6

Penetrating: The Desire to Control Media and Minds

> Remember—once you are a social engineer, you deceive, manipulate, and trick people for a living . . . but you also educate them.
>
> —Sharon Conheady[1]

"I just wanna F you up," says hacker social engineer Jayson Street at DEF CON 19. "I just wanna mess you up in the worst possible way. I wanna be the worst thing to ever happen to you at the worst possible time."[2]

Street is presenting his approach to hacker social engineering, specifically what professional hacker social engineers call "penetration testing" or "pentesting" for short. He has stolen purses, phones, documents, laptops, even cars, all while being paid to do so as a professional pentester hired to seek flaws in an organization's security. His talk, titled "Steal Everything, Kill Everyone, Cause Total Financial Ruin" sounds vicious and prurient. But it's in service to a greater goal: Street is hired by corporations to test their security. He's not an underground hacker—he's a professional. Part of the process involves educating the corporations he's "F'ed

up" on their vulnerabilities. After conducting his tests, he produces reports meant to teach lessons about security to the hapless corporate employees who assume they're safe from interpersonal social engineers.

Professional penetration testing of organizations and their information systems has been formally practiced since at least the mid-1960s.[3] It can be done over networks and via software, and much of the early literature on pentesting focuses on seeking out software exploits in computer operating systems.[4] Our interest here is, of course, the social engineering iteration of pentesting—the manipulation of people in order to gain access to a system to "F it up." An early example of hacker social engineering in professional pentesting occurred in 1985, when NASA hired a computer security firm to test the security of the Goddard Space Flight Center. The security firm used a combination of software and social engineering attacks. Like so many others, the security team found that social engineering was an extremely effective method for penetrating security systems.[5]

An entire industry of social engineering penetration testing services is now available for hire. Security consultants like Jayson Street, Sharon Conheady, Jenny Radcliffe, Johnny Long, Chris Hadnagy, and Kevin Mitnick specialize in using social engineering to break into corporate systems and buildings. Corporations that don't want to hire outside consultants may opt to hire their own internal "Red Teams" to run regular pentests.

Like the other hacker social engineering terms that we're exploring in this book, *penetration* has a rich set of connotations, making it a powerful lens through which to look at other forms of social engineering. We'll start, as usual, with an overview of how interpersonal hacker social engineers have used this term, and then turn our attention to how mass social engineers also rely on logics of penetration. We will see penetrating metaphors—specifically, male sexual conquest and bullets—as we trace both interpersonal and

mass social engineering's desire for control through communication. We will consider how social engineering penetration was professionalized, complete with social scientific theories, standardized methodologies, and metrics for gauging success. And we will also see how all social engineers "F us up" not just out of a desire for domination, but also in order to educate the rest of us about the dangers of being penetrated. They penetrate us for our own good.

Interpersonal Penetration Metaphor: Sexual Conquest

The hacker term "penetration testing," writes Hadnagy in *Social Engineering: The Science of Human Hacking*, "opens itself up for a slew of non-humorous sexual innuendos." He goes on to decry pentesters who claim they have "raped" computer servers. "I do not find that statement funny," he says. Admirably, Hadnagy demands that his colleagues never use such language, noting that it will turn many people away from the field.[6]

But the fact is that hacker social engineers have long articulated "penetration" with sexual metaphors—even violent and misogynistic ones—and they will likely continue to do so. We cannot ignore this connotation. Once again, despite some of the crudity of hacker parlance, a term such as "penetration" reveals underlying logics. In this case, penetration as metaphorical sexual domination contains articulations of *technical mastery* and *control*, often presented in a hyper-masculinized manner. The hacker vision of social engineering as the interpersonal manipulation of other people heavily indulges in this articulation of technique, control, and masculinity.

As we have argued, hacker social engineering is the social side of hacking, belying the idea that hackers are antisocial loners sitting in darkened rooms lit only with the glow of computer screens. It also belies the idea that hackers rely exclusively on mastery of electronic computing technology. Instead, social engineering involves

communicating with others. As such, hacker social engineering arguably involves abilities we might call "soft skills" or "people skills." Running the risk of gender essentialism, we may even say such skills are associated with feminized values.[7]

However, despite its possible associations with "soft" or even feminized social skills and its ostensible lack of *techne*, hacker social engineering is often presented as a highly rationalized and technical practice. As feminist scholars of science and technology have shown, values of rationality and technicity are often articulated with masculinity.[8] Such an articulation is very strong in hacking, because "hackers construct a more intensely masculine version of the already existing male bias in the computer sciences."[9] As for interpersonal hacker social engineering specifically, when we consider its underlying theoretical conceptions of sociality and human communication, we get a vision of other humans as knowable, transparent, manipulable objects, just as programmable as an electronic computer. Alongside this, the manipulator of the object—the hacker social engineer—is seen as a mindful, self-controlled, calculating subject. Say the right things at the right time, the hacker social engineer tells us, and you can get your target to do as you wish, a process US Naval Academy professor Joseph Hatfield aptly calls "technocratic dominance."[10] Social engineering thus sees humans as controllable objects, a means to the end of penetrating information systems. Masculinity, control, and social skill are articulated in hacker social engineering.

That this articulation appears under the label "penetration testing"—bringing with it the sexual innuendos Hadnagy decries—is not a historical accident. Interpersonal hacker social engineers have often associated with the hypermasculine world of pickup artistry. Pickup artists train themselves and other men on how to have sex with as many women as possible. As masculinity studies scholars argue, pickup artistry can be understood as "nerd masculine." Nerd masculinity values "rationality and technological

proficiency," keeps women excluded, and draws on the logics of computer games, rule-bound spaces where the player qua avatar can achieve superhuman feats.[11]

As a nerd masculine field, pickup artistry shares affinities with computer hacking. More to the point, it has a shared history. A key example is Lewis De Payne. De Payne is notable for a variety of reasons: under his pseudonym Roscoe, he was the leader of the "Roscoe Gang," a Los Angeles-based group of phone phreaks and hackers that included Kevin Mitnick and Susan "Thunder" Headley, all of whom included social engineering in their toolkits and were written about extensively by journalists in the 1980s and 1990s.[12] But in addition to being a social engineer, De Payne is also notable for founding one of the internet's first pickup artist discussion forums, the Usenet newsgroup alt.seduction.fast, in the mid-1990s.[13] The alt.seduction.fast newsgroup distributed the teachings of Ross Jeffries, one of the founding fathers of the "seduction community" and a proponent of the 1970s-era psychological theory of neurolinguistic programming (NLP).[14] The social engineer De Payne studied with Jeffries and became well versed in Jeffries' techniques of "speed seduction" in his own right in the 1990s.[15] Journalist Jonathan Littman verifies this in *The Fugitive Game*, even joining De Payne one afternoon to study Jeffries's seduction course. "It's the ultimate hack," Littman writes of De Payne's use of speed seduction, "talking women into going to bed with a computer nerd."[16] De Payne not only brought the teachings of Jeffries to the internet; he also authored his own book on seduction via computer Bulletin Board Services (BBSs), titled *Sensual Access: The High Tech Guide to Seducing Women Using Your Home Computer*.[17]

Later, in the early 2010s, the pickup artist/social engineer relationship was further strengthened by a cell phone phreak turned pickup artist Jordan Harbinger. In 2012, Harbinger joined Hadnagy's *Social-Engineer.org Podcast* to provide the perspective of a pickup artist in discussions of social engineering.[18] He was a member of

the podcast for three and a half years. Prior to joining Hadnagy's podcast, Harbinger was the co-host of another podcast, *The Art of Charm*, which had been running since January 2007 and featured episodes such as "No More Mr. Nice Guy," "The Chemistry of Connection," and "What Women Think About Confident Men."[19] He was also the veteran of another podcast, *The Pickup*, and of a dating consultation talk show on Sirius Radio called *Game On*.[20] But like De Payne, Harbinger was not merely a pickup artist; he was also a phone phreak. His childhood hobby was exploring phone networks. He was fascinated by how cellphones worked and wanted to control them. He even posted information about cellphone hacking to the *2600* message board.[21] Thus, like De Payne before him, Harbinger brought knowledge from two domains, pickup artistry and hacking, to the *Social-Engineer.org Podcast*.

Penetration obviously takes on a literal meaning among the sex-obsessed men of pickup artistry. But the most relevant aspect of the pickup artist game is its emphasis on *controlling* others. Pickup artistry objectifies the other—in this case, women—and claims that the woman-object can be manipulated and controlled with the right behavioral stimuli. For a disturbing example, consider pickup artist Derek Rake's "Shogun Method" of "mind control."[22] Rake's goal is "emotionally enslaving" women, and he relies on a range of systematized verbal and nonverbal communicative techniques to do so. Pickup artistry relies heavily on the conceit that other people are programmable "neural machine[s]" who are thus vulnerable to control through interpersonal communication.[23]

Similarly, penetration among social engineers also emphasizes control of an objectified human. Hadnagy's books feature discussions of manipulating people's emotions—getting them to feel sympathy for him, or using fear—to get them to take the actions he wants.[24] In his first book, Hadnagy also endorses neuro-linguistic programming (NLP)—the psychological theory that pickup artist Ross Jeffries adhered to, even though NLP's vision of programmable

humans has been repeatedly debunked.[25] Sharon Conheady's book *Social Engineering in IT Security* is a bit more sophisticated, drawing on social science to analyze authority, reciprocity, and mindlessness as a means to control the people she interacts with.[26]

Of course, a distinction between the all-male pickup artists and social engineers is that the latter field can include more than just men. Susan "Thunder" Headley is perhaps the most notable example, and she saw feminized sexuality as a powerful technique of control. In her DEF CON presentation in 1995, she recommends that women social engineers use the promise of sex to manipulate men.[27] More recently, with the identity-play possibilities of internet communication, social engineers of any gender identity can use this technique of control; a famous example is the Robin Sage experiment, where a fake "hot girl" persona was used to manipulate members of the defense industry.[28] The pickup artist and phone phreak Jordan Harbinger replicated the Robin Sage experiment on his own, using a fake LinkedIn profile based on his "gorgeous [female] assistant" to gather the personal information of people with top security clearances.[29]

Ultimately, success in penetration among interpersonal social engineers is the conquest of systems, such as computers or buildings. Hacker Johnny Long describes his joy when he is able to "have my way" with penetrated computers, downloading files, altering the contents of the server, or deleting it.[30] As for buildings, Jayson Street boasts, the "number 1 fact" is "I'm getting in, ok?" Social engineer Jenny Radcliffe reports she's gotten into "loads" of buildings, "too many to say."[31] Once inside, Street or Radcliffe can "F everything up" and cause the controlled chaos they are paid to create. Thus, the humans they control and manipulate are not the end goal: penetrating the system itself is. Here, too, penetration among interpersonal hacker social engineers echoes penetration among pickup artists: just as pickup artists are discouraged from settling down with just one woman—instead, their goal is to conquer as

many as possible—hacker social engineers do not fixate on any given human.[32] All humans, for them, represent a means to an end: the penetration of the next system.

Professional Penetration

Professional pentesters don't control people and break into systems for free. They're hired to do so, often by corporations or organizations that are concerned about security. As much fun as it is to have their way with a system, it's still a job. Penetration testers work regular business hours to conduct their tests, write up security reports, and present their findings in meetings.[33] It's a far cry from the stereotypical, lulzy hacker underground of Mountain Dew-fueled 3 a.m. hacking, but it can be lucrative: the US Bureau of Labor Statistics reports that median pay for professional pentesters is around $100K.[34]

Pentesting's professionalization is reflected in changes in the hacker terms we've documented in this book. As we have shown, terms like "trashing" have been transformed into the professional-sounding "OSINT" (open-source intelligence). We've also noted that the more common name for hacker social engineering was once "bullshitting," a term now rarely used. Such transformations have been bolstered by formalized education and career titles such as "penetration tester." As of this writing, people interested in social engineering can take courses on the topic, including a master's level course at the University of Arizona, "MIS 566 Penetration Testing: Ethical Hacking and Social Engineering," or a variety of private instruction courses, such as Chris Hadnagy's "2-Day Social Engineering Bootcamp."[35] These courses are more than just learning how to bullshit: they encompass a whole range of theories, methods, and practices in order to produce professional social engineers who can be hired to conduct penetration tests. Expect to

see more such courses, since the Bureau of Labor Statistics predicts a 32 percent growth in the information security sector over the next decade.[36]

The transformation of the crude terms of phreaks and hackers into terms acceptable in college classrooms and corporate boardrooms reflects the transformation of underground, vilified hackers into professional security consultants, enacting a "melodramatic arc" of the "idealized lifecycle of the hacker," where hackers reform, abstain from their previous illegal activities, and contribute to society by selling their skills in the marketplace.[37] Susan "Thunder" Headley is a pioneering example. As part of De Payne's "Roscoe's Gang," she regularly broke into Pacific Bell's systems in the late 1970s and early 1980s.[38] However, she transformed herself into a professional penetration tester, first appearing on ABC's *20/20* in 1982, instructing Geraldo Rivera on the finer points of hacking.[39] She then testified to the US Senate in 1983 and reportedly provided a social engineering penetration test to the US military.[40] After that, she offered her services as a professional pentester through the 1980s and 1990s before shifting careers to politics, poker, and coin collecting.[41]

Headley's transformation prefigured that of Kevin Mitnick, who would replicate Headley's trajectory almost exactly in the 1990s and 2000s. After serving his prison sentence in the 1990s, Mitnick also appeared on national television—in this case, CBS's *60 Minutes*—and also testified to the US Senate.[42] In 2000, he wrote his first book, *The Art of Deception*.[43] All of these achievements were in service to his longer-term goal: to establish a security consultancy. In mid-2002, he established Mitnick Security, offering his services as a social engineer for penetration testing and as an instructor for training courses to help organizations' employees recognize social engineering in action.[44]

While Headley and Mitnick made the leap from underground to professionalized, social engineering-based penetration testing,

neither of them did much to formalize the field and ensure that it could be taught to others. Credit for this should go to Chris Hadnagy and Sharon Conheady. A key development in professional penetration testing is the development of a core literature. Hadnagy has built such a literature through his podcast. From its 2009 launch to the present day, Hadnagy's *Social-Engineer.org* podcast has brought on guests from law enforcement, academia, business, and the hacker underground, all with the same goal: to explore the expansive, multifaceted dimensions of social engineering as a tool for penetrating testing. And every podcast episode ends with Hadnagy posing the same question to the guests: what books do you recommend? Over the subsequent ten years, Hadnagy has collected his guests' recommendations on a blog post.[45] It's a list of more than 150 books.

The books are dominated by social scientific theories drawn predominantly from evolutionary psychology, communication, marketing, and organizational studies. The library collected by Hadnagy includes the work of mass social engineer Edward Bernays (*Propaganda* and *The Engineering of Consent)*. It includes marketing and business staples, like Robert Cialdini's *Influence*, and Dale Carnegie's *How to Win Friends and Influence People*.[46] It includes guides to reading body language and emotions, including the foundational work of Paul Ekman.[47] It also has analyses on building rapport (Robin Dreeke's *It's Not All About "Me"*), thinking (Daniel Kahneman's *Thinking, Fast and Slow*), and mindfulness (multiple books by Ellen Langer).[48] And, of course, it includes a variety of books specifically focusing on social engineering, such as Johnny Long's *No Tech Hacking*, several books by Mitnick, and Hadnagy's own books.[49]

The literature helps professional social engineers understand how social engineering works for penetration testers. Whereas the phone phreaks of years past may have relied on their raw talents as they bullshitted Bell operators, contemporary social engineers have an array of social science concepts to explain how they can control other humans: reciprocity, rapport, mindfulness (and

mindlessness), microexpressions, and framing. With these concepts, social engineers can describe their work in social scientific terms, further bolstering their claims to professional status, raising their esteem among clients, and reinforcing the perception that "the human is the weakest link" in security.

As a result, the professional social engineering penetration testing literature now features a stable methodology, an implementation of these theoretical concepts into practical, reportable, corporation-friendly steps. Perhaps the clearest explication of the hacker social engineering process is in Sharon Conheady's excellent book, *Social Engineering in IT Security*. The core chapters of that book are:

- Chapter 5: "Research and reconnaissance," which includes gathering OSINT, or open-source intelligence, as well as the time-tested phreak technique of trashing;
- Chapter 6: "Creating the scenario," which involves developing the pretext, including dressing the part and developing a backstory;
- Chapter 7: "Executing the social engineering test," which discusses deploying one's pretext through a variety of channels, including email, telephone, and in person; and
- Chapter 8: "Writing the social engineering report," which details how to report one's findings to the company that contracted you to test their security. This is a requirement for any professional pentester.[50]

As should be clear, we have taken these steps as guidelines for constructing our genealogy of social engineering: our chapters on trashing, pretexting, and bullshitting are roughly analogous to the research and reconnaissance, creating a scenario, and executing phases, respectively.

As for the final phase, report writing, that is the moment that penetration—the control of others, the conquest of systems—is

documented. It is the culmination of a professionalized pentest, the product the client paid the professional social engineer for. As Conheady notes, the report is where the "fun" of social engineering penetration testing is transcribed into "boring" detail in presentations and written documents.[51]

But there is another method of professionally presenting results of a pentest, one that's a bit more exciting: speaking at hacker conferences. The talks given at DEF CON by Jayson Street and Susan Headley are two such examples.[52] Unlike the staid corporate report, the presentation of interpersonal hacker social engineering penetration at a conference often recaptures the fun of penetrating. Street's presentation is full of images of "security fails"—computers left unlocked, passwords left on Post-it notes, smartphones left unattended, unsecured doors. Most damning, however, are his videos of the security guards or corporate employees he's able to social engineer, using the practices of his trade to get past them and into sensitive areas.[53] For her part, Headley tells her stories about using seduction techniques to get passwords and about her habit of giving security tips to the very people she's conning. Their audiences of hackers get the vicarious thrill of seeing corporate security penetrated, again and again, while Street and Headley get credit for their abilities to penetrate.

The tension between the staid reporting Conheady details and the more ribald reporting happening at hacker conventions reflects "the tension between the subversive skills of hacking and the standardizing aims of professional certification."[54] Hacker social engineering derives its authority in part from the sort of underground, illicit activities that give it its reputation as a dangerous form of knowledge. Its professionalization is based on it being recognized by corporate and military organizations as a useful set of skills, amenable to formal reports and business hours. It takes a particular type of person—the ethical penetration tester—who can navigate this tension.

Mass Social Engineering Metaphors: Bullets

As our genealogy shows, the interpersonal hacker social engineering processes and concepts we've discussed throughout can illuminate the practices of the older, mass social engineers. Just as we can observe mass social engineering variants of trashing, pretexting, and bullshitting, we can also find precursors to the hacker logic of penetration in mass social engineering.

Like interpersonal hacker social engineering, mass social engineering is ultimately about control of people and systems. But mass social engineers reverse the relationship between people and systems. In interpersonal hacker social engineering, the social engineer penetrates the mind of his or her target as a means to penetrating the telecommunication or computer system. In mass social engineering, the media system is penetrated with the ultimate goal of penetrating the hearts and minds of human audiences. Nonetheless, mass social engineers not only talk of penetrating minds and systems, they also make similar assumptions as hacker social engineers about the nature of communication and its supposed effects.

Mass social engineering penetration is directed at mastering crowds. The idea that communication and media technologies were important to the formation and maintenance of the United States system of governance began with the founding of the country and reflected an emerging consensus among the United States' founders that media technologies, especially the newspaper, were key to turning unruly crowds into informed publics with a shared sense of understanding and opinion.[55] For example, John Adams spoke of the need for communication and transportation technologies—which were largely the same in those days—to bind the new nation together.[56] In 1787, and in response to Shay's Rebellion, Thomas Jefferson wrote that the prevention of such "interpositions of the people" required the newspaper to "penetrate the whole mass of the people" who should, he said, be sufficiently educated to read

and understand them.[57] These themes would become amplified among the mass social engineers of the early twentieth century.

Penetration for crowd mastering takes on a different metaphorical meaning among mass social engineers than the later hackers. Instead of sexual conquest, the metaphor was weapons of war. An early critic of mass social engineering, Ray Stannard Baker, noted in 1906 how public relations operatives working for the railroad industry engaged in a military-style "campaign" complete with precise "shots"—that is, editorial content—fired at small newspapers around the United States.[58] Later, the WWI-era Creel Committee would adopt the bullet metaphor explicitly. American studies scholar Jonathan Auerbach notes that George Creel himself described the committee's messages as "paper bullets" and "shrapnel" in a battle for American "hearts and minds."[59] These bullets were shot through many media, from broadcast systems like newspapers and radio to more modest forms like buttons, corner speeches, and sign-boards. As Auerbach writes, Creel Committee media messages "penetrated virtually every aspect of American life."[60] The "paper bullets" penetration metaphor would go on to be a common one among analysts of wartime propaganda.[61]

These early attempts at mass social engineering were meant to exploit the lessons of Progressive social science, which taught that human behavior was fully knowable and malleable, so long as it could be penetrated with media messages. Edward Bernays, who started his career working for the Creel Committee, repeated the "paper bullet" metaphor in his 1942 analysis of US World War II propaganda.[62] He developed the penetration metaphor further in his 1947 essay on the "engineering of consent." His media effects theory was unambiguous: "communication is the key to engineering consent for social action" precisely because "the ideas conveyed by the words will become part and parcel of the people themselves."[63] The minds of the people, he argued, will be so thoroughly penetrated by the ideas suggested by the mass social engineer that the people will then act on their own accord.

Overall, the mass social engineers Doris Fleichman, Ivy Lee, George Creel, Edward Bernays, and others believed that they could impact individual perceptions and behaviors, and ultimately society through the use of scientific techniques of mass persuasion, and they often spoke of these effects in metaphors invoking the idea of penetration.[64] Just as hacker social engineering would later assume an instrumentalist model of communication in which language is a means of control through the "programming" ("neuro-linguistic" or otherwise) of the target, mass social engineers adhered to what communication theorist James Carey called the "transmission view of communication" and communication historian Christopher Simpson called "communication as domination." This instrumental model has defined US communication studies from the start, including early attempts at mass social engineering. As Simpson explains, this model of communication, which emerged out of WWI propaganda efforts like the Creel Committee and became more formally codified during WWII and the early years of the Cold War,

> concentrated on how modern technology could be used by elites to manage social change, extract political concessions, or win purchasing decisions from targeted audiences. . . . This orientation reduced the extraordinarily complex, inherently communal social process of communication to simple models based on the dynamics of transmission of persuasive—and, in the final analysis, coercive—messages.[65]

This is penetration as crowd control, paper bullets meant to manage the masses.

Media Penetration by the Numbers

Like the later professional hacker social engineers, mass social engineering was done for clients, who demanded documented results. Whether or not the crowd was penetrated by paper bullets required some form of proof. Thus, mass social engineers worked hard to

prove their prowess by reporting on their successes, and the vehicle they chose was basic quantification, most commonly the counting of news stories—clips—mentioning the client.[66] Simply put, their logic was that the deeper their ideas penetrated media systems—the more mentions of their messages across various media—the more likely they had penetrated the minds of their target audiences.

Fleischman and Bernays present their work on behalf of American Tobacco in metrics. In their effort to influence fashion designers to use the color green (and thus make Lucky Strike cigarette packaging fashionable), they created the pretext of a Color Fashion Bureau.[67] Bernays and Fleischman claimed their effort to penetrate the fashion industry to be a success because of a basic metric: inquiries about green made to their pretext, the bureau.

> Just months after opening, the Color Fashion Bureau was besieged with requests for information—from 77 newspapers, 95 magazines, 29 syndicates, 301 department stores, 145 women's clubs, 175 radio stations, 83 manufacturers of furniture and home decorations, 64 interior decorators, 10 costumers, and 49 photographers and illustrators.[68]

We have such precise numbers from Fleischman and Bernays because they saw such metrics as evidence of penetration. Their work is marked by counting media clips: Bernays's *Biography of an Idea* delights in the sheer number of news stories about their efforts, and Fleischman's edited trade magazine *Contact* shared clips with subscribers as evidence of their firm's success.[69]

Metrification bolsters the mass social engineer's claims that penetration of media systems shapes the perceptions of the crowds. Ivy Lee's campaign on behalf of the Rockefellers and the coal industry in the 1910s was "a virtual avalanche of turn-of-the-century political direct mail," with tens of thousands of leaflets and booklets mailed to influential people across the United States.[70] After the avalanche of mail was sent, Lee measured the results of this by doing what we might call sentiment analysis; he hired a clipping service and an

assistant to analyze news editorials, finding more than half the editorials to be favorable to the Rockefellers and the coal companies.

Of course, such crude metrification pales in comparison to the broader quantification of communication and media research that accelerated after World War II. As communication historian Christopher Simpson notes, communication researchers followed the lead of the mass social engineers in order to see mass media as a tool for social management and as a weapon in social conflict. But unlike the clip-counting practices of the mass social engineers, they proposed more complex quantitative approaches—particularly experimental and quasi-experimental effects research, random sampling, opinion surveys, and quantitative content analysis—as a means of narrowly defining communication as social management.[71] By the 1950s, an article in the academic journal *Public Opinion Quarterly* reported that the field was using a range of standardized "effectiveness studies" to gauge how deeply their messages penetrated a media system: clients "may buy a rating service which reports on the size of a television or magazine audience. [They] may study the degree of penetration which [their] message has achieved in various segments of the public. [They] may pretest the readability of [their] advertising copy."[72] Despite the variations in complexity, both the mass social engineers and the later mass communication researchers conceived of penetrating society as a matter of penetrating media systems with their preferred messages. In mass social engineering and its social scientific descendants, penetration is a numbers game. To share results with a client, point to what you can count.

Penetrating Us for Our Own Good?

Whether they seek to penetrate a building's security, a computer system, a market, or a national media system, all professional social

engineers—mass or interpersonal—do their work on behalf of clients. The mass social engineers style themselves as "public relations counsels," penetrating media systems on behalf of corporations wanting to improve sales or stave off regulation, or governments wanting to improve their geopolitical positions. Professionalized pentesters do their work as consultants to or employees of corporations who want to discover possible holes in their security systems. Thus, these social engineers—like many other types of engineers—offer their technocratic talents to those in power. They penetrate us not in service to some larger ideal, but rather to meet the needs of those who pay them.

The people writing the checks out to social engineers have a lot to lose. Governments fear that some opposing political movement or government will undermine their legitimacy. Corporations dependent upon consumption fear that people will stop buying whatever they're selling. Organizations fear that their secrets will be exfiltrated and sold in black markets. Social engineers theorize all of these problems as problems of communication—specifically, problems of instrumental communication, where people are being penetrated by the wrong messages from the wrong people. This appears in their characterization of social engineering as a neutral process, a value-free "tool" that can be picked up by both "bad guys" and "good guys" alike. In fact, the bad guys, they argue, are already doing it—so the good guys simply have to.

As has been shown throughout this book, Bernays, Lee, Fleischman, and other mass social engineers stoked fears that crowds of common people would be controlled by political demagogues who would penetrate the "common man's" mind with media messages. Bernays argued,

> self-seeking men capitalized on the fact that the common man had been swayed . . . by propaganda. This powerful common man could be influenced by symbols, by words, pictures and actions. Appeals could be made to his prejudices, his loves and his hates, to his unfulfilled desires.[73]

And Lee argued,

> The crowd craves leadership. If it does not get intelligent leadership, it is going to take fallacious leadership. We know that the leadership which the mob has often received not only in this country but in other countries, unless corrected, is liable to produce disastrous consequences.[74]

In essence, Lee, Bernays, Fleischman, and other mass social engineers argued that the control and manipulation of crowds was inevitable, and in fact had already happened (predominantly by Germans and Bolsheviks).

In this sense, their observations map onto those of their critics. Critics of the emerging influence industry, including such prominent voices as John Dewey and Walter Lippmann, warned about the "threat of engineered and coercive opinion" and called for reform and revitalization of both the education system and the press.[75] The concerns expressed by Dewey and Lippmann gained increasing traction from the 1930s and into the early years of the Cold War:

> With the rise of totalitarian regimes, propaganda could no longer be innocently taken as a kind of education, shaping and organizing the intelligence of the American public; now, education was enlisted precisely to counter the power of print, radio, and cinema, all perceived as potentially threatening forms of coercion and pacification.[76]

These fears resulted in Congressional hearings and the creation of organizations like the Institute for Propaganda Analysis, both with the goal of studying the impact and spread of Nazi propaganda in the United States, as well as the creation of educational curricula to help inoculate Americans against the effects of such propaganda.[77]

However, for the mass social engineers, the solution against consent engineering was not more education, but more consent engineering. In 1947, Bernays argued that the inadequacies of Americans' education meant that leaders sometimes could not wait for people to become properly educated before making a decision.

With "pressing crises and decisions" at hand, combined with the fact that "the average American adult has only six years of schooling behind him," Bernays said, leaders had the "obligation" to use consent engineering to bring the public along to their way of thinking. Education, while still important, would not be enough on its own. "The engineering of consent will always be needed as an adjunct to, or a partner of, the educational process."[78] Consent engineers presented themselves as the ethical engineers who could translate the needs of the ruling elites and nimbly combat "fallacious leadership" of crowds through the penetration of minds qua media messages. As Lee argued in 1915, if demagogues get to direct the crowd, "why should not the same process be utilized on behalf of constructive undertakings, on behalf of ideas and principles which do not tear down but really build up?"[79] Bernays echoed Lee's argument, stating, "We must recognize the significance of modern communications not only as a highly organized mechanical web but as a potent force for social good or possible evil" and also that consent engineering practices "may be and sometimes are abused. There are demagogues not only in politics but in all branches of endeavor."[80] Evil must be engineered away, instead of ameliorated through education.

Such views persisted into the Cold War as the United States government worried about the potentially subversive effects of Soviet "psychological warfare" against Americans and others. Though, at the same time, the US government developed its own tools and techniques of political and psychological warfare for use against the Soviets, the Eastern Bloc, and third-world countries believed to be uniquely susceptible to malignant Soviet influence.[81] The penetration of Western mass media and education programs into third-world countries was a key metric for judging the success or failure of "development" and "modernization" efforts.[82] Likewise, psychological warfare techniques were seen as valuable tools for countering communist insurgencies in cases where development efforts had

failed. In short, while the United States worried about the effects of propaganda at home, its ultimate position was propaganda for thee, but not for me.

For their part, professional hacker social engineers adhere to similar logics. First, they acknowledge that their brand of interpersonal social engineering is often used for malicious purposes. In his book *Social Engineering: The Science of Human Hacking*, Hadnagy tells us

> I cannot control how you use this information. You can read this book and go out and attack people and steal their information. Or you can read this book and learn how to be a defender for what is right.[83]

And Conheady's book *Social Engineering in IT Security* welcomes us "to the twisted and deceitful world of social engineering where nothing is as it seems. What you are about to read can be used for good or evil."[84]

Indeed, evil uses of hacker social engineering wisdom are, of course, already among us. As Mitnick writes in *The Art of Deception*, we need to understand "how you, your co-workers, and others in your company are being manipulated." In this vision, social engineers are already breaking our security. We need to be taught how to "stop being victims."[85] We need to become social engineers ourselves and fight for "what is right."

To aid in the fight for what is right, contemporary professional social engineers offer their services to educate the rest of us. Hadnagy is particularly keen to suggest education: "My motto," he writes, "is 'security through education.' Being educated is one of the only surefire ways to remain secure against the increasing threats of social engineering and identity theft."[86] After all, "The only true way to reduce the effect of these attacks is to know that they exist, to know how they are done, and to understand the thinking process and mentality of the people who would do such things."[87] Mitnick and Conheady use similar language.

But ultimately, Hadnagy's ideals of education—a democratic vision, redolent of the mid-twentieth-century push to educate people against propaganda—are not quite what gets put into practice. Consider his "Human Hacking Conference," an annual "educational event where you receive expert training on how to hack thoughts, actions, and the people around you. The skills and insights you gain from attending the HHC benefit you both personally and professionally."[88] Rather than train broad sectors of society on how social engineering works, Hadnagy's conference, and the books by professional social engineers, are aimed at reproducing the field of professional social engineering by educating the next generation of pentesters. The newly minted professional social engineers can then carry on the legacy of offering ethical penetrating services to test the security of large organizations, providing reports to those organizations on how to improve their security. Much as the mass social engineers offered their consent engineering approach as an antidote to malicious propaganda, professional social engineers offer their services to combat malicious social engineers.

Conclusion

What American studies scholar Jonathan Auerbach argues of mass social engineering is equally true of interpersonal hacker social engineering: their penetrative powers are "at once part of the problem as well as a potential solution—a way to control and direct an uncertain, disparate citizenry, but also possibly to mobilize and guide it toward a greater common good."[89] The deployment of ethical hacker social engineers is an attempt to "appropriate the technical authority and mystique of hackers . . . without the stigma of the popular association of hackers with criminal activity."[90] If malicious hacker social engineers are controlling your employees in order to gain access to your corporate systems, then the best defense is to

hire someone to hack, pwn, own, and penetrate those same employees. If malicious mass social engineers are hitting the hapless masses with paper bullets, then in this way of thinking, the only viable response to a bad guy with a message gun is to hire a good guy with a message gun loaded with more and better paper bullets.

Thus, what this analysis of penetration teaches us is that those in power are the ones in a position to wield the trashing, pretexting, and bullshitting capabilities of social engineers. Whether social engineering is intended to subdue crowds or control individuals, it is most often in the service of those with the resources to hire social engineers. These are often the selfsame people who distinguish between good social engineering and bad. And thanks to new developments in media systems—specifically, the advent of corporate social media—social engineering is available in a new form: a masspersonal form. We turn to that next.

Social Engineering

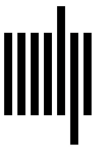
How Crowdmasters, Phreaks, Hackers, and Trolls Created a New Form of Manipulative Communication

By: Robert W. Gehl, Sean T Lawson

Citation:

Social Engineering: How Crowdmasters, Phreaks, Hackers, and Trolls Created a New Form of Manipulative Communication
By: Robert W. Gehl, Sean T Lawson
DOI: 10.7551/mitpress/12984.001.0001
ISBN (electronic): 9780262368926
Publisher: The MIT Press
Published: 2022

The open access edition of this book was made possible by generous funding and support from MIT Press Direct to Open



The MIT Press

The MIT Press would like to thank the anonymous peer reviewers who provided comments on drafts of this book. The generous work of academic experts is essential for establishing the authority and quality of our publications. We acknowledge with gratitude the contributions of these otherwise uncredited readers.

This book was set in ITC Stone Serif Std and ITC Stone Sans Std by New Best-set Typesetters Ltd.

Library of Congress Cataloging-in-Publication Data

Names: Gehl, Robert W., author. | Lawson, Sean T., 1977–author.
Title: Social engineering : how crowdmasters, phreaks, hackers, and trolls created a new form of manipulative communication / Robert W. Gehl and Sean T. Lawson.
Description: Cambridge : The MIT Press, 2022. | Includes bibliographical references and index.
Identifiers: LCCN 2021016750 | ISBN 9780262543453 (paperback)
Subjects: LCSH: Social media—Security measures. | Computer networks—Security measures. | Internet fraud. | Social engineering.
Classification: LCC HM742 .G45 2022 | DDC 364.16/3—dc23
LC record available at https://lccn.loc.gov/2021016750

10 9 8 7 6 5 4 3 2 1