Communications of the Association for Information Systems

Volume 52 Article 12

2023

The Professionalization of Hackers: A Content Analysis of 30 Years of Hacker Communication

Frank Ulrich
Independant Researcher, mail@frankulrich.org

Sune D. Müller
Department of Informatics, University of Oslo

Stephen Flowers
Kent Business School, University of Kent

Communications of the Association for Information Systems

Accepted Manuscript

The Professionalization of Hackers: A Content Analysis of 30 Years of Hacker Communication

Frank Ulrich
Independent researcher
mail@frankulrich.org

Sune Dueholm Müller
Department of Informatics
University of Oslo

Stephen Flowers
Kent Business School
University of Kent

Please cite this article as: Ulrich, Frank; Dueholm Müller, Sune; Flowers, Stephen: The Professionalization of Hackers: A Content Analysis of 30 Years of Hacker Communication, *Communications of the Association for Information Systems* (forthcoming), In Press.

Communications of the Association for Information Systems

Research Paper ISSN: 1529-3181

The Professionalization of Hackers: A Content Analysis of 30 Years of Hacker Communication

Frank Ulrich
Independent researcher
mail@frankulrich.org

Sune Dueholm Müller
Department of Informatics
University of Oslo

Stephen Flowers
Kent Business School
University of Kent

Abstract:

Underground hacking has evolved from its early countercultural roots to become a complex and varied phenomenon. By combining a historical review of the literature with a content analysis of 30 years of underground hacker communication, we show that hacking has evolved in three waves to embrace learning and creativity, intrusion and crime, as well as politics and cyberwarfare. We uncover a paradoxical relationship between hackers and society at large where underground hacking is considered a digital crime while at the same time inspiring and driving corporate innovation, cybersecurity, and even cyberwarfare. The outcome of our research provides a nuanced picture of the hacker underground by highlighting differences between competing discursive themes across time. Moreover, by translating these themes into a set of six contrasting personas of IS professionals, we discuss how knowledge, technologies, and creative practices of underground hackers are being professionalized. We use this discussion to provide implications and a research agenda for IS studies in cybersecurity, innovation, and cyberwarfare.

Keywords: Hacking, Hacker, White Hat, Black Hat, Hacker Underground, Cybercrime, Cyberwarfare, Digital Crime, Criminal IT Professionals, Cybersecurity, Innovation, Creativity, Professionalization.

[Department statements, if appropriate, will be added by the editors. Teaching cases and panel reports will have a statement, which is also added by the editors.]

[Note: this page has no footnotes.]

This manuscript underwent [editorial/peer] review. It was received xx/xx/20xx and was with the authors for XX months for XX revisions. [firstname lastname] served as Associate Editor.] **or** The Associate Editor chose to remain anonymous.]

1 Introduction

This article investigates the evolution of the hacker underground and how hacking is being adopted and adapted by cybercriminals, governments, companies, and activist groups. Information Systems (IS) security research has investigated both theoretically and empirically formal, institutionalized security practices (e.g. Smith et al. 2010; Whalley 2010) but has paid less attention to those associated with criminal behavior and underground hacking (e.g., Mahmood, Raghu, Siponen, Rao, & Straub, 2010; Willison, 2006b; Willison, Warkentin, & Johnston, 2018). However, since the 1982 movie "War Games," the hacker underground has captured the imagination and fascination of the general public (Thomas 2002). In recent years, the public portrayal of "criminal" hackers has likened them to black hat rogues and political activists who break into computer systems and wreak havoc by stealing and publicizing sensitive information (Mahmood et. al., 2010; Olsen, 2013; Shimomura & Markoff, 1996). For example, the main protagonist in the 2015-2019 television series Mr. Robot is a mentally unbalanced hacker who becomes part of a black hat hacktivist group that seeks to overthrow the global financial system. Although this makes for good entertainment, this portrayal is but one element in a number of competing discursive themes underlying hacking (e.g., Levy 1984; Turkle 1984; Wark 2004).

As observed by Mahmood et al. (2010) and Willison, Warkentin, et al., (2018), the "harder-to-conduct black-hat studies" (p. 1188) are under-represented in IS research even though black hat hacking and, more generally, digital crime provide both relevant and timely research opportunities (Mahmood et al., 2010). A more balanced research agenda is needed that possesses a perspective on hacking as something more than criminal activity. Hacking is also "the production of the production" (Wark 2004, p. 158) in the sense of hackers being creative while: (1) collaborating with others outside the boundaries of the law and social norms (Flowers, 2008; Schulz & Wagner, 2008; Turkle, 1984); and (2) building on knowledge, technology, and innovation of others (Coleman, 2013; von Hippel & Paradiso, 2008). In a non-judgmental perspective, hacking is creative play with technology that challenges habitual thinking through rebellious acts (Conti, 2006; Flowers, 2008; Müller & Ulrich, 2015). Similarly, underground hacking is a mixture of criminal and creative activities (Flowers, 2008) that result in both small and large innovations. Sometimes such innovations take the form of modifications to existing products, possibly without the permission of copyright or patent owners (e.g., Flowers 2008; Schulz and Wagner 2008). For example, Lego's acceptance of the "right to hack" originated from hackers illegally cracking the Mindstorms RCX platform to expand its functionality, which in the end changed Lego's business model toward user-driven innovation (Koerner, 2006). Hence, we define the hacker underground as a group of technology actors engaged in transgressive social behavior that is innovative but often unlawful and sometimes threatening to established institutions. This description helps us separate them from other hackers and technology users (e.g., von Hippel and Paradiso 2008).

According to the often quoted hacker manifesto (Wark, 2004), hacking is a continuation of something that already exists—be it in terms of art, technology, or knowledge. Even though associated with the digital age, hacking is not limited to this period in human history. It is no coincidence that the first automobiles looked similar to horse carriages of that time as ideas tend to build on the work of others (Pacey, 1992; Ulrich et. al., 2015). As Graham (2004, p. 21) argues in his seminal work on hackers and painters, "over time, beautiful things tend to thrive, and ugly things tend to get discarded." As such, hacking can be viewed as a form of capital that devaluates itself as "new hacks supersede old hacks, and devaluate them as property" (Wark 2004, p. 80). Hacking is therefore a creative process in which ideas are negotiated and multiplied over time (e.g., Ulrich et al., 2015). By implication, hacking continually evolves and changes with advances in technology and society. Consequently, the concept of hacking has changed in meaning over time, and our current understanding differs from those in the past (e.g., Klimburg 2017).

Based on the premise that hacking is constantly evolving, we argue that hacking is not only concerned with computers and crime but also a cultural and societal phenomenon (e.g., Graham 2004; Levy 1984). In the following, we first discuss the relevance of hacking as an IS research topic and describe the knowledge gap we address. We then provide an historical account of the evolution of hacking from its early roots in the 1950s to its current form where hacking has become an integral part of innovation processes, corporate behavior, national security, political ideologies, and societal changes. To trace this evolution, we perform a content analysis of 30 years of underground hacker communication in Cult of the Dead Cow (cDc) and Phrack Magazine—two world-renowned hacker communication outlets.

2 Identifying the Professionalization Gap in Black Hat Security Research

As basis for this research article, we provide an overview of existing IS security literature. We use the Mahmood's et al.'s (2010) distinction between white and black hat IS research studies to distinguish between the two literature streams and focus on the latter. As summarized in Table 1, the white hat literature takes the "good-guy" perspective, focusing on compliance and accountability (D'Arcy et. al., 2009; Kwon & Johnson, 2014; Smith et al., 2010; Whalley, 2010). For example, Smith et al. (2010) investigated how organizations complied to security accreditation and Whalley (2010) used neutralization and deterrence theory to understand how employees could be held accountable to violations of IS security policies. Other branches of the white hat IS literature are concerned with security behavior in organizations (e.g., Anderson & Agarwal, 2010; Boss et. al., 2015; Mookerjee, Mookerjee, Bensoussan, & Yue, 2011; Ng et. al., 2009). For example, Mookerjee et al. (2011) propose an analytical model that helps distinguish between normal computer behavior and intrusion attempts, e.g. when hackers try to compromise information security. In another study, Anderson and Agarwal (2010) analyze the security behaviors of home computer users and provide security advice.

By contrast, the black hat literature applies the "bad-guy" perspective to understand hacker networks, their tools, and the criminal psychology of hackers (e.g., Henrich et al., 2017; Willison, Warkentin, et al., 2018). Moreover, as Mahmood et al. (2010) and Willison et al. (2018) observe, the "harder-to-conduct black-hat studies" (p. 1188) are under-represented in IS research although they provide new research opportunities and help improve security measures (Mahmood et al., 2010). This article addresses this gap by enhancing our understanding of the professionalization of black hat behavior.

Table 1. Examples of IS Security Research Topics

Perspective	Examples of research topics	Selected references
White hat	Security compliance and accountability	D'Arcy et al. (2009), Kwon and Johnson (2014), Smith et al. (2010), Whalley (2010)
	Security behavior	Mookerjee et al. (2011), Anderson and Agarwal (2010), Ng et al. (2009), Boss et al. (2015)
Black hat	Hacker networks and tools	Benjamin et al. (2016), Holt (2013), Lu et al. (2015), Samtani et al. (2017), Yue et al. (2019)
	Criminal psychology of hackers	Auray and Kaminsky (2007), Henrich et al. (2017), Warren and Leitch (2010), Willison (2006), Willison, Lowry, and Paternoster (2018), Willison, Warkentin, et al. (2018), Young et. al. (2007)

2.1 The Black Hat Literature

The black hat literature in IS can roughly be divided into two streams. The first stream; the literature on hacker networks and tools, focuses on enhancing defensive cyber capabilities of organizations by understanding how black hat hackers communicate, how they network, and what tools they use to identify cyber security vulnerabilities (e.g., Benjamin et al. 2016; Holt 2013; Lu et al. 2015; Samtani et al. 2017; Yue et al. 2019). For example, Benjamin et al. (2016) analyze communication in hacker communities over Internet Relay Chat and identify key hackers. Samtani et al. (2017) focus on new cyber-threats by analyzing malware used by hackers.

The second stream; studies on the criminal psychology of hackers, seek to understand the modus operandi of hackers for the purpose of creating effective countermeasures (e.g., Auray & Kaminsky, 2007; Warren & Leitch, 2010; Willison, 2006; Young et al., 2007). These studies draw on extant research in criminology (e.g., Willison, Lowry, et al., 2018). Hence, similar to the white hat literature on accountability (e.g., D'Arcy et al., 2009; Whalley, 2010), this black hat literature includes theories of criminal deterrence (e.g., Henrich et al., 2017; Willison, Lowry, et al., 2018; Willison, Warkentin, et al., 2018) that take their cue from criminology by arguing "that would-be wrongdoers are sufficiently rational to be influenced by their knowledge of the consequences of criminal actions" (Willison, Warkentin, et al., 2018, p. 1188). According to Young et al. (2007), these "wrongdoers" are motivated by the thrill of hacking and are not deterred by threats of legal punishment. In a similar study, Warren and Leitch (2010) find that hackers who deface webpages are driven by competition against other hackers. Other studies explore the career paths of hackers (Auray & Kaminsky, 2007), their motives, and the influence exerted by the environment (Willison, 2006a).

2.2 Knowledge Gaps and the Present Study

As identified in our review, the black literature in IS security research has attempted to understand how hackers work and their motivations. Prior research has, however, not studied how the verbal interchange of ideas has evolved over time to understand what hacking and hackers are and have become over time. Nor has it investigated how discursive themes (themes underlying the hacker history) influence related themes in the extant literature on network security, innovation, and warfare. Instead, hackers have historically often been described stereotypically as either black hats, (Mahmood et al., 2010), network security intruders (Young et al., 2007), deviants (Lu et al., 2015), cyber criminals (Kim & Kim, 2017), or simply as criminals (Willison, 2006a). In the role of perpetrators of cyberattacks, hackers have been of interest in the IS security literature for decades (e.g., Hoffer and Straub 1989, Mookerjee et al. 2011, Warren and Leitch 2010). Even though some of these labels describe parts of the underground hacker community, they hide the complexity and dissimilarity of hacker groups with different agendas and goals (e.g., Levy 1984; Olsen 2013; Warren and Leitch 2010). Based on this research gap, we ask the following question:

RQ1: How should hacking be considered?

Based on this research question, we challenge the assumption in parts of the literature that underground hacking can be reduced to digital crime. We use content analysis to argue that hacking is being professionalized, and hackers are increasingly becoming IT professionals that serve security needs in both criminal networks, such as organized crime rings, and legitimate organizations such as intelligence services or private companies. To that end, we draw on Abbott (1988) and Muzio, Brock, and Suddaby (2013) to define the process of professionalization and the concept of a profession as basis for our investigation. According to Abbott (1988), professionalization is a process through which professions evolve toward a given form both structurally and culturally. This is consistent with the view of professionalization as "a temporally and spatially contingent process rooted in the power struggles between distinctive groups within a broader political economic order" (Muzio et al, 2013: 702). Professions are relatively homogeneous groups with the potential for some internal differentiation that reflects contingencies of the professionalization process. According to Abbott, professions are "exclusive groups of individuals applying somewhat abstract knowledge to particular cases" (Abbott, 1988, p. 318). He posits that the social structure and cultural claims are more important than the work of professions. With regard to culture, "professions legitimate their control by attaching their expertise to values with general cultural legitimacy" (Abbott, 1988, p. 16). In the case of hackers, such values include creativity, learning, and individuality as shown by the analyses.

Our contribution lies in combining a literature-based historical account with an empirical content analysis of more than three decades of hacker communication. The identified themes are partially described in extant literature (Davies, 2017; Klimburg, 2017; S. Levy, 1984; Turkle, 1984; Wark, 2004). However, by relating the empirical analysis to the literature, we show how those themes have changed over time as a basis for theorizing how hacking has become more professionalized over the last 30 years. We provide novel insights into the history of hacking and the evolution of associated themes and contribute not only to IS security research but also to our understanding of hacker's role in innovation and society. On this basis, we point to unanswered research questions related to IS security, innovation, and policymaking.

3 Research Design

In the following, we describe the empirical basis for our study (section 3.1) and our content analysis of the data (section 3.2).

3.1 Research Setting

To understand how competing discursive themes have evolved across time, we reviewed extant literature and performed content analysis of two electronic magazines (e-zines) tied to the hacker underground. These e-zines provide rich data on two major communities within the hacker underground. Cult of the Dead Cow (cDc) expresses the chaotic and rebellious nature of the hacker underground whereas Phrack Magazine showcases its technical mastery and relationship to the security industry. Both outlets help us understand hacking and how it relates to society at large.

cDc was founded in 1985 and by its own account is a loosely connected network of some of the best network security hackers in the world. cDc publishes an online e-zine by the same name and has released

various tools for hacking and encryption. cDc has an influence on underground hacking that cannot be overstated. For example, they are accredited with coining the word "hacktivism" in the mid-1990s (Olsen, 2013). However, they are also a group of pranksters that jokingly list "professional dominatrix," "crime scene cleanup," and "dog training" as services on their website. cDc is divided organizationally into three subgroups: The first subgroup is Ninja Strike Force, which in their own words is "the elite of the elite" (cDc website). Not much is known about this group due to secrecy and anonymity. However, it is described as a group of highly skilled hackers with the objective of carrying out cDc's objectives in both the physical world and cyberspace. The second subgroup is Hacktivismo, which focuses on political activism, human rights, and freedom of speech. Hacktivismo has previously released different encryption tools to counter state-sponsored censorship and has fostered a software license that emphasizes human rights and anti-spyware. Finally, cDc Communications runs the media outlet of the cDc. They are responsible for the e-zine and public relations, including interviews with mainstream media. Our empirical data includes the content of the e-zine. It is freely available at https://www.cultdeadcow.com and is a large collection of, e.g., hacker manifestos, guides, and stories. There is no particular structure to the publications, and it contains everything from crude humor, UFO observations, trash metal lyrics, diary entries, and guidelines to countless examples of hacks that are both related and unrelated to computers (for elaboration, see Müller and Ulrich 2015).

Phrack Magazine describes itself as an "underground zine, from hackers for hackers" (https://www.phrack.org). The name Phrack is a contraction of the words hack and phreak (a type of phone hacking). Similar to cDc, Phrack is an e-zine that despite federal prosecution has been freely available on the internet since 1985. However, whereas cDc is largely unstructured in its publications, Phrack is structured as an academic journal and grouped into volumes with regular features on, e.g., cybersecurity and hacker culture. Phrack also differs from cDc by having editors with one foot in the hacker underground and the other in the security industry. Moreover, large parts of articles published in Phrack are technical guides describing various hacks. For the same reason Phrack is considered one of the premium hacker outlets, and publishing in the magazine is regarded as a great feat among hackers.

3.2 Research Approach

Our historical account of the evolution of the hacker underground is inspired by similar studies of the history of IS (e.g., Hirschheim and Klein 2012; Stein et al. 2016). Porra et al. (2014) suggest that historical analyses include narratives about the past to communicate the trajectory of future developments (Porra, Hirschheim, & Parks, 2014). In support of such a narrative, we provide a historical account of hacking (Porra et al., 2014) based on a qualitative content analysis (e.g., Indulska, Hovorka, & Recker, 2012; Miles, Huberman, & Saldana, 2014). We begin with its inception in the 1960s counterculture and end with its professionalization in the present and analyze how themes on hacking have evolved. Our research is focused on underground hackers compared to other communities of hackers, such as FLOSS (e.g., Deek and McHugh 2008).

To increase the internal validity of the study, our data analysis is explorative and interpretive in nature (Walsham, 1995, 2006), and is firmly grounded in the academic literature combined with non-academic publications (Layder, 1998). As shown in Table 2, our analysis of the academic literature and the empirical data spans more than a 50-year period. Our analysis includes non-academic publications (e.g., Levy 1984; Lichstein 1963) and empirical data from two prominent hacker e-zines—Cult of the Dead Cow (cDc) Communications (https://www.cultdeadcow.com) and Phrack Magazine (https://www.phrack.org). Our dataset covers the three decades from 1985-2016 and contains over 28.000 pages of text, which translates into 4,6 million words. The data was downloaded from freely available internet sources. The data was first analyzed by the first and second author, then by a commissioned and external research assistant, and then again by the first author. Through this three-step process, we increased the reliability of our analysis by (a) having the first and second author analyze the data to identify and discuss central themes and keywords in the data, (b) having the external research assistant analyze and structure the data according to the identified keywords into an overview of the data, and (c) using this overview to retrace and update the initial (a) analysis as a quality assurance measure. In the following, we provide details on the dataset and procedures in preparing and analyzing the data.

Table 2. Organization of Data

Source	Type	Purpose	Timespan
White/black hat literature in IS research	• Academic literature	• Establishing an overview of modern academic IS literature on hacking • Identifying themes on hacking	2007-2019
Literature on the history of hacking	• Academic literature • Non-academic publications	• Establishing a timeline from past to present • Defining boundaries between evolutionary periods on the timeline • Identifying themes on hacking	1963-2019
Cult of the Dead Cow	• Dataset (e-zine)	• Identifying themes on hacking	1984-2009
Phrack Magazine	• Dataset (e-zine)	• Identifying themes on hacking	1984-2016

Table 3. Eight Themes on Hacking in the Literature

Themes	Emergence	Description	Selected References
Hacking as innovation and entrepreneurship	First wave	This theme describes hackers who operate within the legal boundaries of innovation. Hackers are technology driven entrepreneurs that challenge the status quo by developing novel technologies and bringing them to market.	Davies (2017), Levy (1984)
Hacking as outlaw innovation	Third wave	This theme describes hackers as innovators who operate outside the law by "jail-breaking" existing products to increase their functionality without the consent of intellectual property owners. Hackers are viewed as criminals who explore the possibilities of technologies.	Flowers (2008), Schulz and Wagner (2008)
Hacking as knowledge sharing community	First wave	This theme describes hackers as technology-savvy developers who alter or create technologies to gain knowledge and prestige without bringing the technology to market. Hackers are seen as explorers of technology.	Davies (2017), Turkle (1984)
Hacking as intrusion	First and second wave	This theme describes hackers as intruders of computer networks. Hackers are motivated by the intellectual challenge of bypassing security measures and by the prospect of gaining prestige. They are guided by a code of ethics and will, e.g., not destroy or steal data.	Mitnick and Simon (2005), Thomas (2002)
Hacking as vandalism	Second wave	This theme describes hackers who attack computer networks to wreak havoc. Hackers are viewed as vandals because they seek personal pleasure and gain by destroying or stealing data, crippling computer systems, or defacing homepages.	Shimomura and Markoff, (1996), Sterling (1992)
Hacking as crime	Second wave	This theme describes hackers as private actors engaged in security hacking to obtain profit outside legal boundaries. Hackers are members of organized criminal networks who engage in cybercrime to obtain profit or act as mercenaries for hire by government and non-government entities.	Holt (2013), Mahmood et al. (2010)
Hacking as political activism	Second wave	This theme describes hackers as grassroots actors who promote political goals and actively seek social change. Hacktivists also use technology to prevent the abuse of power by nation states.	Busch and Palmås (2006), Olsen (2013)
Hacking as warfare	Third wave	This theme describes hackers as warfighters who target enemies to obtain intelligence or sabotage infrastructures. Hackers are trained as assets in information warfare between nation states.	Baskerville, (2010), Klimburg (2017)

First, we identified eight themes in the academic and non-academic literature based on our historical account (section 4) of the literature (e.g., Baskerville 2010; Busch and Palmås 2006; Davies 2017; Flowers 2008; Holt 2013; Klimburg 2017; Levy 1984; Mahmood et al. 2010; Mitnick and Simon 2005; Olsen 2013; Schulz and Wagner 2008; Shimomura and Markoff 1996; Sterling 1992; Thomas 2002; Turkle 1984). Although the identified time periods, which we refer to as waves, are not exact, they are

based on historical events, and we were able to identify three waves in the evolution of hacking. For example, we identified how new hacker practices emerged from the 1960s and 1970s counterculture. We identify this period as the first wave. Around 1980, we argue for a second wave that emerged together with the availability of the personal computer. Our conceptualizations of the first and second waves also fits well within the conceptualization of first and second generation hackers, as argued by Levy (1984) and Turkle (1984). We then argue how the third wave emerged in the 2000s alongside the war on terror. Olsen (2013) provides some good examples of this switch in hacker practices, for example, with the emergence of hacktivist groups such as anonymous. From this historical analysis, we identified eight themes in the literature (e.g., Müller and Ulrich 2013). The eight themes are listed in Table 3 with descriptions and examples from the literature.

These were subsequently contrasted with the empirical data in an iterative process, which—through synthesis and consolidation—resulted in the following three themes: Intrusion and crime, creativity and learning, and politics and cyberwarfare (Table 4). These three themes capture key perspectives on hacking that are manifest across the three evolutionary periods of hacking.

Table 4. Consolidation of Themes

Themes identified in the literature	Consolidated themes
Hacking as intrusion	Hacking as intrusion and crime
Hacking as vandalism	
Hacking as crime	
Hacking as innovation and entrepreneurship	Hacking as creativity and learning
Hacking as outlaw innovation	
Hacking as knowledge sharing community	
Hacking as political activism	Hacking as politics and cyberwarfare
Hacking as warfare	

Table 5. Data Analysis Guide

Consolidated themes	Keywords	Description
Hacking as intrusion and crime	crim*, law	Utterances related to hacking and law enforcement, including: • Hackers depicted as criminals by media and governments, and the hackers' response to it • Hacking used in organized crime • Hackers viewing themselves as criminals • Hackers viewing hacking as anything but crime • Hackers discussing governments and media as criminals • Hacking for Lolz without regard for the consequences • Hackers' view of criminality • Hacking and intrusion as art or mastery • Hacking used for vandalism
Hacking as creativity and learning	learn*, creative*, fun	Utterances related to hacking as a learning or innovation activity, including: • Hacking as an innovation activity • Examples of hacker creativity and innovation • How hackers view themselves as innovators • Examples of hackers' perspectives on learning, innovation, and creativity • Hackers' view of learning • Hackers' view of social rules and norms
Hacking as politics and cyberwarfare	Hacktivism, Politic*	Utterances related to hacktivism, nation state warfare, and hackers' political relations to society, including: • Activism using hacking (hacktivism) • Hackers' views of society in general • Hackers' views of government, politics, and warfare • Nation state warfare using hacking • Hacker norms and politics • The role of hackers in society • Society's views of hacking and hackers • Hackers engaged in warfare

Second, using these three themes as starting points, we identified keywords in the literature that encapsulate the essence of each theme and used them as a basis for searching through the dataset. These keywords formed the initial basis for our content analysis. NVivo was then used to conduct a word frequency analysis, and the resulting list of words was compared with the keywords to narrow down the number of words used in the subsequent analysis, selecting keywords that were applicable across time periods and could be used as a basis for data coding. Consequently, we settled on keywords that were both used in the literature and by the hackers themselves while being mindful of time-sensitive words. For example, in analyzing the politics and cyberwarfare theme, we used the word "hacktivism," which has only been used since 1995, in combination with "politics" to capture hackers' perspectives on and conversations around politics, social change, and activism. Based on the selected keywords, a data analysis guide (Table 5) was established as a basis for our subsequent content analysis (Indulska et al., 2012; Miles et al., 2014) of the underground hacker communication.

Our content analysis of hacker communication is consistent with principles for generating movement-relevant theory as argued by Bevington and Dixon (2005): "Foremost in generating useful findings is to start by locating the issues and questions of most importance to movement participants. This requires a direct examination of the discussions taking place within a given movement" (Bevington & Dixon, 2005, pp. 198). In line with their recommendation, we use content analysis to identify issues and questions of importance in the hacker underground and present these as discursive themes.

Having coded and analyzed the content, we structured the data in tables according to keywords, time periods, and quotations (Table 6) for the purpose of establishing an overview of recurring themes and changes across evolutionary periods in the dataset. These tables provided an overview of trends and changes in terms of themes and topics within the three themes as they have evolved over time.

Table 6. Sample Empirical Evidence

Consolidated theme	Keyword	Example quotation	Period	Source
Hacking as intrusion and crime	Crim*	"Computer crime and hacking have always made for uncomfortable bed fellows, splitting hackers into two general camps; The laissez-fair consideration of those who know they commit several technical crimes before even getting out of bed in the morning, and those whose fear of the law drives them, essentially, straight -- condemned to endless nights in front of a debugger with nary an unauthorized rootshell to be seen."	2010s (2010)	Phrack
Hacking as creativity and learning	learn*	"A true hacker DOESN'T get into the system to kill everything or to sell what he gets to someone else. True hackers want to learn, or want to satisfy their curiosity, that's why they get into the system. To search around inside of a place they've never been, to explore all the little nooks and crannies of a world so unlike the boring cess-pool we live in."	1980s (1988)	cDc
Hacking as politics and cyberwarfare	Politic*	"Increasingly I spent time speaking with reporters and academics about hacktivism, commenting on a series of Web defacements and DoS attacks. The press was awash with articles about “hacktivists” who weren’t much more than low-rent computer criminals. It just smelled like the same cheap hacks were being elevated to political protest when, in my opinion, they weren't any more than script kiddy antics in drag. It became increasingly important for me to define hacktivism, mostly because I believed, and continue to believe, that there were very definite tactics that were acceptable for hacktivists. If someone wanted to call his or her actions digital disobedience, or cyber sit-ins, or anything else, that was fine with me. But invoking the term hacktivism was not OK."	2000s (2004)	cDc

Based on the established overview of recurring themes and changes across evolutionary periods, we searched for and identified patterns of professionalization of hacking. This entailed (1) searching for instances of hackers applying abstract knowledge to particular cases and making cultural claims, i.e. attaching their expertise to particular values; and (2) identifying patterns within and across time periods. Through this process, we are able to show how they behave in a consistent and rather uniform manner which serves to establish them as a homogeneous group with degrees of differentiation. This

differentiation is reflected in our synthesis of contrasting hacker personas (see below). This approach is consistent with Abbott (1988) who posits that the emergence of professios can "best be analyzed by specifying forces that affect the content and control of work and by investigating how disturbances in that content and control propagate through the system of professions and jurisdictions" (Abbott, 1988, p. 112). To paraphrase Abbott, professions emerge and evolve by applying abstract knowledge to new domains and appropriate them as areas of expertise. In our analysis, this entailed identifying how hacking has been used for different purposes across industries to achieve particular ends, and not least how this has changed over time periods.

Third, we developed and synthesized a set of contrasting personas based on the consolidated themes. These personas depict stereotyped hacker types that help communicate and reduce the complexity (e.g., Walsham 1995, 2006) of the underground hacker community by transforming discursive themes into personal characteristics (e.g., Miaskiewicz & Kozar, 2011; Turner & Turner, 2011). To describe the personas, we used Mahmood's et al.'s (2010) distinction between black and white hats to create two separate types of personas that constitute each other's counterparts. We then used this distinction and the synthesized themes to distinguish six distinct but contrasting personas that embody the professionalization of hacking across the three waves in the evolution of hacking (Table 9). We used these six personas to formulate questions to drive future IS research, outline future research paths, and provide guidance in terms of how to conduct this research (Table 10).

4 An Historical Account of The Evolution of The Hacker Underground

In the following, we provide a brief historical account of the evolution of the hacker underground. This account helps us clarify its evolutionary periods as waves that we use in our content analysis.

The history of hacking is well-documented (Thomas 2002; Thomas 2005; Levy 1984; Williams 2002; Sterling 1992; Markoff 2005; Olsen 2013; Hafner & Markoff 1995). In this brief historical account, we divide the history of hacking into three evolutionary periods. As summarized in Table 7, the first evolution (1955-1979) originated at MIT where hackers were inspired by the counterculture movement that resulted in the personal computer revolution. During the second evolution (1979-2000), democratization and the spread of technology led to the rise of an underground hacker community preoccupied with computer network security and open source software. During the third evolution (2000-), the different groups and applications of hacking have found their way into aspects of corporate business, political activism, warfare, and digital crime.

Table 7. Evolutionary Waves of Hacking

Wave	Period	Main driver	Historical events
First	1955-1979	The counterculture	• First PDP-1 hack • Homebrew Computer Club • Captain Crunch • The personal computer
Second	1979-2000	Democratization of technology	• Cheap hardware • Bulletin Board Systems • World Wide Web • Hacker crackdowns • Network security industry • FLOSS
Third	2000-	Political activism, cyberwarfare, and digital crime	• Wikileaks and hacktivism • Hacking for profit • The dark web • Cyberwarfare

4.1 The First Wave (1955-1979). Hackers of the Counterculture

The modern definition of the word "hack" originates in the Tech Model Railroad Club (TMRC) where it was used in the late 1950s to describe projects involving "innovation, style, and technical virtuosity" (Levy 1984, p. 23). These early hackers of model trains later became computer engineers when the TX-0 and PDP-1 computers were first used at MIT (S. Levy, 1984). Early hackers, like Steve Russell, used the PDP-1 to create the first popular computer game, Spacewar!, in 1961. Two years later, another group of students at MIT used the PDP-1 to hack the MIT phone system as the first recorded computer-based

network intrusion (Lichstein, 1963). This type of hacking became known as phone phreaking, which involved exploiting vulnerabilities in the phone system to make free long-distance calls (Thomas, 2002).

During the 1970s, the personal computer industry grew out of the counterculture of the 1960s (Markoff, 2005). The counterculture of the 1960s emerged in part as a response to the Vietnam War between 1961 and 1975, because an increasing number of young people were disillusioned and distrustful of government institutions (F. Turner, 2010). The MIT hacker ethos which promoted information sharing, distrust of authorities, and meritocratic values was evident in the counterculture of the 1960s (for elaboration, see Mosakowski, 2002; Markoff, 2005; and Levy, 1984). These early pioneers of personal computing had roots in this counterculture (Levy, 1984; Markoff, 2005; Graham, 2004). For example, Lee Felsenstein, who played a central role in the development of the personal computer was involved in the free speech movement and was one of the original members of the Homebrew Computer Club—a collective of hackers focused on building personal computers (S. Levy, 1984). John Draper, who created one of the first word processors (EasyWriter), wrote the software while serving jail time for cracking the American phone system with a toy from a Captain Crunch cereal box (Lapsley, 2013). Apple co-founders Steve Wozniak and Steve Jobs were hackers and members of the Homebrew Computer Club (S. Levy, 1984). After reading about John Draper's exploits, Wozniak and Jobs built their own "blue box" and sold the technology to students at Berkeley (Sterling, 1992; Thomas, 2002). Wozniak and Jobs would later change history by creating the first personal computer for mass production under the Apple brand, whereas other startups of the time, such as Microsoft, would focus their entrepreneurial energy on software (Levy, 1984; Thomas, 2002). The people behind these startups were bound together by a mental shift from hacking as a hobby to a way of doing business. In reflecting upon software programming at Microsoft, Cusumano and Selby (1997) argue that whereas the early hackers wrote computer code on an ad hoc basis as novel ideas emerged, contemporary software development has increased in complexity and requires formal, structured processes, and quality assurance measures. However, as the software grew more and more complex, the old school hackers left the industry or became members of development teams in which they were no longer allowed to '"bang on a keyboard' and 'hack away' at coding" (Cusumano & Selby, 1997, p. 59). Highly structured project models replaced ad hoc software development in response to the growing complexity of systems requirements. One example of such models is the Capability Maturity Model Integration (CMMI) with its emphasis on stability and control (Müller et. al., 2014). As Levy (1984) elaborates, this new industry was no longer controlled by those early hobbyists but had been turned into businesses creating useful products for the masses.

4.2 The Second Wave (1979-2000). Cyberpunks and Free Software

The personal computer ushered in the digital revolution (S. Levy, 1984; Müller & Ulrich, 2015). During the 1980s and 1990s, access to technology was democratized, which gave rise to a new generation of underground hackers. Whereas access in the 1950-70s was limited to universities and large companies, computers became available for personal use in private homes in the 1980-90s, which paved the way for a generation of technology savvy teenagers (Thomas, 2002). Moreover, the advent of Bulletin Board Systems (BBS) in the late 1970s allowed computer users to communicate via phone lines. BBS became hang-outs for hackers during the 1980s and the means of establishing online identities and sharing ideas (Thomas, 2005). Thomas (2002) describes this period as "post-punk" or "cyberpunk" (p. 31-32) and as distinctly different from the counterculture of the preceding period. This new generation of hackers criticized the older generation for selling out and abandoning the hacker ethos of openness, accessibility, and freedom in the pursuit of wealth (Thomas, 2002; Williams, 2002). Hence, as the old hackers left for employment in the computer industry, hacking came under pressure and split into internet subscenes, such as hackers specializing in breaching the security of computer networks (Sterling, 1992) and developing open source software (Stallman & Gay, 2009).

The underground hacker scene emerged in the late 1970s and early 1980s (Thomas 2005; Levy, 1984) around groups specializing in computer network security. These hacker groups with flamboyant names such as the Legion of Doom and Cult of the Dead Cow had their golden years between 1984-1990. They constituted a close-knit scene motivated by openness, curiosity, and computer mastery (Thomas, 2005; Turkle, 1984; Beveren, 2000; Furnell et. al., 1999). This scene was male dominated, highly secretive, informally organized, and motivated by the intellectual challenge of breaching network security without compromising data integrity (Jordan & Taylor, 1998). However, the hacker crackdowns of the early 1990s ended the golden age of the hacker underground with the arrest of many prominent hackers (Sterling, 1992; Thomas, 2005). Moreover, with the introduction of the World Wide Web in the 1990s, network hacking tools became widely available to people with limited skills, which increased the number of network

intrusions but also further eroded the cultural values of ethical hacking through increases in internet scams, spamming, and other fraudulent schemes (Thomas, 2005). The aggressive stance by law enforcement toward hackers contributed to politicizing the underground community (Jordan & Taylor, 2004; Thomas, 2005). Hacker groups, such as Cult of the Dead Cow, changed their behavior in the mid-1990s and became a hacker activist group that focused on ethical hacking and preventing government censorship on the internet (Jordan & Taylor, 2004).

Political agendas are not foreign to the hacker underground (Jordan & Taylor, 2004) and the hacker manifesto from the mid-1980s is a highly political statement attacking social norms and the educational system (Furnell et al., 1999). Moreover, the free software movement was founded by Richard Stallman in the mid-1980s in response to the increasing commercialization of software that prevented software engineers from sharing their source code (Coleman, 2013; Deek & McHugh, 2008; Williams, 2002). According to Stallman, proprietary software is a betrayal of the hacker ethos from the 1960s and 1970s that advocates knowledge sharing (Stallman & Gay, 2009; Williams, 2002). Stallman and others created the GNU General Public License (GNU GPL) in 1989, guaranteeing users the right to freely use, openly distribute, and modify software released under the license (Bretthauer, 2002; Deek & McHugh, 2008). The GNU GPL has subsequently been used in a variety of different software packages, including the Linux operating system and the Apache Web Server (Bretthauer, 2002), and by the late 1990s most of the internet infrastructure was built on free software (Deek & McHugh, 2008). However, by the late 1990s, it became clear that the GNU GPL was too restrictive, which resulted in the creation of the Open Source Initiative in 1998 (Bretthauer, 2002; Deek & McHugh, 2008). Free / Libre Open Source Software (FLOSS) was not only a revolution in software licensing but also in software development (Raymond 1999). Instead of relying on development in closed teams, FLOSS entails global collaboration in software development (Deek & McHugh, 2008) and new business models of software-based companies (Anderson, 2009; Osterwalder & Pigneur, 2010).

4.3 The Third Wave (2000-). Hacktivists, and Cyberwarfare

The time period since 2000 has been characterized by a series of historical events, including the war on terror, the financial crisis of 2007-08, and the Arab spring. Combined with technological developments, these events have influenced the evolution of hacking.

The war on terror and the financial crisis saw political activism growing out of the underground hacker community (Olsen, 2013). Hacker groups such as Anonymous and LulzSec instigated relatively harmless pranks aimed at the Church of Scientology which were later followed by physical protests and a series of cyberattacks against, e.g., PBS, PayPal, and Sony (Dobusch & Schoeneborn, 2015; Olsen, 2013). The sophistication of these attacks was low, using so-called SQL injections, Denial of Service tools, and Google Hacks to exploit known weaknesses (Hui et al., 2017; Kim & Kim, 2017; Mansfield-Devine, 2011). The actions of these hacktivist groups were crude yet served to attract attention and create awareness around political messages (Coleman, 2013; Mansfield-Devine, 2011). Similarly, activist groups rooted in freedom-of-speech communities such as WikiLeaks used cryptographic technologies to protect their sources, provide funding, and give a voice to citizens in regimes suppressing human rights (Fitri, 2011; Lindgren & Lundström, 2011). An example of these tools is the Tor Browser that provides criminals with access to an entirely new market on the dark web where illegal goods are bought and sold at low risk (Holt, 2013; Martin, 2014). This ability to hide from law enforcement results in the majority of cybercrime going unpunished (Kim et. al., 2012) but globally costs organizations billions of dollars in yearly security investments (Hui et al., 2017) and stolen intellectual property (Benjamin et al., 2016). As Pogrebna and Skilton (2019) argue, a lot of today's hackers are largely motivated by financial gain and the number of network security breaches in the United States has risen by 600% since 2005 although federal spending on cyber security has doubled (Sen, 2018). However, governments are themselves not without blame as they increasingly intercept telecommunications and develop sophisticated tools to gain access to computer networks that give them new means of espionage and warfare (Baskerville, 2010; Klimburg, 2017; Li et. al., 2018). One example of such espionage and warfare is the 2020 SolarWind sunburst cyber-attack where a foreign state actor gained control of critical US infrastructure (Datta, 2021). These technological developments are intricately linked to hacking abandoning its countercultural roots and becoming an established tradecraft used in government espionage, organized crime, and cyberwarfare. In the following sections, we explore this evolution in depth by analyzing the dominant themes on hacking.

5 The Thematic Evolution of Hacking

In the following, we analyze how themes on hacking have either changed or remained intact across the three evolutionary waves. We summarize the results in Table 8.

Table 8. Thematic Evolution of Hacking

	First to Second Wave	*Second Wave*	*Third Wave*
	1955-1989	1990-1999	2000-
Hacking as intrusion and crime	• Hacking is an intellectual challenge • Criminality is a biproduct of technology exploration and network intrusion • Benevolent hacking	• Hacking is becoming a viable profession • Criminality is dependent on intent (Black versus White hats) • Malevolent and benevolent hacking	• Hacking is a profession in either law enforcement or organized crime • Criminality based on hacking is increasingly being organized by third-party actors • Malevolent hacking
Hacking as creativity and learning	• Hacking is creative mastery • Continuous learning and development of new skills • Rebellion against established rules and norms through creative and ingenuity		
Hacking as politics and cyberwarfare	• Hacking is a tool supporting individual freedom • Anti-establishment • Using creativity to nurture freedom • Liberation from centralized power	• Hacking is a technoliberal tool used to fight oppression and ensure human rights • Anti-establishment • Revolution through technology use • Defensive hacktivism	• Hacking is a political power tool used by governments and NGOs alike • Anti- and pro-establishment support • Warfare using technology • Offensive hacktivism

5.1 Hacking as Intrusion and Crime

Intrusion and crime are two themes that run in parallel. Hacking as intrusion positions hacking as an intellectual challenge with the objective of breaching security and gaining access to third-party computer networks. This theme is described in detail in books written by former underground hackers, e.g. "The Art of Intrusion" and "Ghost in the Wires" (Mitnick & Simon, 2005; Mitnick, Wozniak, & Simon, 2011). Hacking as crime portrays underground hackers as organized criminals. Hackers are described as threats to society who should be prosecuted to the full extent of the law. This theme is outlined in large parts of the IS security literature (e.g., Auray & Kaminsky, 2007; Henrich et al., 2017; Hoffer & Straub, 1989; Kim & Kim, 2017; Mookerjee et al., 2011; Samtani et al., 2017; Smith et al., 2010; Warren & Leitch, 2010; Willison & Backhouse, 2006). Other examples of hackers as criminals come from books such as "Takedown" and "The Hacker Crackdown" written by prosecutors and network specialists who have hunted some of the most infamous hackers (Shimomura & Markoff, 1996; Sterling, 1992). Here, intrusion and crime are discussed side by side, although there are differences. Crime implies prosecution where a plaintiff brings a legal action and the defendant is convicted. Intrusion does not necessarily imply wrongdoing and conviction in a court of law. Because the differences are often subtle, the two themes are consolidated.

Our analysis shows that the two themes have been present in hacker communications across decades. These themes and related topics are heavily debated in relation to values of personal freedom and freedom of speech. Hackers have, for example, established guides on how to cope with and circumvent cybercrime legislation, and they have shared stories and experiences of having been convicted in courts of law.

The analysis also shows that many of the 1980s' underground hackers did not consider themselves criminals. They maintain that the difference between crime and intrusion lies in what motivates their behavior. They view hacking for profit or destruction as criminal acts. In their view, true hackers are benevolent because they search for knowledge and do not hack computer networks with profit in mind or with malevolent intentions. However, not everyone shares the sentiment and not everyone is motivated by the search for knowledge. For example, hackers have been convicted for "carding" (credit card fraud) since the 1980s, and there are early examples of credit card numbers being shared on BBS.

In the eyes of the law, the separation between intrusion and crime is inconsequential. Everyone using a phone or computer to access a system or network without permission is considered a criminal. The

inability to find a middle ground between crime and intrusion by hackers and legal authorities, followed by the hacker crackdowns in the early 1990s, resulted in resentment among hackers and direct opposition to the establishment and government policies. The hacker manifesto, first published in Phrack in 1986 under the title "The Conscience of a Hacker," epitomizes this anti-establishment view (Furnell et al., 1999). Later examples in Phrack and cDc build on and broaden this opposition to conventional social, political, and economic principles of society. As the hacker "White Ninja" writes:

> *"They have labeled everyone in the electronic community a potential criminal, and have cracked down on any kind of activity which has not met their standards. In doing so, they have crushed the free flow of ideas, trampled on the constitution, and blatantly encroached upon the civil rights of the people living and working on American computer networks."* (Phrack 1994)

The hacker crackdowns of the late 1980s and early 1990s had an unintended impact on the crime and intrusion theme. During the early 1990s, a lot of prominent and convicted hackers, such as members of The Legion of Doom (LoD), went into computer security consulting. Ironically, these hackers sought employment in the industry, which rose out of the security breaches they instigated. As the hacker known as Bloodaxe pointed out during CyberView 91—the traditional summer gathering of the American hacker underground:

> *"There was simply no future in it. The time had come for LoD to move on, and corporate consultation was their new frontier… We don't want to be flippin' burgers or sellin' life insurance when we're thirty."* (Phrack 1991)

This change from being part of the hacker underground to becoming security consultants impacted the hacker community. Hackers no longer constituted a homogeneous community of peers and during the 1990s labels such as white hats and black hats emerged to distinguish ethical hackers and security consultants from malicious hackers. The advent of the World Wide Web and the accessibility of technology, making it possible for *"any chump [to] buy access to the largest network in the world for $19.95 a month"* (Phrack 2000), led to increased tensions between intrusion and crime and a shift in the underground hacker community. This resulted in a changing perspective on hacking from *a way of living* to *making a living*. As one hacker wrote in the early 2000s:

> *"Everyone who was a real part of the hacking/phreaking scene—at one point or another decided they'd rather make money being legit than risk legal troubles and wrecking their future for nothing. Myself included."* (Phrack 2000)

Consequently, the computer security industry became professionalized. From the 2000s and onward, the black hats (including organized crime syndicates) saw potential in using the knowledge created by earlier hacker generations to generate profit through destructive behavior and by wreaking havoc. By contrast, the white hats generated profit through corporate consulting and by some accounts betrayed their ethos by collaborating with law enforcement and in some instances even becoming part of it. In a sense, *"computer crime and hacking have always made for uncomfortable bed fellows"* (Phrack 2010). Whereas criminals use technologies of the hacker underground (e.g., encryption, filesharing, and blockchain) as a basis for their scams and illegal activities, hackers are outlaws who use technology ingeniously to challenge conventional wisdom and the status quo. Sometimes hacking and the associated technologies are used for purely criminal purposes. For example, phishing was originally about social engineering and hackers exploiting how people behave, and ransomware builds on various technologies that were once associated with the hacker underground. These associations make it increasingly hard to separate hacking from computer crime in mass media, legislation, and legal proceedings.

5.2 Hacking as Creativity and Learning

The creativity and learning theme has roots in the early days of the personal computer (Graham, 2004; Isaacson, 2011; S. Levy, 1984; Turkle, 1984; Williams, 2002). The theme describes hacking as an activity that results in learning through creativity which "pushes the limits of technology" (Conti 2006, p. 33). For the same reason, hacking is associated with current innovation practices that originate in the Free Software Movement (Lin, 2007) and the Makerspace Movement (Davies, 2017). As noted by Flowers (2008), hackers are often end-users who pose challenges for companies and policy-makers, because they are not concerned with copyrights and patents. Instead, they are motivated and intellectually stimulated by tinkering and experimenting with existing products and technologies in the pursuit of innovation (Schulz & Wagner, 2008).

The theme manifests itself across different evolutionary periods. Hacking network security was initially not about stealing information or wreaking havoc. Instead, the hackers of the 1980s broke into computer systems to learn more about them. As one hacker from the 1980s wrote:

> *"Hacking into any system is illegal, so try to use remote dial-ups to do the job. Remember do not abuse any systems you hack into for a true hacker doesn't like to wreck, but to learn."* (Phrack 1988)

In agreement with Levy's (1984) observations, the network security hackers of the 1980s were heavily inspired by the hackers of the counterculture of the 1960s and 1970s. The hackers of the 1980s saw themselves as part of a larger "techno-revolution" (Phrack 1986) in which technological innovation is driven by hackers wanting to *"learn"* and *"satisfy their curiosity"* (cDc 1988). The learning aspect of the theme is clearly displayed in the hacker manifesto (Phrack 1986) which characterizes the hacking of network security as an intellectual challenge rather than an illegal activity. The manifesto also criticizes the school system for being conventional and tedious: *"This is our world now... the world of the electron and the switch, the beauty of the baud"* and *"Yes, I am a criminal. My crime is that of curiosity"* (Phrack 1986). In this view, hacking is an act of creativity and experiential learning, and hackers belong to a new class in an emerging techno-social order.

The theme on creativity and learning has changed very little over time and the espoused values have remained stable despite some hackers leaving the underground for jobs in the computer security industry and the community closing in on itself due to crackdowns by law enforcement in the late 1990s and early 2000s. Thus, the theme is relatively stable across time periods and constitutes an anchor in the underground hacker community. The hacker manifesto, for example, has been reprinted in various formats over the years and again in 2016. Moreover, we found a variety of articles from the early 2000s and onward that remind community members and the surrounding society of the creative and learning aspects of hacking. As one hacker writes:

> *"So, let's use the word hacker here to mean what we know we mean, because no one has invented a better word. We don't mean script kiddies, vandals, or petty thieves. We mean men and women who do original creative work and play at the tip of the bell curve, not in the hump. We mean the best and brightest who cobble together new images of possibility and announce them to the world. Original thinkers. Meme makers. Artists of pixels and empty spaces."* (Phrack 2013)

Such statements may very well have been written in response to the growing problem within the hacker community of younger hackers (known as script kiddies) using scripts or programs developed by others to attack computer systems and breach security networks. This practice is considered of little worth by technically proficient hackers, and it also tends to attract the attention of law enforcement. Hence, reminding younger generations of hackers of the values of creativity, learning, and individuality serves the purpose of teaching younger hackers entering the community about the social norms of acceptable behavior while reminding older hackers of the responsibility to share their knowledge. Moreover, network security hackers have for many years been stigmatized and likened to criminals and even terrorists (e.g., Sterling, 1992; Shimomura & Markoff, 1996). Reminding themselves and each other that being a hacker is about *"individuality, curiosity, and creativity"* (Phrack 2016) is also an attempt to offer an alternative to their portrayal in mass media. Hacking as an act of creativity and learning still dominates despite many hackers of the counterculture having joined forces with the computer industry. Hackers have a long history of being first movers and early adopters of technology and pushing its development forward by adapting it to novel purposes, which in turn makes it attractive to the masses despite resistance from policy-makers, existing business models, and social norms. Such examples are evident in the development of the personal computer in the late 1970s, the use of file sharing technologies in the early 1990s, and the impact of blockchain technologies on data security and the financial system from 2008 and onward. The common denominator is the early technology adoption of hackers and the ensuing controversy and skepticism by the public before widespread diffusion and adoption across society.

5.3 Hacking as Politics and Cyberwarfare

The third theme is that of politics and cyberwarfare. The politics of hacking has been studied extensively (e.g., Coleman, 2011; Davies, 2017; George & Leidner, 2019; Jordan & Taylor, 2004; Lindgren & Lundström, 2011; Olsen, 2013; Taylor, 2005). Extant research portrays some hackers as politically

engaged (e.g., Davies, 2017; Jordan & Taylor, 2004), with hacking increasingly being used by both activist groups and nation states to influence policy-making or procure classified information (George & Leidner, 2019; Jordan & Taylor, 2004; Klimburg, 2017; Shackelford, 2009). As Baskerville (2010) argues, the idea of cyberwarfare is not particularly new, as the internet itself was conceived as a resilient network capable of withstanding attacks. However, Stuxnet and the 2009 Denial of Service attack of the Estonian national infrastructure have made nation states painfully aware of the importance of having both defensive and offensive cyber capabilities (Farwell & Rohozinski, 2011; Shackelford, 2009). Using computers in warfare entered public consciousness with the movie "War Games" from 1982, which is about a young hacker who accesses and triggers AI-based defense systems nearly sparking a nuclear war. The movie presents a nightmare scenario in which a hacker takes control of critical infrastructure and weapon systems. However, the 1980s' hackers had little interest in doing so, being more interested in using technology to liberate themselves and fight centralized power. As the hacker known as "Psychotic Opposition" writes in a political statement:

> *"Unscrupulous, greedy, money and power seekers have dominated our lives and earth for too long and today is the day for each of us to put forth all of our efforts to liberate ourselves and our human family and our earth from the destructive exploitative slavery we live under."* (cDc 1987)

Contrary to Davies (2017), who found that hackers in Makerspaces were apolitical, our analysis reveals that the underground hackers of the 1980s and 1990s were overtly political in their statements and writings. They often articulated anti-government, anti-war, anti-religious, anti-establishment, and environmentally conscious sentiments, and advocated a society free of prejudices and censorship. As such, there is a clear link between how underground hackers view politics and cyberwarfare and how the counterculture preceding them viewed it. As the hacker known as "Swamp Rat" writes in cDc Communications: *"Most of the people in the group tend to be 'liberal' oriented, and many of our files have a political or social message in them."* The political statements range from in-depth analyses of societal problems and government policies to political rants, e.g., characterizing Ronald Reagan as a *"stupid senile old jackass"* (Phrack 1987) and denouncing authorities through statements like: *"I'll wipe my butt with all your flags! I'll drain my bladder on your Bible, your Koran, your fucking manifestos! But I'll keep the Bill of Rights and shove it up your ass!"* (cDc 1988). We also identified accounts of underground hackers voicing such opinions in public, for example, by crashing a Christian rally with signs stating: *"Jesus was a homo!"* and *"Noah's Ark = Bestiality Boat"* (cDc 1995). When combining these findings, the political and cyberwarfare theme shares many characteristics with technoliberalism (Fish, 2017), including an emphasis on technology as the main driver toward personal freedom. However, the hacker underground is also centered around strong anti-establishment sentiments and support for human rights.

By the mid-1990s, the hacker known as Omega summarized the cDc's political ideology and action in one word—*"hacktivism"* (cDc 2004)—which is defined as *"using technology to improve human rights across electronic media"* (cDc 2004). According to the cDc, hacktivism is not about defacing websites or Denial of Service attacks. As another cDc member, Oxblood Ruffin, wrote, such attacks are carried out by *"low-rent computer criminals"* and *"script kiddy antics in drag"* (cDc 2004). Instead, hacktivism is about creating technologies that grant a voice to people in countries where freedom of speech is restricted. Despite its original definition, hacktivism has been adopted by activist groups with no scruples about using less sophisticated hacker tactics to get their message across. Members of the underground hacker community are, however, rarely part of such hacktivist groups. On the contrary, they often distance themselves from such activities. In Phrack Magazine, hacktivism is described as *"poor man's hacking"* (Phrack 2010) and even less flattering words are used when criticizing the inability of, e.g., Anonymous to remain anonymous:

> *"As the RIAA and MPAA attacks showed us, Anonymous ain't so anonymous when they plan their attacks in the open, in front of feds, on 4chan and Darknet."* (Phrack 2010)

However, there is a pattern to the political values of the hacker underground and attitude toward hacktivism over time. With regard to cDc, there is a noticeable change from discussing issues related to freedom of speech to advocating political activism with an impact on policy-making. This change coincides with governments' interests in the capabilities of hackers, which has increased to the point where intelligence services hire and educate network security hackers to strengthen both their defensive and offensive capabilities in cyberspace (known as cyberwarfare) (e.g., Andress & Winterfeld, 2014). As argued by Farwell and Rohozinski (2011; 26), *"nearly every significant cyber event reported since 2005 involves knowledge, techniques, and code tied to the cyber-crime community."* Moreover, hackers have

known for a long time that governments are fighting them publicly while using their tools and knowledge behind the scenes to strengthen their own intelligence services.

The earliest account of intelligence services using underground hackers for espionage is in 1986 when an East German hacker penetrated United States military systems and sold the information obtained to the KGB (Stoll, 1988). The story is revealed in Phrack issue 25. In the same issue, there is anecdotal evidence of German counter-intelligence unsuccessfully attempting to recruit Steffen Wernery and other members of the Chaos Computer Club in the mid-1980s. This shows government interest in the hackers on account of their skills and not only because of their criminal offences as early as the 1980s. As described in relation to the creativity and learning theme, the professionalization of parts of the underground hacker community and the proliferation of hacker tools and knowledge by the mid-1990s caused a rift in the underground hacker community. This rift resulted in changes to the political values. The computer security industry values assets over personal freedom, secrecy over openness, and they built on the tools and knowledge of hackers in support of government-sponsored espionage, cyberwarfare, and restrictions on freedom of speech. Meanwhile, members of the hacker underground have grown in their political awareness. In an interview with Wired Magazine (McKay, 1998) which was later reprinted in Phrack, Oxblood Ruffin (cDc member) explained the evolution from hackers to hacktivists:

> *"When the Cult of the Dead Cow was started in 1984, the average age [of our members] was 14, and they spent their time hacking soda machines … But the last couple of years has marked a turning point for us. Our members are older, politicized, and extremely technically proficient."* (Phrack 1998)

Hence, the evolution of hacker politics is firmly grounded in the ideals embedded in the counterculture, and this evolution led to two competing views of hacktivism. The dataset shows that the early view (1996+) originated in the community around cDc during the second evolution (1979-2000) whereas the later view (2004+) was associated with activist groups that emerged from the underground hacker community during the third evolution (2001-).

The early view focuses on hacktivism as a technology arms race. The espoused goal is to create defensive countermeasures against state-sponsored restrictions on freedom of speech. It does not, however, imply an offensive strategy, because *"one cannot legitimately hope to improve a nation's free access to information by working to disable its data networks"* (cDc 2004). Rather, this view of political activism implies a defensive strategy by operating within the boundaries of the law and by providing tools to counter censorship and encroachments on free speech. This early view of defensive hacktivism is publicly supported by hacker groups such as the cDc and the Chaos Computer Club. By the late 1990s, members of the cDc worked closely with a hacktivist group known as the Hong Kong Blondes to counter state-sponsored surveillance in China and help free speech advocates escape the country (cDc 1998).

The later view is about hacktivism as an offensive countermeasure against national tyranny and international anarchy in the sense of nation states professionalizing hacking, weaponizing technologies, and using both against their own citizens and other nation states. This view implies warfare by means of existing hacker tools and knowledge in launching cyberattacks against government websites, disclosing classified information, and engaging in public protests and practices of misinformation. As evidenced by our findings, this view of offensive hacktivism is an interpretation and adaptation of the early view of hacktivism, but used by political activists outside the underground hacker community. Activist groups such as Anonymous, Antisec, and WikiLeaks show support for this view when using existing hacker tools to carry out cyberattacks or disclosing classified information with more or less clearly defined political agendas in mind.

6 Discussion

Underground hackers are heterogeneous groups of idealists, rebels, pranksters, entrepreneurs, innovators, and social misfits. The hacker underground is—by virtue of being an online community—made up of people from many walks of life with different motivations and agendas (Beveren, 2000; Holt & Strumsky, 2012; Jordan & Taylor, 1998; Klimburg, 2017). On the basis of this premise, we explore the history of hacking and how different evolutionary periods, societal changes, and technology developments have influenced hacking, leading to the professionalization of the hacker underground. Summarizing our findings, we conclude that two themes, namely intrusion and crime as well as politics and cyberwarfare, have changed significantly over time and led to increasing professionalization of hacking. A third theme on

learning and creativity has remained relatively stable. This increasing professionalization of hacking point to unanswered research questions related to IS security, innovation, and policy in this area.

For the purpose of presenting and discussing the new research opportunities, we exemplify the professionalization of hacking by identifying personas of IS professionals that manifest themselves in the empirical data (Table 9). By personas, we mean stereotyped hacker types that transform discursive themes into personal characteristics (e.g., Miaskiewicz & Kozar, 2011; Turner & Turner, 2011). These personas are each other's counterparts by virtue of being either white or black hat hacker types. Whereas the network security specialist (e.g., Dey et. al., 2012), digital innovator (e. g., von Hippel & Paradiso, 2008), and digital warfighter (e.g., Baskerville, 2010) are white hats; the criminal IT professional (e.g., Pogrebna & Skilton, 2019), outlaw innovator (e.g., Flowers, 2008), and digital activist (e.g., Olsen, 2013) are black hats. The network security specialist is the counterpart of the criminal IT professional, the digital innovator is the counterpart of the outlaw innovator, and the digital warfighter is the counterpart of the digital activist.

Table 9. Black and White Hat Personas of IS Professionals

Hacker type	Persona	Consolidated theme	Professional role	Empirical examples from the literature and datasets
White hat	Network security specialist	Intrusion and crime	Building defensive capabilities to prevent cyberattacks and espionage against critical infrastructures in private and public organizations	During the early 1990s, former hackers switch side and become security consultants, establishing a new industry around the problem they created
	Digital Innovator	Creativity and learning	Creating technological innovation within socially accepted norms and legal frameworks	During the late 1970s, former "phone phreaks" become founders of Apple and invent the first mass-produced personal computer
	Digital warfighter	Politics and cyberwarfare	Taking defensive and offensive actions against enemy combatants from nation states or non-governmental activist groups	From the mid-1980s, intelligence services recruit known hackers and use hacking for surveillance and cyber-attacks (e.g., Stuxnet). Lately, intelligence services hire and train people for cyberwarfare purposes
Black hat	Criminal IT professional	Intrusion and crime	Building and using offensive capabilities for personal monetary gain	During the late 1990s, hackers offer hacking-for-hire and botnet services. By the 2010s and forward, tools and knowledge from the hacker underground are increasingly being used by organized crime in blackmailing and online scams
	Outlaw innovator	Creativity and learning	Creating technological innovation outside socially accepted norms and legal frameworks	During the late 1960s, a hacker used a flute from a cereal box to mimic the 2600 hertz tone used by the AT&T telephone system, enabling free long-distance phone calls
	Digital activist	Politics and cyberwarfare	Defensive or offensive actions against nation states and other non-governmental organizations or actors	During the late 1990s and early 2000s, Members of cDc participated in developing defensive capabilities against censorship and government surveillance. In 2010, Wikileaks disclosed classified information as an offensive action against the US government

The mentioned professionalization entails hackers transforming themselves and their practices from some to other of the mentioned stereotyped archetypes. Based on our analysis and this first step toward theorizing personas, we propose the following four propositions as listed in Table 10.

Table 10. Propositions

#	Proposition	Evidence	Contrast in persona
1	Professionalization of hacking will push criminal hackers toward legal and illegal employment	Our analysis shows that hackers from the second wave started out with criminal activities. But as they got older, they went into private security consulting. However, we also found the criminal hackers have increasingly been professionalized since the 1990's	Network security specialist vs. criminal IT professional
2	Institutionalization through legal or illegal employment is a catalyst for further professionalization of hacking	Our analysis shows that the professionalization of hacking is increasing over time. This is evident through the increased professionalization of skills and tools from the mid-1990's to today	Network security specialist vs. criminal IT professional Digital Innovator vs. outlaw innovator
3	Through legal employment, hackers influence organizational culture and in turn innovation management practices through values of creativity, learning, and individuality	Our analysis shows that the hacker mindset is one of curiosity and creativity and can be of great value to organizations if utilized mindfully	Digital Innovator vs. outlaw innovator
4	Hacking will be increasingly weaponized	Our analysis shows that after the 2000's, hacking is increasingly used to achieve political goals	Digital warfighter vs. digital activist

In the following, we build on these personas and propositions in carving out a new agenda for IS security, innovation, and policy research. We do this by contrasting the literature associated with the identified black and white hat personas. Our discussion is summarized in Table 10.

First, Muzio, Brock, and Suddaby (2013, p. 705) argue that professionalization is a form of institutionalization by documenting "the concomitance of professionalization and institutionalization processes". Combined with our analysis pointing to an increasing professionalization of hacking, this institutionalist perspective leads us to suggest that the hacking is not only being professionalized but also institutionalized through, e.g., legal and illegal employment of hackers (proposition 1), but that this process has self-reinfocing effects leading to further professionalization (proposition 2). We invite future research to investigate this institutionalization-professionalization link through longitudinal studies of hacking across industries as well. Such an investigation may include an institutionalist perspective on "actions through which individual and collective actors – such as [hackers] – attempt to disrupt, maintain, or create institutions" Muzio, Brock, and Suddaby (2013, p. 700). From an institutionalist perspective, we also speculate that hackers through their employment influence organizational culture and innovation management practices (proposition 3). This influence may lead to existing values and professions being contested, simply because hackers as an so-called information profession "are, by definition, involved in continuously negotiated and contested professional divisions of labor" (Abbott, 1988: CHAPTER 8). We therefore welcome future research that investigates how established professions, e.g., within the security industry, are challenged and evolve alongside hackers as they join the ranks of employees.

Second, Lowry et al.'s (2017) recent call for a bolder IS security research agenda implies that security and privacy issues should be investigated beyond intentions of perpetrators, drawing on theories and concepts from other disciplines. IS has a tradition for drawing on reference disciplines in investigating and deriving implications for IS topics (e.g., Willison, Lowry, et al., 2018). By drawing on literature from sociology (e.g., Jordan & Taylor, 1998; Turkle, 1984) and psychology (e.g., Beveren, 2000) in further investigating the personas of the "network security specialist" and "criminal IT professional," new insights into the professionalization of crime and security may be generated. Even though the IS security literature uses extant theory for theory building (D'Arcy et al., 2009; Willison, Warkentin, et al., 2018), it lacks systematic reviews of extant literature that can generate new insight through novel theory building (for elaboration, see Webster and Watson 2002). Such new insights can come from social psychology (e.g., Kabay et al. 2012) to neuroscience (e.g., Hu et al. 2015) and provide the field with new opportunities for research, such as novel means of profiling IT criminals (e.g., Rogers 2003) and identifying emerging IT career paths in- and outside legal boundaries (e.g., Auray and Kaminsky 2007). Moreover, rising trends such as big

data and blockchain also affect how criminals and security specialists use technology. Such trends are especially interesting, because they influence the formal and informal economies. Whereas security specialists operate within the formal economy under rules and legislation, hackers often operate within the informal economy (e.g., dark web platforms) where boundaries are blurred and ambiguous (for elaboration, see Webb et. al., 2009). Such cross-boundary activities have a firm basis in the extant literature that attempts to understand the evolution of social movements and activism (Bevington & Dixon, 2005; Koopmans, 2005; Levy, 2010). Comparative case studies (Bryman, 2004; Yin, 2003) that explore the relationships between different types of hacking (e.g., defensive vs. offensive) and how they impact combinations of technology trends can provide new insight to how such trends influence organizational security behavior and give rise to new challenges such as money laundering and criminal supply chains or social movements with criminal intent such as politicized hacker communities.

Third, the “digital innovator” and “outlaw innovator” personas call for more IS innovation research. Hacking as a concept has been adopted by the innovation management discipline in investigating, e.g., lead user innovation (e.g., Flowers, 2008; Von Hippel & Paradiso, 2008). Similarly, the hacker underground community has inspired Free / Libre Open Source Software (FLOSS) communities (e.g., Raymond, 1999), the Maker Movement (e.g., Davies, 2017; Hatch, 2013), and biohacking (Tocchetti & Aguiton, 2015). However, contrary to socially acceptable forms of hacking by the “digital innovator,” as manifested in the FLOSS (Bretthauer, 2002; Raymond, 1999) and the Maker Movement (Davies, 2017; Hatch, 2013), underground hacking by the “outlaw innovator” is carried out in secrecy, away from prying eyes, because the activities and underlying motives are not aligned with widely accepted means of politicking and pursuit of interests (e.g., Flowers, 2008; Schulz & Wagner, 2008). Future research should investigate the validity of these personas, the part played by such actors in shaping the formal and informal economies (e.g., Webb et al. 2009), and the way in which they use new and emerging technologies to achieve their ends (e.g., Flowers 2008). Such research may involve historical analysis (Porra et al., 2014) of new technology trends such as blockchain where hackers have played a role in technology development and dissemination from informal to formal economies. Specifically, it may entail investigating the interplay between technology development, hackers searching for exploits and vulnerabilities, and organizations building up their defensive capabilities both re- and proactively, and how this interplay stimulates innovation. Research questions include: To what extent are there useful spinoffs for non-security related technologies, and how can organizations take advantage of these? What are the effects on competitive advantage of software or non-software firms from such innovation?

The research may also include the identification of new entrepreneurial careers (e.g., Dyer 1995) in the digital economy and the impact of technological innovation in the context of the informal economy (i.e., outlaw innovation) on intellectual property rights and policy making (e.g., Flowers 2008). The interplay between outlaw innovation and IS innovation in organizations is an unexplored IS research topic, and yet this interplay may be important to some organizations' innovation strategy. Comparative historical analysis (e.g., Mahoney and Rueschemeyer 2003) of innovations emerging from informal economies can help researchers challenge conventional innovation processes, product development, and business models, but it may also point to new mechanisms of technology transfer between the informal and formal economies.

Fourth, governments' active role in hacking presents new research opportunities. In agreement with, e.g., Klimburg (2017) and Farwell and Rohozinski (2011), we see evidence of governments trying to depict hacking as digital crime while legitimizing their own use of hacker tools and knowledge in bolstering national defenses and cyberwar capabilities (Proposition 4). Cyberattacks such as those associated with Stuxnet and the Estonia national infrastructure demonstrate the capabilities of nation states and their use of offensive hacktivism to weaken adversaries, crippling or interfering with their ability to act (e.g., Farwell & Rohozinski, 2011). The recent Ukraine conflict have also proven that kinetic war increasingly happens side-by-side with war in cyberspace – both for intelligence gathering as well as propaganda. Hence, simply equating hacking with crime hides a greater threat to modern institutions and organizations—both public and private. The distinction between the “digital warfighter” and “digital activist” personas opens for new research focusing on, e.g., ethics and legal issues (Lowry et al., 2017). Future research may provide valuable insights into the evolution of cyberterrorism and cyberwarfare by approaching it from a political perspective. Such studies may deploy formal theories and statistics (e.g., Bryman 2004) in theorizing the future of digital warfare and providing new insights into defensive and offensive cyberwar strategies. Moreover, the roles, legal issues, and ethics of NGOs and nation states with regard to defensive and offensive hacktivism should also be investigated, although this is likely to present significant methodological and practical challenges. However, such research could but is not exclusive to the use of

historical analysis of archival data (e.g., Nielsen et al. 2014), for example on the events surrounding the Arab spring rebellion. This research is urgently needed and may help raise awareness and identify countermeasures for defending critical social institutions (e.g., election and financial systems). It may also point to needs for policy development in a digital era.

Table 11. An IS Research Agenda Grounded in Hacker Personas

Contrasting personas	Consolidated theme	Research opportunities	Potential research paths	Potential research implications
Network security specialist versus Criminal IT professional	Intrusion and crime	How can related literature streams such as sociology and psychology inform studies of the professionalization of crime and security?	Systematic review and analysis of relevant literature in different academic traditions for theory building	• Improving cybercrime profiling including identification of new IT career paths in- and outside legal boundaries • Improving means of criminal deterrence in IS organizations
		How do trends affect how criminals and security specialists professionalize IT in formal and informal economies?	Comparative case studies of technology trends and developments over time, on the one hand, and types of hacking on the other	• Discovering impacts of security technology trends and changes to organizational security behavior • Identifying challenges to transnational crime including money laundering and new supply chains
Digital Innovator versus Outlaw innovator	Creativity and learning	What role does underground entrepreneurs play in the formal and informal economies?	Historical analysis of the genesis of technology, its impact on the economy, and the role of hackers	• Identifying new entrepreneurial careers in the digital economy • Influence from informal economies on formal economies including impact on intellectual property rights and new policy making
		What is the interplay between formal innovation in IS organizations and outlaw innovation in the hacker underground?	Comparative historical analysis of innovations that have emerged from the hacker underground and related innovations in industry and society	• Discovering novel ways of working with IS innovation including challenges to traditional innovation processes, product development, and business models • Identifying new channels of technology transfer between informal and formal economies
Digital warfighter versus Digital activist	Politics and cyberwarfare	How can IS inform studies on the evolution of cyberterrorism and cyberwarfare?	Formal theory and statistics that demonstrate causal relationships and provide theory for new strategies	• Insights into the future of warfare and digital warfighters • Development of offensive cyberwar strategies (e.g., Hacking back)
		How can IS inform studies on the legality and ethics of defensive and offensive hacktivism when used by NGOs or nation states?	Historical analysis based on archival data	• Development of digital countermeasures in critical social institutions • Future requirements for digital policy making

A word of caution: Although the personas we present here provide examples of the professionalization of hacking, simply labeling them as “network security specialists,” “criminal IT professional,” “digital innovator,” “outlaw innovator,” “digital warfighter,” and “digital activist” is an oversimplification when trying to describe the colorful and varied community of underground hackers. The personal journey of these hackers, their learning outcomes, and the wider implications for organizations and society at large are worth investigating. Such research may shed light on how careers change over time and what behavioral

changes they entail. Questions for future research include: How do hackers' careers evolve over time? To what extent do hackers drift, on the one hand, between stable jobs and freelance work and, on the other hand, between crime and legal employment? To what extent do hacker behaviors change when moving into a corporate position? It is also worth investigating what motivates hackers who end up working for private companies vis-à-vis governmental institutions. Knowing more about the motivational drivers may, among other things, help organizations recruit hackers as future employees Such research can be carried out by asking: What are the differences between hackers that work for industry and government?

Our content analysis reveals hacking as a phenomenon that has been translated into multiple meanings in the pasts and will likely be translated into new meanings in the future. By implication, we demonstrate that ideas, including those associated with technology and its use, travel and are translated as they move across social arenas and time (e.g., Nielsen et. al. 2014; Ulrich et al., 2015). We show that "hacking is adopted, adapted, and repurposed" as an idea or practice by private businesses and government institutions alike (Söderberg and Delfanti 2015, p. 794). In this process, there is risk of misinterpretation and faulty translation when trying to emulate hacker practices for innovation purposes in public and private organizational settings without adapting the underlying values of the underground hacker community. Such translations warrant further investigation. In the preceding, we use different hacker personas (Table 9) to suggest an IS research agenda (Table 10) that takes the need for such translation into account. This agenda includes important questions about security, crime, innovation, and society that future IS research should translate into practical implications. Although we have suggested that such research may draw on reference disciplines in investigating hacking and deriving implications for IS (e.g., Willison, Lowry, et al., 2018), we and others should be mindful of the limitations of our suggestions. First, these suggestions do not account for the full range of issues and possibilities that this important topic suggests. Second, discipline-agnostic, inductive studies of the grounded theory type are also needed. Relying too heavily on reference disciplines may lead to our reinventing the proverbial wheel and experiencing the horseless carriage syndrome (understanding the car from prior knowledge of the horseless carriage), i.e. failing to generate new insights because we limit ourselves to, e.g., tried and tested innovation management theories (akin to the horseless carriage) in our efforts to understand novel hacking practices (the car). Similar arguments are made for closer engagement with the field when investigating other new and emerging topics like digital innovation (Gkeredakis & Constantinides, 2019).

We contribute to the ongoing discussion of cybercrime and cyberwarfare in IS security research (e.g., Baskerville 2010; Mahmood et al. 2010) by highlighting differences between discursive practices—and by all accounts the *real* practices—of underground hackers and external stakeholders like nation states, organized crime, and activist groups. We call for more research into state sponsorships, professionalization of network security hacking, and its impact on public discourse and policy-making (e.g., Auray & Kaminsky, 2007; Shackelford, 2009). Of particular interest is the knowledge transfer (e.g., Agrawal, 2001; Caloghirou et. al., 2004) from the underground hacker community to other industries and governments.

We also contribute to the IS innovation literature by emphasizing the role of rebellious versus structured innovation processes and the relationship between the informal and formal economies. Hacking and innovation are related but different activities. Whereas hacking is chaotic and rebellious in nature and carried out through collaboration in loosely connected networks (e.g., Holt & Strumsky, 2012; Nikitina, 2012), innovation is dominated by well-defined processes within and across organizational boundaries (e.g., Couger, 1996; Osterwalder & Pigneur, 2010). Several attempts have been made at copying hacker practices in different government, corporate, and social settings (Flowers, 2008; Irani, 2015; Lindtner, 2015). We speculate that hacking as an innovation process in modern organizations is likely to be translated into multiple and diverse professional practices that either challenge existing innovation practices or are watered down and aligned with existing corporate or public values. For example, hackathons are widely used by universities and private companies (Irani, 2015) but are often associated with rapid prototyping rather than actual hacking. This agenda takes the values of the underground hacker community into account when exploring how hacking can contribute to innovation and value creation across public and private organizations.

7 Conclusion

In conclusion, this research article contributes valuable insights into the hacker underground, and how hacking has evolved, been interpreted, and contributed to the professionalization of hacking. Our content analysis adds to state-of-the-art knowledge of hacking by contrasting the themes that emerge from the

underground with the discursive constructions of hacking by external stakeholders. Even though our empirical data are limited to underground hackers (and do not cover software pirates and other hacker communities), our article fosters a greater understanding of the complexity of hacking that may serve as inspiration for IS studies that address cyber security, innovation, and public policy. We hypothesize that the professionalization of hacking will continue in the future, and more research is needed to understand the implications of the evolution of hacking.

Acknowledgments

The authors would like to thank the reviewers and editors of the Communications of the Association for Information Systems, who all participated with great feedback and ideas for the development of this paper.

References

Abbott, A. (1988). *The System of Professions: An Essay on the Division of Expert Labor*. Chicago and London: The University of Chicago Press.

Agrawal, A. (2001). University-to-Industry Knowledge Transfer: Literature Review and Unanswered Questions. *International Journal of Management Reviews*, *3*(4), 285–302. https://doi.org/10.1111/1468-2370.00069

Anderson, C. (2009). *Free: The Future of a Radical Price*. London, UK: Random House.

Anderson, C. L., & Agarwal, R. (2010). Practicing Safe Computing: A Multimethod Empirical Examination of Home Computer User Security Behavioral Intentions. *MIS Quarterly*, *34*(3), 613–643. https://doi.org/10.2307/25750694

Andress, J., & Winterfeld, S. (2014). *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners* (2nd ed.). Waltham, MA: Elsevier.

Auray, N., & Kaminsky, D. (2007). The Professionalisation Paths of Hackers in IT Security: The Sociology of a Divided Identity. *Annales Des Telecommunications-Annals of Telecommunications*, *62*(11–12), 1312–1326. https://doi.org/10.1007/BF03253320

Baskerville, R. (2010). Third-Degree Conflicts: Information Warfare. *European Journal of Information Systems*, *19*(1), 1–4. https://doi.org/10.1057/ejis.2010.2

Benjamin, V., Zhang, B., Nunamaker, J. F., & Chen, H. (2016). Examining Hacker Participation Length in Cybercriminal Internet-Relay-Chat Communities. *Journal of Management Information Systems*, *33*(2), 482–510. https://doi.org/10.1080/07421222.2016.1205918

Beveren, J. Van. (2000). A Conceptual Model of Hacker Development and Motivation. *Journal of E-Business*, *1*(2), 1–9. https://doi.org/10.1.1.586.3584

Bevington, D., & Dixon, C. (2005). Movement-Relevant Theory: Rethinking Social Movement Scholarship and Activism. *Social Movement Studies*, *4*(3), 185–208. https://doi.org/10.1080/14742830500329838

Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., & Polak, P. (2015). What Do Systems Users Have to Fear? Using Fear Appeals to Engender Threats and Fear that Motivate Protective Security Behaviors. *MIS Quarterly*, *39*(4), 837–864. https://doi.org/10.25300/misq/2015/39.4.5

Bretthauer, D. (2002). Open Source Software: A History. *Information Technology and Libraries*, *21*(1), 3–10. https://doi.org/No DOI

Bryman, A. (2004). *Social Research Methods* (2nd ed.). New York: Oxford University Press.

Busch, O., & Palmås, K. (2006). *Abstract Hacktivism: The Making of a Hacker Culture*. London: Lightning Source.

Caloghirou, Y., Kastelli, I., & Tsakanikas, A. (2004). Internal Capabilities and External Knowledge Sources: Complements or Substitutes for Innovative Performance? *Technovation*, *24*(1), 29–39. https://doi.org/10.1016/S0166-4972(02)00051-2

Coleman, G. (2011). Hacker Politics and Publics. *Public Culture*, *23*(3 65), 511–516. https://doi.org/10.1215/08992363-1336390

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

Conti, G. (2006). Hacking and Innovation. *Communications of the ACM*, *49*(6), 33–36. https://doi.org/10.1145/3262852

Couger, J. D. (1996). *Creativity & Innovation in Information Systems Organizations*. Danvers, MA: Boyd & Fraser.

Cusumano, M. A., & Selby, R. W. (1997). How Microsoft Builds Software. *Communications of the ACM*, *40*(6), 53–61. https://doi.org/10.1145/255656.255698

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach. *Information Systems Research*, *20*(1), 79–98. https://doi.org/10.1287/isre.1070.0160

Datta, P. (2021). Hannibal at The Gates: Cyberwarfare & The Solarwinds Sunburst Hack. *Journal of Information Technology Teaching Cases*, *March*. https://doi.org/10.1177/2043886921993126

Davies, S. R. (2017). Characterizing Hacking: Mundane Engagement in US Hacker and Makerspaces. *Science, Technology, & Human Values*, *43*(2), 171–197. https://doi.org/10.1177/0162243917703464

Deek, F. P., & McHugh, J. A. M. (2008). *Open Source: Technology and Pollicy*. New York, USA: Cambridge University Press.

Dey, D., Lahiri, A., & Zhang, G. (2012). Hacker Behavior, Network Effects, and the Security Software Market. *Journal of Management Information Systems*, *29*(2), 77–108. https://doi.org/10.2753/MIS0742-1222290204

Dobusch, L., & Schoeneborn, D. (2015). Fluidity, Identity, and Organizationality: The Communicative Constitution of Anonymous. *Journal of Management Studies*, *52*(8), 1005–1035. https://doi.org/10.1111/joms.12139

Dyer, W. J. (1995). Toward a Theory of Entrepreneurial Careers. *Entrepreneurship Theory and Practice*, *19*(2), 7–21. https://doi.org/10.1177/104225879501900202

Farwell, J. P., & Rohozinski, R. (2011). Stuxnet and the Future of Cyber War. *Survival*, *53*(1), 23–40. https://doi.org/10.1080/00396338.2011.555586

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

Fitri, N. (2011). Democracy Discourses through the Internet Communication: Understanding the Hacktivism for the Global Changing. *Online Journal of Communication and Media Technologies*, *1*(2), 1–20. https://doi.org/10.29333/ojcmt/2332

Flowers, S. (2008). Harnessing the Hackers: The Emergence and Exploitation of Outlaw Innovation. *Research Policy*, *37*(2), 177–193. https://doi.org/10.1016/j.respol.2007.10.006

Furnell, S., Dowland, P. S., & Sanders, P. W. (1999). Dissecting the "Hacker Manifesto." *Information Management & Computer Security*, *7*(2), 69–75. https://doi.org/10.1108/09685229910265493

George, J. J., & Leidner, D. E. (2019). From Clicktivism to Hacktivism: Understanding Digital Activism. *Information and Organization*, *29*(3), 100249. https://doi.org/10.1016/j.infoandorg.2019.04.001

Gkeredakis, M., & Constantinides, P. (2019). Phenomenon-Based Problematization: Coordinating in the Digital Era. *Information and Organization*, *29*(3), 100254. https://doi.org/10.1016/j.infoandorg.2019.100254

Graham, P. (2004). *Hackers & Painters: Big Ideas from the Computer Age*. Sebastopol, CA: O'Reilly Media.

Hafner, K., & Markoff, J. (1995). *Cyberpunk: Outlaws and Hackers on the Computer Frontier*. London: Simon & Schuster.

Hatch, M. (2013). *The Maker Movement Manifesto: Rules for Innovation in the New World of Crafters, Hackers, and Tinkerers*. New York: McGraw Hill Professional.

Hirschheim, R., & Klein, H. K. (2012). A Glorious and Not-So-Short History of the Information Systems Field. *Journal of the Association for Information Systems*, *13*(4), 188–235.

Hoffer, J. A., & Straub, D. W. (1989). The 9 To 5 Underground: Are You Policing Computer Crimes? *Sloan Management Review*, *30*(4), 35–43.

Holt, T. J. (2013). Examining the Forces Shaping Cybercrime Markets Online. *Social Science Computer Review*, *31*(2), 165–177. https://doi.org/10.1177/0894439312452998

Holt, T., & Strumsky, D. (2012). Examining the Social Networks of Malware Writers and Hackers. *International Journal of Cyber Criminology*, *6*(1), 891–903. https://doi.org/No DOI

Hu, Q., West, R., & Smarandescu, L. (2015). The Role of Self-Control in Information Security Violations: Insights from a Cognitive Neuroscience Perspective. *Journal of Management Information Systems*, *31*(4), 6–48. https://doi.org/10.1080/07421222.2014.1001255

Hui, K.-L., Kim, S. H., & Wang, Q.-H. (2017). Cybercrime Deterrence and International Legislation: Evidence from Distributed Denial of Service Attacks. *MIS Quarterly*, *41*(2), 497–523. https://doi.org/10.25300/MISQ/2017/41.2.08

Indulska, M., Hovorka, D. S., & Recker, J. (2012). Quantitative Approaches to Content Analysis: Identifying Conceptual Drift across Publication Outlets. *European Journal of Information Systems*, *21*(1), 49–69. https://doi.org/10.1057/ejis.2011.37

Irani, L. (2015). Hackathons and the Making of Entrepreneurial Citizenship. *Science Technology and Human Values*, *40*(5), 799–824. https://doi.org/10.1177/0162243915578486

Isaacson, W. (2011). *Steve Jobs*. New York: Simon & Schuster.

Jordan, T., & Taylor, P. (1998). A Sociology of Hackers. *Sociological Review*, *46*(4), 757–780. https://doi.org/10.1111/1467-954X.00139

Jordan, T., & Taylor, P. A. (2004). *Hacktivism and Cyberwars: Rebels with a Cause? Hacktivism and Cyberwars: Rebels with a Cause?* New York: Routledge. https://doi.org/10.4324/9780203490037

Kabay, M. E., Robertson, B., Akella, M., & Lang, D. T. (2012). Implement Security Policies. In S. Bosworth, M. E. Kabay, & E. Whyne (Eds.), *Computer Security Handbook* (6th ed., Vol. 2, pp. 1–25). New York: John Wiley & Sons. https://doi.org/10.1002/9781118820650.ch50

Kim, S. H., & Kim, B. C. (2017). Differential Effects of Prior Experience on the Malware Resolution Process. *MIS Quarterly*, *38*(3), 655–678. https://doi.org/10.25300/misq/2014/38.3.02

Kim, S. H., Wang, Q.-H., & Ullrich, J. B. (2012). A Comparative Study of Cyberattacks. *Communications of the ACM*, *55*(3), 66. https://doi.org/10.1145/2093548.2093568

Klimburg, A. (2017). *The Darkening Web: The War for Cyberspace*. New York: Penguin Press.

Koerner, B. I. (2006, January 4). Geeks in Toyland. *Wired Magazine*.

Koopmans, R. (2005). The Missing Link between Structure and Agency: Outline of an Evolutionary Approach to Social Movements. *Mobilization: An International Quarterly*, *10*(1), 19–33.

Kwon, J., & Johnson, M. E. (2014). Health-Care Security Strategies for Data Protection and Regulatory Compliance. *Journal of Management Information Systems*, *30*(2), 41–66. https://doi.org/10.2753/mis0742-1222300202

Lapsley, P. (2013). *Exploding the Phone: The Untold Story of the Teenagers and Outlaws who Hacked Ma Bell*. New York: Grove Press.

Layder, D. (1998). *Sociological Practice - Linking Theory and Practice*. London: Sage Publications Ltd.

Levy, C. (2010). Social Histories of Anarchism. *Journal for the Study of Radicalism*, *4*(2), 1–44.

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

Li, C.-Y., Huang, C.-C., Lai, F., Lee, S.-L., & Wu, J. (2018). A Comprehensive Overview of Government Hacking Worldwide. *IEEE Access*, *6*, 1–1. https://doi.org/10.1109/ACCESS.2018.2871762

Lichstein, H. (1963). Telephone Hackers Active. *The Tech*, *83*(24), 1.

Lin, Y. (2007). Hacker Culture and the FLOSS Innovation. In K. St.Amant & B. Still (Eds.), *Handbook of Research on Open Source Software: Technological, Economic, and Social Perspectives* (pp. 34–46). London: Information Science Reference.

Lindgren, S., & Lundström, R. (2011). Pirate Culture and Hacktivist Mobilization: The Cultural and Social Protocols of #Wikileaks on Twitter. *New Media & Society*, *13*(6), 999–1018. https://doi.org/10.1177/1461444811414833

Lindtner, S. (2015). Hacking with Chinese Characteristics: The Promises of the Maker Movement against China's Manufacturing Culture. *Science Technology and Human Values*, *40*(5), 854–879. https://doi.org/10.1177/0162243915590861

Lowry, P. B., Dinev, T., & Willison, R. (2017). Why Security and Privacy Research Lies at The Centre Of the Information Systems (IS) Artefact: Proposing A Bold Research Agenda. *European Journal of Information Systems*, *26*(6), 546–563. https://doi.org/10.1057/s41303-017-0066-x

Lu, Y., Luo, X., Polgar, M., & Cao, Y. (2015). Social Network Analysis of a Criminal Hacker Community. *Journal of Computer Information Systems*, *51*(2), 31–41. https://doi.org/10.1080/08874417.2010.11645466

Mahmood, Raghu, Siponen, Rao, & Straub. (2010). Moving Toward Black Hat Research in Information Systems Security: An Editorial Introduction to the Special Issue. *MIS Quarterly*, *34*(3), 431. https://doi.org/10.2307/25750685

Mahoney, J., & Rueschemeyer, D. (2003). *Comparative Historical Analysis in the Social Sciences*. New York: Cambridge University Press.

Mansfield-Devine, S. (2011). Hacktivism: Assessing the Damage. *Network Security*, *2011*(8), 5–13. https://doi.org/10.1016/S1353-4858(11)70084-8

Markoff, J. (2005). *What the Dormouse said: How the 60s Counterculture Shaped the Personal Computer Industry*. London: Viking Books.

Martin, J. (2014). Lost on the Silk Road: Online Drug Distribution and the 'Cryptomarket.' *Criminology and Criminal Justice*, *14*(3), 351–367. https://doi.org/10.1177/1748895813505234

McKay, N. (1998, September 22). The Golden Age of Hacktivism. *Wired Magazine*.

Miaskiewicz, T., & Kozar, K. A. (2011). Personas and User-Centered Design: How can Personas benefit Product Design Processes? *Design Studies*, *32*(5), 417–430. https://doi.org/10.1016/j.destud.2011.03.003

Miles, M., Huberman, A., & Saldana, J. (2014). *Qualitative Data Analysis: An Expanded Sourcebook*. Thousand Oaks, CA: SAGE Publications.

Mitnick, K., & Simon, W. L. (2005). *The Art of Intrusion: The Real Stories Behind the Exploits of Hackers, Intruders and Deceivers*. Indianapolis: John Wiley & Sons.

Mitnick, K., Wozniak, S., & Simon, W. L. (2011). *Ghost in the Wires*. New York: Little, Brown and Company.

Mookerjee, V., Mookerjee, R., Bensoussan, A., & Yue, W. T. (2011). When Hackers Talk: Managing Information Security Under Variable Attack Rates and Knowledge Dissemination. *Information Systems Research*, *22*(3), 606–623. https://doi.org/10.1287/isre.1100.0341

Mosakowski, E. (2002). Overcoming resource disadvantages in entrepreneurial firms: when less is more. In M. Hitt, M., Ireland, D., Sexton, D., Camp (Ed.), *Strategic Entrepreneurship: Creating an Integrated Mindset* (pp. 106–126). Oxford: Blackwell.

Müller, S. D., & Ulrich, F. (2013). Creativity and Information Systems in a Hypercompetitive Environment : A Literature Review. *Communications of the Association for Information Systems*, *32*(June), 175–200. https://doi.org/10.17705/1CAIS.03207

Müller, S. D., & Ulrich, F. (2015). The Competing Values of Hackers: The Culture Profile that Spawned the Computer Revolution. In *Proceedings of the 48th Annual Hawaii International Conference on System Sciences (HICSS 48)* (pp. 3434–3443). Kauai, Hawaii, USA: IEEE. https://doi.org/10.1109/HICSS.2015.413

Müller, S. D., Ulrich, F., & Nielsen, P. A. (2014). When Process is Getting in the Way of Creativity and Innovation. In *2014 47th Hawaii International Conference on System Sciences* (pp. 221–229). Waikoloa, Hawaii: IEEE. https://doi.org/10.1109/HICSS.2014.36

Muzio, D., Brock, D. M., & Suddaby, R. (2013). Professions and Institutional Change: Towards an Institutionalist Sociology of the Professions. *Journal of Management Studies*, *50*(5), 699–721. https://doi.org/10.1111/joms.12030

Ng, B. Y., Kankanhalli, A., & Xu, Y. (Calvin). (2009). Studying Users' Computer Security Behavior: A Health Belief Perspective. *Decision Support Systems*, *46*(4), 815–825. https://doi.org/10.1016/j.dss.2008.11.010

Nielsen, J. A., Mathiassen, L., & Newell, S. (2014). Theorization and Translation in Information Technology Institutionalization: Evidence from Danish Home Care. *MIS Quarterly*, *38*(1), 165–186. https://doi.org/10.25300/MISQ/2014/38.1.08

Nikitina, S. (2012). Hackers as Tricksters of the Digital Age: Creativity in Hacker Culture. *Journal of Popular Culture*, *45*(1), 133–152. https://doi.org/10.1111/j.1540-5931.2011.00915.x

Olsen, P. (2013). *We are Anonymous*. London, UK: William Heinemann.

Osterwalder, A., & Pigneur, Y. (2010). *Business Model Generation: A Handbook for Visionaries, Game Changers, and Challengers*. New Jersey: John Wiley & Sons.

Pacey, A. (1992). *The Maze of Ingenuity: Ideas and Idealism in The Development of Technology* (2nd ed.). Cambridge, MA: The MIT Press.

Pogrebna, G., & Skilton, M. (2019). A Sneak Peek into the Motivation of a Cybercriminal. In G. Pogrebna & M. Skilton (Eds.), *Navigating New Cyber Risks* (pp. 31–54). London, UK: Springer International Publishing. https://doi.org/10.1007/978-3-030-13527-0

Porra, J., Hirschheim, R., & Parks, M. S. (2014). The Historical Research Method and Information Systems Research. *Journal of the Association for Information Systems*, *15*(9), 536–576. https://doi.org/10.17705/1jais.00373

Raymond, E. S. (1999). *The Cathedral and the Bazaar*. Sebastopol, CA: O'Reilly Media.

Rogers, M. (2003). The Role of Criminal Profiling in the Computer Forensics Process. *Computers and Security*, *22*(4), 292–298. https://doi.org/10.1016/S0167-4048(03)00405-X

Samtani, S., Chinn, R., Chen, H., & Nunamaker, J. F. (2017). Exploring Emerging Hacker Assets and Key Hackers for Proactive Cyber Threat Intelligence. *Journal of Management Information Systems*, *34*(4), 1023–1053. https://doi.org/10.1080/07421222.2017.1394049

Schulz, C., & Wagner, S. (2008). Outlaw Community Innovations. *International Journal of Innovation Management*, *12*(3), 399–418. https://doi.org/10.1142/S1363919608002084

Sen, R. (2018). Challenges to Cybersecurity: Current State of Affairs. *Communications of the Association for Information Systems*, *43*(1), 22–44. https://doi.org/10.17705/1CAIS.04302

Shackelford, S. J. (2009). From Nuclear War to Net War: Analogizing Cyber Attacks in International Law. *Berkeley Journal of International Law*, *27*(1), 192–251. https://doi.org/10.15779/Z38KS9B

Shimomura, T., & Markoff, J. (1996). *Takedown: The Pursuit and Capture of Kevin Mitnick, America's Most Wanted Computer Outlaw - By the Man Who Did It*. New York: Hyperion.

Smith, S., Winchester, D., Jamieson, R., & Bunker, D. (2010). Circuits of Power: A Study of Mandated Compliance to An Information Systems Security De Jure Standard in A Government Organization. *MIS Quarterly*, *34*(3), 463–486. https://doi.org/10.2307/25750687

Söderberg, J., & Delfanti, A. (2015). Hacking Hacked! The Life Cycles of Digital Innovation. *Science Technology and Human Values*, *40*(5), 793–798. https://doi.org/10.1177/0162243915595091

Stallman, R. M., & Gay, J. (2009). *Free Software, Free Society: Selected Essays of Richard M. Stallman*. Paramount: CreateSpace.

Stein, M. K., Galliers, R. D., & Whitley, E. A. (2016). Twenty Years of the European Information Systems Academy at ECIS: Emergent Trends and Research Topics. *European Journal of Information Systems*, *25*(1), 1–15. https://doi.org/10.1057/ejis.2014.25

Sterling, B. (1992). *The Hacker Crackdown: Law and Disorder on the Electronic Frontier*. London, UK: Penguin Books.

Stoll, C. (1988). Stalking the Wily Hacker. *Communications of the ACM*, *31*(5), 484–497. https://doi.org/10.1145/42411.42412

Taylor, P. A. (2005). From Hackers to Hacktivists: Speed Bumps on the Global Superhighway? *New Media & Society*, *7*(5), 625–646. https://doi.org/10.1177/1461444805056009

Thomas, D. (2002). *Hacker Culture*. Minneapolis: University of Minnesota Press.

Thomas, J. (2005). The Moral Ambiguity of Social Control in Cyberspace: A Retro-Assessment of the "Golden Age" of Hacking. *New Media & Society*, *7*(5), 599–624. https://doi.org/10.1177/1461444805056008

Tocchetti, S., & Aguiton, S. A. (2015). Is an FBI Agent a DIY Biologist Like Any Other? A Cultural Analysis of a Biosecurity Risk. *Science Technology and Human Values*, *40*(5), 825–853. https://doi.org/10.1177/0162243915589634

Turkle, S. (1984). *The Second Self: Computers and the Human Spirit*. New York: Simon & Schuster.

Turner, F. (2010). *From Counterculture to Cyberculture: Stewart Brand, the Whole Earth Network, and the Rise of Digital Utopianism*. Chicago and London: The University of Chicago Press.

Turner, P., & Turner, S. (2011). Is Stereotyping Inevitable when Designing with Personas? *Design Studies*, *32*(1), 30–44. https://doi.org/10.1016/j.destud.2010.06.002

Ulrich, F., Mengiste, S. A., & Müller, S. D. (2015). Informal Evaluation and Institutionalization of Neoteric Technology Ideas: The Case of Two Danish Organizations. *Communications of the Association for Information Systems*, *37*(1), 949–974. https://doi.org/10.17705/1cais.03747

von Hippel, E., & Paradiso, J. A. (2008). User Innovation and Hacking. *IEEE Pervasive Computing*, *7*(3), 66–69. https://doi.org/10.1109/MPRV.2008.62

Walsham, G. (1995). Interpretive Case Studies in IS Research: Nature and Method. *European Journal of Information Systems*, *4*(2), 74–81. https://doi.org/10.1057/ejis.1995.9

Walsham, G. (2006). Doing Interpretive Research. *European Journal of Information Systems*, *15*(3), 320–330. https://doi.org/10.1057/palgrave.ejis.3000589

Wark, M. (2004). *A Hacker Manifesto*. Cambridge: Harvard University Press.

Warren, M., & Leitch, S. (2010). Hacker Taggers: A New Type of Hacker. *Information Systems Frontiers*, *12*(4), 425–431. https://doi.org/10.1007/s10796-009-9203-y

Webb, J. W., Tihanyi, L., Ireland, R. D., & Sirmon, D. G. (2009). You Say Illegal, I Say Legitimate: Entrepreneurship in the Informal Economy. *Academy of Management Review*, *34*(3), 492–510. https://doi.org/10.5465/AMR.2009.40632826

Webster, J., & Watson, R. T. (2002). Analyzing the Past to Prepare for the Future: Writing a Literature Review. *Mis Quarterly*, *26*(2), XIII–XXIII.

Whalley, C. (2010). Neutralization: New Insights into The Problem of Employee Information Systems Security Policy Violations. *MIS Quarterly*, *34*(3), 487–502. https://doi.org/10.2307/25750688

Williams, S. (2002). *Free as in Freedom: Richard Stallman's Crusade for Free Software*. CA, USA: O'Reilly.

Willison, R. (2006a). Understanding the Offender/Environment Dynamic for Computer Crimes. *Information Technology and People*, *19*(2), 170–186. https://doi.org/10.1108/09593840610673810

Willison, R. (2006b). Understanding the Perpetration of Employee Computer Crime in the Organisational Context. *Information and Organization*, *16*(4), 304–324. https://doi.org/10.1016/j.infoandorg.2006.08.001

Willison, R., & Backhouse, J. (2006). Opportunities for Computer Crime: Considering Systems Risk from A Criminological Perspective. *European Journal of Information Systems*, *15*(4), 403–414. https://doi.org/10.1057/palgrave.ejis.3000592

Willison, R., Lowry, P. B., & Paternoster, R. (2018). A Tale of Two Deterrents: Considering the Role of Absolute and Restrictive Deterrence to Inspire New Directions in Behavioral and Organizational Security Research. *Journal of the Association for Information Systems*, *19*(12), 1187–1216. https://doi.org/10.17705/1jais.00524

Willison, R., Warkentin, M., & Johnston, A. C. (2018). Examining Employee Computer Abuse Intentions: Insights from Justice, Deterrence and Neutralization Perspectives. *Information Systems Journal*, *28*(2), 266–293. https://doi.org/10.1111/isj.12129

Yin, R. K. (2003). *Case Study Research - Design and Methods* (3rd ed.). London: SAGE Publications Ltd.

Young, R., Zhang, L., & Prybutok, V. R. (2007). Hacking into The Minds of Hackers. *Information Systems Management*, *24*(4), 281–287. https://doi.org/10.1080/10580530701585823

Yue, W. T., Wang, Q.-H., & Hui, K.-L. (2019). See No Evil, Hear No Evil? Dissecting the Impact of Online Hacker Forums. *MIS Quarterly*, *43*(1), 73–95. https://doi.org/10.25300/MISQ/2019/13042.

About the Authors

Frank Ulrich earned his PhD in Information Systems from Aalborg University. He has previously published work on hacker culture, privacy, innovation and creativity, organizational theory, and learning theory. He has published in a range of journals, including the *Communications of the Association for Information Systems, Creativity & Innovation Management, Interactive Learning Environments*, and *Sustainable Development*.

Sune Dueholm Müller received his PhD in process innovation from Aarhus School of Business, Denmark, in 2009, and is employed by University of Oslo as an Associate Professor. His current research focuses on digital innovation and transformation of healthcare services. He has published work in IS and health IS journals such as *Journal of the Association for Information Systems*, *Information Technology & People*, *Journal of Medical Internet Research*, and *Health Informatics Journal*.

Stephen Flowers is an Emeritus Professor at the University of Kent in the UK and has a visiting position at the University of Vaasa in Finland. He works in the areas of Information Systems and Innovation.