital Object." *TSANTSA—Journal of the Swiss Anthropological Association* 25 (2020): 153–60.

Best, Emma. "Behind the Scenes with the Hacktivists Who Took on Microsoft and the FBI." *The Outline*, June 5, 2019. <https://theoutline.com/post/7529/cult-of-the-dead-cow-beto-orourke-hacktivists-bo2k-fbi>.

The New York Times. "BEST SELLERS: February 4, 1990," February 4, 1990. <https://www.nytimes.com/1990/02/04/books/best-sellers-february-4-1990.html>.

BetaFred. "Microsoft Security Bulletin MS98-010 - Critical." Microsoft Documentation, August 4, 1998. <https://docs.microsoft.com/en-us/security-updates/securitybulletins/1998/ms98-010>.

*Beyond HOPE (1997): The LOphT*. Channel2600. Accessed May 26, 2020. <https://www.youtube.com/watch?v=QaAS1l6qigc>.

BO2k. "Back Orifice." BO2k Cyber Security Blog, March 15, 2017. <http://www.bo2k.com/category/back-orifice/>.

Borger, Julian. "Microsoft Hit by Cult of the Dead Cow." *The Guardian*, July 13, 1999, sec. Technology. <https://www.theguardian.com/technology/1999/jul/13/microsoft.business>.

Boyer, Dominic. "Thinking through the Anthropology of Experts." *Anthropology in Action* 15, no. 2 (2008): 38–46.

Brandom, Russell. "Mind the Gap: After a Bruising Lawsuit with Microsoft, Katie Moussouris Is Fighting for Fair Pay." *The Verge*, March 16, 2021. <https://www.theverge.com/22331972/pay-equity-now-pledge-katie-moussouris-microsoft-lawsuit>.

Bratus, Sergey. "What Hackers Learn That the Rest of Us Don't: Notes on Hacker Curriculum." *IEEE Security Privacy* 5, no. 4 (July 2007): 72–75. <https://doi.org/10.1109/MSP.2007.101>.

Bratus, Sergey, Anna Shubina, and Michael E. Locasto. "Teaching the Principles of the Hacker Curriculum to Undergraduates." In *Proceedings of the 41st ACM Technical Symposium on Computer Science Education*, 122–26. SIGCSE'10. Milwaukee, Wisconsin, USA: Association for Computing Machinery, 2010. <https://doi.org/10.1145/1734263.1734303>.

Bridis, Ted. "Hackers Becoming Consultants." *ABC News*. January 6, 2001. <https://abcnews.go.com/Technology/story?id=99325&page=1>.

Buchbinder, Josh. "DEF CON 6 - the Cult of the Dead Cow (CDc) - The Announcement of Back Orifice.M4b." InfoCon Collection: Hacking Conference Archive, August 1, 1998. <https://infocon.org/cons/DEF%20CON/DEF%20CON%206/DEF%20CON%206%20audio/>.

SecurityFocus.com. "BugTraq." Accessed January 25, 2021. <https://www.securityfocus.com/archive/1/description>.

Seclist.org. "Bugtraq: By Date," November 29, 1994. <https://seclists.org/bugtraq/1994/Nov/date.html#136>.

Geek-girl.com (archive.org capture). "Bugtraq Mailing List Archives: 4th Quarter (Oct-Dec) 1993," January 1, 1997. [https://web.archive.org/web/19970101080345/http://geek-girl.com/bugtraq/1993\\_4/](https://web.archive.org/web/19970101080345/http://geek-girl.com/bugtraq/1993_4/).

Buzan, Barry, Ole Wæver, Ole Wæver, and Jaap De Wilde. *Security: A New Framework for Analysis*. Lynne Rienner Publishers, 1998.

Carey, Marcus J. "Black hat and white hat terms have nothing to do with race..." Twitter, June 12, 2020. <https://twitter.com/marcusjcarey/status/1271624977805185024>.

—. "If you think that 'black hat'..." Twitter, July 4, 2020. <https://twitter.com/marcusjcarey/status/1279507103435165696>.

Carey, Marcus J., and Jennifer Jin. *Trope of Hackers: Cybersecurity Advice from the Best Hackers in the World*. John Wiley & Sons, 2019.

CERT Division. "1993 CERT Advisories." Carnegie Mellon University, 2017. <https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=496246>.

Chambers, John T., and John W. Thomson. "Vulnerability Disclosure Framework: Final Report and Recommendations by the Council." National Infrastructure Advisory Council, January 13, 2004. <http://nob.cs.ucdavis.edu/bishop/notes/2004-niacvtf/>

[index.html](#).

Chan, Anita. *Networking Peripheries: Technological Futures and the Myth of Digital Universalism*. MIT Press, 2013.

Chasin, Scott. "MESSAGE FROM MODERATOR - Please Read." Seclist.org: Bugtraq mailing list archives, June 5, 1995. <https://seclists.org/bugtraq/1995/Jun/24>.

Cimpanu, Catalin. "Infosec Community Disagrees with Changing 'black Hat' Term Due to Racial Stereotyping." *ZDNet*. Accessed August 18, 2021. <https://www.zdnet.com/article/infosec-community-disagrees-with-changing-black-hat-term-due-to-racial-stereotyping/>.

CITRIS. *Fireside Chat, Dean Tsu-Jae King Liu and Window Snyder, Square, Inc.*, 2020. <https://www.youtube.com/watch?v=x65Nyy77-Hc>.

Citron, Danielle Keats. *Hate Crimes in Cyberspace*. Harvard University Press, 2014.

Electronic Frontier Foundation. "Coders' Rights Project." Accessed May 26, 2020. <https://www.eff.org/issues/coders>.

Electronic Frontier Foundation. "Coders' Rights Project Vulnerability Reporting FAQ," August 6, 2008. <https://www.eff.org/issues/coders/vulnerability-reporting-faq>.

Cohn, Carol. "Sex and Death in the Rational World of Defense Intellectuals." *Signs* 12, no. 4 (1987): 687-718.

Coleman, Gabriella. *Coding Freedom: The Ethics and Aesthetics of Hacking*. Princeton: Princeton University Press, 2013.

—. *Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous*. Verso books, 2014.

—. "The Public Interest Hack." *Limn*, 2017. <https://limn.it/articles/the-public-interest-hack/>.

"Computer Security in the Federal Government and the Private Sector: Hearings before the Subcommittee on Oversight of Government Management of the Committee on Governmental Affairs." Washington, October 1983. <http://hdl.handle.net/2027/pst.000012047208>.

Computer-underground-digest.org. "Computer Underground Digest Volume 5: Issue 51," July 11, 1993. <http://computer-underground-digest.org/CUDS5/cud551.txt>.

Cooper, Russ. "Announcing the NTBugTraq Mailing List." Seclist.org: Bugtraq mailing list archives, February 1, 1997. <https://seclists.org/bugtraq/1997/Feb/0>.

Cult of the Dead Cow. "Cult of the Dead Cow Responds to Microsoft." [cultdeadcow.com](http://cultdeadcow.com) (archive.org). Accessed August 18, 2021. <https://web.archive.org/web/19990129060839/http://www.cultdeadcow.com/news/rebuttal.txt>.

CULT OF THE DEAD COW. "ST. PAUL, BACK DOOR BOOM, AND ALL THE TEA IN CHINA." [cultdeadcow.bnb.it](http://cultdeadcow.bnb.it). Accessed January 26, 2021. <https://cultdeadcow.bnb.it/news/response.txt>.

Cult of the Dead Cow. "Worst Case Scenario." Internet Archive. Accessed May 26, 2020. [https://web.archive.org/web/19990428131153/http://www.cultdeadcow.com:80/tools/bo\\_press.html](https://web.archive.org/web/19990428131153/http://www.cultdeadcow.com:80/tools/bo_press.html).

[cultdeadcow](http://cultdeadcow.com). *Présentation de BO2K Dans Les Coulisses*. YouTube video, 1999. <https://www.youtube.com/watch?v=oHxNEvklKqE>.

Stanford Law School CENTER FOR INTERNET AND SOCIETY Conference on CyberSecurity, Research, and Disclosure. "CyberSecurity, Research and Disclosure," November 22, 2003. <http://cyberlaw.stanford.edu/security/>.

National Security Archive. "Cybersecurity: When Hackers Went to the Hill - Revisiting the LOpht Hearings of 1998," January 9, 2019. <https://nsarchive.gwu.edu/briefing-book/cyber-vault/2019-01-09/cybersecurity-when-hackers-went-hill-revisiting-l0pht-hearings-1998>.

defcon.org. "DEF CON Conference Transparency Report." Accessed January 25, 2021. <https://www.defcon.org/html/links/dc-transparency.html>.

Denning, Dorothy E. "Concerning Hackers Who Break into Computer Systems." In *Proc. 13th National Computer Security Conference*, 653-64. Washington, D.C., 1990. <http://cpsr.org/prevsite/cpsr/privacy/crime/denning.hackers.html/>.

——. “Concerning Hackers Who Break into Computer Systems.” In *High Noon on the Electronic Frontier: Conceptual Issues in Cyberspace*, edited by Peter Ludlow, 137–64. MIT Press, 1996.

——. “The United States vs. Craig Neidorf: A Debate on Electronic Publishing, Constitutional Rights and Hacking.” *Communications of the ACM* 34, no. 3 (March 1, 1991): 22–43. <https://doi.org/10.1145/102868.102869>.

Dispater. “Phrack #40 File 1 of 14.” *Phrack*, August 1, 1992. <http://www.phrack.org/issues/40/1.html>.

Dr. Mudge. “How to Exploit Mudge by AlephOne by JP AntiOnline.” Seclist.org: Bugtraq mailing list archives, April 24, 1998. <https://seclists.org/bugtraq/1998/Apr/155>.

Driscoll, Kevin. “Demography and Decentralization: Measuring the Bulletin Board Systems of North America.” WiderScreen, June 18, 2020. <http://widerscreen.fi/numerot/2020-2-3/demography-and-decentralization-measuring-the-bulletin-board-systems-of-north-america/>.

——. “Social Media’s Dial-Up Ancestor: The Bulletin Board System.” *IEEE Spectrum*, October 24, 2016. <https://spectrum.ieee.org/tech-history/cyberspace/social-medias-dialup-ancestor-the-bulletin-board-system>.

Dunbar-Hester, Christina. *Hacking Diversity: The Politics of Inclusion in Open Technology Cultures*. Princeton University Press, 2019. <https://press.princeton.edu/books/hardcover/9780691182070/hacking-diversity>.

Duncombe, Stephen. *Dream: Re-Imagining Progressive Politics in an Age of Fantasy*. New Press, 2007.

Dupont, Benoit. “Cybersecurity Futures: How Can We Regulate Emergent Risks?” *Technology Innovation Management Review*, no. July 2013: Cybersecurity (2013): 6–11.

Dyer-Witthford, Nick, and Svitlana Matviyenko. *Cyberwar and Revolution: Digital Subterfuge in Global Capitalism*. U of Minnesota Press, 2019.

Elazari, Amit. “Hacking the Law: Are Bug Bounties a True Safe Harbor?” 2018. <https://www.usenix.org/conference/enigma2018/presentation/elazari>.

Electronic Frontier Foundation. “A ‘Grey Hat’ Guide.” Electronic Frontier Foundation, November 19, 2008. <https://www.eff.org/pages/grey-hat-guide>.

Ellis, David. “After You’ve Beat ‘Em— Join ‘Em.” *Time*, June 24, 1991. <http://content.time.com/time/magazine/article/0,9171,973222,00.html>.

Ellis, Ryan. *Letters, Power Lines, and Other Dangerous Things: The Politics of Infrastructure Security*. Cambridge: The MIT Press, 2020.

Ellis, Ryan, and Yuan Stevens. “Bug Bounties.” Data & Society Research Institute, forthcoming 2021.

Ensmenger, Nathan. *The Computer Boys Take Over: Computers, Programmers, and the Politics of Technical Expertise*. MIT Press, 2010.

Epstein, Steven. *Impure Science: AIDS, Activism, and the Politics of Knowledge*. University of California Press, 1996.

——. “The Construction of Lay Expertise: AIDS Activism and the Forging of Credibility in the Reform of Clinical Trials.” *Science, Technology, & Human Values* 20, no. 4 (1995): 408–37. <https://doi.org/10.1177/016224399502000402>.

Eubanks, Virginia. *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor*. New York, NY: St. Martin’s Press, 2018.

FORMiCA. “How to Exploit AlephOne by JP of AntiOnline.” Seclist.org: Bugtraq mailing list archives, April 24, 1998. <https://seclists.org/bugtraq/1998/Apr/152>.

Fischer, Michael S. “Cracked: WINDOWS.PWL.” Seclist.org: Bugtraq mailing list archives, December 5, 1995. <https://seclists.org/bugtraq/1995/Dec/4>.

Fisher, Dennis. “‘Microsoft Was Freaking Out’: An Oral History of the LØpht, Part 2.” *Decipher*, March 7, 2018. <https://duo.com/decipher/microsoft-was-freaking-out-an-oral-history-of-the-l0pht-part-2>.

——. “Thirty Minutes Or Less: An Oral History of the LØpht, Part Three.” *Decipher*, March 8, 2018. <https://duo.com/decipher/thirty-minutes-or-less-an-oral-history-of-the-l0pht-part-three>.

—. “‘We Got to Be Cool About This’: An Oral History of the L0pht, Part 1.” *Decipher*, March 6, 2018. <https://duo.com/decipher/an-oral-history-of-the-l0pht>.

Fleming, Reid. “CDc Communications Presents: The Journalist’s Cookbook Version 1.0.” Textfiles.com, July 15, 1998. <http://www.textfiles.com/groups/CDC/cDc-0360.html>.

Folch, Christine. *Hydropolitics: The Itaipu Dam, Sovereignty, and the Engineering of Modern South America*. Princeton University Press, 2019.

Fonseca, Brian. “Odd Coupling Links Hackers with Security Firm.” *InfoWorld* (archive.org capture), January 7, 2000. <https://web.archive.org/web/20041116162703/http://www.infoworld.com/articles/ic/xml/00/01/07/000107icstake.html>.

F-Secure. “BO2K Description.” F-Secure Labs. Accessed January 26, 2021. <https://www.f-secure.com/v-descs/bo2k.shtml>.

Seclist.org. “Full Disclosure: An Urgent Warning to All Concerning ~el8 / Project Mayhem (Fwd).” Full Disclosure mailing list archives. Accessed May 27, 2020. <https://seclists.org/fulldisclosure/2002/Aug/368>.

Galison, Peter. *Image and Logic: A Material Culture of Microphysics*. University of Chicago Press, 1997.

—. “Trading Zone: Coordinating Action and Belief (1998 Abridgment).” In *The Science Studies Reader*, edited by Mario Biagioli, 137–60. Routledge, 1999.

Garreau, Joel. “Story about the Treasury Department’s AIS BBS, Whi.” Totse.info. totse.com, June 19, 1993. [https://totseans.com/totse/en/hack/legalities\\_of\\_hacking/aisbbs.html](https://totseans.com/totse/en/hack/legalities_of_hacking/aisbbs.html).

Cult of the Dead Cow Sermons From the Mount: Cult of the Dead Cow Press Releases. “Global Domination Update #20 – June 10th, 1996,” 1996. <http://archive.chibacityblues.org/BCS/cdc/update.html>.

Goerzen, Matt, Elizabeth Anne Watkins, and Gabrielle Lim. “Entanglements and Exploits: Sociotechnical Security as an Analytic Framework.” In *9th {USENIX} Workshop on Free and Open Communications on the Internet*, 2019. <https://www.usenix.org/conference/foci19/presentation/goerzen>.

Goerzen, Matthew. “Critical Trolling.” MA Thesis, McGill University, 2016. <https://escholarship.mcgill.ca/concern/theses/dz010s76k>.

Goode, Sigi, and Sam Cruise. “What Motivates Software Crackers?” *Journal of Business Ethics* 65, no. 2 (2006): 173–201. <https://doi.org/10.1007/s10551-005-4709-9>.

Gorman, Michael E., ed. *Trading Zones and Interactional Expertise: Creating New Kinds of Collaboration. Trading Zones and Interactional Expertise*. MIT Press. Accessed May 13, 2021. <https://mitpress-universitypressscholarship-com.proxy3.library.mcgill.ca/view/10.7551/mitpress/9780262014724.001.0001/upso-9780262014724>.

Gottlieb, Bruce. “HacK, CouNterHaCk.” *The New York Times*, October 3, 1999. <https://archive.nytimes.com/www.nytimes.com/library/magazine/home/19991003mag-hackers.html>.

Granick, Jennifer. “A Review of Several Major Computer Crime Cases from the Past Year or Two.” DEF CON 6 Archive, 1998. <https://www.defcon.org/html/links/dc-archives/dc-6-archive.html#>.

—. “The Law and Hacking.” DEF CON 8, July 2000. <https://www.defcon.org/html/defcon-8/defcon-8-post.html>.

Greenberg, Andy. “Security Isn’t Enough. Silicon Valley Needs ‘Abusability’ Testing.” *Wired*, 2019. <https://www.wired.com/story/abusability-testing-ashkan-soltani/>.

—. *This Machine Kills Secrets: Julian Assange, the Cypherpunks, and Their Fight to Empower Whistleblowers*. New York: Penguin, 2012. <http://search.ebscohost.com/login.aspx?direct=true&scope=site&db=nlebk&db=nlabk&AN=1128584>.

Grimes, Roger A. “Danger: Remote Access Trojans.” Microsoft Documentation, April 24, 2009. [https://docs.microsoft.com/en-us/previous-versions/tn-archive/dd632947\(v=technet.10\)](https://docs.microsoft.com/en-us/previous-versions/tn-archive/dd632947(v=technet.10)).

Hebdige, Dick. *Subculture: The Meaning of Style*. New York: Routledge, 1981.

Hetherington, Gregg. *Guerrilla Auditors: The Politics of Transparency in Neoliberal Paraguay*. Duke University Press, 2011.



Hicks, Mar. *Programmed Inequality: How Britain Discarded Women Technologists and Lost Its Edge in Computing*. MIT Press, 2017.

Ho, Karen. "Disciplining Investment Bankers, Disciplining the Economy: Wall Street's Institutional Culture of Crisis and the Downsizing of 'Corporate America.'" *American Anthropologist* 111, no. 2 (2009): 177–89. <https://doi.org/10.1111/j.1548-1433.2009.01111.x>.

Hobbit. "CIFS: Common Insecurities Fail Scrutiny." Wittys.com, January 1997. <http://www.wittys.com/files/cifs.txt>.

\*Hobbit\*. "Just What Is Full Disclosure...?" Seclists.org: Bugtraq mailing list archives, November 30, 1994. <https://seclists.org/bugtraq/1994/Nov/136>.

Hobbit. *Microsoft LMAthentication, CIFS, and All Kinds of Password Peoblems (Bh-Usa-97-Hobbit-Audio.Rm)*. InfoCon Collection: Hacking Conference Archive, 1997. <https://infocon.org/cons/Black%20Hat/Black%20Hat%20USA/Black%20Hat%20USA%201997/audio/>.

Hopper, Ian, and Richard Stenger. "Large-Scale Phone Invasion Goes Unnoticed by All but FBI." CNN.com, December 14, 1999. <http://archives.cnn.com/1999/TECH/computing/12/14/phone.hacking/index.html>.

Hswe, Patricia, Pamela Lach, Rebecca Sutton Koeser, Caitlin Pollock, Rachel Starry, Lauren Tilton, Amanda Visconti, and Brandon Walsh. "Toward Anti-Racist Technical Terminology." The Association for Computers and the Humanities, n. d. <https://ach.org/toward-anti-racist-technical-terminology/>.

Hull, Matthew S. *Government of Paper: The Materiality of Bureaucracy in Urban Pakistan*. University of California Press, 2012.

Internal Denial of Service Attacks and the Federal Response (2000). [http://commdocs.house.gov/committees/judiciary/hju67303.000/hju67303\\_0.htm](http://commdocs.house.gov/committees/judiciary/hju67303.000/hju67303_0.htm).

Jacquet, Jennifer. *Is Shame Necessary? New Uses for an Old Tool*. Vintage Books, 2016.

jerichoattrition. "That Vulnerability Is 'Theoretical'!" OSVDB (blog), August 13, 2017. <https://vulndb.wordpress.com/2017/08/13/that-vulnerability-is-theoretical/>.

Joe Grand. *LOpht Heavy Industries Video Press Kit (1994-1999)*. From original VHS tape release, 2021. <https://www.youtube.com/watch?v=P5j7chCzzPA>.

Jordan, Tim. *Cyberpower: The Culture and Politics of Cyberspace and the Internet*. London: Routledge, 1999.

Kabay, M. E. "An Interview with Jerry Harding." *Ubiquity* 2004, no. May. Accessed January 26, 2021. <https://ubiquity.acm.org/article.cfm?id=1008529>.

Kaplan, Fred. *Dark Territory: The Secret History of Cyber War*. New York: Simon & Schuster, 2016.

Karger, Paul A., and Roger R. Schell. "Thirty Years Later: Lessons from the Multics Security Evaluation." In *18th Annual Computer Security Applications Conference, 2002. Proceedings.*, 119–26. IEEE, 2002.

Kelty, Christopher. "The Morris Worm." *Limn* Issue 1: Systemic Risk, January 2011. <https://limn.it/articles/the-morris-worm/>.

———. *Two Bits: The Cultural Significance of Free Software*. Durham: Duke University Press, 2008.

Klaus, Christopher. "Full Disclosure Works, Here's Proof." Seclists.org: Bugtraq mailing list archives, December 1, 1994. <https://seclists.org/bugtraq/1994/Dec/1>.

Kuehn, Andreas, and Ryan Ellis. "Bug Bounty Programs: Institutional Variation and the Different Meanings of Security." In *Rewired: Cybersecurity Governance*, edited by Ryan Ellis and Vivek Mohan, 175–94, 2019.

LOpht.com (archive.org capture). "LOpht Heavy Industries: Hot News," April 15, 1997. <https://web.archive.org/web/19970415132515/http://www2.l0pht.com/hotnews.html>.

Lange, Larry. "Enhancements to Windows NT 'hack' Could Cause More Problems." *EE Times (Archive.Org Capture)*, April 1997. <https://web.archive.org/web/19981206114812/http://pubs.cmpnet.com/eet/news/97/948news/enhance.html>.

———. "'Hack' Punches Hole in Microsoft NT Security." *EE Times (Archive.Org Capture)*,

March 31, 1997. <https://web.archive.org/web/19981201072421/http://techweb.cmp.com/eet/news/97/947news/hack.html>.

—. “Hackers Keep the Heat on Windows NT Security.” *EE Times (Archive.Org Capture)*, 1997. <https://web.archive.org/web/19981205132055/http://pubs.cmpnet.com:80/eet/news/97/950news/hackers.html>.

—. “Microsoft Opens Dialogue With NT Hackers.” Blackhat.com, July 15, 1997. <https://www.blackhat.com/media/bh-usa-97/black-hat-eetimes-3.html>.

—. “The Rise of the Underground Engineer.” CMPnet, September 22, 1997. <https://www.blackhat.com/media/bh-usa-97/blackhat-eetimes.html>.

Lapsley, Phil. *Exploding the Phone: The Untold Story of the Teenagers and Outlaws Who Hacked Ma Bell*. New York: Grove Press, 2013.

Lawson, Sean, and Michael K. Middleton. “Cyber Pearl Harbor: Analogy, Fear, and the Framing of Cyber Security Threats in the United States, 1991–2016.” *First Monday*, March 1, 2019. <https://doi.org/10.5210/fm.v24i3.9623>.

Attrition.org. “Legal Threats Against Security Researchers: How Vendors Try to Save Face by Stifling Legitimate Research,” 2008. [http://attrition.org/errata/legal\\_threats/](http://attrition.org/errata/legal_threats/).

Lemos, Robert. “Gates: Security Is Top Priority.” *CNET*, March 2, 2002. <https://www.cnet.com/news/gates-security-is-top-priority/>.

—. “Researcher Attempts to Shed Light on Security Troll.” *SecurityFocus*, October 10, 2006. <https://www.securityfocus.com/news/11419>.

—. “The Thin Gray Line.” *CNET*, September 25, 2002. <https://www.cnet.com/news/the-thin-gray-line/>.

Levy, Steven. *Crypto: How the Code Rebels Beat the Government Saving Privacy in the Digital Age*. New York: Penguin Books, 2002.

—. *Hackers: Heroes of the Computer Revolution*. New York: Delta, 1994.

Leyden, John. “Setback for Security through Obscurity Scheme.” *The Register*, March 19, 2002. [https://www.theregister.co.uk/2002/03/19/setback\\_for\\_security\\_through\\_obscurity/](https://www.theregister.co.uk/2002/03/19/setback_for_security_through_obscurity/).

LHI.com (archive.org capture). “LHI Technologies,” December 19, 1996. <https://web.archive.org/web/19961219062445/http://lhi.com:80/>.

LHI.com (archive.org capture). “LHI Technologies: Tiger Team,” February 21, 1997. <https://web.archive.org/web/19970221194423/http://lhi.com/tiger/>.

Light, Jennifer S. “When Computers Were Women.” *Technology and Culture* 40, no. 3 (1999): 455–83.

Littman, Jonathan. “It Takes a Hacker to Catch a Hacker: Part 2 Beyond the Pranks.” Defcon.org, August 10, 1997. <https://media.defcon.org/DEF%20CON%205/DEF%20CON%205%20articles/DEF%20CON%205%20-%20Johnathan%20Littman%20-%20It%20takes%20a%20hacker%20to%20catch%20a%20hacker%202-4.html>.

Logan, P.Y., and A. Clarkson. “Teaching Students to Hack: Curriculum Issues in Information Security.” In *Proceedings of the 36th SIGCSE Technical Symposium on Computer Science Education*, 37:157–61. 1. New York, USA, 2005.

MalwareTech. “Little Confused by This Whole ‘Black Hat Is Racist’ Argument.” Accessed August 18, 2021. <https://twitter.com/malwaretechblog/status/1279454544422813697>.

Mann, Charles C., and David H. Freedman. *At Large: The Strange Case of the World’s Biggest Internet Invasion*. Simon and Schuster, 1998.

Martinez, Michael J. “Windows Faces Hack Attack.” *abc News (archive.org)*, August 11, 1998. <https://web.archive.org/web/19990507233331/https://abcnews.go.com/sections/tech/DailyNews/backorifice980811.html>.

Masco, Joseph. *The Theater of Operations: National Security Affect from the Cold War to the War on Terror*. United States: Duke University Press, 2014.

Masnick, Mike. “Symantec Buys SecurityFocus/BugTraq.” *Techdirt*, July 17, 2002. <https://www.techdirt.com/articles/20020717/1825218.shtml>.

Matthews, Jeanna Neefe, Graham Northup, Isabella Grasso, Stephen Lorenz,

Marzieh Babaeianjelodar, Hunter Bashaw, Sumona Mondal, Abigail Matthews, Mariama Njie, and Jessica Goldthwaite. "When Trusted Black Boxes Don't Agree: Incentivizing Iterative Improvement and Accountability in Critical Software Systems." In *Proceedings of the AAAI/ACM Conference on AI, Ethics, and Society*, 102–8. AIES'20. New York: Association for Computing Machinery, 2020. <https://doi.org/10.1145/3375627.3375807>.

Maxigas. "Keeping Technological Sovereignty: The Case of Internet Relay Chat." GitBook. Technological Sovereignty, 2018. <https://sobtec.gitbooks.io/sobtec2/en/content/05irc.html>.

Maxigas, and Guillaume Latzko-Toth. "Trusted Commons: Why 'Old' Social Media Matter." *Internet Policy Review* 9, no. 4 (2020). <https://policyreview.info/articles/analysis/trusted-commons-why-old-social-media-matter>.

McIlwain, Charlton D. *Black Software: The Internet & Racial Justice, from the AfroNet to Black Lives Matter*. New York: Oxford University Press, 2019.

McWilliams, Brian. "Hackers Humble Security Experts." *Wired*, January 16, 2003. <https://www.wired.com/2003/01/hackers-humble-security-experts/>.

Mellström, Ulf. "Machines and Masculine Subjectivity: Technology as an Integral Part of Men's Life Experiences." *Men and Masculinities* 6, no. 4 (2004): 368–82.

Menn, Joseph. *All the Rage: The Rise and Fall of Shawn Fanning's Napster*. Crown Publishing Group, 2003.

———. *Cult of the Dead Cow: How the Original Hacking Supergroup Might Just Save the World*. New York: PublicAffairs, 2019.

———. "WhatsApp And Napster Were Spawned From An Elite Security Posse Called 'Woowoo.'" *Business Insider*, March 7, 2014. <https://www.businessinsider.com/r-elite-security-posse-fostered-founders-of-whatsapp-napster-2014-07>.

Merry, Sally Engle. *The Seductions of Quantification: Measuring Human Rights, Gender Violence, and Sex Trafficking*. University of Chicago Press, 2016.

Meyer, Gordon R. "The Social Organization of the Computer Underground - Twentieth Anniversary Edition." Northern Illinois University, 2009. [http://g2meyer.com/cu/The\\_Social\\_Organization\\_of\\_the\\_Computer\\_Underground.html](http://g2meyer.com/cu/The_Social_Organization_of_the_Computer_Underground.html).

MIke. "CERT Advisories Wanted." Seclists.org: Bugtraq mailing list archives, November 17, 1993. <https://seclists.org/bugtraq/1993/Nov/6>.

Molotch, Harvey. *Against Security: How We Go Wrong at Airports, Subways, and Other Sites of Ambiguous Danger - Updated Edition*. Revised edition. Princeton University Press, 2014.

Morgan, Steve. "Cybersecurity Talent Crunch To Create 3.5 Million Unfilled Jobs Globally By 2021." *Cybercrime Magazine* (blog), October 24, 2019. <https://cybersecurityventures.com/jobs/>.

———. "Global Cybersecurity Spending Predicted To Exceed \$1 Trillion From 2017-2021." *Cybercrime Magazine* (blog), June 10, 2019. <https://cybersecurityventures.com/cybersecurity-market-report/>.

Morozov, Evgeny. *To Save Everything, Click Here: The Folly of Technological Solutionism*. New York, NY: PublicAffairs, 2014.

Mudge. *Secure Coding Practices and Source Code Analysis - Black Hat USA 1997 Audio*. InfoCon Collection: Hacking Conference Archive, 1997. <https://infocon.org/cons/Black%20Hat/Black%20Hat%20USA/Black%20Hat%20USA%201997/audio/>.

mudge. "Windows NT Rantings from the L0pht: Who Cares What the Hell Goes into a Gecos Field Anyway!" Bugtraq (Cliplab.org archive), July 24, 1997. <https://cliplab.org/~alopez/bugs/bugtraq2/0162.html>.

Mudge @dotMudge. "The Paper That Moved the Needle..." Twitter. Accessed May 26, 2020. <https://twitter.com/dotmudge/status/1186117644472213505>.

Mullaney, Thomas S., Benjamin Peters, Mar Hicks, and Kavita Philip, eds. *Your Computer Is on Fire*. MIT Press, 2021.

Mundy, Liza. *Code Girls: The Untold Story of the American Women Code Breakers of World War II*. New York: Hachette Books, 2017.

Naraine, Ryan. "Matt Suiche, Comae Technologies." MP3. Security Conversations. Accessed January 25, 2021. <http://securityconversations.fireside.fm/matt-suiche-comae>.

National Infrastructure Advisory Council. "Vulnerability Disclosure Framework: Final Report and Recommendations By The Council," January 13, 2004. <https://www.dhs.gov/xlibrary/assets/vdwdgreport.pdf>.

Nissenbaum, Helen. "Hackers and the Contested Ontology of Cyberspace." *New Media & Society* 6, no. 2 (April 2004): 195–217. <https://doi.org/10.1177/1461444804041445>.

Noble, Safiya Umoja. *Algorithms of Oppression: How Search Engines Reinforce Racism*. New York University Press, 2018.

Seclists.org. "OBSDFtpd Exploit Clarification." Bugtraq mailing list archives. Accessed May 27, 2020. <https://seclists.org/bugtraq/2000/Dec/338>.

odzhan. "How the L0pht (Probably) Optimized Attack against the LanMan Hash." *Modexp* (blog), February 2, 2019. <https://modexp.wordpress.com/2019/02/02/3883/>.

OilPrice.com. "Cybersecurity: The Most Profitable Sector of 2017." *PR Newswire*, July 12, 2017. <https://www.prnewswire.com/news-releases/cybersecurity-the-most-profitable-sector-of-2017-634046713.html>.

"Open Response To Microsoft Security - RE: It's Time to End Information Anarchy," October 17, 2001. <http://lists.jammed.com/vuln-dev/2001/10/0200.html>.

Openbsd.org. "OpenBSD: Security." Accessed January 25, 2021. <https://www.openbsd.org/security.html>.

Oxblood Ruffin. "Blondie Wong And The Hong Kong Blondes: Hacking, Humain Rights, and Hype." *Medium* (archive.org), March 23, 2015. <https://web.archive.org/web/20150830163811/https://medium.com/emerging-networks/blondie-wong-and-the-hong-kong-blondes-9886609dd34b>.

Palmer, C. C. "Ethical Hacking." *IBM Systems Journal* 40, no. 3 (March 1, 2001): 769–80. <https://doi.org/10.1147/sj.403.0769>.

Park, Sunoo, and Kendra Albert. "A Researcher's Guide to Some Legal Risks of Security Research." The Cyberlaw Clinic at Harvard Law School & The Electronic Frontier Foundation, October 2020. [https://clinic.cyber.harvard.edu/files/2020/10/Security\\_Researchers\\_Guide-2.pdf](https://clinic.cyber.harvard.edu/files/2020/10/Security_Researchers_Guide-2.pdf).

Perlroth, Nicole. *This Is How They Tell Me the World Ends: The Cyberweapons Arms Race*. New York: Bloomsbury Publishing, 2021.

Phillips, Whitney. *This Is Why We Can't Have Nice Things: Mapping the Relationship between Online Trolling and Mainstream Culture*. MIT Press, 2015.

Pleon. "Security Design International and Trust Factory Announce Security Vulnerability in Lotus Notes." ResponseSource Press Release Wire, August 2, 2000. <https://pressreleases.responsesource.com/news/8397/security-design-international-and-trust-factory-announce-security-vulnerability-in/>.

Postigo, Hector. *The Digital Rights Movement: The Role of Technology in Subverting Digital Copyright*. Cambridge: The MIT Press, 2012. <https://mitpress.mit.edu/books/digital-rights-movement>.

Poulsen, Kevin. "AtStake Jilts PhiberOptik." *SecurityFocus*, September 1, 2000. <https://www.securityfocus.com/news/79>.

Poulsen, Kevin, and Jennifer Granick. "The Legalities and Practicalities of Searches and Interrogations." DEF CON 7 Archive, July 1999. <https://www.defcon.org/html/links/dc-archives/dc-7-archive.html>.

Powell, Brad. "Re: Wanted: Hackers for Tiger Team (New England Area)." Seclists.org: Bugtraq mailing list archives, October 3, 1994. <https://seclists.org/bugtraq/1994/Oct/35>.

rain forest puppy. "Full Disclosure Policy (RFPolicy) v2.0." Wiretrip.net (archive.org capture), October 17, 2000. <https://web.archive.org/web/20001017192112/http://www.wiretrip.net/rfp/policy.html>.

Ranum, Marcus. "Fear Leads to...the Dark Side." Internet Archive, August 24, 2002. <https://web.archive.org/web/20020824164928/http://www.ranum.com/pubs/dark/index.html>.

Rapoza, Jim. "Security Core: Best Practices." ZDNet, November 24, 2000. <https://www.zdnet.com/article/security-core-best-practices/>.

- Raymond, Eric. "Cracker." *The Jargon File* (version 4.4.7), December 2003. <http://www.catb.org/jargon/html/C/cracker.html>.
- . "How To Become A Hacker." catb.org, 2001. [http://www.catb.org/~esr/faqs/hacker-howto.html#what\\_is](http://www.catb.org/~esr/faqs/hacker-howto.html#what_is).
- Rehn, Alf. "The Politics of Contraband: The Honor Economies of the Warez Scene." *The Journal of Socio-Economics* 33, no. 3 (2004): 359–74.
- Richtel, Matt. "Hacker Group Says Program Can Exploit Microsoft Security Hole." *The New York Times*, August 4, 1998. <https://archive.nytimes.com/www.nytimes.com/library/tech/98/08/cyber/articles/04hacker.html>.
- Richter, Simon. "Announcing New Security Mailing List." Full Disclosure mailing list archives. Seclists.org. Accessed May 27, 2020. <https://seclists.org/fulldisclosure/2002/Jul/7>.
- Riles, Annelise. *Financial Citizenship: Experts, Publics, and the Politics of Central Banking*. Cornell University Press, 2018.
- Rosenbaum, Ron. "Secrets of the Little Blue Box." *Esquire Magazine*, October 1971.
- Rosenblatt, Seth. "Block/Allow: The Changing Face of Hacker Linguistics." *Dark Reading*, July 27, 2020. <https://www.darkreading.com/threat-intelligence/block-allow-the-changing-face-of-hacker-linguistics>.
- Rosencrance, Linda. "Bug Reporting Standard Proposal Pulled from IETF." *IT World Canada*, March 20, 2002. <https://www.itworldcanada.com/article/bug-reporting-standard-proposal-pulled-from-ietf/24144>.
- . "Bug-Reporting Standards Proposed to IETF." Internet Archive. *Computerworld*, February 22, 2002. <https://web.archive.org/web/20030301202821/www.computerworld.com/securitytopics/security/story/0,10801,68558,00.html>.
- Sankin, Aaron. "'The Anarchist Cookbook' and the Rise of DIY Terrorism." *The Daily Dot* (archive.org), March 22, 2015. <https://web.archive.org/web/20170109183816/http://kernelmag.dailydot.com/issue-sections/headline-story/12210/anarchist-cookbook-history-usenet/>.
- Sascha, Segan. "Female of the Species: Hacker Women Are Few But Strong." Internet Archive. abc News. Accessed May 27, 2020. <https://web.archive.org/web/20000815232927/http://www.abcnews.go.com/sections/tech/DailyNews/hackerwomen000602.html>.
- Savage, Annaliza. "Remembering the First DEF CON." ZDNet (defcon.org archive), July 5, 1999. [https://www.defcon.org/html/links/dc\\_press/archives/7/zdnet\\_remembering.htm](https://www.defcon.org/html/links/dc_press/archives/7/zdnet_remembering.htm).
- Schneier, Bruce. "Crypto-Gram." Schneier on Security, August 15, 1999. <https://www.schneier.com/crypto-gram/archives/1999/0815.html>.
- Schorow, Stephanie. "Cutting to the Chase: Hackers Join Forces with Security Firm to Keep the World Safe." *Boston Herald* (archive.org), January 18, 2000. <https://web.archive.org/web/20001018072102/http://www.bostonherald.com/bostonherald/life/net01182000.htm>.
- Segan, Sasha. "Facing a Man's World: Female Hackers Battle Sexism to Get Ahead." abc News (archive.org), June 9, 2001. <https://web.archive.org/web/20010603002603/https://abcnews.go.com/sections/tech/DailyNews/hackerwomen000609.html>.
- Shiple, Peter. "About Pete Shipley." dis.org (archive.org capture), April 20, 2019. <https://web.archive.org/web/20190420173146/http://www.dis.org/shipley/>.
- Shostack, Adam. "Buffer Overflows and History: A Request." Adam Shostack & friends, October 20, 2018. <https://adam.shostack.org/blog/2008/10/buffer-overflows-and-history-a-request/>.
- Slatalla, Michelle, and Joshua Quittner. *Masters of Deception: The Gang That Ruled Cyberspace*. New York: Harper Collins, 1995.
- Slaton, Amy E. "Meritocracy, Technocracy, Democracy: Understandings of Racial and Gender Equity in American Engineering Education." In *International Perspectives on Engineering Education: Engineering Education and Practice in Context, Volume 1*, edited by Steen Hyldgaard Christensen, Christelle Didier, Andrew Jamison, Martin



Meganck, Carl Mitcham, and Byron Newberry, 171–89. *Philosophy of Engineering and Technology*. Cham: Springer International Publishing, 2015. [https://doi.org/10.1007/978-3-319-16169-3\\_8](https://doi.org/10.1007/978-3-319-16169-3_8).

Slayton, Rebecca. "Framing Computer Security, 1967–1992." In *Communities of Computing: Computer Science and Society in the ACM*, edited by Thomas Misa, ACM Press., 282–323. New York, 2016.

———. "The Paradoxical Authority of the Certified Ethical Hacker." *Limn* Issue 8: Hacks, Leaks, and Breaches, February 14, 2017. <https://limn.it/articles/the-paradoxical-authority-of-the-certified-ethical-hacker/>.

———. "What Is a Cyber Warrior? The Emergence of U.S. Military Cyber Expertise, 1967–2018." *Texas National Security Review*, January 11, 2021. <http://dx.doi.org/10.26153/tsw/11705>.

Slayton, Rebecca, and Brian Clarke. "Trusting Infrastructure: The Emergence of Computer Security Incident Response, 1989–2005." *Technology and Culture* 61, no. 1 (2020): 173–206. <https://doi.org/10.1353/tech.2020.0036>.

Smith, George. *The Virus Creation Labs: A Journey into the Underground*. Tucson, Arizona: American Eagle Publications, 1994.

Soltani, Ashkan. "Abusability Testing: Considering the Ways Your Technology Might Be Used for Harm." In *Enigma 2019*, 2019.

Space Rogue. "Hackers Need Not Apply." *SPACE ROGUE: LOpht, Whacked Mac, HNN, CS1* (blog), December 11, 2009. <https://www.spacerogue.net/wordpress/?p=191>.

Spafford, Eugene H. "Are Computer Hacker Break-Ins Ethical?" *Journal of Systems and Software*, Computer Ethics, 17, no. 1 (January 1, 1992): 41–47. [https://doi.org/10.1016/0164-1212\(92\)90079-Y](https://doi.org/10.1016/0164-1212(92)90079-Y).

———. "Are Computer Hacker Break-Ins Ethical? Purdue Technical Report CSD-TR-994." Purdue University, July 1990. [https://www.cerias.purdue.edu/assets/pdf/bibtex\\_archive/90-01.pdf](https://www.cerias.purdue.edu/assets/pdf/bibtex_archive/90-01.pdf).

Spafford, Gene. "Re: [8lgm]-Advisory-14.UNIX.SCO-Prwarn.12-Nov-1994." Seclist.org: Bugtraq mailing list archives, November 29, 1994. <https://seclists.org/bugtraq/1994/Nov/126>.

Steier, Rosalie. "News Track." *Communications of the ACM*, May 1990.

Stephenson, Peter. "Hiring Hackers." *Information Systems Security* 8, no. 2 (June 1, 1999): 10–13. <https://doi.org/10.1201/1086/43305.8.2.19990601/31059.3>.

Sterling, Bruce. *The Hacker Crackdown: Law and Disorder on the Electronic Frontier*. Bantam, 1992.

Stoll, Clifford. *The Cuckoo's Egg: Tracking a Spy through the Maze of Computer Espionage*. New York: Doubleday, 1989.

Straw, Will. "Some Things a Scene Might Be." *Cultural Studies* 29, no. 3 (2015): 476–85. <https://doi.org/10.1080/09502386.2014.937947>.

Subramanian, Ajantha. *The Caste of Merit – Engineering Education in India*. Harvard University Press, 2019.

Sullivan, Bob. "NTBugTraq Goes Corporate." ZDNet, September 20, 2000. <https://www.zdnet.com/article/ntbugtraq-goes-corporate/>.

Tanczer, Leonie Maria. "50 Shades of Hacking: How IT and Cybersecurity Industry Actors Perceive Good, Bad, and Former Hackers." *Contemporary Security Policy* 41, no. 1 (2020): 108–28. <https://doi.org/10.1080/13523260.2019.1669336>.

Taylor, Paul. *Hackers: Crime in the Digital Sublime*. London: Routledge, 1999.

That Whispering Wolf. "Security through Obscurity, Etc." Seclist.org: Bugtraq mailing list archives, November 29, 1994. <https://seclists.org/bugtraq/1994/Nov/127>.

Blackhat.com. "The Black Hat Briefings July 9–10, 1997," July 1997. <https://www.blackhat.com/html/bh-usa-97/info.html>.

Blackhat.com. "The Black Hat Briefings July 9–10, 1997 Speaker List," July 1997. <https://www.blackhat.com/html/bh-usa-97/speakers.html>.

The Deth Vegetable. "RUNNING A MICROSOFT OPERATING SYSTEM ON A NETWORK? OUR CONDOLENCES." *cultdeadcow.com* (archive.org), July 21, 1998.

[https://web.archive.org/web/20000816004036/www.cultdeadcow.com/news/back\\_orifice.txt](https://web.archive.org/web/20000816004036/www.cultdeadcow.com/news/back_orifice.txt).

@stake Events & News (archive.org capture). "The L0pht, Renowned 'hacker Think-Tank,' to Join @stake: Receives \$10 Million in Initial Backing from Battery Ventures," January 6, 2000. [https://web.archive.org/web/20000819004156/http://www.atstake.com/events\\_news/press\\_releases/launch.html](https://web.archive.org/web/20000819004156/http://www.atstake.com/events_news/press_releases/launch.html).

Forbes. "The Lawyer Hackers Call," August 4, 2000. <https://www.forbes.com/2000/08/05/feat.html#273825163211>.

Thomas, Douglas. *Hacker Culture*. Minneapolis: University of Minnesota Press, 2002.

—. "Why Hackers Hate Microsoft." *Online Journal Review*, April 29, 1998. <http://ojr.org/ojr/technology/1017969479.php>.

"UNIX Security Holes Email Thread." Accessed May 26, 2020. <https://groups.google.com/forum/message/raw?msg=comp.security.unix/cSiLUO4Bglg/mg8yp-YbKxcl>.

US Senate. *Computer Security in the Federal Government and the Private Sector: Hearings before the Subcommittee on Oversight of Government Management of the Committee on Governmental Affairs, United States Senate, Ninety-Eighth Congress, First Session*. S. Hrg. ;98-440 iv, 504 p. Washington: US GPO, 1983. <https://hdl.handle.net/2027/pst.000012047208>.

US Senate Governmental Affairs Committee. "Weak Computer Security in the Government: Is the Public at Risk?" US Senate Committee on Homeland Security and Governmental Affairs (archive.org capture), May 19, 1998. [https://web.archive.org/web/20110721062507/http://hsgac.senate.gov/051998\\_summary.htm](https://web.archive.org/web/20110721062507/http://hsgac.senate.gov/051998_summary.htm).

Various. "Phrack #33," September 15, 1991. <http://phrack.org/issues/33/1.html>.

—. "Phrack #64 File 15: International Scenes." *Phrack*, May 27, 2007. <http://phrack.org/archives/issues/64/17.txt>.

—. "The Risks Digest: Volume 2 Issue 50." *The Risks Digest: The Virtual Memorial Garden*, May 8, 1986. <http://catless.ncl.ac.uk/Risks/2/50>.

"Vuln-Dev 2001/10: Open Response To Microsoft Security - RE: It's Time to End Information Anarchy," October 17, 2001. <http://lists.jammed.com/vuln-dev/2001/10/0200.html>.

Wasiak, Patryk. "'Illegal Guys': A History of Digital Subcultures in Europe during the 1980s." *Zeithistorische Forschungen—Studies in Contemporary History* 9, no. 2 (2012): 257–76.

Bugtraq. "Welcome to Bugtraq!," November 8, 1993. <https://groups.google.com/forum/message/raw?msg=comp.security.unix/cSiLUO4Bglg/mg8yp-YbKxcl>.

"Who Is the SDI Group?" Internet Archive. Accessed May 26, 2020. <https://web.archive.org/web/20120921091947/http://www.sdi-group.com/index.php?rop=multi&topic=about>.

Willis, Tim. "Policy and Disclosure: 2021 Edition." *Project Zero* (blog), April 15, 2021. <https://googleprojectzero.blogspot.com/2021/04/policy-and-disclosure-2021-edition.html>.

Wysopal, Chris, and Steve Christey. "Responsible Vulnerability Disclosure Process." IETF.org, February 2002. <https://tools.ietf.org/html/draft-christey-wysopal-vuln-disclosure-00>.

Zatko, Peiter. *Conan O'Brien Jokes about the L0pht Hacker Group*, 2015. <https://www.youtube.com/watch?v=xmSXkA6Xlr4>.

Zetter, Kim. "Three Minutes with Rain Forest Puppy." Internet Archive. *PCWorld*, September 28, 2001. [https://web.archive.org/web/20111205130018/http://www.pcworld.com/article/63944/three\\_minutes\\_with\\_rain\\_forest\\_puppy.html](https://web.archive.org/web/20111205130018/http://www.pcworld.com/article/63944/three_minutes_with_rain_forest_puppy.html).

Data & Society is an independent nonprofit research institute that advances new frames for understanding the implications of data-centric and automated technology. We conduct research and build the field of actors to ensure that knowledge guides debate, decision-making, and technical choices.

[www.datasociety.net](http://www.datasociety.net)

[@datasociety](https://twitter.com/datasociety)

Cover illustration by Brian Stauffer | Graphic design by Andrea Carrillo

January 2022