50 shades of hacking: How IT and cybersecurity industry actors perceive good, bad, and former hackers

Author and affiliation

Leonie Maria Tanczer

Department of Science, Technology, Engineering and Public Policy, University College London, UK.

ORCID iD: 0000-0002-2618-6208.

Correspondence details

Leonie Maria Tanczer, Department of Science, Technology, Engineering and Public Policy (STEaPP), University College London, Shropshire House (4th Floor) Capper Street, London, WC1E 6JA, United Kingdom.

Email: l.tanczer@ucl.ac.uk

Abstract

The hacker is the epitome of a cybersecurity threat and the embodied misuse of the Internet. However, in recent years, notions of hacking have begun to change. Blurred boundaries mark the term, best expressed in its overlap with "security researcher." This article draws on a 3.5-year research project on the hacker community and applies an international political sociology framework to uncover routines of rationalization. Interviews with IT and cybersecurity industry experts expose accepted identities, practices, and behaviors of hackers, which allows for the construction of in-group and out-group members in the IT and cybersecurity field. Additionally, the empirical findings are used to propose a conceptual framework (the *Möbius strip*) to situate the moral valence of hackers on a flexible model. Thus, the article provides insight into the ontological and normative complexities that define the study of hackers, as well as the perception of IT and cybersecurity professionals.

***Keywords*:** Hacker, hacking, security researcher, identity, cybersecurity, industry.

Acknowledgements

This research builds on previously published and unpublished scholarship, including a PhD dissertation at Queen's University Belfast (2013-2017), a book chapter (*), and conference presentations at international and national conferences such as the International Studies Association Annual Convention (2015, 2017), the British Studies Association Conference (2015, 2016), the 32nd Chaos Communication Congress in Hamburg (2015), and the Netzpolitischer Abend in Berlin (2015).

(*) Tanczer, L. M. (2017). The Terrorist – Hacker/Hacktivist Distinction: An Investigation of Self-Identified Hackers and Hacktivists. In M. Conway, L. Jarvis, S. Lehane, S. Macdonald, & L. Nouri (Eds.), *Terrorists' Use of the Internet* (pp. 77–92). Amsterdam: IOS Press.

Funding information

This research was supported by funding received from Northern Ireland's Department of Employment and Learning, Queen's University Belfast's School of History, Anthropology, Philosophy and Politics, the Larmor University Scholarship, the Santander Mobility Scholarship, and various academic travel grants received in the course of the author's doctoral studies.

Disclosure Statement

No potential conflict of interest has been reported by the author.

Notes on contributor

Leonie Maria Tanczer is Lecturer in International Security and Emerging Technologies at University College London's Department of Science, Technology, Engineering and Public Policy (STEaPP). She is member of the Advisory Council of the Open Rights Group (ORG), affiliated with UCL's Academic Centre of Excellence in Cyber Security Research (ACE-CSR), and former Fellow at the Alexander von Humboldt Institute for Internet and Society (HIIG) in Berlin. Her research focuses on questions related to Internet security and is inherently interdisciplinary. She is specifically interested in the intersection points of technology, security and gender and thereby draws on different fields, stretching from International Relations, Gender Studies to Computer Science.

On the August 31, 2018, a job advertisement entitled “Become an ethical hacker!”[i] was published in the technology magazine *PC-WELT* by the German *BWI GmbH*, an in-house consulting firm of the German armed forces (PC-WELT, 2018). The advertisement was posted a few days after Germany announced a new agency[ii] to fund innovative research on cybersecurity (Reuters, 2018). The advertisement challenged the costmary idea that hackers were malicious criminals and put forward the concept of “ethical hackers,” differentiating between "good" and "bad" forms of hacking. It further dissected the concepts of “cracking,” which the job ad associated with the “black hat sector” and equated with illegal activities; “hacktivism” which it defined as politically-motivated hacking; and “script kiddies” which according to the publication would be individuals that lacked real technical skill and knowledge. These terms are commonly confused and misinterpreted in cybersecurity debates, which is why *BWI GmbH* probably saw a need to differentiate between them. Through the offered explanation, *BWI GmbH* hoped to recruit interested parties that affiliate with their idea of being a law-abiding and legitimate ethical hacker and would consider applying for such a role in their firm.

The *PC-WELT* advertisement reflects how the definition, ideas, and perception of hacking are multifaceted. One might easily envision a hacker as the stereotypical black-hoodie wearing male, a blend of Elliot Alderson from the TV series *Mr. Robot* and the fading memories of David Lightman from the 1983 film *WarGames* (Shires, in this issue). Others might equate hackers with terrorists, depicting a sensational *Anonymous*-type "keyboard warrior" that creates mayhem from behind a computer screen. Still others might picture a hacker to be Silicon Valley-like entrepreneur who works on a start-up and pitches ideas to potential funders.

The typology of hackers is wide-reaching, especially as the identity of hackers has shifted and changed continuously since the 1980s (Söderberg, 2010). To account for the different shades that characterize this community, this article sets out to examine the blurred boundaries that represent hackers and associated concepts such as hacktivists within the Information Technology (IT) and cybersecurity sector. The article draws on a 3.5-year research project on the hacker community and applies an international political sociology framework to uncover routines of rationalization (Bigo, 2008a). Interviews with IT and cybersecurity industry experts expose accepted identities, practices, and behaviors of hackers, which allows for the construction of in-group and out-group members in the IT and cybersecurity field. The article showcases how IT and cybersecurity professionals perceive hackers in an ambivalent light and in subtle contrast to themselves. It is therefore that interviewees use discursive strategies such as added explanatory adjectives like "former" or "good" hackers to reconcile with the idea that hackers may not always be positively connoted but can, nonetheless, participate in the commercial IT and cybersecurity sector.

Additionally, the empirical findings are used to propose a conceptual framework (the *Möbius strip*) to situate the moral valence of hackers on a flexible model. The strip helps to illustrate the fluidity and flexibility that the term hacker embodies and allows not only to visualize the historically-ambivalent status of hackers but also to situate different hacker categories and definitions on this malleable framework.

The article proceeds as follows: In the next section, the term and concept of hacking is defined in light of the current literature. The examination of the state of the academic debate exposes a gap in the analysis of industry actors' perception of hackers, which sets the scene for the current study. The section immediately following this introduction describes the study's methodology which leads over to the main part of the article. The latter uncovers the shifting identities and three distinct that derived from the qualitative analysis. These include: (a) We employ hackers; (b) We employ "former" hackers; (c) We employ "good" hackers. The empirical results provide the foundation for the introduction of the *Möbius strip*. The conclusion summarizes the main points and highlights how the article adds to the long trajectory of academic scholarship on the hacker community and provides insight into the ontological and normative complexities that define the study of hackers.

The hacker: The epitome of a cybersecurity threat?

The term "hack" emerged in the 1960s from the *Tech Model Railroad Club* at the Massachusetts Institute of Technology. For club members, hacking was used as a broad term to describe any action characterized by a particular innovation, style, and technical virtuosity when solving problems, such as connecting relays or fixing trains and racks (Levy, 1984). The hacker, as a persona, emerged later and amalgamated these ideas of artistry with a predilection for misuse, technological obsession, and resistance (Söderberg, 2010). Nowadays, hacking is seen as an idealized activity, which is not only intended to meet individual ambitions, but also performed to others in the hacker community (Jordan & Taylor, 2004). Scholars frequently relate hacking to craft(y)ness (Coleman, 2016; Steinmetz, 2015) with hackers being often just as much fascinated as they are frustrated by technology (Maxigas, 2017).

The identity of hackers does not exclusively pertain to cybersecurity. For example, the term hacker also describes members of the free and open source software (F\OSS) movement (Coleman, 2013b; Kelty, 2008). As such, the definition of hacking has broadened to represent a multitude of identities and activities situated in and around computing, as well as a variety of practices involving legal and illegal acts. In the context of information security, these acts span from tactics such as learning, tinkering, testing, breaking, phreaking[iii], pirating, exposing, leaking[iv], whistleblowing[v], to doxing[vi]. Hackers' behavior is

characterized by anti-establishment views and subversion (Gröndahl, 2000) and a commitment to engage in a "critique through making" (Kelty, 2018, p. 291). These features are particularly well expressed by groups such as *Hacktivsmo*, the *Electronic Disturbance Theater*, or *Telecomix* that use hacking to address issues such as online censorship (Tanczer, 2015).

Hacking is part of a larger discourse on and practices around the security of technology, because of hackers' tendency to identify, uncover, and exploit security flaws. Their portrayal became concurrent with the criminalization of computer crime (e.g., U.S. *Computer Fraud and Abuse Act* passed in 1986 and UK *Computer Misuse Act* in 1990). Cases such as the 1984 *BTX Hack* by the German *Chaos Computer Club* (CCC), computer break-ins by Milwaukee teenagers *The 414s* (Vollmann, 2015) or the decentralized *Anonymous* movement (Coleman, 2014) further solidified the image of the hacker. Up to this point, "hackers induce hysteria" with the U.S. defense lawyer Tor Ekeland (2017) arguing that they represent "the unknown, the terrifying, the enigma."

However, hackers are as much as a figure of destruction as of hope (Kelty, 2018). Hackers play an important role in countering surveillance and groups such as the *CCC* analyze existing technologies such as voting machines to point out fundamental privacy and security risks (Kubitschko, 2015). Hackers also built alternative infrastructures, such as the anonymous communication network *TOR*, and articulate technical information to a wide range of audiences. Most profoundly, hackers also need to hold regular jobs. In the context of their employment, they may draw on their technical expertise learned through hacking (Wark, 2004).

The U.S. national security community has embraced the expertise of hackers for a long time. For instance, in 1998 the hacking collective *L0pht* provided a congressional testimony on the state of computer security (McGraw, 2016). Since then, many of its members, including Chris Wysopal aka "Weld Pond," Peiter Zatko aka "Mudge," and Cris Thomas aka "Space Rogue" have gone on to prestigious careers in the U.S. government and the cybersecurity sector (Fitzgerald, 2007). In 2010, the keynote at *DEFCON*, the world's largest hacker conference, was presented by acting director of the National Security Agency (NSA), General Keith Alexander. In the keynote, Alexander courted the hackers in attendance, encouraging them to consider employment at the NSA by drawing parallels between the hacker community and the national security sector.

As Irani (2015, p. 801) observed, the term hacker has become associated with a kind of "entrepreneurial citizenship," with hackathons[vii] now hosted by a broad range of public and private actors. Outside the United States, similar attitudes have been documented by hardware hacker Andrew "bunnie" Huang (2017), who studied the markets and factories that produce innovative computing hardware in China. Practices such as bug bounty programs,

capture the flag competitions, and device jailbreaking demonstrated the variety of ways in which hacking has become associated with the mode of production, and is embraced by employers and the public.

There is long-standing scholarly interest in the contradictory portrayal of hackers as both *exploiters* and *solvers* of security issues. "Hackademia" research has explored the sociology of hackers (Jordan & Taylor, 1998), their cultural practices and social organization (Coleman, 2013a; Décary-Hétu & Dupont, 2012; Meyer, 1989) as well as their depiction in the literature, media, and film (Alper, 2014; Klein, 2015; Leonard, 2014; Stańczyk, 2017). Most recently, this body of work was given prominence in a special issue of *Limn* (Kelty & Coleman, 2017).

Overall, hackers received far more academic scrutiny than many other technical communities (Bialski, 2017). However, there is limited attention to how they are perceived, both within and in relation to the IT and cybersecurity sector. The commercial IT and cybersecurity sector plays an important role in the security of the Internet and technical systems more broadly. The sector's significance is also reflected in its market share, which is estimated to grow by 8% per year to reach $143 billion by 2022 (Millman, 2018). Additionally, corporate actors such as IT and cybersecurity professionals profit from their "expert" status. Due to their authority, professionals can claim to provide explanations and solutions to perils but are also detrimental in the framing of risks (Kessler & Werner, 2013; Quigley, Burns, & Stallard, 2015).

In this context, IT and cybersecurity companies and consultancies stand to benefit not only from the expansion of technical systems across many aspects of everyday life but also from a reciprocal depiction of and engagement with hackers. On the one hand, stereotypical illustrations of hackers in balaclavas make for sensational imageries and icons in briefings and reports. Besides, cybersecurity statistics sound even more alarming when one is able to refer to nebulous personas such as hacktivists. The alleged dichotomy and binary opposition of hackers *versus* IT and cybersecurity professionals, thus, gives clarity about who is doing "good" and who is acting "bad" and what is considered "secure" or "insecure." On the other hand, the hacker has become one of the most desirable terms within the IT and cybersecurity industry. For example, *Facebook* (2012) define their culture and management approach, in which they embrace technological idealism, as "The Hacker Way." Similarly, *HackerOne* (2016), a vulnerability and bug bounty platform, base their business model on that of a purposeful hacker association.

Grounded in this ambivalent relationship between hackers and IT and cybersecurity actors, this article examines how IT and cybersecurity professionals perceive hackers in relation to themselves. The article applies an international political sociology framework (Bigo, 2008a) and draws on Bourdieu's (1985) notion of "the field." The latter is considered

as an autonomous social space with corresponding institutions, powers, and forces (Grenfell, 2014; Leander, 2011). The field analogy is used to distinguish a "field of hackers" from a "field of professionals." The article uses this separation to examine how hackers fit into private actors' routines and conceptualizes how these two fields coexist. Interviews with IT and cybersecurity industry experts expose accepted identities, practices, and behaviors of hackers, which allows for the construction of in-group and out-group members in the IT and cybersecurity field. A later part of the article draws on the empirical findings to propose a conceptual framework. The framework provides insight into the operationalization of hacking as a concept, and further offers a novel contribution for situate the moral valence of hackers within a flexible model.

Method

The analysis is based on interview data collected in 2015, drawing from a self-selected sample of 11 representatives of the IT and cybersecurity sector. The researcher enlisted participants through a variety of ways, including recruitment emails sent to a range of known organizations and industry actors; and conference participation such as the invite-only *Berliner Forum zur Cyber-Sicherheit*. The single inclusion criteria for the participation in this study was that participants were actively engaged in or somehow related to the IT or cybersecurity sector. All participants were male. The researcher had no personal connection to any of the participants before the interview.

The semi-structured, nonrecurring interview outline comprised seven open questions with prompts to examine industry representatives' perceptions of hacking and hacktivism. On average, interviews lasted approximately 45 minutes and were conducted in German (9) and English (2). Interviews were audio-recorded and thereafter transcribed and anonymized. Moreover, six of the participants operated in an industry sector that was mainly based in and focused on Germany, while five were tied to corporations that acted on an international level with offices spread across the globe.

Following the guidelines set out by Braun and Clarke (Thomson, 2014), thematic analysis was used to analyze the interview transcripts. An inductive approach for identifying themes was applied, which examined content on a semantic and interpretative level. Data was assessed in its native tongue with cited quotes translated into English. Participants are referred to as PM plus identifying number (e.g., PM1) while the researcher who conducted all interviews is referred to as L. The symbol (…) is used to identify negligible sections of the interview, "…" signifies short pauses, while the symbol [X] is used to hide words or phrases that could lead to the identification of participants.

Shifting hacker identities

This section explores the perceptions of hackers by the field of IT and cybersecurity professionals. It puts a specific focus on the identities, practices, and behaviors that would distinguish IT and cybersecurity actors from the hacker community. Using interview data, the analysis identified three interrelated themes that characterize professionals' ambivalent understanding, which in turn underpins the expressed flexibility of the hacker concept. These themes include: (a) We employ hackers; (b) We employ "former" hackers; (c) We employ "good" hackers. Across these themes, interviewees acknowledge that while hackers are not always positively connoted, they can participate in the commercial IT and cybersecurity sector. Most profoundly, the analysis reveals the appropriation of hacking that impacts on the identity construction of the IT and cybersecurity field. While these three themes are not clear-cut, they show the evident differences in accepted practices, and behaviors, and there is value recognizing these. The themes reveal the shifting identities that dominate concepts such as hackers to date.

We employ hackers

Parts of the discussions within the IT and cybersecurity sector involve the idea that the field of professionals employs hackers. Both businesses and independent consultants instrumentalize hackers' skills for commercial purposes. In this regard, the field of professionals is not only about selling services, but also about purchasing hacking expertise. Jarvis, Macdonald, and Nouri (2014, p. 79) inquired about this dynamic in their survey of academic researchers on the threat posed by cyberterrorism. Three percent of the 118 respondents indicated that one of the "most effective countermeasures" against cyberterrorism would be to hire hackers. In Jarvis, Macdonald, and Nouris' (2014) study as much as this theme, hacking is not purely seen as a malicious activity one must defend against, but also a skill that one can obtain. Hence, hacking becomes a service rather than a risk, and hackers become a valuable resource rather than a threat.

This viewpoint is evident across the interviews, where participants highlight that "hacking is part of our process to make a product and to review it ourselves" (PME). It allows for the identification of "weak spots" (PMB) and stands in contrast to the testing of systems in "conventional way[s]" (PME) which would not encompass the same level of innovation and technical sophistication as standardized penetration tests. Hacking permits seeing things that an "enterprise in the course of quality tests would simply not detect on their own" (PMB). Hackers are considered to understand technologies far better than other actors and are familiar with attack scenarios. As one participant said "[i]f I do not understand

how hacking is executed and how systems are attacked, then you will have difficulties to protect yourself appropriately" (PMG). Hackers' situatedness and knowledge on "how attackers proceed" (PMG) allows for the protection of systems. Hacking and the field of hackers are therefore a resource that industry representatives are keen to use for their advantage, as is evident in the following extracts.

Extract 1

PME: I think hacking should generally be used more to our advantage. For instance, by involving it in the course of the product development. But I think that many already do that – they let the penetration testing be done by hackers [laughing]. Ahm... I think that the hacker is not always the enemy. Otherwise I would put our own employees under general suspicion.

Extract 2

PMB: [laughing]. Ahm... well, so I... in the meantime there's already a lot of companies that say on their own accord "we employ hackers," right. Or they say "our security is tested by hackers" or something like that. That's... because even manufacturers are very open about that. This is... so there's already a strong convergence taking place.

These two quotes not only emphasize the helpful element of hacking, but also indicate that hackers are actually *part of* the IT and cybersecurity sector. PMD accentuated this by saying "I would also include all of those people [hackers] into the [cybersecurity] community" (PMD). Indeed, the value of hackers to commercial businesses was recognized as early as 1981. In a *New York Times* article on a security breach of one of America's largest timesharing company, the journalist McLellan (1981) identified the positive benefits of hackers' technical expertise and argued that "[d]espite their seemingly subversive role, hackers are a recognized asset in the computer industry, often highly prized."

The field of hackers is in this first theme closely related to notion of penetration testers or security researcher. Both engage in activities such as security assessments to identify the scale to which organizations are vulnerable to software flaws or attack scenarios such as social engineering and phishing (Watkins, 2018). As tech companies have a vested interest in producing secure products, they increasingly rely on both internal and external audits (i.e., bug bounties) which may involve hackers and should ultimately ensure that systems are not prone to failures or security flaws.

We employ "former" hackers

Along the lines of the theme discussed above, some participants show reluctance to fully embrace the idea that hackers are working within the commercial IT and cybersecurity sector. Interviewees might acknowledge the value of hackers' technical skill sets, but want to distinguish between hackers and no longer "active hackers" (PMK). References relating to the idea of "former" hackers, indicate that the field of professionals is creating distinct boundaries. The field of IT and cybersecurity professionals is seeking to articulate their identity against a constitutive other. For example, one participant very strongly rejected the idea that he would work "with hackers" (PMJ). He insists that the kind of hackers his company would employ are no longer engaged within the hacker community, as evidenced in the following passage.

Extract 3

L:	But you have just said that you are working with hackers.
PMJ:	I did not say that we are working with hackers – you interpret this slightly wrong. – I said that if you are looking for a very, very good security specialists today, then in most cases these are hackers. However, these are then no longer active hackers. This is a small but mighty difference.

This notion of inactivity fosters a sentiment of hackers' alleged domestication. As if parts of the hacker community have been made compliant, and given up their hacker existence for "six-figure salaries, luxurious suites in Las Vegas" and "business class traveling" (Guarnieri, 2017). For instance, Kevin Mitnick was arrested in 1995 for computer and wire fraud and served five years in prison. He is now famous for running his own security consultancy, *Mitnick Security*, and is the personification of a 'reformed' hacker. Such transformations have been criticized by parts of the hacker scene. For example, security researcher Claudio Guarnieri (2017) is concerned by the shift that the hacker slash security research community is experiencing and the moral failures that this drive for hackers' commercialization is creating.

Extract 3 also points the problematic relationship that marks the field of IT and cybersecurity professionals from the field of hackers. For some participants, it makes a "small but mighty difference" (PMJ) to differentiate between "current" and "former" hackers. The argument also aligns with those participants who completely resisted the idea that hackers would work in the commercial IT and cybersecurity field. As interviewee PMK

said, “I wouldn’t necessarily say hackers” (PMK) to describe IT and cybersecurity professionals. The interviewee sees standards involved in the field of professionals that would not apply to the larger hacking community.

The dynamic to distinguish between *accepted insiders* and *rejected outsiders*, resembles views about “strangers” discussed by Bauman (1990, p. 146). He highlights how strangers, as a category of actors, embody uncertainty. Strangers, akin to hackers, are undecidable. It is unclear whether they are working *for* or *against* the field of professionals and how they relate to one’s own identity, behavior, and practices. This ambiguity makes hackers uncomfortable and to carriers of a sense of danger. In comparison, static classifications such as “enemy” and “friend” give certainty about the relational association and position to oneself. Bauman (1990, p. 146) pointedly notes that “underdetermination is their [i.e., strangers] potency: because they are nothing, they may be all.” Thus, the opposition that is being created by talking about “no longer active hackers” (PMJ) enables the field of professionals to uphold knowledge and action. It eliminates the inherent ambivalence and fluidity that hackers embody and moves beyond the paralysis that the vagueness of the term creates. This intrinsic ambiguity makes both strangers, as much as hackers, expose the “fragility” of deliberate separations that the field of professionals in all interviews tries to construct (Bauman, 1990, p. 146).

The need to differentiate between hackers and no longer “active hackers” (PMK) further emphasizes how the hacker identity continues to conveys negative connotations. In this second theme, the field of professionals is primarily perceived as the “good side” (PMC, PMJ) and the counterpart of a profoundly amorphous and possible hostile group. The theme echoes findings by Johnston (2009) who studied the antivirus industry, and the ways that employees both stigmatize and depend on malware writers and hackers. Antivirus professionals would consider themselves as law-abiding “white hats” who work to ensure the security of computational and especially corporate systems. Their professional identities and logics are in constant tension with the opposing *other*. This makes virus writers as much as hackers to a reverse image of the IT and cybersecurity professionals and helps the construction of hackers as bogeymen one needs to act upon.

Similarly, IT consultant Peter Stephenson (1999, p. 13) wrote a critical piece in the *Information Systems Security* journal against the idea that hackers are nor should be working for corporations. He argues: “Hire a hacker? Why not have banks hire bank robbers as guards?” Stephenson (1999, p. 13) lacks trust in hackers ability to change. For hiring purposes, he would rather “consider [employing] a security professional with hacking skills” and does not treat felony convictions as any legitimate qualification for the job.

Corporate actors’ unwillingness to employ and work with ‘active’ hackers further compares to Backmann’s (2017) analysis of industry-financed computer engineers and

Bialski's (2017) observation of corporate software developers. Both groups would avoid association with the hacker label. For example, during Bialski's (2017) engagements with developers, her interviewees would negate the idea that they hacked. For participants, the term encompassed associations with anarchist activism and the direct work with security systems. Yet, while Bialski's (2017) research subjects carried out actions that resembled those commonly attributed to the field of hackers, including experimentation, political gestures, and craftiness, they did not feel comfortable being affiliated with the hacker community (Bialski, 2017).

Such attitudes, together with interviews analyzed in this article, exemplify how the field of professionals carefully delineates their "field of security" from an alleged criminal field of hackers. While such viewpoints are increasingly being challenges by initiatives such as UK's National Crime Agency's cybercrime intervention workshops that aim to reform teenage hackers (Collins, 2018), the interviewees devise different moral grounds upon which professionals and hackers operate. In turn, the generated moral valence influences the status and power relations between the two social spaces. These power relations shape the discourse of accepted identifies, behaviors, and practices and helps the construction of in-group and out-group members in the IT and cybersecurity field.

We employ "good" hackers

A third and final theme creates a distinction between allegedly "good" and "bad" hackers akin to "former" and "current" hackers explored above (Extract 3). This theme translates into the categorization of "beneficial versus malicious" hacking. These alleged "good" hackers are often referred to as "security specialist[s]" (PMJ). Such specialists "know what's going on… and therefore they ultimately know how to secure these things [technical systems]" (PMJ). "Good" hackers' knowledge makes them valuable experts, with participants accepting that these are "hacker[s] – in the positive sense" (PMG).

Extract 4

PMC: (...) the colleague here [X] – ahm with whom we also, who still has contacts [with the hacker community] and who also said "I can make this [the contacts, hacking] available to you and I can offer you this service". Hacker – really good people – for the good side.

Extract 4 directs the attention to ideas around professional solidarities and moral valence (Bigo, 2013). Hackers would be legitimate as long as they operate alongside the

field of professional's interests and behaviors, and resist the possibility of working against the IT and cybersecurity field. Having hackers act for one's cause not only correlates with professional's concern to secure technical systems, but also with the ability to secure the "financial assets" of the IT and cybersecurity sector (PMC). Such a commercialization of hacking points to the importance of economic capital for businesses and the cooption of hacking into corporate and institutional territories, seen in Extract 5.

Extract 5

L:	Just briefly, because you said "the good hackers" – this means that you do see a difference there?
PMC:	Yes.
L:	Where lays the difference? What is a good hacker?
PMC:	Quite egoistically argued, it is of course someone ah who protects my clients and [X] and does not attack us. Someone who contributes, who wants to contribute to protect ahm... financial assets. – We are now talking about capital, of [X]. – It is vital to protect this and whoever hacker proposes to be on this side and wants to make an active contribution, that would be a good hacker for me.

Such references make hackers part of the entrepreneurial thinking of the field of professionals. This perspective echoes Delfanti and Söderberg (2018), who highlight how hacker practices such as the usage of platforms for distributed production and sharing are adopted, adapted, and repurposed by corporate and political actors. Similarly, ideas of hackerspaces and hackathons and other hacker-associated innovations are harnessed by firms as long as they align with the routines and demands of the field of professionals (Irani, 2019; Söderberg & Delfanti, 2015)

In order to allow for the unambiguous use of the term hacking, some participants prefer to refer to malicious hackers as "[c]rackers" (PMD, PMH). However, the latter term is considered to be demeaning and deprecated in most cybersecurity contexts (Söderberg, 2010). Thus, it is becoming more common to refer to such "respectable" hackers who work for "the good side" (PMC) through other means. The idea of penetration testers and security researchers can in this theme be expanded towards notions of "ethical," "white hat," or "certified" hackers–all of which are concepts that encompassed in the idea of a "good hacker" (PMC). While these terms are not mutually exclusive, and all describe the simulation of attacks and methods used by malicious actors, the latter three (i.e., ethical,

white hat, certified hacker) actively embrace the hacker identify by explicitly referring to hacking in their title.

Nonetheless, these concepts also disentangle themselves from any negative associations that hackers and affiliated groups may carry, including popular stereotypes of their sloppiness and adolescence. References in which white hat hackers are described to "have come out of the back bedroom and are heading for the board-room" (Caldwell, 2011, p. 11) mark attempts to destigmatize professionals' own practice through disassociation. These are examples in which the concepts ambiguity and flexibility helps to facilitate an identity as much as an image shift

Slayton (2017) showcased this change in association in her research on certified ethical hackers (CEH). Just like the job advertisement in *PC-WELT*, the CEH credential is seeking to appropriate the connotations of technical savvy of the field of hackers, the US military, and intelligence agencies, while distancing itself from its untrustworthy and morally suspect image and stigma of hackers (Slayton, 2017). Such dynamics elucidate to the appropriation of the expertise, knowledge, and authority that the field of hackers is considered to carry and packages it under the banner of professionalization, similar to the domestication aspects reasoned before.

These shifts to civilize the hacker identity and their practices towards a proclaimed "legitimate" or "good" side, also go along with professional ethics, and norms, and codes of conducts (Slayton, 2017). In interviews, these "good" hackers are associated with particular behaviors, specifically the idea of "responsible disclosure" (PMF). The latter is, according to one participant, "the gentleman's agreement of the industry" (PMF). Actors that want to release security research have to consider the "different criticalities" (PMF) of vulnerabilities prior to their (mis-)use or release. Such an assessment would ensure that vulnerabilities can be evaluated in light of their potential impact and extent of harm. While the practice of ethical disclosure is shaped by numerous factors, the interviewees argue that hackers can show their willingness to side with "them" (i.e., the field of professionals) by making use of such accepted practices. Hackers behaviors must consequently guarantee an aptness for businesses, for hackers to be considered respectable and "good."

The *Möbius Strip*: Situating hacker identities on a flexible model

The analysis of interviews with IT and cybersecurity professionals on their perception of hackers resulted in three overlapping themes, including: (a) We employ hackers; (b) We employ "former" hackers; (c) We employ "good" hackers. Across these themes, participants acknowledge that hackers may not always be positively connoted but can, nonetheless, participate in the commercial IT and cybersecurity sector. Most

profoundly, the study indicates an appropriation of hacking that impacts on the identity construction of the IT and cybersecurity field. Together, the themes help to reveal the shifting identities and blurred boundaries that dominate the hacker concept to date.

Different scholars and practitioners have tried to categorize and differentiate the diverse notions that make up the hacker community before. They added adjectives or found new expressions to describe their amorphous identities, behaviors, and practices. Nowadays, one can speak of civic, state, non-state, or even proto-state hackers (Schrock, 2016; Skare, 2018), distinguish between "three moral genres" of hacking (Coleman & Golub, 2008, p. 256), with Rogers (2006) offering at least eight classification variables of hackers, including novices, cyber-punks, or petty thieves. For Kelty (2018, p. 291), who has traditionally mobilized a very narrow conception of hackers, hacking comes in an "under-appreciated variety of flavours." Some authors may even relate hackers to journalists (di Salvo, 2017) and in tension with concepts such as makers (Braybrooke & Jordan, 2017; Davies, 2017) and geeks (Buhs, 2010). Thus, the perceptions towards hackers are not only diverse but also pliable.

While such classifications are helpful, they fail to illustrate the fluidity and flexibility that the term embodies. In order to make sense of the shifting and ambivalent identities, the present article moves away from hacker categories and definitions. Instead, the article puts forward a more malleable approach to consolidate these different hacker personas. The proposed framework offers a basis to think of and visualize the historically-ambivalent status of hackers and associated concepts. It breaks with the in-group and out-group construction that the IT and cybersecurity field expressed and instead offers a novel contribution for situating the moral valence of hackers on a flexible model.

Drawing on the empirical findings outlined above, the article proposes to not only speak of a spectrum but a band upon which different identities or shades of hackers can be placed. By envisioning all the discussed concepts of "good" and "former" hackers on a *Möbius strip,* one can apprehend the ambivalent but at the same time dual relationship between accepted and rejected identities and practices. A *Möbius strip* is a graphical figure obtained by, for example, taking a rectangular piece of ribbon, twisting one end through 180◦, and then joining the ends, creating a one-sided surface (Starostin & Heijden, 2007). The developable form enables the strip to undergo large deformations. It bends and can be twisted to bring forward the *inside* as well as the *outside*.

The *Möbius strip*--or Möbius ribbon, as it is sometimes referred to--has been used as a tool within the academic literature to scrutinize accepted dualisms, categories, and borders (Bigo & Walker, 2007). It represents the mathematical property of being unorientable. In the context of the contested nature of hackers, the *Möbius strip* allows for a flexibility that previous categorical definitions have not guaranteed. One can project all of the above

discussed identities, behaviors, and practices onto the band. Associations such as the legality of an action or the affiliation with different terms (e.g., hacker, penetration tester) lie in the eye of the beholder. A viewers' situatedness, power relationship, and orientation towards the field of hackers influences their standpoint. Whoever owns or holds the ribbon (or rather the discourse and practices around the ribbon) can twist and bend the strip and, thus, modify the perceptions that will be seen. As showcased in the empirical part of this article, IT and cybersecurity professionals may use this process to bring forward a particular aspect they aspire an observer to focus on. Without the opportunity to rotate the strip, one will not be able to appreciate all features of its surface.

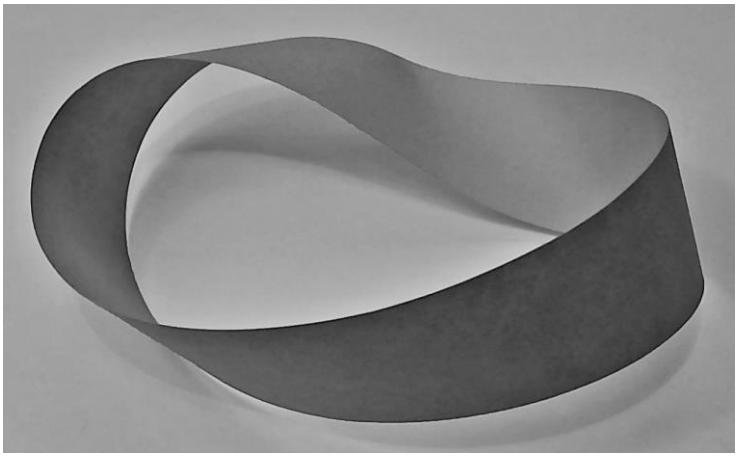

Figure 1: *Möbius strip*. Adapted from David Benbennick (2005).

While the ribbon offers an element of indeterminacy, it also contains the element of duality, due to its *perceived* two-sided character. The strip, therefore, reflects the polar nature expressed by interviewees (i.e., hacker/IT and cybersecurity professional, "good"/"bad," "current"/"former"). However, the strip is curved to create an undeterminable state that seamlessly merges both the inner as well as the outer part of the ribbon. The suspension of these edges and the actual single-sided nature of the ribbon creates an *in-between* space for hacker identities. This space gives room to blurred boundaries such as evidenced by the ambivalent concept of "gray" hackers. The latter is a term used to describe hackers who are considered to be situated between the black and white labels that have come to distinguish malicious hackers from more benevolent ones (Coleman, 2014). Additionally, this blurred space helps to explain how both the field of hackers as well as the field or professional coexist. Just as hackers may work in the industry, IT and cybersecurity professionals may be hackers. Conversely, not all hackers work in the industry, and not all employed IT and cybersecurity professionals are hackers. On the single-sided strip, one can flexibly move and exchange these identities.

The *Möbius strip* concept also offers a novel way to situating the morality of hackers on a flexible model. The ribbon can malleably categorize hackers' behaviors in regard to

another actors' moral valence and provides a more dynamic perspective to contextualize hackers and associated concepts. Even disputed conducts such as political acts can through material changes of the strip be brought forward and presented to the viewer as legitimate. Besides, each actor or field may believe that the ribbon has to be twisted and shifted to create a particular shape of their own terms. The hacker–as, of course, many other contested concepts–is an agent that across this endless ribbon is neither inside nor outside and has in the space of Internet security no longer a fixed position but is a concept that is fluent and flexible.

The graphical figure of the *Möbius strip* therefore acknowledges the fluidity and ambivalence of hackers, which was hinted at in the earlier section of the article. It leaves doors open for struggles over hacker definitions and classifications and gives the hacker identity the elasticity that categorical distinctions have so far missed to offer. The *Möbius strip* further helps to visualize the transformations the term and its associations have undergone. Its shape and, thus, its meaning have continuously changed through the pressures (e.g., criminalization) the ribbon was subjected to over time and will most likely continue to be exposed to in the future.

Conclusion

This research explored the blurred boundaries between definitions of the term hacker. The first part of the article offered a qualitative study of interviews with IT and cybersecurity professionals on their perception of hackers. The analysis resulted in three themes: (a) We employ hackers; (b) We employ "former" hackers; (c) We employ "good" hackers. Across these themes, participants acknowledge that hackers may not always be positively connoted but can, nonetheless, be part of the commercial IT and cybersecurity field. Thus, participants justified their engagement and coexistence with the field of hackers by creating their own professional in-group identity in contrast to theirs. Hence, interviewees used discursive strategies and either devised new terms such as security researcher or added explanatory adjectives such as "former" or "good" to the hacker term.

The second part of the article draws on the empirical findings to propose a conceptual framework which not only provides insight into the operationalization of hacking as a concept but further offers a novel contribution for situating the moral valence of hackers on a flexible model. This framework breaks with the in-group and out-group separation and rather offers a flexible template upon shifting identities of hackers and associated concepts such as hacktivists can be placed. Representing the mathematical property of being unorientable, the strip gives the ability to not only create an *in-between* space (e.g., "former" hacker) but also to change meanings in the eye of the beholder. It further helps to visualize hackers' contested

nature and offers a means to modify the different perceptions towards hackers that will be seen.

These empirical findings also hold some limitations. The narrow sample size, dominance of male interviewees, and demographic restrictions inhibit broader statements about the perceptions of hackers within the wider industry sector. Instead, the analysis contributes to a body of knowledge about a certain class of professional, which may not reflect perspectives upheld outside of the analyzed sample. At the time of writing, the data was collected four years ago. While one cannot rule out that the data is outdated and responses consequently skewed, the findings still demonstrate dynamics that have been observed by other scholars such as Söderberg (2010), Halbert (1997), and Irani (2015).

Thus, the article speaks to the long trajectory of academic scholarship on the hacker community (Kelty & Coleman, 2017). The uncovered ontological and normative complexities offer a window in the rationale of a selected sample of IT and cybersecurity industry representatives. Moreover, the analysis feeds into discussions on the intellectual challenge of studying the social and political construction of amorphous concepts, which has previously been shown in research on immigrants, citizens, terrorists, and activists (Bigo, 2008b; Isin, 2009). Future research can respond to the here outlined limitation and use the qualitative analysis as well as the conceptual framework as a starting point for further hacker examinations.

Endnotes

[i] German: "Werden Sie doch Ethical Hacker!"

[ii] German: "Agentur für Innovation in der Cybersicherheit."

[iii] Phreaking describes the manipulate of phone systems to, for example, make phone calls without paying for a used service (Turgeman-Goldschmidt, 2005).

[iv] Leaking is the act of publishing exfiltrated digital content. A newer form of leaking that describes the close intersection between leaking and hacking has been classified by Coleman (2017) as "public interest hack." The tactic enables to increase the public value of leaked documents by the material having been gathered through the high-risk activity of computer intrusion.

[v] Whistleblowing is the official reporting as well as the leaking of information concerning wrongdoing and done by insiders (Züger, Milan, & Tanczer, 2015).

[vi] Doxing is the act of collecting and publishing information online on a person, organization, or company and has become a controversial tactic to shame and intimidate targets (Donovan, 2017).

[vii] Hackathons are a type of event that bring programmers together with other communities to solve problems.

Reference list

Alper, M. (2014). “Can Our Kids Hack It with Computers?”: Constructing Youth Hackers in Family Computing Magazines (1983–1987). *International Journal of Communication*, *8*, 26.

Backmann, G. (2017). Utopian Hacks. *Limn*, *8*. Retrieved from https://limn.it/articles/utopian-hacks/

Bauman, Z. (1990). Modernity and Ambivalence. *Theory, Culture & Society*, *7*(2–3), 143–169. https://doi.org/10.1177/026327690007002010

Benbennick, D. (2005). *Möbius Strip*. Retrieved from https://commons.wikimedia.org/wiki/File:M%C3%B6bius_strip.jpg

Bialski, P. (2017). I Am Not a Hacker. *Limn*, *8*. Retrieved from https://limn.it/articles/i-am-not-a-hacker/

Bigo, D. (2008a). International Political Sociology. In P. Williams (Ed.), *Security Studies: An Introduction* (pp. 116–129). London: Routledge.

Bigo, D. (2008b). The Emergence of a Consensus: Global Terrorism, Global Insecurity, and Global Security. In A. Chebel d’Appollonia & S. Reich (Eds.), *Immigration, Integration and Security: America and Europe in Comparative Perspective* (pp. 67–94). Pittsburgh, PA: University of Pittsburgh Press.

Bigo, D. (2013). The Transnational Feld of Computerised Exchange of Information in Police Matters and Its European Guilds. In N. Kauppi & M. R. Madsen (Eds.), *Transnational Power Elites: The New Professionals of Governance, Law and Security* (pp. 155–182). London: Routledge.

Bigo, D., & Walker, R. B. (2007). Political Sociology and the Problem of the International. *Millennium: Journal of International Studies*, *35*, 725–739. https://doi.org/10.1177/03058298070350030401

Bourdieu, P. (1985). The Genesis of the Concepts of Habitus and Field. *Sociocriticism*, *2*(2), 11–24. https://doi.org/10.1177/0038038504040870

Braun, V., & Clarke, V. (2006). Using Thematic Analysis in Psychology. *Qualitative Research in Psychology*, *3*(2), 77–101. https://doi.org/10.1191/1478088706qp063oa

Braybrooke, K., & Jordan, T. (2017). Genealogy, Culture and Technomyth: Decolonizing Western Information Technologies, From Open Source to The Maker Movement. *Digital Culture & Society*, *3*(1), 25–46. https://doi.org/10.14361/dcs-2017-0103

Buhs, J. B. (2010). Wildmen on the Cyberfrontier: The Computer Geek as an Iteration in the American Wildman Lore Cycle. *Folklore*, *121*(1), 61–80. https://doi.org/10.1080/00155870903482015

Caldwell, T. (2011). Ethical Hackers: Putting on The White Hat. *Network Security*, *2011*(7), 10–13. https://doi.org/10.1016/S1353-4858(11)70075-7

Coleman, G. (2013a). *Anonymous in Context: The Politics and Power behind the Mask* (No. 3). Waterloo: Centre for International Governance Innovation.

Coleman, G. (2013b). *Coding Freedom: The Ethics and Aesthetics of Hacking*. Princeton, NJ: Princeton University Press.

Coleman, G. (2014). *Hacker, Hoaxer, Whilstleblower, Spy: The Many Faces of Anonymous*. London, New York, NY: Verso.

Coleman, G. (2016). Hacker. In B. Peters (Ed.), *Digital Keywords: A Vocabulary of Information Society and Culture* (pp. 158–172). Princeton; Oxford: Princeton University Press.

Coleman, G., & Golub, A. (2008). Hacker Practice: Moral Genres and the Cultural Articulation of Liberalism. *Anthropological Theory*, *8*, 255–277. https://doi.org/10.1177/1463499608093814

Collins, K. (2018, August 6). Inside The Boot Camp Reforming Teenage Hackers. *CNET*. Retrieved from https://www.cnet.com/news/inside-the-boot-camp-reforming-teenage-hackers/

Conway, M. (2003). Hackers as Terrorists? Why It Doesn't Compute. *Computer Fraud & Security*, *12*, 10–13. https://doi.org/10.1016/S1361-3723(03)00007-1

Davies, S. R. (2018). Characterizing Hacking: Mundane Engagement in US Hacker and Makerspaces*. *Science, Technology, & Human Values*, *43*, 171–197. https://doi.org/10.1177/0162243917703464

Décary-Hétu, D., & Dupont, B. (2012). The Social Network of Hackers. *Global Crime*, *13*, 160–175. https://doi.org/10.1080/17440572.2012.702523

Delfanti, A., & Söderberg, J. (2018). Repurposing the Hacker. Three Cycles of Recuperation in The Evolution of Hacking and Capitalism. *Ephemera. Theory and Politics in Organization*, *18*, 457–476.

di Salvo, P. (2017). Hacking/Journalism. *Limn*, *8*. Retrieved from https://limn.it/articles/hackingjournalism/

Ekeland, T. (2017). Hacker Madness. *Limn*, *8*. Retrieved from https://limn.it/articles/hacker-madness/

Facebook. (2012). *Registration Statement on Form S-1: Facebook, Inc.* (pp. 1–150). Retrieved from Securities and Exchange Commission website: https://www.sec.gov/Archives/edgar/data/1326801/000119312512034517/d287954ds1.htm#toc287954_10

Fitzgerald, M. (2007, April 17). L0pht in Transition. *CSO Online*. Retrieved from https://www.csoonline.com/article/2121870/lopht-in-transition.html

Grenfell, M. (2014). *Pierre Bourdieu. Key Concepts* (2nd ed.). London: Routledge.

Gröndahl, B. (2000). *Hacker*. Hamburg: Rotbuch.

Guarnieri, C. (2017). What Is to Be Hacked? *Limn, 8*. Retrieved from http://limn.it/what-is-to-be-hacked/

HackerOne. (2016). *2016 Bug Bounty Hacker Report*. HackerOne. Retrieved from https://hackerone.app.box.com/s/04uvkrh3sojep65g0ol9at63r3fyibv8

Halbert, D. (1997). Discourses of Danger and the Computer Hacker. *The Information Society*, *13*, 361–374. https://doi.org/10.1080/019722497129061

Huang, A. "bunnie." (2017). *The Hardware Hacker: Adventures in Making & Breaking Hardware*. San Francisco, CA: No Starch Press.

Irani, L. (2015). Hackathons and The Making of Entrepreneurial Citizenship. *Science, Technology & Human Values*, *40*, 799–824. https://doi.org/10.1177/0162243915578486

Irani, L. (2019). *Chasing Innovation: Making Entrepreneurial Citizens in Modern India* (Vol. 22). Princeton, NJ: Princeton University Press.

Isin, E. F. (2009). Citizenship in Flux: The Figure of the Activist Citizen. *Subjectivity, 29*, 367–388. https://doi.org/10.1057/sub.2009.25

Jarvis, L., Macdonald, S., & Nouri, L. (2014). The Cyberterrorism Threat: Findings from a Survey of Researchers. *Studies in Conflict & Terrorism*, *37*, 68–90. https://doi.org/10.1080/1057610X.2014.853603

Johnston, J. R. (2009). *Technological Turf Wars: A Case Study of the Computer Antivirus Industry*. Philadelphia, PA: Temple University Press.

Jordan, T., & Taylor, P. (1998). A Sociology of Hackers. *The Sociological Review*, *46*, 757–780. https://doi.org/10.1111/1467-954X.00139

Jordan, T., & Taylor, P. A. (2004). *Hacktivism and Cyberwars: Rebels with a Cause?* New York, NY: Routledge.

Kelty, C. M. (2008). *Two Bits: The Cultural Significance of Free Software*. Durham, NC: Duke University Press.

Kelty, C. M. (2018). Hacking the Social? In N. Marres, M. Guggenheim, & A. Wilkie (Eds.), *Inventing the Social* (pp. 287–297). Manchester: Mattering Press.

Kelty, C. M., & Coleman, G. (2017). Preface: Hacks, Leaks, and Breaches. *Limn*, *8*. Retrieved from https://limn.it/articles/preface-hacks-leaks-and-breaches/

Kessler, O., & Werner, W. (2013). Expertise, Uncertainty, and International Law: A Study of the Tallinn Manual on Cyberwarfare. *Leiden Journal of International Law*, *26*, 793–810. https://doi.org/10.1017/S0922156513000411

Klein, A. G. (2015). Vigilante Media: Unveiling Anonymous and the Hacktivist Persona in the Global Press. *Communication Monographs*, *82*, 379–401. https://doi.org/10.1080/03637751.2015.1030682

Kubitschko, S. (2015). The Role of Hackers in Countering Surveillance and Promoting Democracy. *Media and Communication*, *3*(2), 77–87. http://dx.doi.org/10.17645/mac.v3i2.281

Leander, A. (2011). The Promises, Problems, and Potentials of a Bourdieu-Inspired Staging of International Relations. *International Political Sociology*, *5*, 294–313. https://doi.org/10.1111/j.1749-5687.2011.00135.x

Leonard, P. (2014). 'A Revolution in Code'? Hari Kunzru's Transmission and the Cultural Politics of Hacking. *Textual Practice*, *28*, 267–287. https://doi.org/10.1080/0950236X.2013.824501

Levy, S. (1984). *Hackers: Heroes of the Computer Revolution*. New York, NY: Doubleday.

Maxigas. (2017). Hackers Against Technology: Critique and Recuperation in Technological Cycles. *Social Studies of Science*, *47*, 841–860. https://doi.org/10.1177/0306312717736387

McGraw, G. (2016). Silver Bullet Talks with Peiter (Mudge) Zatko. *IEEE Security & Privacy*, *14*(1), 7–10. https://doi.org/10.1109/MSP.2016.11

McLellan, V. (1981, July 26). Case of the Purloined Password. *The New York Times*. Retrieved from https://www.nytimes.com/1981/07/26/business/case-of-the-purloined-password.html

Meyer, G. R. (1989). *The Social Organization of the Computer Underground* (Master of Arts, Criminology, Northern Illinois University). Retrieved from http://www.dtic.mil/docs/citations/ADA390834

Millman, R. (2018, July 5). The SC Media UK Global Top 50 Companies in the Cyber-Security Market. *SC Media UK*. Retrieved from https://www.scmagazineuk.com/article/1487005

PC-WELT. (2018, August 31). Werden Sie doch Ethical Hacker! - Anzeige. *PC-WELT*. Retrieved from https://www.pcwelt.de/a/werden-sie-doch-ethical-hacker-anzeige,3452042

Quigley, K., Burns, C., & Stallard, K. (2015). 'Cyber Gurus': A Rhetorical Analysis of the Language of Cybersecurity Specialists and the Implications for Security Policy and Critical Infrastructure Protection. *Government Information Quarterly*, *32*, 108–117. https://doi.org/10.1016/j.giq.2015.02.001

Reuters. (2018, August 29). Germany, seeking independence from U.S., pushes cyber security research. *Reuters*. Retrieved from https://www.reuters.com/article/us-

germany-cyber/germany-seeking-independence-from-u-s-pushes-cyber-security-research-idUSKCN1LE1FX

Rogers, M. K. (2006). A Two-Dimensional Circumplex Approach to the Development of a Hacker Taxonomy. *Digital Investigation*, *3*(2), 97–102. https://doi.org/10.1016/j.diin.2006.03.001

Schrock, A. R. (2016). Civic Hacking as Data Activism and Advocacy: A History from Publicity to Open Government Data. *New Media & Society*, *18*, 581–599. https://doi.org/10.1177/1461444816629469

Skare, E. (2018). Digital Surveillance/Militant Resistance: Categorizing the "Proto-state Hacker." *Television & New Media*, Advance online publication.

Slayton, R. (2017). The Paradoxical Authority of the Certified Ethical Hacker. *Limn*, *8*. Retrieved from https://limn.it/articles/the-paradoxical-authority-of-the-certified-ethical-hacker/

Söderberg, J. (2010). Misuser Inventions and the Invention of the Misuser: Hackers, Crackers and Filesharers. *Science as Culture*, *19*, 151–179. https://doi.org/10.1080/09505430903168177

Söderberg, J., & Delfanti, A. (2015). Hacking Hacked! The Life Cycles of Digital Innovation. *Science, Technology, & Human Values*, *40*, 793–798. https://doi.org/10.1177/0162243915595091

Stańczyk, M. (2017). Unseen War? Hackers, Tactical Media, and Their Depiction in Hollywood Cinema. *TransMissions: The Journal of Film and Media Studies*, *2*, 62–77. http://transmissions.edu.pl/unseen-war-hackers-tactical-media-and-their-depiction-in-hollywood-cinema/

Starostin, E. L., & Heijden, G. H. M. van der. (2007). The Shape of a Möbius Strip. *Nature Materials*, *6*, 563–567.

Steinmetz, K. F. (2015). Craft(y)ness: An Ethnographic Study of Hacking. *British Journal of Criminology*, *55*, 125–145. https://doi.org/10.1093/bjc/azu061

Stephenson, P. (1999). Hiring Hackers. *Information Systems Security*, *8*(2), 10–13. https://doi.org/10.1201/1086/43305.8.2.19990601/31059.3

Tanczer, L. M. (2015). Hacking the Label: Hacktivism, Race, and Gender. *Ada: A Journal of Gender, New Media, and Technology*, (6). Retrieved from https://adanewmedia.org/2015/01/issue6-tanczer/

Tanczer, L. M. (2017). The Terrorist – Hacker/Hacktivist Distinction: An Investigation of Self-Identified Hackers and Hacktivists. In M. Conway, L. Jarvis, S. Lehane, S. Macdonald, & L. Nouri (Eds.), *Terrorists' Use of the Internet* (pp. 77–92). Amsterdam: IOS Press.

Vollmann, M. T. (2015). *The 414s: The Original Teenage Hackers* [Documentary]. Retrieved from http://www.the414s.com/

Wark, M. (2004). *A Hacker Manifesto* (Vol. 23). Cambridge, MA: Harvard College.

Watkins, J. (2018). No Good Deed Goes Unpunished: The Duties Held by Malware Researchers, Penetration Testers, and White Hat Hackers. *Minnesota Journal of Law, Science & Technology*, *19*, 535-563.