Volume 6 Number 2 Special Issue 2018

Journal of Qualitative Criminal Justice and Criminology

JQCJC

Southwestern Association of Criminal Justice

Journal of Qualitative Criminal Justice & Criminology (JQCJC)

JOURNAL OF QUALITATIVE
CRIMINAL JUSTICE & CRIMINOLOGY

SPECIAL ISSUE:
CRITICAL OR MARGINAL PERSPECTIVES AND ISSUES IN THE STUDY OF TECHNOCRIME

Volume 6 **Number 2** **Special Issue 2018**

Technocrime at the Margins: Introduction to the Special Issue on Critical or Marginal Perspectives and Issues in the Study of Technocrime

Kevin F. Steinmetz
Kansas State University

When first asked to guest edit a special issue of the *Journal of Qualitative Criminal Justice and Criminology*, I admit that I was hesitant. I knew from helping Willard Oliver start this journal and from working as its first book review editor that editorship can be trying—and often under-appreciated—work. Tom Holt, the editor of the journal at the time, however, was ambitious and willing to take some risks in his mission to carry the journal forward. As such, he offered me tremendous latitude and support for pursuing my unique vision for a special issue on technocrime issues from a diverse arrangement of perspectives. The opportunity was too good to pass up. Guest editing this journal allowed me to cultivate a novel issue of important topics in the field of technocrime from noteworthy authors on a variety of topics including hacking, phishing and malware victimization, presidential rhetoric, sexting, and even a disciplinary critique.

I am thrilled that others saw the value in such research and seized the opportunity contribute to this special issue. Technocrime and victimization are a growing concern both within the academy and the public consciousness. In the past two years we have seen distributed denial of service attacks launched from a botnet populating the Internet of Things called "Mirai;" one of the most significant data breaches ever—the Equifax breach—which compromised extremely sensitive personal and financial information of hundreds of millions of people; the proliferation of ransomware such as Petya, NotPetya, and BadRabbit; and Russia's use of hackers and trolls to influence the 2016 U.S. Presidential election, to name a few examples. The point is that concerns continue to mount and there is tremendous work to be done by criminologists. It is critical at this juncture that we employ a kaleidoscopic array of perspectives to make sense of the variegated issues with which we are confronted. This issue presents one step in this direction.

On a different note, the reader may wonder why the term technocrime is used throughout this issue, especially considering that cybercrime is the accepted nomenclature in both the field and beyond. The choice of vernacular is purposive. As I have detailed elsewhere (Steinmetz & Nobles, 2018), I have difficulty with the political and conceptual baggage involved in the invocation of "cyber." Instead, I prefer to use the term technocrime which I borrow from the work of Leman-Langlois (2013), though the term technically predates his work (Bequai, 1987). For my money, Leman-Langlois' use of the term is more suited for social scientific endeavors than cybercrime. It acknowledges the often ephemeral, elusive, and ambiguous dimensions of high-technology crime and information security while eschewing the political connotations now attached to "cyber." As he explains,

> Technocrime does not exist. It is a figment of our imaginations. It is simply a convenient way to refer to a set of concepts, practices, frames and knowledges shaping the ways in which we understand matters having to do with the impact of technology on crime, criminals and our reactions to crime – and vice versa: since crime, criminals and reactions also transform technology. (Leman-Langlois, 2013, p. 1)

Cyber, on the other hand, tends to give us the impression that our conversations concerning high-technology and crime are "closer to the natural laws that gave us computers than to the artificial laws that gave us crimes" (Leman-Langlois, 2008, p. 4). Since we are ultimately involved in social scientific endeavors, the judicious use of the criminological imagination (Young, 2011) demands that we reject false equivalencies with the "natural sciences" and adopt concepts which are more appropriate to the socio-cultural realm. To borrow McGuire's (this issue) eloquent articulation of the matter, the term cyber tends to prioritize "syntax" over "semantics." My view is that Leman-Langlois' use of technocrime avoids—or at least mitigates—this issue. That said, it should be noted that not every author in this volume eschews the term cyber in the same way I do. Rather than act as an autocrat, I decided it was best to allow each author to make a decision for themselves about which terms they would prefer to use. As such, technocrime, cybercrime, Internet crimes, and other terms are invoked throughout this issue at the discretion of the authors.

The first article in this special issue, "CONs, CONstructions and CONcepts of Computer Related Crime: From a Digital Syntax to a Social Semantics," M. R. McGuire provides an examination of a key conceptual and linguistic issue which confronts criminology's approach to technocrime or cybercrime. In short, he argues that our current thinking on the subject is mired in a discourse that privileges technical (*syntactic*) approaches over the socio-cultural (*semantic*) dimensions. The distinction between the syntactic and the semantic is important. As McGuire rightly points out, we are too often preoccupied with viewing computer-related crime and security issues as constellations of technical problems to be solved through technical means. Firewalls, machine learning algorithms, simulation analyses, advanced statistical modeling often seem to dominate our imaginations in the realm of "cyber." As argued in this essay, such thinking is seemingly coded into the very discourse which frames the issue. Thinking syntactically structures our thinking about technocrime and security which may be useful to some extent, but it also limits our capacity to imagine alternative perspectives, approaches, and solutions. McGuire thus argues that we seriously need to reconsider our entire orientation to the field—an argument that, from my view, is difficult to contradict.

Wytske van der Wagen provides the second article comprising this issue—"The Cyborgian Deviant: An Assessment of the Hacker through the Lens of Actor-Network Theory." Involved is an analysis of hackers through Latour's articulations of Actor-Network theory (1992; 2005). Latour argues for a reassessment of our understandings of "social." Instead of framing the social as a separate realm of existence which exists outside of human experience and engagement, Latour argues that the social exists entirely at the relational level. In this capacity, society is but a constellation of actors networked together through social relationships. He thus redefines sociology "not as the 'science of the social', but as the *tracing of associations*" (Latour, 2005, p. 5; emphasis in original). He further explains that "in this meaning of the adjective, social does not designate a thing among other things, like a black sheep among other white sheep, but *a type of connection* between things that are not themselves social" (ibid; emphasis in original). As things are not *inherently* social but, rather, *become* social through particular kinds of associations, then non-human entities can be social including animals and even objects. Humans and technology, therefore, can enter into social relationships. In a manner described as "cyborgian", van der Wagen argues that hacker identity is characterized by social relationships with technology which blurs the distinction between the human and the technological. Her discussion is segmented into five parts, all of which are attuned to the relational dimensions between hackers and tech. This analysis builds from prior analyses which have applied actor-network theory to the study of technocrime, such as

van der Wagen's own study on botnets (van der Wagen & Pieters, 2015). Van der Wagen's research indicates a rich path forward for Latourian analyses of technocrime.

This special issue also includes an analysis of presidential rhetoric on "cybercrime" by Joshua B. Hill and Nancy E. Marion entitled "The Use of Mythic Narratives in Presidential Rhetoric on Cybercrime." Though some may dismiss the utterances of American presidents as having little long-standing and significant effect on public opinion beyond short-lived attention-grabbing headlines, Hill and Marion argue that people are influenced by presidential rhetoric in significant ways which, in turn, may have lasting impacts on public policy. The authors thus build on prior analyses to examine presidential speeches invoking cyber-related terms (like cybercrime, cyberterrorism, and cyber-attack) between the years 1995 and 2015. Their analysis focuses on how U.S. presidential speeches frame "cyber" issues as threats in such a way that seem to propagate a mythology conducive to fear and a political agenda of securitization. Studies of this sort are important as criminological research into technocrime (and other areas of criminology more generally) tend of focus on lower-level criminal actors rather than policy and power. Hill and Marion's work stands as a noteworthy contribution in this regard.

The final two analyses presented in this special issue both concern technocrime victimization. In "Coping with Cybercrime Victimization: An Exploratory Study into Impact and Change," Jurgen Jansen and Rutger Leukfeldt examine how a sample of 30 online banking customers cope with the impact of phishing and malware attacks. Their study documented multiple impacts experienced by victims include financial, emotional, and psychological damages. Further, secondary forms of victimization were also found as participants reported feeling that banks and the police did not aid them property in recovery. These participants also reported frustrations at time lost in dealing with banks and the police. As a result of these victimization experiences, behavioral changes were documented. Perhaps the most useful discussion in this analysis occurs when the authors frame the coping strategies adopted by victims and ruminate on potential policy implications. Despite a slew of studies emerging on online victimization (see Button & Cross, 2017, for an overview of online fraud victimization research, for example), further work is still needed in this domain, particularly in regards to two of the most prevalent sources of technocrime victimization today: phishing and malware. Jansen and Leukfeldt's analysis thus provides a significant advancement in this regard.

Finally, this issue ends with a moral panic analysis of sexing by Karen Holt entitled, "Seductive Events: A Critical Examination of Youth Sexting." Drawing from narrative criminology (Presser & Sandberg, 2015), Holt details two narratives which have emerged surrounding sexting: the victim narrative and the moral panic narrative. The former includes "stories of tragedy" which "portrays sexting youth as a vulnerable population, at risk for both victimization and exploitation" as well as criminality (page 231). The latter "asserts that the reaction to sexting is disproportionate to the threats presented by engaging in this behavior, and that much of the focus has been solely on the negative consequences of sexting, which are statistical anomalies" (page 231). Though perhaps marginal for the time being, narrative criminology is quickly gathering steam and is on the verge of becoming a popular orientation across both mainstream and critical criminologies. Holt's analysis is one example of the power of narrative analysis to make sense of what Ferrell (2013, p. 258) calls the "politics of meaning" surrounding teen sexting.

I would also like to take a moment to thank all of the reviewers who contributed to this special issue. They answered the call in brilliant fashion and I am still overwhelmed by their insights and graciousness. The reviewers for this issue are enumerated below:

- James Aho
- James Banks
- Alayna Colburn
- Heith Copes
- Thomas Crofts
- Cassandra Cross
- Kelly Cronin
- Jonathan Grubb
- Thomas Holt
- Alison Marganski
- Alyce McGovern
- Lisa Melander
- Willard Oliver
- Duncan Philpot
- Brian Schaefer
- Brian Sellers
- Peter Simi
- Robin Valeri
- Lindsey Upton
- David Wall
- Ashley Wellman
- Majid Yar

In conclusion, I am greatly indebted to the effort of these authors and the reviewers. They are responsible for making this special issue novel and noteworthy. I hope the reader finds these studies as interesting as I do. I would also like to thank Tom Holt for extending this opportunity to contribute to *JQCJC*. The study of technocrime issues—though gaining traction—is still relatively marginal in the field of criminology. It is important that venues like *JQCJC* create spaces for this kind of scholarship. There is more work that needs to be done.

REFERENCES

Bequai, A. (1987). *Technocrimes.* Lexington, MA: Lexington Books.

Button, M., & Cross, C. (2017). *Cyber frauds, scams and their victims.* New York, NY: Routledge.

Ferrell, J. (2013). Cultural criminology and the politics of meaning. *Critical Criminology, 21*, 257-271.

Latour, B. (1992). Where are the missing masses? The sociology of a few mundane artifacts. In W. E. Bijker and J. Law (eds.) *Shaping technology/building society: Studies in sociotechnical change* (pp. 225-258). Cambridge, MA: MIT Press.

Latour, B. (2005). *Reassembling the social: An introduction to actor-network-theory.* Cambridge, MA: Oxford University Press.

Leman-Langlois, S. (2008). Introduction: Technocrime. In S. Leman-Langlois (ed.) *Technocrime: Technology, Crime and Social Change* (pp. 1-13). Portland, OR: Willan Publishing.

Leman-Langlois, S. (2013). Introduction. In S. Leman-Langlois (ed.) *Technocrime, policing and surveillance* (pp. 1-12). New York, NY: Routledge.

Presser, L. & Sandberg, S. (2015). *Narrative criminology: Understanding stories of crime.* New York, NY: NYU Press.

Steinmetz, K. F. & Nobles, M. R. (2018). Introduction. In K. F. Steinmetz and M. R. Nobles (eds.) *Technocrime and criminological theory* (pp. 1-10). New York, NY: Routledge.

Van der Wagen, W., & Pieters, W. (2015). From cybercrime to cyborg crime: Botnets as hybrid criminal actor-networks. *British Journal of Criminology*, *55*(3), 578-595.

Young, J. (2011). *The criminological imagination.* Malden, MA: Polity Press.

CONS, CONSTRUCTIONS AND MISCONCEPTIONS OF COMPUTER RELATED CRIME: FROM A DIGITAL SYNTAX TO A SOCIAL SEMANTICS

M.R. McGuire
University of Surrey

Abstract

Has the framing of computer crime been a process which has, in effect, left us all framed? What is it that we think that we understand when we use terms like "internet crime," "cybercrime," or "technocrime," and in what sense does this understanding constitute *knowledge?* In particular, the kind of knowledge which can be defined as "social scientific?" In this paper, I apply one of the key distinctions used to define computational processes – that made between a *syntax* and a *semantics* – to illustrate some of the problems that have affected our thinking about cybercrime and undermined our responses to it. I argue that the construction of cybercrime in terms of syntactic rather than semantic considerations has fostered the myth that it is a technical crime requiring technical solutions. Worse, by emphasizing cybercrime's machinic over its human origins, syntactic interpretations have inflated its risks and directly contributed to the 'culture of fear' surrounding cybercrime. Drawing upon qualitative analytic techniques such as thematic visualization, I outline the need for a more sociocultural account of the origins of cybercriminality, one that might not only help stem the increasingly counterproductive influences of the cybersecurity industry, but can also contribute to more effective ways of containing it.

Keywords: computer crime, cybercrime, thematic visualization

INTRODUCTION

It is now accepted as a given that there is a "crisis" around the use and misuse of our most significant contemporary technology – the information and communication systems that pervade every aspect of everyday life. At its worst, this is a crisis which has been regarded as potentially catastrophic (Noik, 2011). Back in 2008, I surveyed the emerging criminal landscape around the internet and information technology (McGuire, 2008) and found a number of recurring themes as to how this problem was being framed. Specifically, there was an abject failure to properly appreciate that problems rooted in social interaction are ultimately problems of social interaction rather than how those interactions are mediated. In cybercrime, the medium remains very much only part of the message.

In this paper, I will examine this contention in relation to a distinction that has received little or no attention in the context of cybercrime – that made between a *syntax* and a *semantics*. Though the distinction is one that has traditionally been explored more within standard linguistics and the philosophy of language (see for example Lycan, 2000), it has acquired obvious significance within computer science given the centrality of programming languages in this field. Although there are differences in the way the distinction is applied across these contexts (cf. Leonhardt & Röttger, 2006), the general idea (roughly) is to say that a syntax involves grammar - the rules which determine the correct use of symbols and their combinations in any language while a semantics determines what a syntactically correct sequence of symbols *mean* (Anderson, 2009). For example,

in English, the syntactic rules say that “the cat is on the mat” is a well-formed sentence, but “cat mat on is the” is not. Semantically, the correct syntactic formation allows us to *understand* that a cat is on a mat (as opposed for example to a mat being on a cat). In computational terms, syntax has often been granted a more elevated status than semantics because effectively “what we call computation takes place on the level of syntax. It is a purely formal procedure taking place in a physical mechanism” (Müller, 2008, p. 222). Put more simply, it is because the syntactic states of a program can be linked to the physical states of a machine that computation becomes possible. As a result, syntax appears to possess *causal* as well as grammatical significance – serving to mediate relations between physical states and abstract symbols. In this sense, syntax determines whether a machine works at all, or whether its program results in malfunctions (for example, similar to those described by the Halting Problem (Parkes, 2002).[1] Thus, in a programming language like C++, the syntactic symbol “;” acts as a statement terminator, thereby allowing “x = y”; “y = z + 1” to be treated as *different* statements rather than parts of the same command. In doing so, this simple syntactic symbol and the rules which govern its use have profound effects on the functioning of any C++ program.

A number of examples demonstrate the way syntactic responses to cybercrime have been favored over more complex, semantic measures. For example, we all know that malware infections can be strongly related to human factors like the intention to do harm, failures and errors in taking simple security precautions or emotions like greed, curiosity, lust, fear, and so on which drive individuals to click on links they should not. Yet, according to the UK National Cybersecurity Centre (2016), protections against malware infections center largely upon end-user device protection**,** antivirus and malicious code checking solutions, content filtering capability on all external gateways, installing firewalls, disabling certain browser plugins or scripting languages, disabling a device’s *autorun* function, or “ensuring systems and components are well configured according to the secure baseline build” (NCSC, 2017). Even offenses like phishing – which depend heavily upon a successful social engineering of meanings between perpetrator and victim – have often been thought to be best addressed by syntactically driven measures such as Secure Connections (HTTPS), Secure Login Features, Web Browser Features and Settings, Email Client Configuration, SPAM Filters or Alternative Transaction Verification Channels (cf. Infosec, 2017).

I argue that reflecting upon the elevated status of syntax and the way it is distinguished from semantics offers a more precise way of revisiting the familiar debates about cybercrime as a technical crime or one driven more by human factors (Leukfeldt, 2017). Not only is the latter term highly vague (what is and what is not a human factor?), it is also clear that human interactions with information technology are fundamentally dependent upon the meanings and interpretations involved. In other words, the relevant semantics. Similarly, syntax is well understood, in both conceptual and operational terms, while ‘technical’ is not. In turn, invoking the syntax/semantics divide not only has value in clarifying some of the governing perceptions around cybercrime and the mythologies which have developed around it, but it also helps challenge some of current assumptions about the kind of methodology best suited to developing appropriate, and actionable knowledge about cybercrime. In this paper, I will review three kinds of clarifications which the application of this distinction can offer and the need this implies for a more powerful hermeneutic toolbox than has been applied to cybercrime to date.

First, one of the most common taken-for-granted assumptions underlying standard conceptions of cybercrime – that it is a novel crime because it is a *technical* crime – becomes far less self-evident when the underlying association with syntactic criminality is made more explicit. Given that syntax is effectively a synonym for “digital code”, it becomes obvious why actions like

[1] This occurs when a program does not produce a definitive outcome therefore causing the machine to ‘halt.’ Instead, its syntax causes the machine to produce strings of (meaningless) symbols without ever halting.

malware distribution and DDoS attacks are not just perceived as novel crimes, but also the most typically "cyber" of cybercrimes. The distinctive character of cybercrime is based on the fact that it can be generated by code and driven by the algorithms which depend upon code (Lessig, 1999), which is really to say, syntax. This also explains why a further popular prejudice has also developed - that it is only by way of other species of code/syntactic tools that such criminalities can be tackled.

A second benefit of reflecting upon the syntax-semantic distinction lies in what it tells us about the cultures of alarm and fear which have developed around cybercrime (Wall, 2008). The idea that there is some fundamental discontinuity between semantics and syntax has been widely debated within computational philosophy (Searle, 1999; Stich, 1983), so it is not surprising that discussions of cybercrime have also assumed that syntactically driven computational states somehow stand "outside" the rich, complex world of the human-semantic. And given this, the further assumption that the behavior of algorithms represents something alien or other follows naturally enough. From there, it is a short step to the tacit belief that syntactic machines are something to be feared as much as they are to be admired.

Finally – and crucially to what follows – by unpacking the syntax-semantic distinction, we can begin to make sense of one of the most troubling aspects of the current thinking around cybercrime – why proper critical discussion of the phenomenon has been so limited. A key feature of any formally correct syntactic language system is the property of "completeness," the requirement that all truths within the language can be proven by correct application of the rules and symbols of the language (cf. Hackstaff, 1966). This implies that nothing *external* to these rules is required to secure truth. It is striking (but telling) how often discussions of cybercrime have tended to mirror this line of thinking, for if knowledge of syntax and its algorithmic outputs suffice to determine the truth about such offending, what need is there for alternative perspectives? Seen in this light, a syntactic view of cybercriminality appears disturbingly close to an article of religious faith because it encourages us to view cybercrime as a phenomenon which we may be able to *describe* in various ways, but interpret only in terms of a single way.

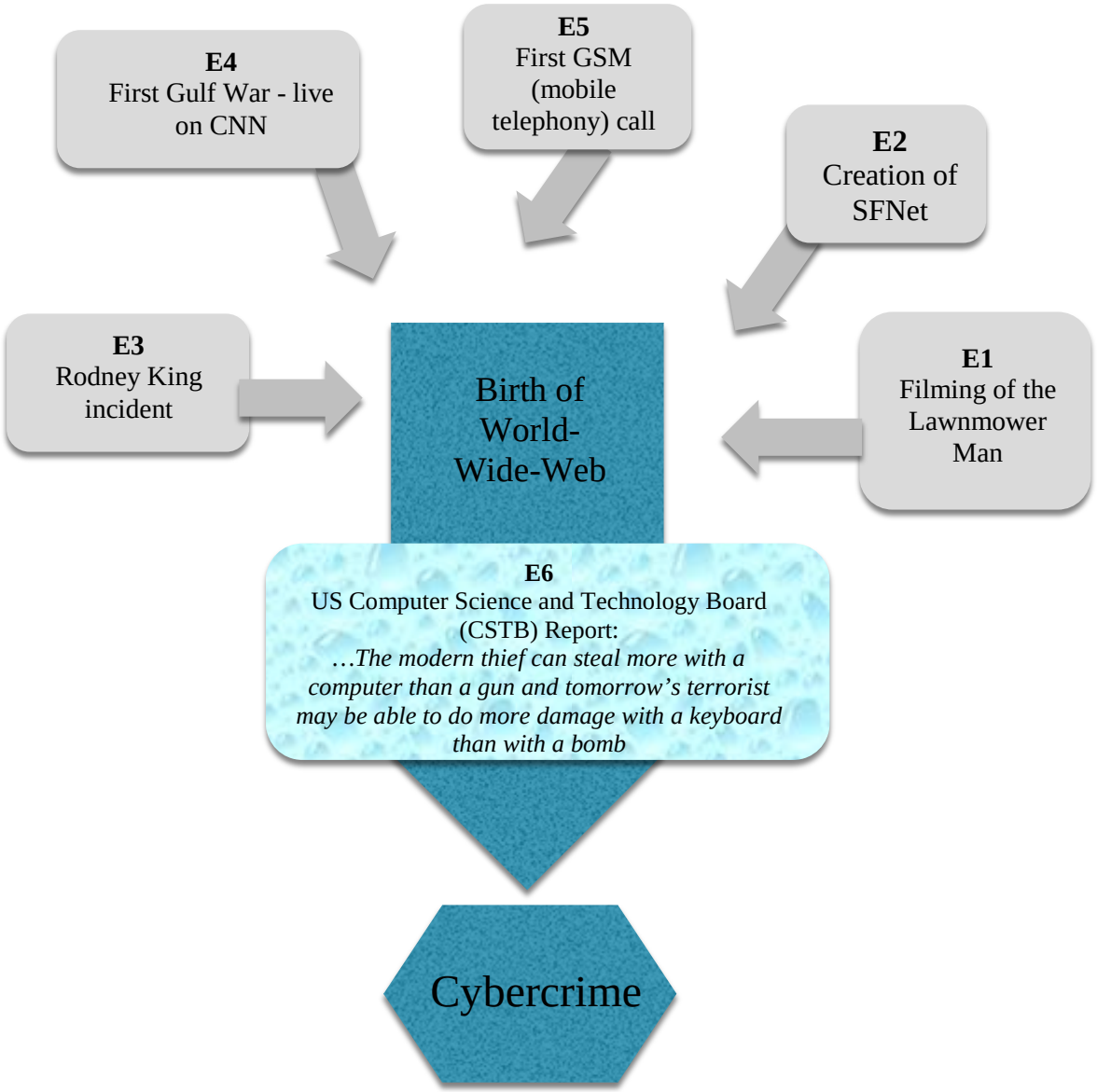
This kind of doctrinaire faith in the all-encompassing explanatory power of syntactic/algorithmic interpretations of cybercrime has been enormously damaging, not just too effective critical analysis of the phenomenon, but also to the kinds of responses to it which have (so far) been developed. In what follows, I will begin by setting out a provisional genealogy of how our perceptions of cybercrime have developed. By winding the clock back to some of the circumstances surrounding the origins of this variety of offending, some corrections to the syntactic interpretation will be outlined. This will set the scene for a more critical interrogation of the way certain foundational assumptions, in particular those involving the syntax-semantics distinction, continue to impede effective understanding. As a result, it will also suggest an outline of some richer methodological approaches to the cybercrime problem.

1991: GENEALOGY, ORIGINS & INFLUENCE – A THEMATIC VISUALIZATION

One immediate, but surprisingly underused framework for developing a richer, more semantically focused approach to cybercrime is by way of its genealogy. This might involve the socio-technic trajectories of information technology crime over time and how, in turn, our perceptions of this evolution have been shaped by various cultural and ethnographic influences. There are many ways in which a genealogical method for cybercrime could be delineated (Bowman, 2007 Anaïs, 2013), but I will use *thematic visualization* as one such approach (Tufte, 2006). Thematic visualization involves visual representations of overtly qualitative data which complements the increasing utility of (quantitative) data visualization methods (Banks, 2001). I will use it here to highlight the convergence of a series of (ostensibly) unrelated events in **1991** – a year

which arguably represents a crucial juncture in the development of cybercrime. Specifically, given that it was in this year that the world-wide-web first became active, 1991 could reasonably be characterized as the "ur-year" for cybercrime – the year when it properly 'began'.[2] By interweaving key events which impacted the origins of our thinking about cybercrime with the technical origins of cybercrime itself, a thematic visualization of 1991 can situate these early technical developments within a wider field of cultural influences. In turn, the changing perceptions of our newly connected world and the various pros and cons we have attributed to this can be revealed in more granular detail. An example of this kind of visualization is seen in Figure 1 (below).

It is important to stress that the events detailed in this particular visualization are by no means exhaustive as other kinds of indicator events are possible. What they do suggest however is that there are many more ways of interpreting the subsequent development of cybercriminality than simply pointing to changes in information technology or to the oft-repeated construct of an "arms race" between cybercriminals and law enforcement agencies.



[2] See my 2016a paper for an argument which proposes a far longer history of cybercrime, with 1991 serving as the start point for what could be called its "2.0" manifestation.

Figure 1: 1991 and the Origins of Cybercrime: A Thematic Visualization.

More details of each of these themes and some of their implications for how we think about cybercrime are examined in Table 1. It is striking how, by utilizing just six thematic indicators, we can begin to look beyond the more familiar "technical-syntactic" events (shaded in blue) behind cybercrime. Instead, a more complex, more semantically oriented toolbox begins to emerge, one which allows us to excavate a far wider range of influences (shaded in grey) which have informed our perceptions of this variety of crime.

Table 1: Developing the Thematic Visualization

Theme	1991 Event	Thematic	Cyber Implications
E1	The filming of the *Lawnmower Man*	Featuring a computer animated journey into virtual space, the film was seminal in the gradual reinforcing of associations between the newly forged web and the fantasy of a non-physical alternative reality. This was one of several cultural productions (together with "cyberpunk" books like Neal Stephenson's *Snowcrash*[3]), which appeared to indicate how William Gibson's earlier idea of a "cyberspace" had become a material fact.	Enhancing the sense that a new frontier of boundless possibility had opened up where anything (legitimate **or** illegitimate) could now occur.
E2	Creation of the SFNet Coffee House Network in San Francisco	One of the key precursors of the "cyber-cafe" phenomenon (Bishop, 1992). The SFNet (which reified earlier online communities like the Well) was followed by several more developed examples such as Cyberia in London, which provided an early sense of the impacts of the web upon social interaction.	Highlighting the possibility that digital social connectivity might not only sponsor new varieties of digital community, but new ways of judging conduct and assigning blame. Online hate and trolling are among the results.
E3	'Rodney King' Incident	Images of the beating of Rodney King by LA police, recorded (in those pre-mobile cam days) on video-tape by a passer-by, were rapidly disseminated across the world. A key moment in the development of instantaneous witness and the "all-at-onceness" of contemporary life.	Anticipating the significant power of digital media to generate viral news stories and to create the sense that criminal accountability might both be far more universal while also becoming more subject to 'spin' and distortion.
E4	First Gulf War	As semi-automated, remotely controlled cruise missiles rained down upon Iraqi cities, viewers were able – for the first time –to tune in live to war via the new 24 hour news stations like CNN. With this, the idea developed of sanitized, "safe" war driven by the power of syntax/code to ensure maximum force with minimum casualties.	Indicating how the imagery of war would become blurred with the imagery of computer gaming and recycled as mass entertainment. The result would be a virtualization of destruction, where the borders between slaughter and spectacle were no longer clear.
E5	World's first GSM (2G digital mobile phone) call	In a curious coincidence with the origins of the web, this year saw the first successful demonstration of GSM (Global System for Mobile Communications), the (2G) protocols which set the first accepted standard for mobile communications networks. GSM now has over 90% market share.	Presaging a utopian future of seamless digital connectivity.
E6	Publication of "Safe Computing in the Information Age" (CSTB 1991)	One of the first significantly alarmist computer crime assessments, this report anticipated many of the key assumptions around how computers would come to dominate the crime landscape, from new varieties of digital theft through to the advent of cyber-terrorism	Creating the foundations of new certainty that the advent of connected computers means the advent of wholly new kinds of crimes waves.

[3] Completed in 1991, published in 1992.

By applying this (still relatively limited) toolbox, it becomes possible to make far more complex inferences about the development of cybercrime as opposed to recording exploits of gaps in Java or observing new variants in malware types. Consequently, by further combining these thematic indicators, wider inferences become possible. For example:

- **E2** + **E3** suggest how the link between spatio-temporally extended communities fostered by cybercafés, online fora, bulletin boards, and the globally circulated footage of the Rodney King beating contributed to the genesis of the "synopticon" (Mathieson, 1997) – and with that, the phenomenon of mass witness and instant accountability on the part of globalized audiences. The failure of this prototypical "citizen journalism" (Allen & Thorsen, 2009) to bring justice (all the officers filmed beating King were acquitted) predicted a further, darker side to the new digital society – a world where social media becomes so blurred with fake news that police officers captured on film in the act of shooting African American citizens are able to escape any criminal consequences.

- **E1 + E6** suggest how the eerily prescient claims about the potential of online fraud and terrorism contained in the Computer Science and Telecommunications Board (CSTB) report were quickly linked to the idea of a cyberspace. Not only does this evidence how far back many of the now familiar assumptions about the riskiness of the internet can be traced, but it also suggests how dissonances between utopian/dystopian perceptions of the virtual have contributed to the idea of a boundless, endlessly rising, or continually changing crime-type.

CONS – TWO FOUNDATIONAL MYTHS:

Thematic visualization offers only one among many other more "polymorphic" approaches to decoding the genealogy of discourses around cybercrime. Another potential approach involves textual analysis of how the terminology used to define perceived risks of digital connectivity evolved. For example, data-analysis tools such as Google's Ngram, which enables users to search for the frequency of terms within over 24 million published sources (Ophir, 2016), can help provide fascinating insights into our changing perceptions of the cyber-world. Even a cursory examination of the period from 1991 - 2000 highlights how, as the frequency of terms like "cybercrime" or "cyber threats" increase, the use of more positive terms like "cyberrights" gradually declines.[4]

What is striking when triangulating insights about cybercriminality on the basis of techniques like thematic visualization, textual analysis and so on, is just how profoundly conflicted our perceptions of digital connectivity were from the very outset. Two broad trends in our thinking about the "cyber" world and its benefits and harms soon become apparent; trends which now approach the status of foundational myths about online interaction and deviance. Since these myths remain central influences upon the contemporary understanding of digital technology and its criminal potentials, it is worth spelling them out in a little more detail. The first myth – which we can call "CON 1"– usually went something like this:

> **CON 1**
> Internet connectivity and online interaction offer one of the most significant social shifts in human history. Not only does it provide opportunities for radical improvements to life, enhancements to rights and unbounded freedoms, but also access to a wholly new kind of reality.

In hindsight, it is easy now to see how unrealistic CON 1 was and how it reflected the overly optimistic sense of faith in the magic of virtual space and its capacity to stand outside traditional

[4] See my 2008) paper for some specific analyses of this kind.

structures of governance. In other words, CON1 offers a clear manifestation of what has been called "digital utopianism" (cf. Turner, 2006, Dickel & Schrape, 2017), the excessively idealistic perception of new digital technologies common within sources of this early period (cf. Barlow, 1996, Levy, 1984, Rheingold, 1993).[5] As ever however, our often ambiguous perceptions of technology meant that such optimism was quickly tempered (Winner, 1997). Instead, the kinds of latent suspicions seen in E6 above fostered a growing belief that digital technology was more likely to *harm* society – especially by way of the new criminal opportunities it seemingly offered. Early texts such as Parker's (1976) *Crime by Computer* had proposed the conceptual *possibility* of computer crime, but the limited connectivity available at this time meant that by the onset of the 1980s, less than a thousand computer crimes had been recorded and many of these involved nothing more than the theft of a computer. Thus, the stark warnings about the criminal risks of information technology drawn out in the earlier thematic visualization were only a kind of prologue to a far more negative mindset which began to coalesce. Very quickly, the image of the hacker was recalibrated from romanticized technical genius to malevolent criminal mastermind (Steinmetz, 2016; Sterling, 1992); the media became increasingly obsessed with the internet as a site for sexual risk and shadowy predators, and an ever more insistent framing of online criminal activity in terms of striking, staggering, or exponential rises begin to typify coverage of cybercrime within the key sources of the time (McGuire, 2008). And, as the realities of all pervasive digital surveillance began to undermine the idea of cyberspace as a liberated (and liberating) space, a far more skeptical body of literature around internet life and culture began to develop (see amongst many examples, Carr, 2010; Margolis & Resnik, 2000; Morozov, 2011; Resnik, 1998). The scene was set for a catastrophization of online interaction, and with this, a second foundational myth about online activities – one now almost entirely inverse to the perceptions reflected in CON 1.

CON 2
Internet connectivity and online interaction constitute one of the greatest dangers ever posed to society, threatening a world of increasing risk, criminality, and/or social control.

Thinking in terms of CON2 did not just come to dominate the public imagination about cybercrime, it soon acquired a particular cachet within governance, criminal justice and media circles. Cyberspace was transformed from a space of exhilarating possibility into an unregulated, *anarchic* space – with the image of a digital "Wild-West" now serving as one of the recurring metaphors used to characterize it (Morris, 1998; Yen, 2002).

This catastrophic reinvention of cyberspace, which more varied methodological approaches can help tease out more clearly, remains integral to contemporary interpretations of cybercrime. In particular, it does much to explain why cybercrime has now become a kind of catch all explanation for almost every kind of criminal wrong. For example, even one of the best evidenced and most striking of longitudinal criminological trends – the ongoing fall in crime rates referred to as the "crime drop" (Farrell, 2013, Matthews, 2016, Tcherni et al., 2016) has now been brought into question when seen through the cybercrime lens. That is, rather than accepting more economical explanations for the crime drop – that it is a product of superior crime control, changes in the economic background, or simply part of a longer-term cyclical shift – there is now a suggestion that this was really a kind of fiction all along – a criminological equivalent of fake news. Rather, crime rates have been steadily rising all the time because of the explosive (though - of course – largely undetected) rises in cyber offenses (see Fitzgerald, 2014). Sweeping methodological changes imposed upon well-established crime metrics such as the England and Wales crime survey in order to detect and represent this hidden crime or to demonstrate how falling crime rates are offset by rises in cybercrime are among the many results of this shift in perceptions.

[5] Majid Yars' (2014) *Cultural Imaginary of the Internet* is well worth consulting on the way utopian and dystopian conceptions have shaped our perception of the internet.

The fact that both CON1 and CON2 manifest such simplistic "binaristic" views of digital technology (i.e., internet = "good" or internet = "bad") may be more than mere coincidence. Specifically, the influence of syntactic views of cybercrime suggest that such interpretations inherit a kind of machinic perspective – one where the opposing realities form a parallel *emotional* syntax – a "Boolean logic" of despair and fear. Within such an alphabet, hyperreal polarities like utopian/dystopian or liberating/enslaving act together with catastrophic binaries such bad/disastrous, serious/very serious, or out of control/beyond any control, to determine the very foundations of our thinking about cybercrime. In turn, the contradictory logics behind CON 1 & 2 and the growth in cyber-hysteria in the early to mid-phase of cybercrime development, are evidence for the contribution of syntactic views to the "cultures of fear" associated with cybercrime (Wall, 2008). Syntax is central to such fears for it merges neatly with a familiar cultural nightmare - the dread of man-made monsters, creatures we create, but which eventually act autonomously – i.e., outside of human jurisdiction. Such fears are deeply rooted within all human cultures and can be evidenced in various folk-nightmares such the Golem, Frankenstein (Curran, 2010), or more recently, the Skynet (King, 2017). In the cyber context, it is precisely because of the incomprehensible language of syntax which drives our digital machines that we see outcomes beyond our control. For though they are (ostensibly) mediated by human agents, machine behaviors - generated as they are by the cold logic of syntax, are not just "otherly", but alien.

CONstructions – The novelty of technical crime?

No matter how pervasive the culture of fear produced by the syntactic engines which drive cybercrime, such feelings could not have been sustained for long without more concrete and credible rationales. Key to such rationales has been a second line of thought which the thematic analysis suggested, and which is clearly discernible within CON1. This is the sense that "cyber" presents us with a form of criminal action and agency that is wholly unlike anything previously witnessed. Criminologists have often failed to point out the basic implausibility of this conclusion. The number of ways in which humans can harm other humans is ultimately rather limited - so genuinely novel harms are therefore rare. It is also clear that technological advances have regularly been associated with new kinds of crime or harm - whether these involve the increase in casualties following the introduction of gunpowder, the surge in intellectual property crime which arose with new printing technologies, worries about new risks posed by railway, automobile and other transport technologies, or the concerns about gambling and prostitution which arose with the development of the telephone (for these and other examples see McGuire, 2016b).

Why then has it been assumed that the information technology revolution has not followed the criminogenic template seen with these previous technological shifts and has instead spawned wholly *new* kinds of crime altogether? Here we see a second reason why drilling down into the distinction between syntactic and semantic views of cybercrime is valuable. That is, this perception of novelty is very much founded upon the use of syntactic devices like viruses and malware so that the uniqueness of cybercrime is not secured by its *technical* basis per se, but by syntax. Moreover, since code can play a causal role in such crime – often the primary causal role – computational crime does not appear to depend upon human agency to quite the same degree as traditional crime. Indeed, so different is this (technical) crime that the syntax which drives it seems as indifferent to its *own* well-being as it is to that of others. Particularly, as we know, not only can there be crimes *of* the machine, there can be crimes *against* the machine (Wall, 2005) (as for example where a DDos attack brings down a system or a network). The deference to syntax as the defining characteristic of cybercrime can be seen in the various attempts to characterize it. For example, malware and other code based forms of offending have sometimes been thought of as "pure" cybercrimes (Wall, 2004), just as the distinction often made between computer *dependent* and computer *enabled* crime (McGuire & Dowling, 2012) is really fundamentally a distinction between crime *driven* by syntax and more traditional crime types, which may have been syntactically augmented but which do not require it for their commission.

The influence of syntax in persuading us that cybercrime is best perceived as a novel (because technical) kind of offense has also been central in persuading us that the problem of regulating and responding to cybercrime represents something equally new. For when constructed as a problem of technical management cybercrime has appeared to confront criminal justice agencies with major, if not insurmountable challenges. Claims that police are too poorly equipped, undertrained, or lacking in technical skills for dealing with this range of offenses (HMIC, 2014; Leyden, 2001; Wall & Williams, 2013,) are familiar complaints, and similar concerns have been raised about how fit for purpose our legal systems are to cope with the transformation of crime into syntax. The view that legal practitioners cannot understand how to conduct cases requiring digital evidence has been suggested (see Brenner, 2012; Graff, 2016), but more serious consequences which may threaten the very foundation of legal process have also been recommended. Complications around digital evidence (e.g. difficulties of retrieval or suspicions of manipulation); an increasing dependence upon expert witnesses rather than legal professionals; or the recurring problem of transjurisdictionality, where the reach of domestic jurisdictions is limited by the capacity of cybercriminals to commit offenses abroad are all among the problems regularly identified here (McGuire, 2017).

But how sustainable is the idea that cybercrime poses such potentially destructive challenges to policing and the law? Do such difficulties really represent the kind of tipping point for policing and for criminal justice that a syntactic view of cybercrime suggests? The fact is that the history of policing has always been one marked by continual technological change and adaptation, from police whistles to the patrol car, and as such, policing is already a technical social institution (Bain, 2017). There has also been a string of successful policing operations in dealing with cybercrimes, such as the recent closure of the Silk Road dark web drugs market (Zetter, 2013), the apprehension of a Ukrainian broker behind the BTCe bitcoin money laundering scam (Gibbs, 2017), or various shutdowns of major botnets such Ramnit (Fox-Brewster, 2015). All of which suggests that law enforcement agencies are far from powerless when confronted with syntax driven criminality. It is equally clear that qualms about the "fit-for-purposeness" of the legal response to cybercrime may also be premature. There is no in principle difference between how the law prosecutes a cybercriminal and more traditional offenders given that in both cases, potential culprits must be identified and appropriate evidence gathered, which is then presented to neutral arbiters. There is also a long history of ways in which different technologies have been policed and legally managed. From the printing press to the motor car and beyond, new legal structures have invariably evolved to deal with new technologies. And such adaptations have usually occurred without the sense of crisis which now appears to confound attempts to enforce cybercrime legislation (McGuire, 2016b).

The construction of cybercrime as a wholly novel (because syntactic) kind of offense is thus open to a number of critical challenges. So too is the assumption that cybercrime is best defined in terms of its technical-syntactic nature. Take for example the idea that computer-dependent crime is a valid way of distinguishing the "real" cybercrimes from those which are merely "computer-enabled" or "assisted". On closer inspection, this distinction is not so easy to sustain. For example, though it is true that computer-enabled crimes (like fraud or theft) appear to be independent of syntax in that such offenses can also be enacted without computational support, it is also true that they are significant precisely because of the way that computers increase their scale, range, and force – properties which are of course wholly syntax dependent. Questions about the salience of such distinctions emerge with particular resonance in the legal context. Though laws like the U.K. Computer Misuse Act or the U.S. Computer Fraud and Abuse Act have created offenses around computer misuse, there is no significant difference in the legal principles driving prosecution of computer dependent *or* enabled offenses. That is, whether a prosecution involves defining examples of technical/syntactic criminality like malware creation or more simple offenses like the dissemination of a phishing email scam, convictions can only be obtained on the basis of a *mens rea* - an intention to do wrong. If, then, the law must treat cyber dependent crime like any other kind of

crime – as a fusion between the actual event (the *actus reus*) and a perpetrators intention to do wrong (the *mens rea*) – where then does this leave any substantive idea of criminal novelty?

Definitional problems of this kind echo those found in the broader literature around the syntax-semantics distinction. Here we see a range of difficulties in trying to demonstrate that syntax is *definitively* distinct from any semantics or that a semantics "comes out of a syntax". Searle's classic "Chinese room" argument can be considered as one example of the problems here (Searle, 1999). This thought experiment asks us to imagine someone in a sealed room who is shown cards inscribed with Chinese symbols. While they do not know the meaning of the symbols, they *do* know the rules (i.e., the syntax) which govern their use – that is, what kinds of symbol can legitimately follow other symbols. Thus, their responses to questions or communications should, in principle, be indistinguishable from a native speaker. However, this cannot be taken to mean that they understand Chinese, only that they can follow rules correctly. Searle's thought experiment was specifically designed to demonstrate that semantic facts like intelligence cannot be solely determined by a syntax. Specifically, even where every syntactic rule is being followed consistently and correctly, this is not a sufficient condition for meaning to emerge. Thus, any assumption that "real" or "pure" cybercrime is a purely technical crime will be hard to sustain if, as it seems it must, this definition relies on a viable distinction of the syntactic from the semantic. In the following section, some further consequences of such an assumption will be expanded upon, and the resulting need to revisit the idea of cybercrime as a technological rather than a technical offense will be explored.

misCON-ceptions

The tenuous reasoning behind any conclusion that cybercrime is technical *because* it is syntactic also needs to be examined in relation to a further, perhaps still more fundamental misconception that has shaped our views of cybercrime since the early 1990s – the failure to read it in terms of technology rather than the merely technical. The consequences of this failure have been serious. First, it has driven us towards technical solutions rather than responses to technology in its richer sense. Second, it has obscured the kinds of epistemic methods that might be effective in delivering actionable knowledge about cybercrime *as a species* of technology crime. In particular, it has diminished proper appreciation of key social-semantic aspects of cybercrime, such as the meanings or interpretations of what technological misuse involves or the varying modalities of its impact upon victims. Third, by focusing our attention so fully on the kinds of risks which syntax generates through malware or code, it has tended to obscure a more insidious range of risks posed by information technologies – not least their misuse by control agents. Finally, it has impeded effective evaluation of the comparative risks posed by other, arguably far more deadly technological forms.

Given that cybercrime is supposed to be the archetypical "technology crime," one might expect to find copious studies of how digital technology as a technology has engendered and furthered it. Yet, instead of some of the more critical discussions of technology as a construct found in earlier cybercrime literatures (Grabosky, 2001; McGuire, 2008; Yar, 2006), the technological aspects of cybercrime now tend to be taken for granted when evaluating cyber risk. We might justifiably ask then, what warrants the view that cybercrime represents one of the most serious of contemporary threats posed (by technology)? We know, for example, that automobile technologies generate a level of annual road casualties which far exceed any threat arising from computer misuse (cf. WHO, 2017). We know that the misuse of biological or chemical weaponry threatens a far greater catastrophe to human society than a temporary loss of internet connectivity (McGuire, 2012). And if – as every piece of credible scientific evidence suggests – the technologies contributing to climate change now threaten wholesale environmental disaster, why is this being treated as a lesser problem than data-theft by the corporate-State axis (Yeh, 2017)? Why are these and other examples not even discussed as "technology crimes?" Not only has the perceived threat from digital technology effectively drowned out the risks posed by other technologies, the perceived

seriousness of this threat has created an assumed need for "special powers" to manage it. The consequence has been more akin to a society on the brink of war than one where a new technology has impacted crime rates – and also in ways which structurally parallel previous technological shifts.

It is here that questions about the relationship between syntax and method in our understanding of cybercrime become central. That is, the assumption that cybercrime is a predominantly technical/syntactically driven issue has been a key driver behind the further assumption that *knowledge* about cybercrime is best gathered in largely technical, ergo numeric/syntactic – ways. Thus, the kind of cybercrime research seen as that with the highest utility has been the kind which favors those methods best attuned to numeric, codable representations of the problem. Take for example the prodigious flow of charts, tables, graphs, and other devices produced by internet security companies aimed at depicting the volumes, varieties, and spreads of global malware infections. These are familiar documents to any cybercrime researcher, and while they provide some degree of insight, they offer little understanding about the causes and characteristics of cybercriminality. Specifically, no matter how graphically or emotively compelling such tables may be, all that is really recorded are certain kinds of volumes, many involving incidents which are not even definitively criminal. As we all know, such "research," even though it is usually laden with vested interests (Yar, 2008) has been responsible for many of the alarmist headlines about cybercrime, and its emotional impacts have often deflected appropriate critical attention paid to the methods used. In spite of this, there has often been as much dependence upon such sources within scholarly research as there has been in the popular media and this has decisively colored what we (think) we know. The predilection for prevalence metrics, cost metrics (Anderson et al., 2013), or measures of percentage rises or falls (invariably rises) in various categories of cybercrime has been one obvious result. And even though research using vague descriptive variables such as "experience of cybervictimization" or "understanding of cybersecurity" has provided a façade of greater sophistication, the ultimate aim usually remains centered upon the goal of producing findings amenable to display in graphs or tables. Even where there have been attempts to deepen understanding – for example by examining the character or motivations of the (remarkably few) cybercriminals who have been apprehended, such studies have tended to rely upon fairly limited demographic or psychological indicators, such as age or willingness to take risks (Aiken et al., 2016; Bachmann, 2010).

The governing perception that our most reliable insights about cybercrime are those obtained via syntactic approaches like quantitative survey research or numeric measures like cost has tended to obscure three methodological problems. First, there is an epistemic gap that lies between technical, cybersecurity driven evaluations of cybercrime and conclusions obtained via more robust social research methods. Since there are no agreed ways of relating – say – a malware report to a survey measure of cybervictimization, there can be no robust justifications for claiming that examples of the former either supports or refutes the latter. Put bluntly, there are simply no reliable comparative metrics which permit us to make the kinds of associations between data gathered in cybersecurity contexts and social science data relating to agency and intention in cybercriminality. Yet, such associations have often been the foundation of causal claims about cybercrime (see amongst many others, Cisco, 2016; Macaffe, 2016; NCA, 2016; Symantec, 2017,). Second, the relative novelty of cybercrime as a criminological phenomenon means that there is little in the way of long-term, well-documented trends against which any credible quantitative patterns that have been detected can be tested or compared. We are literally "in the dark" about meaningful longitudinal trends here, though one would never know it given the authoritative tone in which cataclysmic judgments about the direction of cybercrime are so often made. Third, even judged in terms of fairly limited criteria for quantitative research, knowledge about cybercrime has rarely met very exacting standards or been based on any very advanced methodological techniques. For example, there has been little in the way of effective random control testing and minimal use of

more sophisticated analytic techniques such as multivariate analysis, multi-level modeling, factor analysis, Bayesian estimation, simulation, and so on.

Cybercrime research is of course not alone in the naive assumption that what Jock Young (2011) once called "the numbers game" offers the most reliable basis for conclusions about the social world. As Young (2011) pointed out, like social research in general, within cybercrime research, "reality has been lost in a sea of statistical symbols and dubious analysis" (p.viii). Yet, if cybercrime poses the kinds of societal risk we are told that it does, then dependence upon such a limited epistemological palette surely poses a greater risk - that we end up missing significant threats hidden within the granular details. It is not that the kind of data which could provide this more comprehensive picture is wholly absent, and there have certainly been some attempts to view the problem at the micro-level. For example, Williams (2006) research was an early attempt to deploy ethnographic methods in studying online regulation; Holt and Graves (2007) used a qualitative approach to analyze the content of advance fee fraud messages; Hutchings, (2013) combined findings from an analysis of selected court documents with interview data from law enforcement officers within computer crime or fraud specialist units to develop a qualitative study of motivational factors in online fraud and hacking. Elsewhere, Whitty's (2012) work and similar research used posts from online support groups or interview data with victims to construct a picture of online dating scams. It would be interesting to do a comparison of the relative proportions here, yet the suspicion must be that the volume of qualitative cybercrime data remains inferior to its quantitative counterpart. And even where it is available, the depth of insight in interpreting the data has often been limited. It is one thing to collect interview data with perpetrators, victims, cybersecurity professionals, and other relevant agents, or to point to thematic commonalities within such data; however, it is quite another to draw out the kinds of rich conclusions from such interviews about social life that are foundational to the best kinds of qualitative research such as Benjamin's (1999) Arcades Project, Park and Burgess's (1925) fieldwork in Chicago, or Goffman's (1959) micro analyses of the all-but invisible rituals, norms, and behavioral expectations which striate social life. Existing qualitative work has also often tended to be preoccupied with an underlying policing or criminal justice agenda (how do findings 'prevent cybercrime' or lead to more arrests of cybercriminals) rather than developing the kind of deeper variable set required to move our understanding of cybercrime onto a properly social scientific footing.

What options then are there for building up more qualitatively focused cybercrime research, research which might act as a better balance to the volume of numeric/syntactic work that is available? One relatively straightforward option would be to draw upon a greater range of informants to widen understanding, or perform more detailed studies of the behavior of cybercriminals. An additional approach might involve adding to or enhancing existing discourse analysis of online discussions in chatrooms or web forum data (see for example Wong et al.'s, 2015 analysis of white supremacists' online discussions). Fostering better understanding of the dynamics and strategies of cybercriminality similar to those explored in Holt and Bossler's (2016) work on "honeypots" offers another option. Enhancing the range of case studies available to researchers would also permit a more full-spectrum exploration of specific instances of cybercriminality. For example, it might generate more detailed profiles about relevant protagonists - from the planning and inception stage through to the crime and subsequent criminal justice response. Genealogical approaches such as that seen in the earlier thematic analysis might usefully contribute to case study work by setting it an appropriate socio-historical framework (even if that history only stretches back to 1991, or to earlier "proto-histories" of digitally connected interaction). More temporally focused work is lacking – especially in relation to time dynamic factors like the evolution of cybercrime events or co-evolutionary interactions between cybercriminal and cybersecurity actors (McGuire, 2018, in preparation). There is also ambitious work to be done in developing more detailed ethnographies around cybercrime, including those that foster greater understanding of the cultural or wider societal factors in the framing of cybercriminality. More ambitious still would be the use of phenomenological approaches in order to construct a more vivid portrait of the subjective life

worlds of cybercriminals, their victims, those who attempt to regulate such offenses and beyond, as well as a wider selection of actors who contribute to the cybercrime act. The use of phenomenological tools like the *epoché* or *bracketing* of experience (cf. Psathas, 1973; Schutz, 1967,) to discern the key constituents of such acts offers the prospect of the kind of perspectives which have barely been considered as of yet.

However, major problems inevitably remain for the construction of a more effective qualitative cybercrime knowledge base. Aside from the usual questions about how objectively useful qualitative data can be (cf Kirk & Miller, 1985), there is always a suspicion that where qualitative cybercrime research *has* been conducted, it has tended to be received with a degree of condescension. Worthy, but little more than a corrective footnote to the "more reliable" syntactic/quantitative approaches. Such research has also tended to depend upon those types of respondents who are the most accessible - i.e., those from the control side (such as law enforcement) or the very few victims and perpetrators who are willing to talk. The danger then is that this leaves us with lopsided perspectives on the problem which – however unintentionally – simply reinforces the authority of more syntactically driven perspectives rather than counterbalancing them. At the same time, the fact that certain forms of cybercriminality (like malware creation) do have a strong syntactic element means that ways must be found which balance qualitative with quantitative understanding while avoiding one set of insights becoming submerged or sidelined by the other. At present, we are far away from any kind of useful interplay between quantitative and qualitative approaches to cybercrime. And appeals to mixed methods approaches will not fill the gap since they tells us little about how to tease out the relevant theoretical and empirical correlations and continuities across differing dataset types.

A crucial consideration for any more developed approach to cybercrime knowledge is the need to avoid over mechanical applications of established criminological theories as a device to suggest that a greater understanding has been attained. While it is of course useful to explore how standard criminological frameworks like routine activities, strain theory, subcultural theory, control theory, and the like can help ground our understanding of cybercriminality (see Hay et al., 2010; Holt, 2013; Yar, 2006, for discussions here), this should never stand as a substitute for more direct engagements with the problem. Instead, a more distinctive and self-standing body of cybercrime theory is required, one which can bring together traditional criminological thought and method with new frameworks more appropriate for digital technologies and the psycho-social spatial transformations these induce. In general, the failure to properly engage with the wealth of theory about technology that exists has been a particularly striking omission in this regard. The kind of human-social understanding of technology which has been such a central factor within the philosophy and sociology of technology would do much in helping redress the assumption that cybercrime is a technical rather than a technological problem. In particular, Heidegger's (1977) observation that the "essence of technology is not technological" (p.4) or the phenomenological approaches to technology it inspired like Ellul (1964) or Borgmann (1984) have never been properly related to the implications of digital technology. This is despite their value in explaining why technology is as much a cultural artefact as it is a technical one. Other influential perspectives about technology arguably provide a still more tangible human-centered understanding, with the extensionalist approach pioneered by McLuhan (1964 as well as Brey, 2016; Gehlen 1965,) of special note here. Extensional views that treat technology as a literal "extension" of the body help rule out the "instrumentalist" claim that technology is a socially neutral object merely waiting to be used by humans (Feenberg, 2002). And, since extension entails that technology is not just part of us, it *is* us, such views also help explain why technology crimes are just as human-centered as crimes involving our hands or other parts of our bodies. "Post-human" perspectives on technology go even further than this, positing the kind of fusions between the human body and technology – whether as a cyborg or as an actor-network – which make it completely impossible to separate the technical from the human (Haraway 1991; Latour 1987). In so doing, post-humanism also undermines any credible sense in which syntactic/semantic distinctions illuminate the coupling of

criminal agency with digital technology. There are the glimmerings of a realization that such richer frameworks might be useful (see van der Wagen, 2018, this issue). For the most part however, technology has usually been taken as a given in most discussions of cybercrime. Where there has been a direct focus upon it, this has tended to involve obsessive descriptions of the relevant "kit," such as the kinds of operating systems in play, the variety of software protections being utilized, or the influence of emerging digital technologies like IoT, the Cloud, and so on.

Thus, to create an effective semantics of cybercrime, one which can reclaim it as the socio-cultural process that it always has been, we will need interpretations of digital technology that transcend its operations as a syntactic engine and which bridge the ostensibly opposing polarity between syntactic and semantic considerations. If this can be done, it will help underline just how far the more challenging perspectives seen at the early stages of cybercrime research have become confined within self-justifying intellectual loops which tell us what we want to hear rather than what we need to know. In turn, it would offer vital support to the kind of cybercrime scholarship which properly engages with the socio-technical fusions which now surround us. In a post-truth age, it is perhaps appropriate that our understanding of what is so regularly characterized as "one of the most novel of all contemporary criminal threats" centers on little more than the oft repeated tautology that "it is one of the most novel of all contemporary criminal threats" rather than proper, structured comparative evaluation of its technological risk and the human factors behind it.

CONCLUSION

It is hard to evade the feeling of having been framed in the framing of computer crime. Computer crime's genealogy, distorted as it has been by the two foundational myths of digital utopianism and digital catastrophe, has never been properly situated within the complex social realities which gave rise to digital crime; nor has its construction as a predominantly syntactic-technical form of crime ever been effectively challenged or related to the rich body of thought about technology and its relations with the social world which is available. The result has been a series of misconceptions – not just about what cybercrime is, or the methods required to develop properly evidenced knowledge around it, but more seriously about the kinds of risk it poses. Even those originally responsible for developing the technical structure of the web have been long been aware that its structure now needs to move beyond the simple syntax which underpinned its origins and to be rethought in more semantic terms – such as in the Web 3.0 idea (Antoniou & Harmelen, 2008). What this means in practice is still a moot point, but at minimum, most agree that it must involve better integration of social factors like trust into the way we interact online. It is odd then that the "social-semantic factors" (cf. Breslin et al., 2010) which are the real facilitators of cybercrime remain so minimally explored within cybercrime theory itself. For the meanings of cybercrime to those who perpetrate it, those who are victims of it, and those who seek to control it remain largely untapped methodological resources at present. A new stage of cybercrime scholarship, one as equally tuned to its real foundation as to those technical solutions imagined to "really work" awaits development.

REFERENCES

Aiken, M., Davidson, J, & Amann, P. (2016). *Youth pathways into cybercrime*. Research Whitepaper. Retrieved from https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/Pathways-White-Paper.pdf.

Allen, S., & Thorsen, E (Eds.) (2009). *Citizen Journalism: Global Perspectives*, Peter Lang

Anaïs, S. (2013). Genealogy and critical discourse analysis in conversation. *Critical Discourse Studies*, 10(2), 123-135.

Anderson, R., Barton, C., Böhme, R., Clayton, R., Van Eeten, M. J., Levi, M., Moore, T., & Savage, S. (2013). Measuring the cost of cybercrime. In R. Böhme (Ed.), *The economics of information security and privacy* (pp. 265-300). Heidelberg: Springer.

Antoniou, G., & van Harmelen, F. (2008). *A Semantic Web Primer*, (2nd Edition), MIT Press.

Bachmann, M. (2010). The risk propensity and rationality of computer hackers. *International Journal of Cyber Criminology*, 4(1 & 2), 643–656.

Bain, A. (2017). *Law enforcement and technology: Understanding the use of technology for policing*. London: Palgrave Macmillan.

Banks, M. (2001). *Visual methods in social research*. London: Sage.

Barlow, J. P. (1996). A declaration of the independence of cyberspace. In J. Casimir (Ed.), *Postcards from the Net: An intrepid guide to the wired world* (pp. 365-367). Sydney, Australia: Allen and Unwin.

Benjamin, W. (1999). *The arcades project*. Cambridge: Belknap Press of Harvard University Press

Bishop, K. (1992, August 2). The electronic coffeehouse. *The New York Times*, p. V3. Retrieved August 16, 2018 from http://search.proquest.com.er.lib.k-state.edu/docview/108873126?accountid=11789.

Breslin, J. Passant, A., & Decker, S. (2010). *The social semantic web*. Berlin: Springer.

Borgmann, A. (1984). *Technology and the character of contemporary life*. Chicago: University of Chicago Press.

Bowman B. (2007). Foucault's "philosophy of the event": Genealogical method and the deployment of the abnormal. In Hook, D. (Ed.), Foucault, *psychology and the analytics of power: Critical theory and practice in psychology and the human sciences*. London: Palgrave Macmillan.

Brenner, S. (2012). *Cybercrime and the law: Challenges, issues, and outcomes*. Boston MA: North Eastern University Press.

Brey, P. (2016). Theorising technology and its role in crime and law enforcement. In M. McGuire & T. Holt (Eds.), *The handbook of technology, crime and justice* (pp. 17-34). London: Routledge.

Carr, N. (2010). *The shallows: How the internet is changing the way we think, read and remember*. New York: W.V. Norton and Company.

Cisco, (2017). Cisco annual security report. Retrieved from http://www.cisco.com/c/en/us/products/security/security-reports.html.

CSTB. (1991). Computers at risk: safe computing in the information age. Computer Science and Telecommunications Board, National Academies Press. Retrieved from http://www.nap.edu/books/0309043883/html/index.html.

Curran, B. (2010). *Man-made monsters: A field guide to golems, patchwork soldiers, homunculi, and other created creatures*. Wayne, NJ: Career Press.

Deleuze, G. (1992). *Postscript on the societies of control*. *October* Vol. 59. (Winter, 1992), pp. 3-7.

Dickel, S., & Schrape, J. (2017). The logic of digital utopianism. *NanoEthics*, 11(1), 47-58

Ellul, J. (1964). *The technological society*. New York: Vintage Books.

Farrell, G. (2013). Five tests for a theory of the crime drop**.** *Crime Science: An Interdisciplinary Journal*, 2:5 DOI: 10.1186/2193-7680-2-5

Feenberg, A. (2002). *Transforming technology: A critical theory revisited*. New York: OUP.

Fitzgerald, M. (2014). The curious case of the fall in crime. The Economist (20 July 2014)

Fox-Brewster, T. (2015, February 25). European cyber police try to shut down ramnit botnet that infected 3 million. *Forbes*. Retrieved from https://www.forbes.com/consent/?toURL=https://www.forbes.com/sites/thomasbrewster/2015/02/25/ramnit-cybercrime-malware-takedown/.

Gehlen, A. (1965). Anthropologische ansicht der technik. In H. Freyer, H., J. C. Papalekas, & G. Weippert (Eds.), *Technik im technischen zeitlater* (pp. 101-118). Dusseldorf, Germany: J Schilling.

Gibbs, S. (2017, July 7). ”Criminal mastermind” of $4bn bitcoin laundering scheme arrested. *Guardian*. Retrieved from https://www.theguardian.com/technology/2017/jul/27/russian-criminal-mastermind-4bn-bitcoin-laundering-scheme-arrested-mt-gox-exchange-alexander-vinnik.

Goffman, E. (1959). *The presentation of self in everyday life*. Harmondsworth, UK: Penguin.

Grabosky, P. (2001). Virtual criminality: Old wine in new bottles? *Social and Legal Studies*, 10(2), 243-249.

Graff, G. (2016, September 23). Government lawyers don’t understand the internet. *The Washington Post*. Retrieved from https://www.washingtonpost.com/posteverything/wp/2016/09/23/government-lawyers-dont-understand-the-internet-thats-a-problem/?utm_term=.4607e03c8c71.

Hackstaff, L. H. (1966). The consistency and completeness of formal systems. In his *Systems of formal logic*, p.193-206, Dordrecht, Holland: Springer, Dordrecht.

Haraway, D. (1991). A cyborg manifesto: science, technology, and socialist- feminism in the late twentieth century. In *Simians, cyborgs and women: The reinvention of nature* (pp. 149-181). New York; Routledge.

Hay, C., Meldrum, R., & Mann, K. (2010). Traditional bullying, cyber-bullying and deviance: A general strain theory approach. *Journal of Contemporary Criminal Justice*, 26, 130-147.

Heidegger, M. (1977). The question concerning technology. In W. Lovitt (Ed.), *The question concerning technology and other essays* (pp. 3-35). New York: Harper & Row.

HMIC. (2014). The strategic policing requirement: large scale cyber-incidents. *Her Majesty's Inspectorate of Constabulary Report*. Retrieved from https://www.justiceinspectorates.gov.uk/hmic/wp-content/uploads/strategic-policing-requirement-cyber-crime-2014-06.pdf.

Holt, T. (Ed) (2013) *Cybercrime and Criminological Theory Fundamental Readings on Hacking, Piracy, Theft, and Harassment*, San Diego, Cognella

Holt, T., & Bossler, A. (2016). *Cybercrime in progress: Theory and prevention of technology enabled offenses*. London: Routledge.

Holt, T., & Graves, D. (2007). A qualitative analysis of advance fee fraud e-mail schemes. *International Journal of Cybercriminology*, 1, 137-154.

Hutchings, A. (2013). Hacking and fraud: A qualitative analysis of online offending and victimisation. In K. Jaishanker (Ed.), *Global criminology: Crime and victimization in a globalized era*. London UK: CRC Press.

Infosec (2017) 'Technical Anti-Phishing Measures'. Retrieved from http://resources.infosecinstitute.com/category/enterprise/phishing/phishing-countermeasures/technical-anti-phishing-techniques/#gref

King, B. (Ed) (2017) *Frankenstein's Legacy: Four Conversations about Artificial Intelligence, Machine Learning, and the Modern World*, Carnegie Mellon University: ETC Press

Kirk, J., & Miller, M. (1985). *Reliability and validity in qualitative research.* London: Sage.

Leonhardt, E., & Röttger, S. (2006). Semantics in philosophy and computer science. University of Dresden technical papers. Retrieved from http://www-st.inf.tu-dresden.de/files/teaching/ws06/HS/Leonhardt-Paper-Introduction.pdf.

` Latour, B. (1987). *Science in action: How to follow scientists and engineers through society*. Cambridge: Harvard University Press.

Lessig, L. (1999). *Code and other laws of cyberspace*. New York: Basic Books.

Leukfeldt, R. (Ed) (2017) *Research Agenda: the Human Factor in Cybercrime and Cybersecurity, Hague*: Eleven

Levy, S. (1984) *Hackers: Heroes of the Computer Revolution,* Sebastopol CA: O'Reilly Media

Leyden J. (2001, June 30). European police ill-equipped to tackle cybercrime. *Register*. Retrieved from https://www.theregister.co.uk/2001/06/30/european_police_illequipped_to_tackle/.

Lycan, W. (2000). *Philosophy of language: A contemporary introduction*. London: Routledge.

MacAfee (2016) *McAfee Labs 2016 Threats Predictions* report, Retrieved from https://securingtomorrow.mcafee.com/mcafee-labs/mcafee-labs-2016-threats-predictions-report-forecasts-changes/

Marcuse, H. (1982). Some social implications of modern technology. In A. Arato & E. Gebhardt (Eds.), *The essential Frankfurt school reader* (pp. 138-162). New York: Continuum.

Matthews, R. (2016). Realist criminology, the new aetiological crisis and the crime drop. *International Journal for Crime, Justice and Social Democracy*, 5(3), 2-11.

Mathiesen, T. (1997). The viewer society. *Theoretical Criminology*, 1(2), 215-234

McGuire, M. (2008). *Hypercrime: The new geometry of harm*. London: Glasshouse.

McGuire, M. (2012) *Technology, Crime and Justice*, London: Routledge

McGuire, M. (2016a) 'Cybercrime 4.0: Now what is to be done?' in Matthews, R. *What is to be Done about Crime and Punishment*?. Palgrave

McGuire, M. (2016b) Technology Crime and Technology Control; Contexts and History, in McGuire & Holt (Eds.) *The Handbook of Technology, Crime and Justice*, London: Routledge pp. 35-60

McGuire, M. (2017) "Law in The Balance: The Challenge of Cybercrime 4.0" (*forthcoming*)

McGuire, M. (2018) "Cybercrime as a co-evolutionary relationship: Findings from the ACCEPT project (*in preparation*)

McLuhan, M. (1964). *Understanding media: The extensions of man*. New York: McGraw Hill.

Morriss, A. (1998). The Wild West meets cyberspace. *The Freeman*, Retrieved from https://fee.org/articles/the-wild-west-meets-cyberspace/

Morozov, E. (2011). *The Net delusion: The dark side of internet freedom*, New York: PublicAffairs

Müller, V. C. (2014). Pancomputationalism: Theory or metaphor?. In R. Hagengruber & U. Riss (Eds.), *Philosophy, computing and information science: History and philosophy of technoscience 3* (pp. 213-221). London: Pickering & Chatto.

NCA. (2016). Cybercrime assessment 2016. *National Crime Agency*. Retrieved from http://www.nationalcrimeagency.gov.uk/publications/709-cyber-crime-assessment-2016/file.

NCSC. (2016) 10 Steps: Malware Prevention, UK National Cyber Security Centre advice note 8/8/2016 Retrieved from: https://www.ncsc.gov.uk/guidance/10-steps-malware-prevention)

Noik, R. (2011). AVG report warns about cybercrime catastrophe, *TechSmart*, Retrieved from http://www.techsmart.co.za/features/news/AVG_report_warns_about_cyber_crime_catastrophe.html

Ophir, S. (2016) 'Big data for the humanities using Google Ngrams: Discovering hidden patterns of conceptual trends' *First Monday*, 21(7) doi: http://dx.doi.org/10.5210/fm.v21i7.5567

Park, R. E., Burgess, E., & McKenzie, R. (1925). *The city*. Chicago: University of Chicago Press.

Parkes, A. (2002). *Introduction to languages, machines and logic: Computable languages, abstract machines and formal logic*. London, UK: Springer-Verlag.

Psathas, George, ed. (1973). *Phenomenological sociology: Issues and applications*. New York USA: John Wiley & Sons.

Resnik D. (1998). Politics on the internet: The normalization of cyberspace, in Toulouse, C. & Luke, T. (Eds) *The Politics of Cyberspace,* 48-68, London: Routledge

Rheingold, H. (1993). *The virtual community: Homesteading on the electronic frontier*. Reading, MA: Addison-Wesley.

Savat, D., & Poster, M. (2005). *Deleuze and new technology*. Edinburgh, UK: Edinburgh University Press.

Schutz. A. (1967). Phenomenology and the social sciences', in Natanson, M.A., van Breda, H.L. (Eds.) *Collected Papers: I. The problem of social reality*. 118-139, La Haya, Martinus Nihoff

Searle, J. (1999). The Chinese room. In Wilson, R. & Keil, F. (Eds.), *The MIT encyclopedia of the cognitive sciences*. Cambridge, MA: MIT Press.

Steinmetz, K. (2016). *Hacked: A radical approach to hacker culture and crime*. New York: NYU Press.

Sterling, B. (1992) *The hacker crackdown: Law and disorder on the electronic frontier*. New York NY: Bantam Books.

Stich, S.P. (1983). *From folk psychology to cognitive science*. Cambridge, MA: MIT Press.

Symantec (2017) Internet Security Threat Report 2017, Retrieved from https://www.symantec.com/security-center/threat-report

Tcherni, M., Davies, A., Lopes, G., & Lizotte, A. (2016). The dark figure of online property crime: Is cyberspace hiding a crime wave? *Justice Quarterly*, *33*(5), 890-911.

Tufte, E. R. (2006). *Beautiful evidence,* Cheshire, CT: Graphics Press.

Turner, F. (2006). How digital technology found utopian ideology: lessons from the first hackers' conference. In D. Silver & A. Massanari (Eds.), *Critical cyberculture studies: Current terrains, future directions,* 257-269. New York, NY: New York University Press.

Van der Wagen, W. (2018). The cyborgian deviant: An assessment of the hacker through the lens of Actor-Network Theory. *Journal of Qualitative Criminal Justice and Criminology, 6(2)*157-178.

Wall, D. S. (2004). 'Digital realism and the governance of spam as cybercrime. *European Journal of Criminal Policy and Research,* 10(4) 309-335.

Wall, D.S. (2005, revised in 2010). 'The internet as a conduit for criminal activity'. In Pattavina, A. (Ed.), *Information technology and the criminal justice system* 78-94. Thousand Oaks, CA: Sage Publications.

Wall, D.S. 2008 'Cybercrime and The Culture Of Fear', *Information, Communication & Society*, 11:6, 861-884,

Wall, D., & Williams, M. (2013). Policing cybercrime: Networked and social media technologies and the challenges for policing. *Policing and Society: An International Journal of Research and Policy,* 23(4), 409-412.

WHO (2017). Road Traffic Deaths (by country)' World Health Organization, Retrieved from http://apps.who.int/gho/data/node.main.A997

Whitty, M. (2012). The Psychology of the Online Dating Romance Scam, Project report, Retrieved from https://www2.le.ac.uk/departments/media/people/monica-whitty/Whitty_romance_scam_report.pdf

Williams, M. (2006). *Virtually criminal*. London: Routledge.

Winner, L. (1997). Technology today - utopia or dystopia? *Social Research* 64(3), 989-1017

Wong, M., Frank, R., & Allsup, R. (2015). The supremacy of online white supremacists – an analysis of online discussions by white supremacists, *Information & Communications Technology Law*, 24(1), 41-73

Yar, M. (2005). The novelty of cybercrime: An assessment in light of routine activity theory, *European Journal of Criminology*, 2, 407-427.

Yar, M. (2006) *Cybercrime and Society*, London: Sage

Yar, M. (2008) "The Computer Crime Control Industry: The Emerging Market in Information Security" in K. Franko-Aas (Ed) *Technologies of InSecurity: Surveillance and Securitisation of Everyday Life*, 189-204, London: Routledge

Yar, M. 2014 *The Cultural Imaginary of the Internet: Virtual Utopias and Dystopias,* London: Routledge

Yeh, J. (Ed) (2017) *Climate Change Liability and Beyond*, Taiwan: National Taiwan University Press

Yen, A. C. (2002). Western frontier or feudal society? Metaphors and perceptions of cyberspace. *Berkeley Technology Law Journal*, 17, 1207-1263

Young J. (2011). *The criminological imagination*, London: Polity.

Zetter, K. (2013, November 18). 'How the feds took down the silk road drug wonderland'. *Wired*. Retrieved from https://www.wired.com/2013/11/silk-road/.

Michael McGuire (m.mcguire@surrey.ac.uk) is a senior lecturer in criminology at the University of Surrey. His work has focused upon critical approaches to cybercrime and to the study of technology and the justice system more widely. His most recent book *The Handbook of Technology, Crime and Justice*, (Routledge 2016, with Tom Holt) sets out the first holistic view of the role of differing technologies across each stage of the criminal justice process.

The Cyborgian Deviant: An Assessment of the Hacker through the lens of Actor-Network Theory

Wytske van der Wagen[1]
Erasmus School of Law, Department of Criminology

Abstract

When we think of technocrime, it is immediately "the hacker" who comes to mind, a somewhat mystical figure who can do seemingly magical as well as malicious things with technology. Throughout history, various scholars, including criminologists, have sought to grasp the hacker phenomenon so as to unravel hackers' techno-culture, identity, and mentality. The current study is one of them, yet it does so from a novel, less anthropocentric angle. Drawing on the cyborg-lens of actor-network theory, which considers the human and the technical as non-separable, this study conceives the hacker as a "cyborgian deviant:" a transgressive blend of human and technology. Such perspective puts the human-technology relationship more on the frontline of the analysis, enabling us to gain a more nuanced understanding of how hackers' (deviant) relationship with technology can take shape. Based on 10 interviews with hackers, the study revealed that being and becoming a hacker cannot be understood in separation from how they interact with, through, and against technology. Whether engaged in licit or illicit hacks, hackers seek to simultaneously set, explore, and extend the boundaries of technology and themselves, while also blurring the boundaries between good and evil along the way.

Keywords: hackers, cyber deviance, cyborgs, actor-network theory, human-technology relationship

INTRODUCTION

Over the last few decades, hacking and other forms of technocrime have become a major public concern. Almost on a daily basis, we are confronted with cyber incidents that lead to severe technological and financial damage for companies, organizations, governments, and people. In 2012 in the Netherlands for example, a 17-year-old hacker was arrested and prosecuted for hacking several servers of a major Dutch telecom company wherein he was nearly successful in making the national emergency number completely unreachable (see NOS, 2012). In 2013, a

[1] I would like to thank René van Swaaningen, Martina Althoff, and the three anonymous reviewers for their constructive and valuable comments on the earlier draft of this article. Address correspondence to: P.O. Box 1738, 3000 DR Rotterdam/The Netherlands. Email: vanderwagen@law.eur.nl. Website: https://www.eur.nl/people/wytske-van-der-wagen/

19-year-old hacker was arrested for hacking at least 2,000 computers and webcams by means of a so called "remote access toolkit" (RAT), an easy online to purchase tool on the Internet that enables someone to remotely take over a computer. He stole nude photos from the hacked computers and spread them on social media. The involved hacker claimed in court that he was "hypnotized by the opportunities of technology" (see Tweakers, 2014). Apparently, for some youngsters, Information and Communication Technology (ICT) has become an interesting new field or toy to play with (Turgeman-Goldschmidt, 2005) and engage in illicit activities. Moreover, the Internet nowadays provides the tools, information, and videos on how to do it anonymously without any restrictions barring the (malicious) usage and exploration of computer technology.

At the same time, a large part, or even the majority of the hacker community, (still) consists of hackers who do not intend to cause any harm (Steinmetz, 2015), and who explicitly dissociate themselves from the above types of "hacks" or hackers (Van der Wagen, Van Swaaningen & Althoff, 2016). For instance, so called "white hat" or ethical hackers search for leaks or "bugs" in security systems in order for them to get fixed and they also have their own specific ethical beliefs (Van't Hof, 2015). The same counts for those active in "hacker spaces," offline meeting places where people gather to tinker with hardware, software, and electronics. Hence, it is worth keeping in mind that the hacker landscape consists of different hacker groups with various skills, moral perceptions, and "usages" of computer technology (Holt & Kilger, 2008), both licit and illicit or somewhere in between (Blankwater, 2011; Steinmetz, 2015).

Over time, various scholars, including criminologists, have sought to grasp the hacker phenomenon so as to unravel the features of hacker culture and ethics (e.g., Himanen, 2001; Levy, 1984; Taylor, 1999), hackers' relationship with technology (e.g., Jordan & Taylor, 1998; Turkle, 1984), and how hackers construct their deviant identity (e.g., Turgeman-Goldschmidt, 2008; Van der Wagen et al. 2016). The current study is one of them, yet it does so from a novel approach. It departs from the notion that hackers – whether they are engaged with technology in a deviant or non-deviant manner – require an approach that puts the human-technology relationship more on the frontline of the analysis. It argues that we can obtain a more nuanced view of their drives, perceptions, and beliefs when we move beyond the anthropocentric lens of existing approaches (e.g., Becker, 1963; Katz, 1988; Matza, 1969), which ultimately place human agency in the center of inquiry and treat technology in a rather passive way (see also Brown, 2006). Against this background, this study uses the cyborg-perspective of actor-network theory (Latour, 2005), which presumes that human actions, decision-making, and sense-making cannot be separated from the objects, technologies, and artifacts they use or engage with. It offers a framework that enables us to grasp the various ways in which the human-technology relationship can take shape. Accordingly, this study conceives and studies the hacker as a "cyborgian deviant:" a transgressive blend of human and technology. In this context, the article builds on the "cyborg-crime" perspective outlined by Van der Wagen and Pieters (2015), which proposes a hybrid understanding of agency in the course of deviant action.[2] In the current study, this perspective is used to examine and interpret the manner in which the human-technology relationship manifests itself in the hacker phenomenon. The main question the study seeks to

[2] See also Suarez's (2015) study, which considers the cyborg-concept valuable for a thorough understanding of cybercrime.

answer is: How do hackers give meaning to themselves and their actions, and how is this co-shaped by their (deviant) relationship and engagement with technology?

For this study, 10 in-depth interviews were conducted with both hackers that were engaged in illicit hacking activities, and those that mainly act(ed) within the boundaries of the law. The findings revealed that hackers - whether engaged in licit or illicit hacks - perceived themselves as actors with a specific skillset and mindset that set them apart from ordinary people and criminals. Through their engagement with hacking, they sought to simultaneously set, explore, and extend the boundaries of technology and themselves, while also blurring the boundaries between good and evil along the way. The interviewed hackers believed to embody various features of the cyborg figure, which was both visible in the way they described their relationship with technology and in regards to how they saw themselves in relation to others.

The article starts with a short discussion on the social construction of hackers, which includes an examination of the inseparability of hackers and the world of computer technology. Hereafter, the article discusses how existing studies capture the hacker-technology relationship and why the cyborg-perspective of actor-network theory (ANT) is a valuable alternative. First, the Methods section provides a description of the data and research method followed by presentation of the research findings. In the final section, the article summarizes the main findings and also reflects on the value and future potential of ANT's cyborg-perspective for grasping hacking and other forms of technical deviance.

HACKERS AND TECHNOLOGY: TWO INSEPARABLE WORLDS

Historically, hackers have always been perceived as figures that have a specific relationship with the worlds of objects and computer technologies. In the 1960s and 1970s, hackers were viewed as computer enthusiasts or "whiz kids" who explore and expand the boundaries and potential of computer technology (e.g. Chandler, 1996; Levy, 1984). Hackers were admired for having an almost organic relationship with computers (Skibell, 2002), and to be a hacker was to wear a badge of honor (Chandler, 1996). Hackers were also considered as members of a specific subculture that adheres to an ethic that is also specifically orientated towards technology, e.g., the idea that information should be free, viewing software in terms of art and beauty and an emphasis on skill (Levy, 1984; Nissenbaum, 2004; Thomas, 2005). Their ethic also promoted distrust in authorities and the resistance to a conventional lifestyle (Blankwater 2011; Steinmetz & Gerber, 2014, 2015; Taylor, 1999; Yar, 2005). Although hackers were not part of the mainstream establishment, the public attitude towards them was generally positive in the early days (Nissenbaum, 2004).

This more positive perception of hackers shifted gradually to a considerably more negative one. In the 1980s, hackers were more and more perceived as pathological computer addicts who were better able to socialize with machines than with people (Skibell, 2002; Sterling, 1993; Turkle, 1984; Yar, 2005). Additionally, their "magical" power with computers relatively quickly became a source of fear and danger (Skibell, 2002; Wall, 2008). Of course, there were also developments within the hacker community itself that affected both the meaning of hacking and the public perception. For example, hackers known as "crackers" entered the scene and hacked to break or sabotage systems (Chandler, 1996; Wall, 2007). The term cracker actually emerged in the hacker community itself to differentiate between hackers that create code or use

something in an unconventional way, and crackers who break things (see Holt, 2010), although crackers can also be divided in various subgroups as well (see Wall, 2007). However, crackers were (and still are) a minority within the hacker community at large (Steinmetz, 2015; Taylor, 1999). It is important to stress that there are also other categorizations to distinguish "good hackers" from the "bad hackers;" the most known one is the division between white-hat, grey-hat, and black hat hackers to which the current study applies (see Method section).

From the 1990s onwards, hackers were mainly viewed as criminals, an image that was further reinforced by the security industry (Taylor, 1999), the government (Yar, 2005), and the media alike (Halbert, 1997; Nissenbaum, 2004). Indeed, as Churchill (2016) pointed out, the social construction of the hacker shows some similarity with that of the scientific burglar: Their (perceived) skills, intelligence, and sophistication attracts both fear and admiration, and they are also viewed and treated as the representatives of the dark side of technical progress. Paradoxically, hackers have also been important enablers of the same technical progress themselves (Blankwater, 2011; Chandler, 1996; Levy, 1984), and perhaps also (unwillingly) co-produced the construction or "myth" of hackers as dangerous criminals (see Skibell, 2002).

The fact that hackers have a specific relationship with technology is also displayed in studies that seek to understand hacking from the perspective of hackers themselves (Levy, 1984; Taylor, 1999). The work of psychologist and sociologist Sherry Turkle (1982, 1984), is perhaps most prolific on this topic. She pictures hackers as figures that are deeply engaged with the world of machines and technology. Rather than a gifted and beautiful body, hackers are believed to possess a gifted mind that gives them mastery over technology. Mastery is generally considered as a key element of hacker culture (Holt & Kilger, 2008), but also conceived as a valuable concept for understanding how hackers relate to technology. It refers to "the extensive breadth and depth of technical knowledge an individual possesses that is necessary to understand and manipulate digital technologies in sophisticated ways" (Kilger, 2010, p. 208). According to Turkle (1984), mastery over technology is also strongly intertwined with how hackers view themselves. Some of the hackers she interviewed had an image of themselves as "non-persons" or "non-real people" because they liked to be more engaged with "machine things" than with "flesh things" (humans), which they considered as two separate domains. Hackers feel proud of their ability to master their medium perfectly or by winning the battle with the machines, rather than through their engagement with humans (idem).

The hacker-technology relationship has also been understood through the notion of "craft" (Holt & Kilger, 2008; Nissenbaum, 2004; Steinmetz, 2015). Like mastery, craft deals with the manner in which hackers are able to manipulate technology, although it puts more emphasis on skills, labor, and creativity than on the dimension of control outlined by Turkle (1984). Holt and Kilger (2008) for instance made a division between "tech crafters" and "make crafters." The first type of hacker is considered as the consumer of existing materials, and the latter as the one that is engaged in producing or creating materials (e.g., new scripts, tools). Steinmetz (2015) conceptualized hacking as "craftwork," considering hacking as a specific kind of late modern work in which process is more important than the result. The study also showed that hackers are driven by technological challenges, feel the urge to explore and control systems, and also possess a specific technology-orientated mentality. Others underline the importance of ego in relation to mastery and hacker motivation, which refers to the "internal satisfaction that is achieved in getting the digital device to do exactly what one intended it to do" (Kilger, 2010, p. 208; see also

Nissen, 1998). Turgeman-Goldschmidt (2005) drew on Katz's (1988) work on the seduction of crime to grasp the hacker-technology relationship. She considered fun, thrill, and excitement as the most essential features of the hacker experience and argued that all the aspects brought up by her participants e.g., curiosity, power, revenge, and the interaction with machines, can be associated with feelings of fun. Like Turkle (1984), Turgeman-Goldschmidt (2008) also highlighted the fact that hackers feel proud of themselves when it comes to their computer talent. While the outside world views them as deviants or criminals, hackers consider themselves as positive deviants: They have no shortcomings, but something *extra* (see also Van der Wagen et al. 2016).

While these and other studies provide valuable insights on hackers as a deviant group, including their specific relationship and engagement with computer technology, they continue to examine the hacker-technology relationship from a rather anthropocentric angle. Concepts such as mastery, craft, ego, and fun ultimately place human agency in the center of the inquiry and treat technology itself as a more passive and subordinate element in the deviant process. Existing studies and frameworks also somewhat treat the human-technology relationship in a rather dualistic manner. Goals or intentions are attributed to the human agent and the means to the tools and the technology. It can be argued that this dualism works counterproductive for grasping the various and hybrid modes the hacker-technology can take shape. This brings us to the discussion of the cyborg-perspective of actor-network theory, the central approach of this study.

THE CYBORG-PERSPECTIVE OF ACTOR-NETWORK THEORY

> *"If action is limited a priori to what 'intentional', 'meaningful' humans do, it is hard to see how a hammer, a basket, a rug, a mug, a list, or a tag could act. They might exist in the domain of 'material' 'causal' relations, but not in the 'reflexive' symbolic' domain of social relations" (Latour, 2005, p. 71).*

Actor-network theory (ANT) can be regarded as a constructivist and critical approach that explicitly assigns a more active role to non-humans (e.g., technologies, objects, animals) in the course of (inter) action (Latour 1992, 2005). Actor-network theory does not consider humans and non-humans as two separate agents or entities, but speaks of heterogeneous alliances or hybrid collectives of both (Latour 1993; Van der Wagen & Pieters, 2015; Verbeek 2005). In this respect, there is a clear parallel with the more familiar notion of the "cyborg," the term that is also used in this study. The term cyborg, short for "cybernetic organism," was introduced in the 1960s as a term for "artifact-organisms" or "man-machine systems" in the context of space travel (see Clynes & Kline, 1960). The cyborg signified the idea that the human body could be extended with technological artifacts in order to accomplish greater things and/or to explore new frontiers, a theme that we can obviously find in many science fiction movies. In her *Cyborg Manifesto* (1987), Donna Haraway used the cyborg figure as a metaphor to overcome the boundaries or dichotomies between science and (science) fiction, human and animal, organism and machine, and physical and non-physical, which she perceived as Western dualisms that lie underneath the "logics and practices of domination of women, people of colour, nature, workers [and] animals" (Haraway, 1987, p. 32). Hence, she presented the cyborg figure not exclusively as a physical melt

of humans and technology, but much more as a post-human[3] metaphor for questioning the extent in which we are human or technological ("constructed") (see Verbeek, 2008). This particular interpretation of the cyborg figure we can also find in ANT's notion of the "hybrid," which not only seeks to abandon dualistic modes of thinking, but also offers a framework that can grasp the various ways in which the blend of the human and the technical can concretely take shape. We can roughly distinguish three main ways in which ANT defines the cyborgian relationship between the human and the technical.

First, ANT presumes that interactions between humans and non-humans are not only functional (e.g., when we write, we have to use a pen and paper), but are also intertwined and shape one another's actions. To give a concrete example, driving a car is seen as a performance of the driver and the car since both enable and complete the action: The driver needs to have the skills and the car the functionality to drive (see also Dant, 2004). This dimension closely resembles the original meaning of the cyborg, the notion that the tool enhances or augments the bodily functions of the human (see also Suarez, 2015; Wells, 2014). Driving also involves an interaction between the driver and the car and a process in which the driver has to gain control over the car. Humans consciously experience both of these aspects when they have to learn to drive, and both change or partly disappear once they are able to drive.[4] Accordingly, for ANT, the relationship between humans and non-humans is not merely and continuously one of master and slave. It can be also interactive and mutual (see also Van der Wagen & Pieters, 2015). Latour (2005) himself illustrated a parallel in this context with the manner in which puppeteers interact with their puppets:

> Although marionettes offer, it seems, the most extreme case of direct causality – just follow the strings – puppeteers will rarely behave as having control over their puppets. They will say queer things like "their marionettes suggest them to do things they will have never thought possible by themselves." (pp. 59-60)

This dimension might also be relevant to the manner in which hackers engage with computers. As Turgeman-Goldschmidt (2005) pointed out: "Despite (or because of) the fact that the computer is a machine, it invites play and movement" (p. 20).

Secondly, alongside this principle of "joint (inter)action" or "human-machine cooperation," Latour (1992, 2005) argues that non-humans are not passive, static, or neutral entities. Based on their "script" or "prescription," they can provoke certain actions or usage (positive or negative), can make people do things they would ordinarily not do (e.g., shoot somebody when they have access to a gun[5]), and restrict human action (e.g., traffic lights or speed bumps that regulate traffic behavior) (Van der Wagen & Pieters, 2015; Verbeek, 2005). In other words, for ANT, non-humans (including their material features) can affect human thoughts, morality, and behavior just like other humans do. Also, here the "car-driver hybrid" is very

[3] Note that this is not the same as the "transhuman" view, which considers the cyborg as a new life form rather than merely as a metaphor (Verbeek, 2008).

[4] Once you learn to drive, driving becomes a routine and takes place in a more automatic fashion (see Ihde, 1990; Verbeek, 2005). Of course, with the emergence of today's self-driving cars, the relationship between the driver and the car again has changed. In this case, the car is the main (primary) driving agent, while the role of human is secondary.

[5] See for example the study of Bourne (2012) entitled "Guns don't kill people, Cyborgs do."

illustrative. Lupton's (1999) ANT-based study on road rage showed that the car as a physical object also co-shapes the behavior of the (aggressive) driver:

> The pleasure of mastery of the machine, of speed, the sense of power and liberation that movement in the car may bring, is conducive to travelling above the speed limit for example, and other reckless driving actions, such as running red lights or travelling too close to others' vehicles. (p. 63)

The fact that drivers have to move in a heavy regulated space does not completely match up with the emotions and sensations that come along with the act of driving. Both of these aspects are worth consideration in the context of hacking as well, since hackers both interact (or "become one") with the machine –and act or have to act in a certain legally restrictive context.

Thirdly, although Latour (2005) did not explicitly mention it in his work, we can also add here a more subjective or intimate relationship between humans and non-humans. For instance, when people (mostly men) speak about their car, they often speak in terms of love, passion, emotion, and character, perhaps in a similar vein as hackers speak about their computer or technology in general. This dimension is also strongly present in the work of Turkle (1982, 1984) discussed earlier. To sum up, ANT does not view tools, objects, and technology in merely functional or instrumental terms. Instead, it views them as an integrative element of human action, capabilities, (self) perception, meaning giving, and even one's intent. Drawing on ANT, this study conceives and studies the hacker as a cyborgian deviant: a transgressive blend of human and technology. By adopting this approach, it aims to gain a more nuanced understanding of how hackers' relationship with technology takes shape, functionally, experientially, and intentionally too.

RESEARCH METHODS

The current study is part of a larger study on cybercrime, offenders, and victims, which primarily draws on ANT and its notion of hybrid agency or actorship (see Van der Wagen & Pieters, 2015; Van der Wagen, 2018). Actor-network theory's methodological assumptions generally reflect viewpoints from both (symbolic) interactionism and ethnomethodology (Garfinkel, 1967), which also assert that social reality is composed of *interaction*s and should be studied as such (Latour, 2005; Law, 2004). Actor-network theory also prescribes an ethnographic approach that aims to grasp "the world-making activities" of the actors under study, and to express and report *their* words, self-reflections, and "own theory of action" as much as possible (Latour, 2005, p. 57). In that sense, ANT's view also closely connects to the notion of "verstehen" within the cultural criminological approach (Ferrell, 1997). However, ANT adds an extra theoretical and methodological dimension. As pointed out, ANT is also interested in the non-human participants of social reality, especially in the manner in which humans and non-humans interact and form alliances.[6] For this study, this theoretical (cyborgian) element is used to gain a more profound understanding of how hackers give meaning to themselves and their actions.

For this study, 10 semi-structured interviews with hackers were conducted in which the

[6] In this respect, ANT is actually a valuable approach for cultural criminologists to consider as they also aim to understand the practice of deviance itself and how deviants give meaning to that practice (see O'Brien, 2005)

participants were asked to reflect on their definition of hacking, their drives and motivations, their skills, their experiences with hacking, and how they viewed themselves. Of these interviews, eight interviews were face-to-face, one was conducted by email, and one took place through Skype.[7] All face-to-face interviews, except for one, were recorded and transcribed. The interviews generally lasted one to three hours. The interviewed hackers were found through hacker spaces, student-contacts, and by means of "snowballing." As the small group of participants reveals, it was extremely difficult to find hackers willing to participate in an interview. The members of hacker spaces mentioned that hackers are generally tired of journalists and researchers that approach them for interviews, and also fear being associated with cybercrime or cybercriminals. Persons that declared to know some hackers personally also mentioned that hackers generally have the feeling that: "Ah, again a researcher who does not understand our world."

The (small) group of participants that was willing to engage in an interview consisted of (mainly Dutch) adult males participating or have completed an education program, mostly IT related. Although participants shared commonalities in that they viewed themselves as hackers, they differed in terms of their hacking activities, motives, normative position towards hacking, and criminal record. Half of the participants considered themselves as ethical or white hat hackers. They searched for vulnerabilities in systems/networks (for example those which hold privacy-sensitive information) and reported it the company. The other half of the participants perceived themselves as (ex) black hat or grey hat hackers (or crackers). They also searched for vulnerabilities in systems (which can be a website, a server, public Wi-Fi, or a program), but did/do not inform the owner. Two of these five participants had been imprisoned for their engagement in hacking and were employed at a security company at the time of the interview. Two other hackers had been active in the black hat scene, but indicated that they did not hack illegally anymore. The last participant was involved in virtual theft involving the spread of malware for four years and had never been caught. He was the only participant who pointed out that he was motivated by financial drives.

Having such a small and differentiated participant group makes it hard, even impossible, to produce general statements about the hacking community at large, which this study does not proclaim to do. The material however is rich and does enable us to acquire a feeling and understanding of the world of (rather different) hackers, how they perceive themselves as actors, and how they define their relationship with technology. In light of the theoretical approach of this study, the diversity of the participants can also be beneficial for exploring whether the hacker-technology relationship varies across different types of hackers or hacks. The analytical or coding approach in this study can be considered as a combination of both inductive and deductive techniques (see Hennink, Hutter, & Bailey, 2011). The concepts emerged throughout a structured though flexible and creative approach (Charmaz, 2006) in which the narratives of the interviewees were coded and interpreted in light of ANT's conceptualization of the human-technology relationship. In turn, this interactive cycle or process produced themes, categories, and concepts, which reflect and highlight certain aspects on how hackers give meaning to what they do and who/what they are. In the analysis that follows, I sought to represent the reality,

[7] From these interviews, five interviews I conducted between May 2013 and May 2015. The other five interviews were, under my supervision, carried out by students from the University of Groningen in the scope of a course on cybercrime in the period April/May 2013. Although the interviews have been conducted by different interviewers and in different contexts, the discussed topics were mainly overlapping.

thoughts, and perceptions of the hackers as thoroughly as possible. In order to safeguard the anonymity of the participants, I assigned pseudonyms to each of them. To provide context for participants' words, the findings section indicates what type of hacker the interviewee "generally" considered himself to be or in what type of hacking activities he was involved.

RESEARCH FINDINGS: WHAT IT MEANS TO BE A HACKER

The interviewed hackers provided different definitions or descriptions of hacking, ranging from narrow to broad. For example, the more narrow definitions include: "Taking over someone else's computer" and "breaking into a system without informing the owner," definitions that also stress the illicit character of hacking, which not all interviewees considered as hacking. Rather, they preferred to call it "cracking." "Moving beyond existing patterns," a "state of mind," or "assigning a different functionality to an existing object or technology" can be regarded as more broad and neutral definitions, and were shared by most interviewees. Whether engaged in licit or illicit hacks, they immediately dissociated themselves from the criminal image - which they believed to be predominant in the public discourse. Instead, they viewed themselves as (male) hobbyists who possess a very specific mindset and skillset, which set them apart from ordinary people and criminals. We assess how they gave meaning to their hacker reality in the following five sections: cyborg mind, cyborg performance, cyborg identity, cyborg body, and cyborg transgression. Each section highlights a different but complementary dimension of how the hacker-technology relationship takes shape.

Cyborg mind – how hackers view their "usage" of technology

The way hackers perceive their usage of technology is one of the key aspects that defines the hacker practice and mindset. Firstly, the interviewed hackers did not consider themselves as passive "users" of technology, but claimed to be interested in the underlying processes that operate a system; what makes it work or *not* work. To illustrate this point, Jan explained: "Restart your computer. I find the most deadly and annoying comment you can get because then you still don't know what is going on." In this context, participants also highlighted their ability to see through and scrutinize a system and their "investigative attitude." Paul (grey hat hacker) emphasized that you have to be very analytical when you want to become a successful (black hat) hacker:

> You need to be able to estimate a network, to map a network, to map its employees, what they do, how they behave, before you actually start, if you don't do that and prepare yourself, you won't manage the hack.

In this respect, a hack also shares some similarity with the system of robbery, involving "discipline, preparation, planning and conspiracy" (Churchill, 2016, p. 864). Ex-black hat hacker, Eric framed the analytical ability pointed out by Paul as "empathy." The word empathy is usually associated with being sensitive to the emotions of other people, yet Eric used the same word in relation to technical systems. Understanding the technical system so well that it can result in empathy for technology very clearly illustrates the deep and almost inner connection some hackers believe they have with technology.

Secondly, most of the interviewed hackers pointed out that they enjoyed the interplay with the goal-means-end rhetoric of devices or technologies, an aspect that is also stressed in the definition of hacking as: "The use of systems or equipment for purposes for which they were not originally designed." Jack, a hacker who was active in a hacker space and a skilled programmer, pointed out that hacking is not merely about being technically advanced, but much more about unconventional thinking, creativity, and imagination:

> There are many kinds of hacks, for example using a cd-tray as coffee stand, using plastic sealers that they use for bread as a way to clip cables. When you have these small playful things in your room, I will call you a hacker.

Actor-network theory's notion that the functionality of objects merges with or connects with the human actor who uses them also manifests itself here. Hackers seem to be consciously aware of the features and functionalities of the objects that they use or engage with, and are also sensitive to their construction. They do not see the object (e.g., a computer) as a singular and fixed entity, but consider it and treat it as a network of different interacting elements and mechanisms. Hackers are therefore engaged in the almost scientific practice of what ANT denotes as "reversible blackboxing" (Latour, 1992). They do not only think outside of the box (see later), but are also able to deconstruct the (black) box (see also Forlano & Jungnickel, 2015), which in hacker terms is often called "reverse engineering" (Nikitina, 2012, p. 143). Moreover, they are able to change the functionality of the object in accordance with their own desire. This suggests that hackers not only strive to master their machine perfectly (Turkle, 1984), but also seek to establish the perfect master-slave relationship in which they are in control and the master of the object and every single component of it.

Cyborg performance – how hackers view their abilities in relation to the tools they use

Apart from their non-instrumental usage or relationship with technology, the interviewees stressed the explorative and interactive nature of this relationship. They not only acted alone, but somewhat cooperated or formed an alliance with technology in the process of becoming a skilled hacker. Firstly, some participants pointed out that they learned from other hackers, but also while they interact with technology, as a sort of trial and error or "trying and trying again." 'Paul described the learning process as an interplay, and also pointed out that he received "feedback" from the system:

> I learned things from school and the Internet, but the majority was experimenting. At home I had several servers, I then downloaded software, installed it and just looked what would happen, to try things and check what will happen. I cannot break it anyway, or yes, I can, but then I can install it again. Playing-wise you have to learn it.

A deeper understanding how technology works – referred to before as "technical empathy" - requires constant concurrent exploration and interaction with technology. This aspect demonstrates (again) that the interviewed hackers consciously experience an interaction with the technology rather than merely consider themselves as users of technology, perhaps in a similar vein as the puppeteers mentioned by Latour (2005) who also received input from their puppets. For them, the interaction with technology also seems to have a permanent nature. Unlike (most)

drivers, hackers never stop learning and never want to stop learning. Learning to hack is a continuous process and the opportunities are endless. As Daniel (white hat hacker) stated: "The more you get to know, the more there will be to learn." In other words, the earlier mentioned master-slave relationship occurred alongside or in alternation with a more cooperative, interactive, and mutual engagement. The interviewed hackers seemed to experience and to enjoy both of these processes.

Secondly, some interviewees mentioned that the tools and technologies they used co-shaped their abilities and possibilities. For instance, they did not continually proclaim to "invent the wheel" by themselves, but rather depended on the abilities or functionalities of the tools they used. According to Jeffrey (ex-black hat hacker), there was always a combination of existing tools and some personal input: "Every hacker has his weapons tank with his own tools he has chosen to use. Usually you use an already created and existing code someone else has written and you adapt it to your problem." This aspect also aligns with Nikitina's (2012) claim that hacking is more a process of recycling and "rearranging the givens of existing systems" (p. 144) than true creativity. Gunkel (2001) spoke in this context in relation to the parasitical nature of hacking in order to emphasize that hackers draw their "strength, strategies and tools from the system on which and in which it operates" (p. 6), a claim that is rather similar to ANT's view that not all the credits should be granted to the human agent.

In this context, Vincent's story is also relevant to consider. He was involved in hacking the accounts of counter players in a virtual game. As these virtual goods have real value, he was able to earn large sums of money with the theft. Vincent explained that he (initially) made use of "ready to use" tools. He pointed out that he never really was a "computer nerd" who had this born fascination for computers and technology. He was merely curious about what he could accomplish with certain programs rather than unraveling how they work. He came across so called RATs, which relatively easily enabled him to control someone's computer and webcam. Vincent asserted that: "If these RATs would not exist, I would not be bothered to get involved in hacking in the first place." Over time, he became skilled in various malicious cyber activities, including phishing and the use of botnets. This example illustrates that certain tools can bring new options and opportunities, and eventually also new skills. At the same time, something is occurring on the intentional level. Without the easy access to and existence of these tools, Vincent would, as he claimed, not have been engaged in hacking. Like ANT's example of guns, a RAT seems to be not merely a "neutral" tool to use, but might also, at least for some youngsters, invite or encourage their engagement in cyber deviant conduct (see also Van der Wagen & Pieters, 2015).

Cyborg identity – how hackers view themselves in relation to others

In the previous sections, we discussed how participants perceived their usage of technology, which is an important part of their specific mindset and how they view themselves. However, there are also other elements that are important to consider, which particularly highlight how they viewed themselves in relation to others. Firstly, most of the interviewed hackers explained that they had a rather natural connection with technology, which gave them the feeling of being different than other people. They had an extreme fascination for how computers, systems, or devices work, an interest they developed at a young age. For example, Jan, who considered himself to be an ethical hacker, explained that:

> As a child I wanted to push all kinds of buttons just to see what would happen. I think that there is an innate need involved when it comes to dealing with technology, that you have a certain connection with technology.

This affinity or special connection was also considered to be essential in the process of learning to become a (skilled) hacker. As some of the interviewees pointed out, hacking requires quite some time, energy, and discipline. Participants were only willing to invest this time and energy if they were truly dedicated to it and loved computers. They seemed to say that not everybody can become a hacker, even though he or she wants to or has the (technical) recourses and knowledge to do so. Technology needs to be your "second nature," an affinity you have to possess naturally.

Secondly, the interviewees not only highlighted their ability to unravel the inner workings of technology, as discussed already, but also defined themselves as actors with the ability to think outside of the box or beyond existing patterns. For example, Eric explained:

> You need to be this kind of person who can come up with something weird, vague and new that no one ever thought about before. You need to think in a different way. I can sometimes enter a room and then immediately I know how to open the doors, while other people don't see it.

Although they generally dissociated themselves from criminals, some interviewees explicitly drew a parallel with professional burglars to describe hacking. To rob a house by finding the key under the doormat does not require skill and applies to "wannabe" hackers or so-called "scriptkiddies" who merely use existing tools. A *real* hacker would find an inventive way of breaking the lock and would not even need a key to be able to open it up. Moreover, in assessing whether a hack(er) can be qualified as a (good) hack(er), cleverness ultimately seemed to be more vital than whether the act was legal or illegal. Jan for instance explained: "Some criminal actions are also quite brilliant. If you in a smart way rob a store, for instance, by digging a tunnel underneath, that is what I find funny. It is a cool hack, even though it is illegal." As pointed out by Nikitina (2012), hackers somewhat seem to "blur the line between the creative and the criminal on the way" (p. 150).

Thirdly, the ability to think differently also applied to non-technical issues. Some of the interviewed hackers expressed that they were critical and sensitive about "the system," society, and the government in general. This aspect was highlighted by participant Jan who perceived ethical hackers as whistleblowers who bring major abuses in society to light. He argued that many companies or organizations hold privacy sensitive information, yet have extremely poor security. According to Jan, they are actually the real "violators," while the hackers who expose their misconduct are treated as the criminals. This can lead to major feelings of frustration among hackers: "Why don't you see that the grass is green? Why don't you see it?" By stating that hackers "pick up signals" other people do not, Jan seemed to stress that hackers hold an extra "sense," sensor, or pair of glasses that enables them to see certain things other people are blind to. We could interpret this particular image of the self as another representation of the hacker as a cyborg-figure in terms of imagining oneself to have extra-sensory abilities. Hackers are not only gifted with a brilliant mind or a mind than enables them to master technology (Turkle, 1984), but perhaps also have an extended mind/body that enables them to track down injustice.

Connected with the ability to see certain things or wrongdoings, some participants also highlighted some heroic features of the hacker. The most prolific example was again provided by Jan, who compared hackers with members of the resistance movement in WWII who killed the Germans. He stressed that certain problems require extraordinary measures and ultimately those actions would be rewarded and appreciated. In a different vein, doing more good than bad or being a "savior" or "helper," was also mentioned by some of the black hat hackers. For example, Dylan, who was involved in breaking into systems mentioned that "I did quite some bad things in my hacker career. Yet, the companies would be eaten alive, if we low or mid-tier hackers would not exist to educate them." Whether engaged in licit or illicit hacking, hackers generally adhere to their own moral rules or principles in which they strongly believe. This also suggests that you can break rules or "rip off the system" when you do not agree with it[8] or find it unfair. In this context, Kevin (ex-black hat hacker) provided a rather different example:

> There was this "free-to-play" game where users could receive in-game advantages by paying money. I really hated the idea that someone can be better in a competitive environment just because he has money. So I've used what should really matter in gaming – skill. I've hacked into the site and generated retrievable codes for the in-game currency/advantages.

The notion of breaking rules and having personal ethical standards is something that can also be connected to what Blankwater (2011) referred to as "an attitude of *everything is possible*: Do not let barriers (like security, laws, copyrights) hold you back, but take it a step further" (p. 47, emphasis in original). Hackers generally seek to explore new frontiers and go against existing frontiers. For them, "boundaries are seen as unnatural" (Turgeman-Goldschmidt, 2005, p. 20). According to Jan, hackers also feel the strong urge to prove that they are right, even if this requires that you have to do something illicit. In this context, he referred to an example in which a hacker informed a web shop about a leak, which enabled it to order goods for free. When the company refused to listen, the hacker ordered one of their couches and sent it straight to the office of the company. Jan reflected on this example by saying: "As a hacker you want to be the master and ruler of the system. This is what I call: releasing the hacker inside of you."

Cyborg body – how hackers (simultaneously) compete with technology and themselves

The hacker-technology relationship also manifests itself in a competitive way in the sense that hackers feel the urge to explore and extend their mental and physical capabilities and limits (e.g., "Am I able do it? "How much power do I have on the Internet?"), as well as the technical ones (e.g., "What can it do?" and "What will happen when I do this?"). For most of the interviewed hackers, challenge was a necessary condition to enjoy hacking, which explains why they consistently set loftier goals for themselves. For example, Paul stressed that he always selected the more challenging targets to hack rather than the easy ones. According to Eric, the challenge can also fade away once you are able to hack everything you already wanted to hack. Yet, he still considered this challenge to be important in his work in the field of incident response. Eric explained:

[8] This element of resistance is actually also a theme in Latour's work, which is why the perspective is also valuable for understanding hacktivism (see Taylor, 2005).

> If something goes wrong and managers stress out, I perform perfectly. I like the feeling when you are in the middle of it, everything goes wrong, everything collapses, people cry and go home. Then you know, it is no time for joking, now it is serious. You are not allowed to make mistakes.

The example that Eric provided clearly resembles Lyng's (2004) proposition that edgeworkers have to and like to rely on their body to "instinctively" respond to evolving and overwhelming circumstances. Yet, in the case of hackers, they generally rely much more on their mind than on their physical body. In this context, we can also draw a parallel with the robbers described by Katz (1988). He pointed to their "ability to always know what to do" when facing chaos (p. 235). Robbers also have a superior ability in terms of using street smarts rather than physical force to conduct their "work," which similarly applies to hackers. In addition, Katz spoke of game-like and sport-like features in the context of robberies, elements that are also highlighted by some of the interviewed hackers. Paul always took, what he called, a "cooling down period" after he managed a hack, a term used in sports. In relation to sports, the capabilities of the physical body are still important to hacking as well, e.g., hackers often exhaust their body without proper sleep (see also Turkle, 1984). Like sports and gaming, hacking also has a strong element of competition with peers: to be better and faster than other hackers. Paul stated that he was proud of the fact that he was able to hack one of the largest companies in the world: "Then you really think: I did it. There are hundreds of them out there, but I did it. Pride yes, victory." Eric pointed out that he always left a sign on the servers that he hacked: "I wanted to let others know that I was there, that they would think, ah him again. That is the feeling I wanted generate." Here, we see similarities with graffiti writers who also seek to leave lasting marks and images (see Ferrell, 1996).

Yet, as Nikitina (2012) and Turkle (1984) also argued, hacking also entails the desire to "beat the system" rather than merely another person. In that sense, hackers do not merely compete with themselves and with other hackers, but also with the machine. This aspect can be also found in Paul's description: "You can be busy for weeks and still realize that you won't manage, but still you keep looking for that one spot you might have missed." The importance of challenge and competition allows for a different conceptualization of the proposition that for hackers, the process is more important than the result (see e.g., Steinmetz, 2015). Perhaps for hackers, at least for those mainly active in illicit hacking, process and result might be of equal importance or could be intertwined.

Cyborg transgression – how hacker's experiences and intentions are co-shaped by technology

The interviewed hackers also referred to their relationship with technology in the context of emotions, decision-making, and intentions. It is this (interactive) process that generated many aspects of the hackers' experience, feelings, and emotions. Kevin for example explained:

> When I hacked the first time I was very well aware that it was illegal. However, when you do this the first few times you get in a sort of trance. You forget everything and are just amazed and pumped with adrenaline because you have just entered a system which might hold information you are not supposed to see, or the

> system has very big specifications (big hard drive, a lot of memory etc.) which you have never seen before.

The quote suggests that there is not merely "the invitational edge" of doing something illegal, which produces the thrill, but that the features or "beauty" of the system also co-produces the adrenaline rush. For Paul, managing the hack was actually more important than doing something illegal per se. He explained: "You dedicate yourself to one particular thing you are good at [hacking], that is your passion. Whether it is legal or illegal, it did not bother me at all that time." Paul frequently used the expression of "going (completely) wild on the system," which, as he explained, gave him a feeling or sensation that nothing else can resemble. He also mentioned that there were periods in which he was not able to sleep without the sound of the computer on in the background. Hence, also through sound, the hacker can become *one* with the machine.

While black hat hackers are not always aware of the boundaries between licit and illicit hackers and do not care or like the thrill of doing something illegal, white hat hackers are more cognizant and respectful of rules and regulations. According to Jan, for instance, one must strictly follow the rules of "responsible disclosure" when reporting a security issue—that a person should do nothing else than necessary for exposing the security leak. Yet, after you are (finally) able to enter a server, you have to stop and really need "to control yourself," something that, according to Jan, is difficult for many young hackers. He explained that once you are able to enter the system, you can become "too curious," e.g., by reading all the information on the server you encounter. In other words, the original intention (to expose a leak) might change or, to speak in ANT terms, "translate" into something more *illicit* once a hacker crosses the technical edge of entering the system. At the same time, like driving a car, the feeling that a hack generates does not match with the rules that you need to follow. Paul, who did not seek to hack illegally after he got released, also brought up this issue.

> I want to do it good now, but I did it wrong as well. But I have to say that, I am often seduced to do it again when I look at certain systems. 'Breaking in' is still in my way of thinking, but I try not to do. Once I will start I will drown in it again.

Finally, alongside the legally restrictive context, hackers maneuver in an online environment where a different set of rules applies or where there is an absence of any rules. Eric explained how it worked in the black hat scene: "There are borders but they get blurry fast. If you are raised in a group where everybody carries guns, then you will find it normal after a while to carry one yourself." According to Jeffrey (ex-black hat hacker), young hackers often do not know what to do with their computer talent. He said:

> They are physically not in the right environment and there is no one to tell them that their actions might be malicious after all. There is no one to help them in their development and growth and to guide them in the right direction.

Hence, intentions and moral perceptions cannot be understood in isolation from the digital (anonymous) environment in which the hackers are "flowing" and "acting." Some interviewees also pointed out that they considered their online life or identity as something secretive, or a "hidden side" of themselves. In other words, digital technology enabled them also to be released

from the body and to explore multiple identities simultaneously. Also, this aspect can be linked to the notion of cyborg (see also De Mul, 2002).

CONCLUSION

"*What people do with computers weaves itself into the way they see the world"* (Turkle, 1982, p. 173) and *"see themselves"* (p. 183).

This study aimed to shed light on how hackers give meaning to themselves and their actions by drawing more explicit attention to the hacker-technology relationship. By employing the cyborg-perspective of ANT, this study was able to illustrate and explore the various ways in which this relationship takes shape, ranging from directive, functional and cooperative to more intimate, emphatic, competitive, and mutually affecting. In accordance with Turgeman-Goldschmidt (2008), this study also found that the "good" and "bad" hackers, as far as you can make this division, have more similarities than initially expected. The interviewed hackers generally perceived themselves as non-criminal actors who possessed a very specific skillset and mindset which set them apart from others. They pictured themselves as figures who possessed an "extended mind" or "extra sense" that enabled them to see and move through, beyond and against systems, not only technical ones. Whether black, grey, or white, the participants all explored the boundaries and capabilities of technology and themselves simultaneously, and each believed to do more good than bad. To some extent, they also viewed themselves as superior and somewhat superhuman, almost like the cyborgs we encounter in science fiction movies: Superhuman rebels fighting evil (Wood, 1998). Yet, rather than relying on the force or strength of the body, hackers seem to count on their "innate" technological, mental, and creative skill, and consider themselves (or imagine themselves) as being equipped with certain abilities that most people do not possess. Hacking also seems to involve some hybrid type(s) of (embodied) experiences of its own, e.g., visible in the example of "not being able to sleep without the sound of the computer." Despite their (perceived) differences, hackers also resemble other deviant groups (e.g., professional thieves, robbers or graffiti writers), and other non-criminological phenomena such as gaming and sports. Hence, we should perhaps also not over-exaggerate their uniqueness, although they would probably not mind.

This study also aimed to make a contribution to the conceptual understanding of hackers by applying the cyborg-perspective of ANT. It explored whether ANT's way of looking at the human-technology relationship enables us to unravel aspects of hacking more comprehensively than a traditional criminological (anthropocentric) lens. While valuable studies have been conducted to grasp the hacker phenomenon, ANT's cyborgian lens certainly brought a new layer to the conversation – theoretically and methodologically. Firstly, ANT draws attention not only to how humans relate to and learn from other humans, but also to how they interact with or relate to their device, computer, and technologies, and what such an interaction entails and means for them. Rather than looking at the hacker as a human actor, ANT enabled us to look at the "hybrid" capacities in which a hacker can act, ranging from the "hacker-tool," "hacker-software" and the "hacker-gun" hybrid. By adopting this perspective, this study was able to reveal that interacting with technology is intrinsically linked to becoming a hacker and experiencing hacking, and the associated intentions, perceptions, and emotions. Secondly – like Haraway's (1997) broader notion of cyborg - ANT provides a perspective that seeks to eliminate dualistic thinking, an approach that particularly fits well with hacking as both a practice and a particular type of

transgression. This study revealed that hackers somewhat drift across several boundaries simultaneously: the human and the technical, the online and the offline, the real and the virtual, the creative and the parasitic, the rational and the irrational, the licit and the illicit, the good and the evil, and so on. At the same time, hackers seem to be engaged in establishing boundaries themselves. For instance, participants had a clear view on who/what can call himself a (skilled) hacker and to which rules they should obey. The complexity and co-existence of boundary breaking and boundary fixing we were/are only able to capture more comprehensively if we do not *a priori* maintain any such boundaries, and only look at the boundary performing activities of the actors that we study.

To conclude, if we criminologists want to explore and understand the world of hackers and other high tech cyber deviants more deeply and profoundly in the future, we have to extend our focus *beyond* the human, gain more criminological knowledge on the (deviant) human-technology relationship, and seek to dismantle existing dualism and dichotomies that still prevail in criminology. The cyborg-lens of ANT provides a valuable and thought-provoking framework that can contribute to such endeavor. Future research could further enhance this perspective by conducting additional and more extensive fieldwork among different groups of hackers. The perspective is also worth considering in the context of other forms of technical deviance. As mentioned in the introduction, many tools that can be used to cause severe damage (e.g. RATs or tools for launching a DDoS attack) are ready at hand for the current young generations. It would be worthwhile considering whether the accessibility and commodification of such tools truly contribute to youth's engagement in technocrime.

REFERENCES

Becker, H. (1963). *Outsiders. Studies in the sociology of deviance*. New York, NY: The Free Press.

Blankwater, E. (2011). *Hacking the field. An ethnographic and historical study of the Dutch hacker field*. Sociology Master's Thesis. University of Amsterdam. Retrieved from https://issuu.com/elginno/docs/hacking_the_field

Bourne, M. (2012). Guns don't kill people, cyborgs do: A Latourian provocation for transformatory arms control and disarmament. *Global Change, Peace & Security*, *24*(1), 141-163.

Brown, S. (2006). The criminology of hybrids. Rethinking crime and law in technosocial networks. *Theoretical Criminology, 1*(4), 223-244.

Charmaz, K. (2006). *Constructing grounded theory: A practical guide through qualitative analysis.* London: Sage Publications.

Chandler, A. (1996). The changing definition and image of hackers in popular discourse. *International Journal of the Sociology of Law. 24*(2), 229-251.

Churchill, D. (2016). Security and visions of the criminal: Technology, professional criminality and social change in Victorian and Edwardian Britain. *British Journal of Criminology, 56*(5), 857-876.

Clynes, M.E., & Kline N.S. (1960). Cyborgs and space. *Astronautics, 5*(9), 26-27.

Dant, T. (2004). The driver-car. *Theory, culture & society, 21*(4/5), 61-79.

Ferrell, J. (1996). *Crimes of style: Urban graffiti and the politics of criminality*. Boston, MA: Northeastern University Press.

Ferrell, J. (1997). Criminological verstehen: Inside the immediacy of crime. *Justice Quarterly, 14*(1), 3-23.

Forlano, L., & Jungnickel, K. (2015). Hacking binaries/hacking hybrids: Understanding the black/white binary as a socio-technical practice. *Ada: A Journal of Gender, New Media and Technology*, no 6. Retrieved from http://adanewmedia.org/2015/01/issue6-forlano-jungnickel/.

Garfinkel, H. (1967). *Studies in ethnomethodology*. New Jersey: Prentice Hall Inc.

Gunkel, D. (2001). *Hacking cyberspace.* Boulder, CO: Westview Press.

Halbert, D. (1997). Discourses of danger and the computer hacker. *The Information Society, 13*(4), 361-374.

Haraway, D.A. (1987). A Manifesto for cyborgs: Science, technology, and socialist feminism in the 1980s. *Australian Feminist Studies, 2*(4), 1-42.

Himanen, P. (2001). *The hacker ethic and the spirits of the information age*. New York, NY: Random House.

Holt, T.J. & Kilger, M. (2008). Techcrafters and makecrafters: A comparison of two populations of hackers. *Workshop On Information Security Threats Data Collection and Sharing*, 67-78. DOI 10.1109/WISTDCS.2008.9

Holt, T.J. (2010). Examining the role of technology in the formation of deviant subcultures. *Social Science Computer review*, *28*(4), 466-481.

Hennink, M., Hutter, I., & Bailey, A. (2011). *Qualitative research methods*. London: Sage.

Ihde, D. (1990). Technology and the lifeworld. Bloomington, IN: Indiana University Press.

Jordan, T., & Taylor, P. (1998). A sociology of hackers. *The Sociological Review*, 46(4), 757-780.

Katz, J. (1988). *The seductions of crime: Moral and sensual attraction in doing evil*. New York, NY: Basic Books.

Kilger, M. (2010). Social dynamics and the future of technology-driven crime. In T.J. Holt & B. Schell (Eds.), *Corporate hacking and technology-driven crime: Social dynamics and implications* (pp. 205-227). Hershey, PA: IGI-Global.

Latour, B. (1992). Where are the missing masses? The sociology of a few mundane artifacts. In W.E. Bijker & J. Law (Eds.), *Shaping technology/building society: Studies in sociotechnical change* (pp. 225-258). Cambridge, MA: MIT Press.

Latour, B. (2005). *Reassembling the social. An introduction to actor-network-theory*. New York: Oxford University Press.

Law, J. (2004). *After Method: Mess in Social Science Research.* London: Routledge.

Levy, S. (1984). *Hackers heroes of the information age.* New York, NY: Double Day.

Lupton, D. (1999). Monsters in metal cocoons: 'Road range' and cyborg bodies. *Body & Society, 5*(1), 57-72.

Lyng, S. (2004). Crime, edgework and corporeal transaction. *Theoretical Criminology,* 8(3), 359-375.

Matza, D. (1969). *Becoming Deviant.* Englewood Cliffs: Prentice Hall.

Nikitina, S. (2012). Hackers as trickster of the digital age: Creativity in hacker culture. *Journal of Popular Culture, 45*(1), 133- 152.

NOS (2012, February 9). Hoogste alarmfase na hack. [news article] Retrieved from https://nos.nl/artikel/339192-hoogste-alarmfase-na-hack-kpn.html

Mul, J. de (2002). *Cyberspace Odysee*. Kampen: Klement.

Nissen, J. (1998). Hackers: Masters of modernity and modern technology. In J. Sefton- Green (Ed.), *Digital Diversions: Youth Culture in the Age of Multimedia* (pp. 149–171). London: UCL Press.

Nissenbaum, H. (2004). Hackers and the contested ontology of cyberspace. *New Media Society 6*(2), 195-217.

O'Brien, M. (2005). What is cultural about cultural criminology? *British Journal of Criminology, 45*(5), 599-612.

Skibell, R. (2002). The myth of the computer hacker. *Information, Communication and Society,* 5, 336-356.

Steinmetz, K.F. (2015). Craft(y)ness. An ethnographic study of hacking. *British Journal of Criminology, 55*(1), 125-145.

Steinmetz, K.F. (2014). The greatest crime syndicate since the gambino's: A hacker critique of government, law, and law enforcement, *Deviant Behavior, 35*, 243-261.

Steinmetz, K.F. & Gerber, J. (2015). "It doesn't have be this way": Hacker perspectives on privacy. *Social Justice, 41*(3), 29-51.

Sterling, B. (1993). *The Hacker Crackdown: Law and Disorder on the Electronic Frontier*. London: Viking.

Suarez, J.R.P. (2015). *We are cyborgs: Developing a Theoretical model for understanding criminal behaviour on the internet*. Doctoral Thesis, University of Huddersfield. Retrieved from http://eprints.hud.ac.uk/id/eprint/28324/

Taylor, P.A. (1999). *Hackers. Crime in the digital sublime.* London and New York: Routledge.

Taylor, P.A. (2005). From hackers to hacktivists: Speed bumps on the global superhighway?. *New Media Society, 7*(5), 625-646.

Thomas, D. (2005). Hacking the body: code, performance and corporeality. *New Media & Society*, 7(5), 647-662.

Turgeman-Goldschmidt, O. (2005). Hacker's accounts: Hacking as a social entertainment. *Social Science Computer Review, 23*(1), 8-23.

Turgeman-Goldschmidt, O. (2008). Meanings that hackers assign to their being a hacker. *International Journal of Cyber Criminology, 2*(2), 382-396.

Turkle, S. (1982). The subjective computer: A study in the psychology of personal computation. *Social Studies of Science, 12*, 173-205.

Turkle, S. (1984). Hackers: Loving the machine for itself, In S. Turkle, *The Second Self: Computers and the Human Spirit* (pp.196-238). New York, NY: Simon & Schuster .

Turkle, S. (2005). *The Second Self: Computers and the Human Spirit*. Cambridge, MA: MIT press.

Tweakers (2014, September 4). Rotterdamse Hacker krijgt een maand celstraf [news article]. Retrieved from https://tweakers.net/nieuws/98247/rotterdamse-hacker-krijgt-een-maand-celstraf.html

Verbeek P-P. (2005). *What Things Do: Philosophical Relations on Technology, Agency, and Design*. University Park, PA: Pennsylvania State University Press.

Verbeek, P-P. (2008). De grens van de mens. Over de relatie tussen mens en techniek. In I.L. Consolie & R. Hoekstra (Eds.), *Annalen van het Thijmgenootschap* (pp. 14-36). Nijmegen: Valkhof Pers.

Van der Wagen, W. (2018). *From Cybercrime to Cyborg Crime: An exploration of high-tech cybercrime, offenders and victims through the lens of Actor-Network Theory*. Doctoral Thesis, University of Groningen. Retrieved from https://www.rug.nl/research/portal/en/publications/from-cybercrime-to-cyborg-crime(f3a5c5e0-ff0f-4dad-ac6c-2bc91d96a1b4).html

Van der Wagen W, Althoff M. & Van Swaaningen R. (2016). De andere 'anderen'. Een exploratieve studie naar processen van labelling van, door en tussen hackers. *Tijdschrift over Cultuur en Criminaliteit, 6*(1), 27-41.

Van der Wagen, W., & Pieters, W. (2015). From cybercrime to cyborg crime: Botnets as hybrid criminal actor-networks. *British Journal of Criminology, 55*(3), 578-595

Van't Hof, C. (2015). *Helpende Hackers. Verantwoorde onthullingen in het digitale polderlandschap*. Rotterdam: Uitgeverij Tek Tok.

Wall, D. (2007). Cybercrime. *The Transformation of Crime in the Information Age*. Cambridge, UK: Polity Press.

Wall, D. (2008). Cybercrime and the culture of fear. Social Science fiction(s) and the production of knowledge about cybercrime. *Information, Communication & Society, 11*(6), 861-884.

Wood, M. (1998). Agency and organization: Toward a cyborg-consciousness. *Human Relations, 51*(10), 1209-1226.

Yar, M. (2005). Computer hacking: Just another case of juvenile delinquency? *The Howard Journal, 44*(4), 387-399.

Wytske van der Wagen recently completed her PhD project "From cybercrime to cyborg crime: an exploration of high-tech cybercrime, offenders and victims through the lens of actor-network theory" at the University of Groningen (Netherlands). She currently works as an assistant professor at the Erasmus School of Law (Department of Criminology) in Rotterdam. Here she will continue doing criminological research on cybercrime, particularly qualitative research on cyber offenders and theoretical issues.

The Use of Mythic Narratives in Presidential Rhetoric on Cybercrime

Joshua B. Hill[1]
The University of Southern Mississippi

Nancy E. Marion
The University of Akron

Abstract

What politicians say about crime matters, both because of the impact their rhetoric has on public opinion and the policies and motives those words often portend. This is no different when presidents speak about the relatively new area of technocrime. As with other types of crime, political rhetoric on technocrime relies on previous social constructions of the problem, which are (in part) based on myths rooted in popular culture. These myths can be used to help forward political agendas in ways that may be useful to the politician, but that do not address the causes or effects of technocrime. Using ethnographic content analysis, we examine presidential speeches on technocrime, specifically cybercrime, for reliance on mythic narratives, a set of characteristics including threats to common values, the construction of a hero, the existence of innocent victims, and reliance on a deviant population. Our findings indicate that presidents often rely on mythic narratives in their speeches regarding cybercrime. This reliance can best be understood through the lens of securitization, which allows presidents to use myths to further their security agendas.

Keywords: cybercrime, technopanic, myths, presidential rhetoric, criminal justice

INTRODUCTION

Cybercrime has become an increasingly large part of the public discourse of crime and criminal justice and has recently started entering the legal lexicon as well (Wall, 2011). This has occurred despite the amorphous nature of the term "cybercrime" and the lack of technical understanding of policymakers and a significant part of society more broadly regarding the issue (Brenner, 2011). The reasons for the increasing attention are centered in the public's ever-broadening uses of technology, as well as more deep-seeded social issues surrounding the fear that new technology raises (Thierer, 2013; Wall, 2011). While rooted in the science fiction of the early 1970s, this fear has come to dominate significant parts of the contemporary discourse surrounding cybercrimes (Wall, 2011).

[1] Corresponding Author: Joshua B. Hill. 118 College Drive #5127, Hattiesburg, MS 39406-0001 Phone: 601.266.4176. Email: Joshua.b.hill@usm.edu

As the public conversation invariably involves political elements, so too does cybercrime and its presentation by politicians and other authorities (Cavelty, 2013). David S. Wall (2011) pointed out that when pressed for an answer to why dramatic or impactful events happen, politicians are often quick to point to "the Internet" as the reason without significant causal justification. This is perhaps even truer when referencing crimes that use the Internet or other technology as part of the crime itself, and the responses to them has been additional public fear (Lewis & Fox, 2001). While increasing the public's overall feeling of security, politicians can often use this fear to assist in furthering their political agendas, precisely because the issues they reference are not well-understood (Altheide, 2006; Potter & Potter, 2001). Thus, it is important to examine political responses to cybercrime, as these responses often drive public fear and the policy responses to that fear (Cavelty, 2008, 2013). These responses can be used to link subjects that are not necessarily linked – like cybercrime and national security (Cavelty, 2013; Hill & Marion, 2016). In some cases, these responses have gone as far as to help develop moral panics (Bowman-Grieve, 2015; Hawdon, 2001; Levi, 2009). Presidents, in particular, have a unique role in terms of their responses to crime. As the most visible public figure in American politics, and one of the most visible political figures worldwide, presidents' statements are often covered by both the news and social media. This coverage can have a significant impact on public opinions regarding crime and criminal justice issues (Hill, Oliver, & Marion, 2010), and can help shape the discourse regarding these crimes within society writ large (Howdon, 2001).

This paper examines questions of how presidents speak about the issue of cybercrime through an examination of mythic narratives within presidential speeches on cybercrime. The analysis is rooted in the historical development of "cybercrime" as a specific type of public crime myth, and the use of elements within that myth by Presidents Clinton, Bush (George W. Bush), and Obama in their rhetoric about cybercrime. Specifically, using an ethnographic content analysis (ECA), we examine elements of criminal justice myth derived from Kappeler and Potter (2005) and Bottici (2010) showing that these myths are often used by presidents to further fear, although their use differs across administrations and time.

TECHNOCRIME AND CYBERCRIME

There is a good deal of consternation regarding the terminology surrounding cybercrime and technocrime (Brenner, 2011; Hill & Marion, 2016; Leman-Langlois, 2013; Sheptycki, 2013; Steinmetz, 2015). Debates about what term is appropriate stem from the difficulty of defining specifically which crimes constitute "cybercrime" versus "computer crimes" as well as fundamental disagreements over what constitutes activities like "hacking" within the realm of technocrime (Steinmetz, 2015). These debates are important to assist in defining the scope of academic inquiry, but in the public mind, "cybercrime" has become the most widely used term, and hacking the focus of much attention (Brenner, 2011; Hill & Marion, 2016; Wall, 2008, Yar, 2013). Because of the ubiquity of the use of the term cybercrime in particular within presidential speech, this analysis makes use of that term while acknowledging that more accurate terms like technocrime would be more appropriate.

Despite our use of the term cybercrime, we cannot proceed without understanding the social underpinning of how cybercrime came into the presidential discourse, and how this is intimately linked with the social understanding of the idea of "cyber." There exists a kind of

dualism of cultural technophobia and technological salvation in relation to cyber issues, which is played out in presidential use of mythic narratives about cybercrime. While we can trace much of this back to the development of the "hacker" mythos in popular culture (Skibell, 2002; Steinmetz, 2015; Wall, 2011), politicians and other interested parties have attempted to securitize the discourse surrounding cybercrime in the method described by the Copenhagen School (Hansen & Nissenbaum, 2009).

One of the elements of the securitization perspective of the Copenhagen School is that types of security discourse contain their own "grammar" (Hansen & Nissenbaum, 2009). In the case of cyber security, the grammar is one that does not characterize specific referents to "cyber security" (e.g., the nation), but instead is a grammar that cuts across referents, tying them together. In some respects, this is in line with the perspective of Foucault, as articulated by Skibell (2002), but also corresponds directly to the speeches of presidents. This link happens primarily through the articulation of *how* threats within the mythic narrative framework are described and the "evil" characters who will carry out this threat. For example, linking hackers and terrorists regularly in political rhetoric serves to underscore how these mythic narratives function, and how the grammar of cybersecurity functions to make sense of the elements of mythic narratives. In some respects, the entire myth of cybercrime is predicated on these cross-cutting rhetorical elements as the regular pairing of cybercrime with national security issues show (Cavelty, 2013; Hill & Marion, 2016).

Effectively, the spaces of politics, popular culture, and political discourse work in tandem to define cybercrime in specific, securitized ways, and mythic narratives are the threads that weave the popular and political together. Within the popular cultural context identified by Skibell (2002) and Wall (2011), hackers, as the cultural representatives of cybercrime, develop certain deviant characteristics, and perhaps more saliently, develop in terms of their seeming ability to affect all parts of society. This narrative can help shape the perceptions of cybercrime not just for the general public, but for political elites as well, and certainly helps shape the ways in which presidents can speak to the public about issues like cybercrime.

Presidents themselves have an effect on the public through their speech and have regularly used this in relation to crime (Brace & Hinkley, 1992; Denton &Hahn, 1986; Eshbaugh-Soha, 2004; Firchild & Webb, 1985). Cybercrime, though more recent, has also been a topic of presidential rhetoric, and presidents have often linked it with security issues salient to their agendas (Hill & Marion, 2016). Given their ability to help shape public opinion, and even to help shape moral panics (Hawdon, 2001), examination of presidential discourse is important to understanding the place of cybercrime in both the popular and political landscapes.

Leman-Langlois (2008) also pointed out that the specific discourse surrounding cybercrime matters. When the president speaks of "DNS attacks" and "bot-nets," it technologizes the language in a way that makes it sound first, more technically difficult than it may be, and second, as if there is objective certainty about *what* constitutes a crime in cyberspace. This type of language is perhaps most evident in the recent "aggravated identity theft" charge against the hacker Guccifer for "unauthorized access to a protected computer" (Bayly, 2016, n.p.) involving the release of private information publically. While certainly a crime, the "aggravated" element of identity theft is far from clear – as is the presence of identity theft to begin with.

Ironically, in speeches and other statements, presidents rely on the fear that cybercrimes have helped to create in the already transparently insecure atmosphere of late modernity (Young, 2007). In essence, they rely on "the critical flaws of late modern society, the fragility of its technological structure, the unknown consequences of the deep demographic and social changes it had triggered and the general insecurity it has failed to alleviate" (Leman-Langlois, 2008, p. 4). This is relatable because of the space technology has come to occupy in late modern society – that is to say, nearly all of it. It is also supported by the constant reiteration of the danger of cyberspace within popular culture and political discourse (Hansen & Nissenbaum, 2009). Fractures in the way we see technology, like those presented by cybercrimes in films, create fractures in our very reality, which is itself defined by those technologies.

Myths then, both popular and political, are important constituent elements of our understanding of cybercrime (Skibell, 2002; Wall, 2011). While these myths arise in the context of the development of the cultural understanding of hacking, and cybercrime more broadly, they have significant impact on the political discourse as well, with the combination of cybercrime myths being coupled with mythic narratives presidents use in furthering their agenda. One way to characterize the use of these myths is through an expansion of the framework of mythic narratives (Griffin & Miller, 2008; Sicafuse & Miller, 2010, 2012), which themselves can be couched in the literature on symbolic rhetoric and policy.

> Symbolic rhetoric has been defined as the communication by political actors to others for a purpose, in which the specific object referred to conveys a larger meaning, typically with emotional, oral, or psychological impact (for which) this larger meaning need not be independently or factually true, but will tap ideas people want to believe in as true. (Hinckley, 1990, p.7)

This integrates and makes the elements of mythic narrative useful to political actors. Thus, the symbolic rhetoric of the president can influence society by calling on myths already present within society. These, when applied to crime, can be used by presidents for a variety of political purposes, including garnering support for his or her security agenda, claims-making about a new issue, or even helping to generate moral panics (Hawdon, 2001).

This process is not straightforward. As Esch (2010) states, "the process of layering meaning over a narrative is complex and contested; it mythologizes the narrative so that it holds shared significance for a group" (p. 357). This meaning-making process, and the evocative nature of myths within popular culture that are relied upon in presidential rhetoric, often require multiple techniques in order to become useful at moving forward an agenda (Socia & Brown, 2016). Presidents can use symbolic rhetoric that relies on a securitization grammar as a tool of mythic narrative to achieve a policy goal, either tangible or symbolic.

Consequently, while couched in symbolic rhetoric, presidents often rely on mythic narratives to evoke a reaction from the public (Edelman, 1975). There are four elements within mythic narratives, which allow both their identification within any given discourse as well as for examination of how each contributes to a myth (Bottici, 2010; Kappeler & Potter, 2004). Briefly, these are a deviant population, a hero, a threat to social norms, and the presence of innocent

victims. The way these elements constitute themselves in the context of presidential discourse on cybercrime is unique, and in some ways, paradoxical.

The analysis below examines these four elements across three presidents in order to better understand how the elements of myth are used in political discourses on cybercrime. The analytical framework assumes that symbolic rhetoric is the overarching concept, in which presidents make use of mythic narratives to further their policy agenda or inspire action within society. This, in turn, can make use of, or sometimes help generate, moral panics in the realm of technology – more specifically, technopanics, to use Therier's (2013) language. The symbolic language used within cybercrime rhetoric relies on the grammar of securitization in order to make the elements of mythic narrative useful for furthering the President's political agenda. This reflects the process identified by McLeod (1999, p.360), "…political rhetoric in modern cultural contexts are designed and organized events…and orchestrated for quantitative effects. The process…is nothing less than symbolic manipulation by design, playing on deeply held beliefs in the electorate."

METHODOLOGY

Data

The *American Presidency Project* (2015) was the primary source for the speeches made by presidents regarding cybercrime, which maintains an online, searchable database of presidential papers, including presidential speeches. As the goal of the project was to explore the use of presidential rhetoric on cybercrime though the lens of mythic narratives, presidential speeches were the unit of analysis.

Searching for instances of cybercrime is difficult since many countries and organizations use different definitions to define these acts (Wall, 2008). Moreover, the term is sometimes used interchangeably with terms such as "computer-related crime," "technocrime," and "computer crime." This only serves to cause more confusion among the public, though there is little reason to believe it is better when politicians use the terms (Gordon & Ford, 2006; Kshetri, 2013; Wall, 2011; Yar 2013). The matter gets yet more complicated when terms like "cyberterrorism" and "cyber-attack" are used. These terms, in particular "cyberterrorism," are equally amorphous as the term "cybercrime," and are often used in conjunction with it (Cavelty, 2007; Hill & Marion, 2016; Wall, 2011). However, recent scholarship has stated that regardless of the accuracy of the term, "cybercrime" has become the accepted terminology (Wall, 2011). To that end, in the current analysis, the term cybercrime was construed to include illegal activity conducted over the Internet or other networked systems. Thus, the study includes rhetoric about a wide variety of criminal activity ranging from child pornography to so-called cyberterrorism.

It is important to note that this includes some threats that are traditionally linked to national security rather than criminality. Though we focus on rhetoric regarding criminality, we did not exclude speeches that focus primarily on national security. This is because the two areas have been linked in past speeches, and presidents do not often draw bright lines between the two (Hill & Marion, 2016). Additionally, and perhaps more importantly, this analysis shows that presidents often group technologically complex issues, some related to cybercrime and some not, together under the rubric of "cyber."

As such, the search term “cyber” was used to find presidential speeches on cybercrime. This generated a large number of results and captured a large number of the speeches given by presidents involving issues ranging from cybercrime to cyberbullying. More specific search terms such as “Internet,” “online,” or “identity theft” were then used to find speeches that dealt with cyber issues that did not include the prefix “cyber.” This captured speeches on those topics and others such as Internet predators, Internet pornography, or Internet stalking.

The original search, which generated results from the years 1995-2015, returned 491 cases. The first years of Clinton’s term was excluded based on the fact that he did not speak substantively on cybercrime before 1995, and the last year of Obama’s term was excluded based on the date of original data collection (early 2016). Many of the speeches in the original sample were references to elements outside the issues addressed in this study (cybernetics, for instance), and some were given by presidential staff rather than by the president himself, which reduced the original number of speeches to 380. Rhetoric that was formulaic in nature, like proclamations, fact-sheets, and statements of administration policy were also eliminated, as were statements by administrative representatives rather than presidents, reducing the sample to 209 speeches.

This sample was further reduced by subsampling among the three presidents who have thus far spoken about cybercrime: Bill Clinton, George W. Bush, and Barack Obama. As the data did not present a specific pattern of speeches based on the first read-through, speeches were randomly selected for coding – 25 from each president for a total of 75 speeches.

Analytical Methodology

The method of analysis used to examine the data is ethnographic content analysis (ECA). ECA is an inductive approach to qualitative data, allowing both for theoretical sampling of the data, as well as a recursively constructed codebook (Altheide, 1996). In the current case, ECA was used to help identify elements of mythic narrative and how they were being used within the context of presidential rhetoric. While the basic four parts of mythic narratives served as the original basis for the coding scheme, other elements were quickly identified as sub-themes, including the type of actors identified as deviant, types of heroes, and the ways in which threats to society were presented.

Symbolic Rhetoric, Mythic Narratives, and Moral Panics

Moral panics have become an increasingly contested part of the criminological literature (David, Rohloff, Petley, & Hughes, 2011). Arguments over what constitutes a moral panic, and which moral panics are worthy of study, are consistently being rehashed within the literature (Cohen, 2011; Young, 2011). However, despite this contestation, and arguably because of it (David, Rohloff, Petley, & Hughes, 2011), the concept of moral panics has been used fruitfully in a variety of areas, including those examining the role of presidential rhetoric in their genesis (Hawdon, 2001). It is therefore worth noting the relationship posited regarding symbolic rhetoric, mythic narratives, and moral panics.

There are obvious and strong relationships between the concept of mythic narratives and the concept of moral panics, particularly in regards to the deviant population and threats to conventional values, but they are not identical. One way to conceptualize the difference between

the two is that while moral panic is largely a reaction by the public to a perceived issue (Cohen, 1972), mythic narrative is a structured response to a moral panic, and may contribute to its continuation. In short, they have a symbiotic relationship: Moral panics rely on mythic narratives, and mythic narratives are often used in the context of moral panics (Griffin & Miller, 2008; Kappeler & Potter, 2004). Specifically, mythic narratives convey the crucial beliefs of a social group or society in an emotionally effective way and may not be associated with actual policies (Bottici, 2010). In the sense that political actors can operate both to create myths and communicate them, presidents seem to qualify as media and as mythmaker.

Mythic narratives function in the context of symbolic rhetoric, though they can be used to motivate specific policies – sometimes effective, sometimes not (Griffin & Miller, 2010). While there has been much research on the uses and functions of symbolic rhetoric in criminal justice and criminology (Hill & Marion, 2016; Oliver, 2001; Oliver, Marion & Hill, 2016; Stoltz, 1985), there have not been many attempts to examine what elements within symbolic speech are being used by presidents, nor a model proposed of how these elements function to change public behavior. The general framework here is that mythic narratives operate through the grammar of securitization, which serves to bridge the gap between the symbolic rhetoric of crime and the specific context of cybercrime.

The four elements of mythic narrative can operate independently from one another, but often operate in tandem when those speaking are relying directly on crime myths to motivate specific policy changes – through the process of securitization. The examination below looks at how presidential rhetoric makes use of the elements of mythic narrative through an ECA approach to presidential speeches. Specifically, it examines each of the elements of mythic narrative within presidential speeches to see how they change both in terms of their use across administrations and over time, and then examines how we can make sense of mythic narratives of cybercrime through the lens of Hansen and Nissenbaum's (2009) cybersecuritization.

FINDINGS

The findings of the study can be broadly broken into two parts. First, the examination of the different elements of mythic narrative is undertaken with an emphasis on contextual understanding of the use of each. Second, an examination across presidents is extrapolated from the data in an attempt to track how different political actors across different administrations have used mythic narratives of cybercrime to further their interests.

Contextualizing the Speeches

One of the primary concerns of ECA is making sure that there is an understanding of, and sensitivity to, how the material being studied is constructed. In the current context, that of presidential speeches, it is therefore important to understand that speeches are used differently, and rhetoric differs, depending on the audience (Ragsdale, 1987; Teten, 2003). The speeches examined in this analysis ranged in terms of both their focus on cybercrime – with several mentioning the topic as simply an adjoining problem to things like terrorism or attacks on children – and their audience. The total number of speeches that talked about cybercrime or cybersecurity, by president, can be seen in Table 1 below.

Table 1. Total number of speeches, by President

President	Number of Speeches
Clinton	74
Bush	46
Obama	89

As can be seen in Table 1, the number of speeches containing the topic of cybercrime was not evenly distributed among the presidents; nor does it correlate directly with the development and increasing use of the Internet and network technology. One potential reason is that the focus of the Bush administration was drawn out of the realm of "cyber" and into the "real world" with the many issues surrounding terrorism at the time, and Bush's reliance on it as a policy-motivating issue (Altheide, 2006).

Within speeches, there was also an uneven distribution of rhetoric regarding cybercrime. Those speeches that tended to contain much of the rhetoric were either on the occasions of signing a law that the president felt somehow dealt with cybercrime or to agencies that were specifically tasked with fighting cybercrime. The latter tended to be the most rhetorically rich in terms of gaining understanding of how presidents dealt with cybercrime, but even those speeches with short mentions often shed light on how cybercrime was being used as a tool by different administrations. This was accomplished through both what was coupled with cybercrime rhetoric, and frequently, what types of "attacks" or actors were thought of as threatening.

As can be seen in Table 2 below, the number of quotations regarding the four elements of mythic narrative in the sample varied, with President Obama having (by far) the most quotations across the four dimensions. However, in part, that may be because the speeches sampled for Obama were directed more towards those geared towards cybercrime and national security than Bush or Clinton. All told, given the sampling methodology and the focus on the development of the elements of mythic narrative, rather than the counts of quotations or speeches, the relative number is only informative insofar as it contextualizes the analysis below.

Table 2. Mentions of the elements of mythic narrative in speeches, by president

	Deviant Population	**Hero**	**Innocent Victims**	**Threat to Established Values**
Bush	13	17	9	21
Clinton	38	47	40	79
Obama	22	28	26	28
Total	*73*	*90*	*75*	*128*

A Deviant Population

The first criterion of mythic narratives refers to the existence of a "deviant population" (Kappeler & Potter, 2004). This population, because of cultural, religious and other differences, are labeled as "deviant" and can become targets for negative rhetoric, instigating fear in people. In this research, deviant populations appeared 73 times in 75 speeches, though some speeches contained more than a single instance of deviant populations. For example, in remarks on May 5, 2000, President Clinton argued: "[Because of the internet] You will see, more and more, drug cartels, organized criminals, gunrunners, terrorists working together."

As mentioned above, elements of mythic narrative within cybercrime can be used within a securitization framework to increase their salience (Cavelty, 2008, 2013; Hansen & Nissenbaum, 2009). This is clear from the identifications made between the presidential references to cybercrime and criminals committing other acts. While most of these references were to issues of national security – comporting well with Hill and Marion (2016) – some were in reference to other criminal issues, like gangs, drugs, and organized crime. The rhetorical suggestion is that cybercrime is amorphous – that it does not have a specific nature or link to a specific type of illicit activity (Ohm, 2007). This vague definition can make it useful for policy-makers to help forward a security agenda (Cavelty, 2008).

Within this context, the persona of the "hacker" takes on greater importance. While hackers have been defined in multiple ways (Steinmetz, 2015; Wall, 2011; Yar, 2013), what is notable in the presidential rhetoric regarding cybercrime is the often-undefined nature of the hacker. Because hacking is considered an activity that bridges any kind of illicit online activity, hackers become divorced from the skill they have and are instead thought of as a complete criminal category that may do anything illicit. As Yar (2013) said, "for many people cybercrime and hacking have become synonymous" (Chapter 2, Section 2, para. 1), which links hackers ineluctably to cybercrime, and this is reflected in presidential speeches. It is perhaps most clearly seen in rhetoric by presidents about the nearly omnipotent nature that hackers are thought to have. For example, President Clinton on January 7, 2000 stated,

> I want to talk just a moment about steps we are taking today to defend our citizens from those who would use cyberspace to do us harm. There has never been a time like this in which we have the power to create knowledge and the power to create havoc, and both those powers rest in the same hands... Yet, someone can sit at the same computer, hack into a computer system and potentially paralyze a company, a city, or a government.

This quote shows both the moral ambiguity seen in the online environment itself, but more importantly in terms of rhetorical conceptualizations of hackers, it demonstrates the near omnipotence that s/he is seen to have – the power to create or destroy at will – a position supported by earlier literature on perspectives of hackers (Ohm, 2007).

Because the hacker is amorphous, the concept is useful to presidents when linked with other topics, and presidents take advantage of this (Hill & Marion, 2016). Often, for instance, hacking is linked to other forms of criminality, particularly to drug cartels, organized crime, and

terrorism. This, coupled with the omnipotent nature of the hacker in presidential rhetoric, positions her in some respects as the ultimate criminal in late modernity, and takes advantage of the perception of technology as potentially threatening (Taylor, 1999).

This portrait of hackers as the ultimate criminal archetype comports well with earlier literature (Wall, 2011). It also shows the reliance on popular cultural myths by presidents regarding their views on cybercrime (Halbert, 1997; Yar 2013). Indeed, President Clinton was explicit in this reliance, stating in an interview on January 21, 1999 that,

> I also find that reading novels, futuristic novels—sometimes people with an imagination are not wrong... And then I read another book about a group of terrorists shutting down the telephone networks in the Northeast and the Midwest... and a lot of times it's just for thrills, but a lot of times these people [authors of science fiction] are not far off.

While this demonstrates the influence of social science fiction (Wall, 2011) on President Clinton specifically, it is likely that other presidents were influenced as well.

Other deviant populations. While hackers are the most frequently referenced specific category of cybercriminals within presidential rhetoric, they are not always cited by presidents. Often, the type of crime is referenced in relation to the Internet. So, the use of the Internet by pre-existing categories of criminals – drug runners, cartels, organized crime, child pornographers – constitutes a significant portion of the mentions of cybercriminals within presidential rhetoric. These mentions, however, most frequently reference the use of technology as a tool for the groups rather than as the medium used within a given incident. On July 8th, President Clinton, stated,

> In fact, all of the openness, the communications revolution, what all you can find on the Internet, all of the things that have given so much opportunity in the world and brought us so much closer together have created a new vulnerability to the organized forces of destruction, to the terrorists, the organized criminals, and the narcotraffickers.

This relies on a slightly different conception of the deviant populations as *already existing*. The Internet, and technology more generally, is referenced as a *tool* for those who are already engaged in some kind of illicit activity. This can be using networks to better coordinate activity, or for finding information that can be of assistance in offline activity – bomb-making instructions were consistently referenced by President Clinton, for instance.

Cybercriminals – a portmanteau enemy. In total, hackers are frequently referenced in presidential rhetoric as nearly omnipotent, ineluctably criminal technology users who engage in a variety of illicit online activity. They are most often coupled with other forms of criminality, underlying both their dangerousness and their amorphous nature. Cybercriminals are often situated as a threat to the general moral order, often manifested through targeting innocent victims – the subject of the next section. On the other hand, non-hacking cybercriminals are almost always a pre-existing reference group with already deviant identities. They, rather than use the internet or other networks as an instrument to carry out cybercrimes, use it as a tool to

enhance their already existing illicit activities. They are not, however, seen as simple extensions of the previous criminal types. For instance, President Obama (2015), remarked, "We want cyber criminals to feel the full force of American justice, because they are doing as much damage, if not more, these days as folks who are involved in more conventional crime," thus demonstrating the conceptual independence of cybercriminality from general crime.

Perhaps the best way to conceive of cybercriminals in presidential rhetoric is as a *portmanteau enemy*. A portmanteau is a combination of two words to create a third containing elements of both reference words. Similarly, when referencing deviant populations in terms of cybercrime, presidents rely on existing categories – hackers and other pre-existing deviant populations – to create multiple types of cybercriminals ranging from cyberterrorists to online identity thieves that threaten both societal values and innocent victims.

The Presence of Innocent Victims.

The second criterion to define mythic narratives is the presence of "innocent" or "helpless" victims. Three of the most likely victims in the literature are children, pregnant women, and the elderly, because they garner high levels of sympathy from the public (Miko & Miller, 2010). Mythic narratives encompass the idea that the more innocent a population affected by a crime myth, the more likely people will support the crime myth targeting "deviant populations" hurting "helpless" victims. Statements focused on victimization appeared 75 times in the presidential speeches examined. President Bush's remarks in 2012 were exemplary of this kind of victimization, where he said, "in the hands of incredibly wicked people, the Internet is a tool that lures children into real danger."

Innocent victims. In general, there were several types of victims presented by presidents in their rhetoric, only some of which fit the classic example of innocence. Children, as seen in the quotation above, were often the subject of this rhetoric in two ways. The first, as potential victims of online pornography, is interesting because it does not fit the traditional definitions of cybercrime, though accessing pornography below the age of 18 is considered a crime in nearly all jurisdictions (Yar, 2013). This was a constant concern of Presidents Clinton and Bush, who frequently referenced the need to protect children from pornography. A second way in which children needed to be protected from cybercriminality, and are thus presented as victims, is from exploitation, including online child pornography (as part of the content, rather than the issue of access), and recruitment by terrorist and other extremist organizations. This is frequently coupled with announcements of how the government (and frequently, the private sector), is working to protect the children from exploitation, lending itself to the presentation of government as heroic. In fact, it was frequently difficult to differentiate the heroic elements of "saving" victims – or empowering people to save them – from the rhetorical elements focusing on threats to the existing social order.

One of the easiest places to identify this coupling was within the context of child-victimization. While the type of victimization presented changed across administrations, it was always presented in concert with the government providing either direct protection, or support for parents in protecting their children. President Bush, on October 23, 2002, provided an excellent example of the latter type of statement, saying, "Share your experience with your

children. Make it clear to your children about the potential online dangers they face. Make it clear to them the kinds of web sites they need to avoid."

Other groups that require special protection are also featured in presidential rhetoric about cybercrime. Notably, the elderly in regards to fraud schemes and the infirm through the threats to "healthcare systems," though these tended to be subsumed by the second category of victimization – general victimization.

General victimization. Within presidential speeches, the rhetorical presentation of a general victimization was used more often than the presentation of an "innocent" victim. This was sometimes couched within the language of groups, like "consumers" or "businesses," with the implication that everyone is a potential victim. One example of this type of presentation was by President Obama in a January 2015 address where he remarked, "so this [connectivity that was being taken advantage of by cybercriminals] is a direct threat to the economic security of American families, not just the economy overall, and to the well-being of our children".

A different mode of rhetorical presentations of victims involved elements in our infrastructure – often banking or other financial institutions. However, oftentimes the specific victim, or category of victim, was not named. Rather, presidents relied on a generalized threat to everyone, a construction which itself relies on the fact that more and more individuals are connected to the Internet. These presentations of a generalized victimhood are closely tied to the presentation of deviant individuals as threatening social values. These underlying values focus on private industry, infrastructure (generally), or general citizenry. For example, on May 10, 2006, President Bush made remarks regarding identity theft online, saying, "Identity theft is a serious problem in America. I have just listened to the horror stories from fellow citizens who have had their identities stolen." Here, "fellow citizens," are an undefined category, with the implication that anyone could be affected.

Who gets victimized? Given the rhetoric from presidents on victims within cybercrime rhetoric, there are two basic groups: the innocent and everyone. Within the innocent victims, there is a focus on the traditional groups considered innocent – children, the elderly, or the infirm (Miko & Miller, 2010). Within the generalized victimization category, there is a focus on underlying structures, and private industry is one of the consistent victims. This is of note as they also play a role in the element of "hero" within mythic narratives of cybercrime, and are often couched as part of the institutions under threat from cybercrime.

The generalized victimization is one that is particularly interesting from a rhetorical perspective. As there is a generalized anxiety in modern society (Young, 2007), the fact of a generalized potential for victimization within presidential rhetoric is telling. Presidents have often used fear to advance their agendas, with crime creating a portion of that fear (Altheide, 2006, 2009; Hawdon, 2001), and the possibility of anyone being a victim (a discourse frequently seen in speeches on terrorism) may be seen as a way in which society itself is undermined. Additionally, crime (more generally) has also served as a way for politicians to help replace the welfare state with a security state (Beckett & Sasson, 2000), increase surveillance (Halbert, 1997), and the method by which they have done this, rhetorically speaking, is by focusing on increasing fear (Beckett & Sasson, 2000; Hawdon & Wood, 2014).

Mythic victims. In short, there are two primary representations of victims within presidential rhetoric on cybercrime. The first focuses on traditional groups of innocent victims – particularly children. The second focuses on a generalized victimhood with an emphasis on anyone's ability to become a victim of cybercrime in the future. This second group, sometimes couched in the language of capitalism, has important implications for thinking about how presidential rhetoric shapes public fear of cybercrime. The potential for a generalized victimization underlies the idea of a threat to the country's (and sometimes, rhetorically, the world's) values.

The Threat to Established Values

The third criterion for mythic narrative is the presence of a threat to established norms and values (Griffin & Miller, 2008). It is perhaps the most difficult of the elements of mythic narrative to understand, as it assumes foreknowledge of shared values within a society, and assumes – partially – that values are homogenous within societies. Politics plays an important role in characterizing public myths (Esch, 1999), and myths about cybercrime are no different in this regard. Indeed, politicians have used myths to suggest that organized crime threatening and corrupting American values is due to a massive flow of foreign minorities invading the United States in order to change immigration laws, which has moved the US from a welfare state towards a security state (Beckett & Sasson, 2000; Hawdon & Wood, 2014). Politicians have also previously used public narratives of threats to common values like hard work to persecute drug users and sellers (Hawdon, 2001).

In the context of presidential speech on cybercrime, "threats" are often posited as attacks to specific perceived foundations of American society. For instance, in remarks on May 22, 1998, President Clinton declared that, "adversaries may attempt cyberattacks against our military and our economic base" – the polis and the economy being two important institutions in which values reside (Messner & Rosenfeld, 2007). Threats to established values was the criterion most frequently used by presidents when speaking about cybercrime. It was used 128 times across all of the speeches, making it by far the most frequently used element of mythic narrative.

One interesting iteration of the threat to common values by presidents was couching cybercrime and criminality as part of warfare, itself an existential threat. For instance, President Bush in a statement on March 3, 2006, stated, "Today, our nations [India and the United States] are cooperating closely on critical areas like...cyber security.... America and India are in this war [on terrorism] together, and we will win this war together." This narrative of warfare involving technological elements, which itself relies on a generalized threat to the country, was not limited to the Bush administration. President Clinton, too, relied on the idea of a generalized threat through technological attacks on the United States, often pairing cyber-attacks with terrorism. In a statement from March 23, 1999, President Clinton stated,

> And the darkest nightmare—I told you my happy dream for the future—the darkest nightmares of the future are the marriage of modern technology and primitive hatred, because terrorists can figure out how to get on the Internet and make bombs. You can get on the Internet and figure out how to make that bomb that blew up the building in Oklahoma City.

This statement about generalized threats is somewhat exemplary of the dual nature that technology represents in presidential discourse on cybercrime. The idea that these technological threats – and cybercrime specifically – can be dealt with through the means that created them, is a consistent theme throughout the rhetoric examined in this analysis. But there is a suggestion by presidents that *technology itself* is a threatening factor. In the statement above, primitive hatred by itself is not enough to constitute a nightmare, it is only its marriage to technology – notably non-specific – that makes it truly dark.

This is well in line with our understanding of issues of cybercrime as suggested by Therier (2013), Yar (2013), and Wall (2008). It also suggests that, in some ways, presidents consider the development of technology as part of the threat to society itself, though it is very frequently tempered by positive elements of technological developments, in terms of presidential rhetoric. This idea is linked to the moral ambivalence that is often referred to by presidents in relation to technology. In their assessment of threats, presidents often refer to the positive importance of developing technology, but then very frequently immediately refer to its use to do "evil." For example, in remarks at the Federal Trade Commission Constitution Center on January 12, 2015, President Obama said,

> And with these benefits come risks: Major companies get hacked; America's personal information, including financial information, gets stolen. And the problem is growing, and it costs us billions of dollars. In one survey, 9 out of 10 Americans say they feel like they've lost control of their personal information. In recent breaches, more than a hundred million Americans have had their personal data compromised, like credit card information. When these cyber criminals start racking up charges on your card, it can destroy your credit rating. It can turn your life upside down. It may take you months to get your finances back in order. So this is a direct threat to the economic security of American families, and we've got to stop it.

This moral ambivalence, in some respects, reinforces the perception of the criminogenic nature of the Internet and technology more generally, and underlies the threat that technology represents in the public imagination (Therier, 2013). So, in the case of cybercrime, even when presidents argue that cybercrime is being successfully challenged, they are inculcating to their listeners the idea that cybercrime is still dangerous.

One interesting threat that presidents frequently addressed was the risk to privacy. While this changed over the course of the three presidencies, privacy was usually considered in juxtaposition with increases in security. Privacy has become one of the frequently referenced American ideals that are under threat from a variety of locales (e.g., the government itself, private industry), and there is a recognition of this within presidential rhetoric, with presidents often noting the threats to privacy that individuals face, as well as their responsibility to protect it. Often, however, threats to privacy were couched within conversations about technology itself, emphasizing the increasing interconnectivity as a potential threat to both privacy and security. For example, in remarks on February 29, 2016, President Obama said,

> If we are trying to track a network that is planning to carry out attacks in New York or Berlin or Paris, and they are communicating primarily in cyberspace, and we have the capacity to stop an attack like that, but that requires us then being able to operate within that cyberspace, how do we make sure that we're able to do that, carry out those functions, while still meeting our core principles of respecting the privacy of all our people?

In short, the threats posed by technology, and cybercrime more specifically, are presented as the necessary correlate of technological development itself. The moral ambivalence of the Internet is frequently referenced, and the other elements of mythic narrative are linked with Internet use deemed to be negative (e.g., terrorists finding bomb plans online). Specific threats tend to be towards generalized normative morality (e.g., threats towards children's "innocence") or towards specific institutions like families, or notably, the economy, though there is a concern about maintaining the institution of privacy within the protection of other institutions.

The Creation of a Hero

The fourth and final criterion follows Stroud's (2001) idea of the creation of a "hero." With the development of the media, and the Internet specifically, having the community save the "innocents" and catch the "bad guys" can be a way to incorporate the listeners into the mythic narrative. With the use of mythic narratives, people are given the opportunity to be the hero and save their community (Stroud, 2001). This was common within presidential rhetoric regarding cybercrime. For instance, in 1998, President Clinton mentioned "We must give parents the tools they need to help protect their children from inappropriate material on the Internet..." More interesting, perhaps, is the focus on the private sector as potential heroes. In remarks from 1997, President Clinton said, "I call on the private sector to help us meet one of the greatest challenges of electronic commerce, ensuring that we develop effective methods of protecting the privacy of every American, especially children who use the Internet." This suggests, somewhat ironically, that the private sector is a potential savior for threats to security – including privacy. Named heroes, either specific individuals or groups, were found 90 times in the speeches examined. This criterion was the second most widely used by presidents.

Who are the heroes? Governmental heroes were often present in the rhetoric of presidents regarding cybercrime, but those heroes were often presented in different ways. An important distinction was between individually recognized heroes, often heads of agencies, and more general groups. An example of the latter came from President Obama in 2015 while at the National Cybersecurity and Communications Integration Center. He stated,

> This center is one of the critical lines of America's cyber defenses. These men and women work around the clock, 24/7, monitoring threats, issuing warnings, sharing information with the private sector, and keeping Americans safe. So as a nation, we owe them thanks...

In addition, presidents would often credit-claim in regard to protecting society from cyber-threats. This is in line with the work of Conley (2013) on signing statements, which suggests that presidents often try to gain political capital by emphasizing their role in particular legislation that has been passed. In the case of rhetoric on cybercrime, presidents frequently

employed this tactic. For example, in the 2013 State of the Union Address, President Obama stated, “I signed a new executive order that will strengthen our cyber defenses by increasing information sharing and developing standards to protect our national security, our jobs, and our privacy,” clearly claiming credit for protection of three important areas of our national identity. President Bush also claimed credit for protecting society from cybercrime, as was clear in his statement on July 27, 2006 that, “We also launched Operation Predator to help law enforcement track down and arrest foreign pedophiles and human traffickers and sex tourists and Internet pornographers who prey on our children.” These types of statements place the president and their administration in the role of hero and the protectors of the potential victims of devious cybercriminals, and allow them to capitalize on the credit they receive for the protection.

The Evolution of the Cybercrime Myth

Use of all four elements of mythic narrative was apparent in presidential rhetoric, though occasionally not in the ways traditionally used in other crime myths. Unsurprisingly, the use of the mythic elements was closely tied together in rhetoric, with recognizable deviant populations presenting threats to values through examples of victimization, and heroes, in whatever form, providing protection from future threats. This underlies the idea that what is being developed in the context of presidential rhetoric is, in fact, a complete myth regarding technocrime, rather than presidents simply relying on a single mythic element.

While the findings regarding the specific elements of mythic narrative, and within specific presidencies, are interesting, perhaps the most helpful way to interpret these findings is across all presidencies as a specific narrative arc regarding cybercrime. This narrative arc, embraced by presidents in their rhetoric, is contextualized within developing technology and popular conceptions of the hacker and “cyberspace.” The arc presented represents the influence and development of existing myths and the discourse of the securitization of cybercrime.

Existing Myths. In 2011, David S. Wall published an article focused on how science fiction has influenced the development of the production of knowledge about cybercrime. In it, he traces the development of specific myths about cybercrime and where they stem from in popular culture – with a particular emphasis on movies featuring hackers. Specifically, Wall (2011) identified seven myths regarding cybercrime, “cybercrime is dramatic; the internet is unsafe and criminogenic; hackers are all powerful ‘bad guys’; hackers have become part of organized crime; hackers are anonymous...individual users need to be protected” (p. 868).

While each of these myths is clearly embodied in the above analysis examining presidential rhetoric, the focus on the development of the science fiction(s) of cybercrime is even more telling. Presidents have roughly tracked the same trajectory that Wall (2011) identified regarding the depiction of hackers/hacking in popular films. Most salient is the movement from what Wall terms second generation haxploitation movies, based around the hacking of different types of virtualized environments (e.g., *Swordfish*), to third-generation haxploitation movies, where increasingly networked technology comes to define a space where both hacker and hack exist together (e.g., *The Matrix*).

This movement, in some senses, embodies the movement from *getting* to *doing* things online. The development in terms of rhetoric is perhaps best exemplified with regards to

presidential rhetoric about cyberterrorism. President Clinton, especially early in his presidency, often spoke about the issue of terrorists retrieving information on how to make bombs or spread ideology online. This can be contrasted with the idea of terrorist online recruiting, seen in President Obama's remarks on February 8, 2015, "The use of social media, terrorist Twitter accounts—it's all designed to target today's young people online, in cyberspace."

The salient difference between those two approaches is what "space" the interaction occurs in. In the first instance, terrorists are leaving information to be found by others on the Internet, but there is little interaction. One can leave information and one can retrieve information. The danger in the transaction is *the information*. In the latter case, *the interaction* is the danger, and that interaction happens in cyberspace. These reflect the social science fiction understanding of the development of technology as a space, and the subsequent dangers that development represents (Wall, 2011).

While the completion of this development is most clearly seen in comparison between Clinton and Obama, the changes were already happening within the Clinton administration. Of note was the rhetoric regarding "v-chips for computers," which would control access to information found online, paralleling the v-chip within TVs that could limit juvenile access to specifically rated television shows. This, however, was seemingly abandoned by the end of the Clinton presidency, with focus increasingly turning towards crimes happening online – especially identity theft.

It is important to note that presidents were not just affected by this development in the public perception of cybercrime through social science fiction, but also *used* the myths embedded within it to further securitize the idea of cybercrime. The change in rhetoric from a focus on computers used in crime to computers used *for* crime was coupled with elements that were likely to increase fear. For instance, while there was regular reference in the Clinton administration to terrorists using the Internet to gain knowledge, the idea of the "urgent and growing danger of cyber threats" was used mostly in the Obama administration. This change in the myths of cybercrime and other technocrime can best be through the cybersecuritization paradigm of Hansen and Nissenbaum (2009).

Securitization. Hansen and Nissenbaum (2009) examined the idea of the grammar of security in the context of "cyber" issues. They showed that several elements make cybersecurity unique in the context of securitization, including the integration of multiple, historically separate spheres of security.

> Cybersecurity discourse moves seamlessly across distinctions.... between individual and collective security, between public authorities and private institutions, and between economic and political military security (Hansen & Nissenbaum, 2009, p. 1161).

This movement toward securitization is apparent in presidential rhetoric across administrations, especially through the integration of the normally distinct spheres of "private" and "public." A quote from a speech President Obama gave on January 13, 2015 is particularly apt:

> Much of our critical infrastructure—our financial systems, power grids, pipelines, health care systems—run on networks connected to the Internet. So this is a matter of public safety and of public health. And most of this infrastructure is owned and operated by the private sector. So neither Government nor the private sector can defend the Nation alone. It's going to have to be a shared mission: Government and industry working hand in hand, as partners.

In addition to the integration of distinct areas of security, there is also the element of "increasing threat." President Obama, in particular, emphasized the growing nature of the problem of cybercrime and related issues. The increasing emphasis on a requirement for action to prevent future catastrophe is a key element of the securitizing discourse and part of what has been termed hypersecuritization (Hansen & Nissenbaum, 2009).

Interestingly, however, neither President Bush nor President Clinton focused much on the growth of the "cyber threat," though they had concerns about criminality online. President Bush, to the extent that he focused on issues related to cybercrime, spoke most frequently about cyberterrorism, which was unsurprising given his administration's focus on terrorism and the politics of fear (Altheide, 2006). President Obama, however, spoke with regularity about the importance of focusing on growing threats in the online environment, often incorporating the elements of cybersecurity discourse that cut across both public and private spheres. One speech from President Obama on February 12, 2015 provides a good example,

> America must also face the rapidly growing threat from cyber attacks. Now, we know hackers steal people's identities and infiltrate private e-mails. We know foreign countries and companies swipe our corporate secrets. Now our enemies are also seeking the ability to sabotage our power grid, our financial institutions, our air traffic control systems. We cannot look back years from now and wonder why we did nothing in the face of real threats to our security and our economy.

This combination – of increasing threat and a lack of division between spheres of life in conjunction with the idea that we need protection drawn from popular social science fiction – leads to a situation in which citizens can be increasingly convinced of a president's specific security agenda – in this case related to technocrime, but often linked to other forms of criminality, as examined above. This comports with previous literature suggesting that political actors use cybersecurity to advance their overall security agendas (Bowman-Grieve, 2015; Cavelty, 2008, 2013; Hill & Marion, 2016), and that creating fear can enhance their ability to achieve their goals (Altheide, 2006).

One of the most regularly occurring categories within presidential rhetoric on cybercrime was the moral ambivalence of the Internet and other technology, a position in line with the literature examining the public's relation to technology (Ohm, 2007; Therier, 2013;). This ambivalence was manifested by presidents consistently speaking about the fact that while technology has allowed for significant development – usually framed in economic terms – it can be used by deviant others to commit crime. Perhaps unsurprisingly, this was most prevalent in the speeches by Bill Clinton as the Internet was still a growing phenomenon and the scope of

change offered by the Internet was perhaps not yet clear. For example, in a speech on April 26, 1999, Clinton said,

> The Internet offers scientists the way to exchange information and fight disease, offers poor children the way to access libraries. It's amazing how many kids in high school now are filing research papers, and they don't have a—every single source they got, they got off the Internet. But the Internet also offers websites that glorify death, lionize Hitler, and tell teenagers to make pipe bombs. It is not a thing, in and of itself, that is good.

This moral ambivalence underlies their increasing securitization of cybercrime by presidents in their rhetoric. The implication is that, because the Internet can be, and is, used for cybercrime, that there needs to be a hero to save us from the criminogenic part of the Internet (Wall, 2011). The heroes presented are most frequently the government or a combination of the government and private sector, reinforcing the lack of traditional institutional boundaries necessary for cyber-securitization (Hansen & Nissenbaum, 2009).

While pointing to both the morally ambivalent nature of the Internet and the "increasing threat" of cybercrime, presidents also reinforced this with past incidents of cybercrime to demonstrate the *potential* for more significant impact in the future. President Obama did this regularly, often referring to the Sony Hack, as he did in a speech on January 13, 2015 as an example of cybercrime that portended worse in the future:

> With the Sony attacks that took place, with the Twitter account that was hacked by Islamist jihadist sympathizers yesterday, it just goes to show how much more work we need to do, both public and private sector, to strengthen our cybersecurity to make sure that families' bank accounts are safe, to make sure that our public infrastructure is safe. (Obama, 2015)

This is an example of what Hansen and Nissenbaum (2009) termed "everyday security practice," which ties individual experiences to technological threats to both ensure individuals' participation in securing networks (either themselves or through cooperation with the security agenda), and demonstrate their link to potential disasters to make hypersecuritization more plausible (p. 1165). This type of link has been common across all presidents, but the discourse has shifted based on the plausibility of online disaster, itself based on the mythic narratives explored above. President Obama's consistent reference to previous cyber attacks, the plausibility of future disasters, and their tie to normal individuals' use of the Internet, is perhaps the most complete example of securitization regarding technocrime.

The idea of everyday security practices makes sense of two elements of mythic narratives explored above. The first is that everyone is a potential victim of cybercrime, thus explaining why presidents often used a generalized victimization in their approach to innocent victims. Second, by including individuals as part of those people who can assist in the fight against cybercrime through linking people to everyday security practices, they effectively recruit them as potential "heroes" within the fight against cybercrime. This has been consistent across

presidents, with the public often being included in people who can assist in reducing cybercrime – particularly regarding elements like juvenile access to pornography.

At the same time that people are recruited through the grammar of everyday security practices, technification is a process whereby there is a particularly important role for experts in protecting people from harm in cyberspace. This, in the context of mythic narratives, relies on the "hero" trope. Technical heroes were common in presidential rhetoric, as mentioned above, but they were much more common in President Obama's speeches than either President Clinton's or President Bush's. This, perhaps, reflects a growth in the level of securitization of cybercrime across presidents. Interestingly, presidents often used this technification to justify the entrance of the private sector into the security environment, explaining that the government could not protect citizens on its own. This reinforces both the technical experts in the private sector as heroes and the government's position as hero as well.

Another manifestation of technification is the consistent call from presidents to have future generations of technical experts and for current law enforcement to have additional training. In reference to fraud on the Internet, President Clinton said in a speech on May 4, 1999,

> I find that law enforcement, compared to people who are doing criminal activity in this area, are rather like parents trying to keep up with their children on the computer. [*Laughter*] It is an endless effort, and we need to organize and systematize a continuous training and retraining effort so that we can stay ahead of the curve.

The implication here is that *technical expertise* is the key to success, and that this expertise is beyond that of the average computer user. This is a specific kind of hero, one that is outside of the political world. This, in turn, allows the grammar of securitization within cybercrime and technocrime to seem more "apolitical," and thus can help to legitimate the security position of the president.

All told, the grammar of securitization helps make sense of the development of the elements of mythic narratives of cybercrime within presidential rhetoric. Through hypersecuritization, everyday security practices, and technification, presidents are able to integrate the elements of mythic narrative in a way that is useful to pursuing their security agenda. The fact that cybercrime is so often linked to other forms of already securitized problems suggests that presidents are attempting to incorporate cybercrime into a larger security framework. However, despite these links, the development of the rhetoric of cybercrime among presidents is unique because of the distinctive nature of the mythic narratives regarding cybercrime (e.g., its ability to affect everyone as victims and our ability to "assist" in protecting vulnerable victims).

CONCLUSIONS AND IMPLICATIONS

We should be concerned about presidents' use of mythic narratives in the context of the securitization paradigm. This is because, through the integration of the social science fictions that the elements of mythic narrative rely on and security policy, we are often treating elements

like cybercrime as part of a security system that they are outside of. Consequently, this can expand executive power into areas within our lives that would normally fall outside of governmental purview. This, of course, is not theoretical, as the governmental surveillance of emails and other internet communication demonstrates (Halbert, 1997).

The incorporation of cybercrime into broader issues of security has another problematic factor as well – this one academic. If there is to be a critical analysis of cybercrime and cybersecurity policy broadly construed, the ability of academics to critique specific approaches is limited because the rhetoric has moved the topic outside the realm of normal academic debate to "technical" experts who can "objectively" decide policy (Hansen & Nissenbaum, 2009). In particular, criminal justice academics may be unable to actively critique elements of cybercrime because it will have been moved into the realm of "cybersecurity."

These securitization movements rely on the elements of mythic narrative mentioned above. The fact that cybercrime is a threat to everyone, that the deviant others committing acts of cybercrime are seemingly omnipotent, and that the public needs the government and private sector to save them, suggest that cybercrime is *not* normal crime. This, of course, is contested within the literature (Yar, 2005), but most criminologists and criminal justice academics would agree that not all cybercrime should be subject to a broader security agenda.

While this study generally supports the contention that presidents rely on mythic narratives using the grammar of securitization when it comes to issues related to cybercrime, there are some limitations. First, while presidents spoke frequently about cybercrime, most of the time it was couched in terms of other topical elements within speeches on issues such as national security, terrorism, or technocrime more generally. In some respects, this supports the above analysis, but it also poses a limitation because the number of full speeches about *only* cybercrime were relatively few. Additionally, given the fact that cybercrime is such a new topic and that only three presidents have spoken about it at any length, the study is inherently limited in terms of its scope. It also suggests that there is more to do to see if other political leaders engage in the use of mythic narratives and adhere to the grammar of securitization on the topic of cybercrime.

Overall then, presidents have good reasons to use mythic narratives when it comes to the topic of cybercrime, and seem to have done so. Through taking advantage of mythic narratives, presidents may be able to generate support for policies whose effectiveness may be questionable. Moreover, it is possible that by linking the topic of cybercrime to other salient policies, presidents can gain more definite support, and this can be done through the grammar of securitization.

While the analysis here supports the both the framework of mythic narratives and securitization, at least in regard to cybercrime, there are significant questions that remain. Because cybercrime is a relatively new topic for the executive branch, there needs to be long-term research to determine how presidents respond to cybercrime or other issues both rhetorically and in terms of policy. Additionally, presidential responses to moral panics that emerge outside of the issue of cybercrime can be examined for similar use of securitization. Finally, there is the question of other actors at the federal level. Does congress use mythic narratives to frame questions in hearings? Do these narratives have a definable impact on policy?

Additional research into this area will help to answer these questions and advance our knowledge about the role that mythic narratives play and their impacts on criminal justice policy.

REFERENCES

Altheide, D. L. (1996). *Qualitative media analysis*. Thousand Oaks, CA: Sage Publications.

Altheide, D. L. (2006). *Terrorism and the politics of fear*. Lanham, MD: Altamira Press.

Altheide, D. L. (2009). Moral panic. From sociological concept to the public discourse. *Crime, Media, Culture, 5*, 79-99. doi: 10.1177/1741659008102063

Bayly, L. (September 1, 2016). 'Clinton hacker' Guccifer sentenced to 52 months in jail. *NBC News*. Retrieved from http://www.nbcnews.com/tech/tech-news/clinton-hacker-guccifer-sentenced-52-months-jail-n641401.

Beckett, K., & Sasson, T. (2000). *The politics of injustice: Crime and punishment in America*. Thousand Oaks, CA: Pine Forge Press.

Bottici, C. (2010). Mythic narrative. In M. Bevir (Ed.), *Encyclopedia of political theory*. (pp. 915-916). Thousand Oaks, CA: Sage Publications, Inc. doi: http://dx.doi.org/10.4135/9781412958660.n296

Bowman-Grieve, L. (2015). Cyberterrorism and moral panics. A reflection on the discourse of cyberterrorism. In Jarvis, L., Macdonald, S., and Chen, T (Eds.). *Terrorism online, politics, law and technology*. (pp. 86-106). Abingdon, Oxon: Routledge.

Brace, P., & Hinckley, B. (1992). *Follow the leader: Opinion polls and the modern presidents.* New York, NY: Basic Books.

Brenner, S. (2011). Defining cybercrime. In R. D. Clifford (Ed.), *Cybercrime: The investigation, prosecution and defense of a computer related crime* (pp. 15-104). Durham, NC: Carolina Academic Press.

Cavelty, M. D. (2007). Cyber-terror – looming threat or phantom menace? The framing of the US cyber-threat debate. *Journal of Information Technology & Politics, 4*, 19-36.

Cavelty, M. D. (2008). *Cyber-security and threat politics.* New York, NY: Routledge.

Cavelty, M. D. (2013). From cyber-bombs to political fallout: Threat representations with impact in the cyber-security discourse. *International Studies Review, 15*, 105-122.

Cohen, S. (1972). *Folk devils and moral panics: The creation of the mods and rockers*. London, UK: Routledge.

Conley, R. S. (2013). Signing on and sounding off: Presidential signing statements in the Eisenhower administration, 1953–61. *Congress & the Presidency, 40*, 61-83.

Denton, R. F., Jr., & Hahn, D. F. (1986). *Presidential communication.* New York, NY: Praeger.

Eshbaugh-Soha, M., & Peake, J. S. (2004). Presidential influence over the systemic agenda. *Congress and the Presidency, 31*(2), 181-201.

Fairchild, E. S., & Webb, V. J. (1985). *The politics of crime and criminal justice*. Beverly Hills, CA: Sage Publications.

Gordon, S., & Ford, R. (2006). On the definition and classification of cybercrime. *Journal of Computer Virology, 2*, 13-20.

Griffin, T., & Miller, M. K. (2008). Child abduction, AMBER Alert and "crime control theater." *Criminal Justice Review, 33*, 159-176.

Halbert, D. (1997). Discourses of danger and the computer hacker. *The Information Society, 13*, 361-374.

Hammond, M., Miller, M. K., & Griffin, T. (2010). Safe haven laws as crime control theater. *Child Abuse and Neglect, 34*, 545-552.

Hansen, L., & Nissenbaum, H. (2009). Digital disaster, cyber security, and the Copenhagen School. *International Studies Quarterly, 53*, 1155-1175.

Hawdon, J. E. (2001). The role of presidential rhetoric in the creation of a moral panic: Reagan, Bush, and the war on drugs. *Deviant Behavior: An Interdisciplinary Journal, 22*, 419-445.

Hawdon, J., & Wood, R. (2014). Crime, fear, and legitimating ideologies: State of the Union addresses as hegemonic strategy. *Criminal Justice Review, 39*, 377-393.

Hill, J. B., & Marion N. E. (2016). Presidential rhetoric on cybercrime: Links to terrorism? *Criminal Justice Studies, 29*, 163-177.

Hill, J. B., & Marion, N. E. (2016b). Presidential rhetoric and cybercrime: Tangible and symbolic policy statements. *Criminology, Criminal Justice Law & Society, 17*, 1-17.

Kappeler, V. E., & Potter, G. W. (2004). *The mythology of crime and criminal justice* (4th Ed.). Long Grove, IL: Waveland.

Kshetri, N. (2013). Reliability, validity, comparability and practical utility of cybercrime-related data, metrics, and information. *Information, 4*, 117-123.

Leman-Langlois, S. (2013). Introduction. In S. Leman-Langlois (Ed.), *Technocrime, policing and surveillance* (pp. 1-12). New York, NY: Routledge.

Levi, M. (2009). Suite revenge? The shaping of folk devils and moral panics about white-collar crimes. *British Journal of Criminology, 49*, 48-67.

Lewis, O., & Fox, S. (2001). *Fear of online crime*. Pew Research Center. Retrieved from: http://www.pewinternet.org/2001/04/02/fear-of-online-crime/.

McLeod, J. (1999). The sociodrama of presidential politics: Rhetoric, ritual, and power in the era of teledemocracy. *American Anthropologist, 101*(2), 359-373. Retrieved from http://www.jstor.org/stable/683206

Messner, S. F., & Rosenfeld, R. (2007). *Crime and the American Dream*. Belmont, CA: Thomson Wadsworth.

Miko, A, & Miller, M. K. (2010). Mandatory influenza vaccinations: An example of health promotion theater. *Global Health Governance, 1*(6), 1-15.

Obama, B. H. (April 1, 2015). "Statement on signing an executive order blocking the property of certain persons engaging in significant malicious cyber-enabled activities," Online by Gerhard Peters and John T. Woolley, *The American Presidency Project*. Retrieved from http://www.presidency.ucsb.edu/ws/?pid=109913.

Ohm, P. (2007). The myth of the superuser: Fear, risk, and harm online. *UC Davis Law Review, 41*, 1327-1402.

Oliver, W. M. (2001). Executive orders: Symbolic politics, criminal justice policy, and the American presidency. *American Journal of Criminal Justice, 26*(1), 1-21.

Peters, G., & Woolley, J. T. (2015). *The American Presidency Project*. Retrieved from http://www.presidency.ucsb.edu/ws/index.php.

Potter, R. H., & Potter, L. A. (2001). The internet, cyberporn, and sexual exploitation of children: Media moral panics and urban myths for middle-class parents? *Sexuality and Culture, 5*(3), 31-48.

Ragsdale, L. (1984). The politics of presidential speechmaking, 1949-1980. *American Political Science Review, 78*, 971-984.

Sheptycki, J. (2013). Technocrime, criminology and Marshall McLuhan. In S. Leman-Langlois (Ed.), *Technocrime, Policing and Surveillance* (pp. 133-150). New York, NY: Routledge.

Sicafuse, L. L., & Miller M. K. (2010). Social psychological influences on the popularity of Amber Alerts. *Criminal Justice and Behavior, 37*(11), 1237-1254.

Sicafuse, L. L., & Miller M. K. (2012). The effects of information processing and message quality on attitudes toward the Amber Alert system. *Applied Psychology in Criminal Justice, 8*(2), 69-86.

Steinmetz, K. F. (2015). Craft(y)ness: An ethnographic study of hacking. *British Journal of Criminology, 55*, 125-145.

Stolz, Barbara Ann. "Congress and criminal justice policy making: The impact of interest groups and symbolic politics." *Journal of Criminal Justice* 13.4 (1985): 307-319.

Stroud, S. R. (2001). Technology and mythic narrative: *The matrix* as technological hero-quest. *Western Journal of Communication, 65*(4), 416-441.

Taylor, P. (1999). *Hackers: Crime in the digital sublime.* London, UK: Routledge.

Teten, R. L. (2003). Evolution of the modern rhetorical presidency: Presidential presentation and development of the State of the Union address. *Presidential Studies Quarterly, 33,* 333-346.

Thierer, A. (2013). Technopanics, threat inflation, and the danger of an information technology precautionary principle. *Minnesota Journal of Law, Science & Technology*, *14*, 309-440.

Wall, D. S. (2008). Cybercrime, media and insecurity: The shaping of public perceptions of cybercrime. *International Review of Law Computers and Technology*, *22*, 45-63.

Wall, D. S. (2011). Cybercrime and the culture of fear: Social science fiction(s) and the production of knowledge about cybercrime. *Information, Communication & Society, 11*, 861-884.

Yar, M. (2005). The novelty of 'cybercrime': An assessment in light of routine activity theory. *European Journal of Criminology*, *2*, 407-427.

Yar, M. (2013). *Cybercrime and society* (2nd Ed.) [Kindle DX Version]. Retrieved from amazon.com.

Young, J. (2007). *The vertigo of late modernity*. Thousand Oaks, CA: Sage.

Joshua Hill is an Assistant Professor of Criminal Justice at The University of Southern Mississippi. His research areas include the politics of crime as well as terrorism and homeland security.

Nancy Marion is a Professor and Chair of the Criminal Justice Studies Program at the University of Akron. Her research revolves around the politics of criminal justice.

COPING WITH CYBERCRIME VICTIMIZATION: AN EXPLORATORY STUDY INTO IMPACT AND CHANGE

Jurjen Jansen
NHL Stenden University of Applied Sciences[1]

Rutger Leukfeldt
The Hague University of Applied Sciences
Netherlands Institute for the Study of Crime
and Law Enforcement

Abstract

An increasing number of Internet users are dealing with cybercrime victimization. In order to find out whether victims adequately recover from cybercrime incidents, it is important to gain insight into its effects and impact on users. However, as it stands now, there is not much literature on the impact of cybercrime. We address this gap by qualitatively examining the impact of two types of cybercrime, namely phishing and malware attacks targeting online banking customers. We used the coping approach as a framework to study how victims deal with the negative events they have experienced. In order to study the impact of cybercrime and how victims cope with it, 30 cybercrime victims were interviewed. We observed that, next to financial damage, victims described different forms of psychological and emotional effects. Victims also reported various kinds of secondary impacts, such as time loss and not being treated properly when handling the incident. In addition, the interview data provided insight into cognitive and behavioral change, which potentially offers opportunities for cybercrime prevention. Our study demonstrates that the level of impact varies among cybercrime victims, ranging from little or no impact to severe impact. In addition, while some victims were only affected for a few days, some were still feeling the effects. The effects and impact of these fraudulent schemes on victims should therefore not be underestimated. We conclude that the coping approach provides a useful framework to study the effects and impact of cybercrime victimization and how victims recover from it. The results of our study provide a steppingstone for future studies on this topic.

Keywords: Cybercrime, financial impact, psychological and emotional impact, secondary impact, cognitive and behavioral change, coping theory

INTRODUCTION

The advances of technology provide opportunities for individuals, such as business and leisure activities, but they also offer opportunities for criminals to commit crime (Bossler & Holt, 2009; van Wilsem, 2011). In 2015, 5% of Dutch citizens aged 15 and over were victims of hacking, 4% of marketplace fraud, and 1% of identity fraud (Statistics Netherlands

[1] Corresponding author details: NHL Stenden University of Applied Sciences, Rengerslaan 10, P.O. Box 1080, 8900 CB Leeuwarden, the Netherlands. Telephone: +31 6 2830 3830. Fax: +31 5 8251 1950. E-mail: j.jansen@nhl.nl.

[CBS], 2016). Furthermore, the Crime Survey for England and Wales reported 3.6 million fraud incidents in the year prior to the study (Office for National Statistics [ONS], 2016). Of these, 1.9 million were cyber related. Additionally, about 2 million computer misuse incidents were reported, including malware and unauthorized access to personal information. Cybercrime therefore poses serious risks to society. Besides financial damages, the effects of cybercrime may lead to reputational damage and loss of goodwill and trust.

Because a substantial number of people have to deal with these types of crime, it is important to gain insight into their effects and impact on victims. However, victim perspectives on cybercrime are an underexposed topic in the literature. In addition, we need to understand whether victims adequately recover from, or effectively cope with, cybercrime incidents. Green, Choi, and Kane (2010) stressed that a better understanding of factors related to adaption after a crime event is crucial, primarily for victims' well-being. We contribute to this understanding for a particular type of cybercrime, namely online banking fraud.

This paper examines online banking fraud victimization and how victims recover from it. More specifically, we study the effects – financial, psychological, emotional and secondary victimization – and impact of phishing and malware attacks on online banking customers, two common fraudulent schemes affecting online banking in the Netherlands (Jansen & Leukfeldt, 2016). Phishing is the process that uses deception, i.e., impersonation, to retrieve personal information (Lastdrager, 2014). Phishing often starts with a deceptive e-mail, but fake websites and fraudulent phone calls are also used to intercept user credentials. Malware is defined as malicious software designed to infect a device, including viruses, worms, Trojan horses, and spyware. In this case, the malware targets online banking. Although malware can be considered a type of technical engineering, in some cases human action is necessary for such an attack to succeed; for example, by opening an infected attachment in an e-mail.

Research that considers online and offline fraud and the psychological impact on its victims is scarce (Button, Nicholls, Kerr, & Owen, 2014b; Schoepfer & Piquero, 2009; Whitty & Buchanan, 2016). When online fraud is studied, the focus is often on prevalence, financial impact, and victim characteristics (Kunst & van Dijk, 2009). Moreover, there is little research available that involves speaking with online fraud victims about their experiences (Cross, Richards, & Smith, 2016).

Button, Lewis, and Tapley (2014a) argued that the public perception of (online) fraud is often that of a victimless or low-impact crime. For example, the public may believe online fraud is instigated by credit card fraud in which victims tend to be financially compensated for their losses, or committed against larger companies who have adequate resources to compensate for the damages. However, they exposed this as a myth by showing that some of the fraud victims that they interviewed and surveyed reported devastating impacts. The fraud scams that they investigated included identity fraud, boiler room fraud, investment fraud, and lottery fraud. We contribute to literature by studying the consequences of, and recovery from, online banking fraud victimization.

We believe that insight into cognitive and behavioral coping responses that fraud victims use might present opportunities for online fraud prevention. Extensive research on these aspects is currently lacking in the cybercrime domain. We take a critical (victimology) angle to broaden the scope of analysis to include a consideration of harm rather than crime, and social justice rather than criminal justice (McLaughlin & Muncie, 2005). Whereas criminal law is about doing justice, victims are interested in coping with injustice or the harm that is done to them.

The remainder of this paper is structured as follows. In Section 2, the theoretical background is outlined. We describe what is known in the literature about the effects and impact of crime and coping strategies related to victimization. Section 3 covers the methodology adopted in the current study and the results are presented in Section 4. The limitations and discussion are the central themes of Section 5, and the concluding remarks are addressed in Section 6. In sum, our study tries to answer the following research questions:

RQ1: What are the financial, psychological and emotional effects of online banking fraud victimization?

RQ2: What are the secondary victimization effects of online banking fraud victimization?

RQ3: What impact does online banking fraud have on its victims?

RQ4: What are the cognitive and behavioral coping responses to online banking fraud victimization?

BACKGROUND LITERATURE

The background literature provides theoretical insight into the effects and impact of crimes and coping strategies to deal with the effects and impact of crimes. This information will be used to reflect on our findings. Because the topic of interest belongs to a small field of work, the literature review was broadened to more general crime and victimization studies.

Effects and impact of victimization

Dignan (2005) described victimization as a highly complex process as it is made up of at least three different elements, two of which are discussed at the end of this section. The first element that he described is the interaction between the victim and the offender and the effects from that interaction or from the offense itself. Crime in general can have several possible effects on victims. The effects can be divided into the following categories: physical, financial (both direct and indirect), psychological and emotional (both short-term and long-term), and social relationships (Dignan, 2005; Lamet & Wittebrood, 2009; Shapland & Hall, 2007), and are also applicable to online fraud victimization (Button et al., 2014a; Cross et al., 2016). Furthermore, the effects can be felt by the social environment of the victim (indirect victimization), such as family, friends, and colleagues (Shapland & Hall, 2007).

A wide range of possible effects of crime victimization – both online and offline – are reported in the literature. Such effects include distress, irritation, anxiety, concentration problems, sleeping trouble, lowered self-esteem, posttraumatic stress disorder, and losing trust in online commerce (Cross et al., 2016; DeValve, 2005; Kirlappos & Sasse, 2012; Sharp, Shreve-Neiger, Fremouw, Kane, & Hutton, 2003). Additionally, victims lose the perception that they are invulnerable to victimization (Frieze, Hymer, & Greenberg, 1987). However, it is difficult to accurately describe the precise effects of certain types of crime as they can be similar to one another (Shapland & Hall, 2007). For example, Schoepfer and Piquero (2009) pointed out that victims of fraud – which can be considered as a type of non-violent financial crime – experience similar effects to those felt by victims of violent street crimes. Thus, fraud crimes may also have serious consequences for victims.

Dignan (2005) made an important distinction between effects and impact. According to him, impact relates to the perceived intensity of the effects plus their duration from a victim's (subjective) viewpoint. The precise effects and impact of victimization may differ from crime to crime, but can also differ for the same crimes, prompted by individual characteristics, including age, gender, and income (Button, et al., 2014a; Gale & Coupe, 2005; Lamet & Wittebrood, 2009). Women, for example, often experience more or more severe psychological consequences than men, at least for offline financial crimes (Gale & Coupe, 2005; Lamet & Wittebrood, 2009). Shapland and Hall (2007) also mentioned that domestic circumstances and certain life events can have an influence on how the effects of victimization are perceived. They concluded that it is "extremely difficult to predict which individual victim will suffer which effects to what extent" (p. 179).

Green et al. (2010) argued that victims make adjustments to the effects of crime on a continuous basis. Frieze et al. (1987) distinguished between immediate, short-term, and long-term reactions. According to them, the first stage lasts from hours to days and reactions typically include numbness, disorientation, denial, disbelief, and helplessness. The second stage lasts from three to eight months, and includes fluctuations in feelings such as from fear to anger, from sadness to elation, and from self-pity to guilt. In the last stage, the victims resolve the trauma they have experienced by adopting successful coping strategies. However, Frieze et al. (1987) also argued that long-term effects can be problematic for the victim's well-being, leading to depression, fear, guilt, low self-esteem, and relationship difficulties for instance, which has also been demonstrated in more recent studies (Denkers & Winkel, 1998; Hanslmaier, 2013). For instance, a study on white-collar crime victims by Shover, Fox, and Mills (1994) reported that victims suffered from psychological and financial harm even years after the incident. For online fraud victimization, anecdotal evidence is provided by Cross et al.'s (2016) study that reported long-term emotional effects of some of the victims they interviewed.

The second and third elements Dignan (2005) identified were victims' reactions to the offense and interactions of victims with other parties as a consequence of the offense. The former relates to changes in self-perception, attitudes, and behavioral responses (these changes are examined in greater detail in the next section). Within the current context, the latter deals with organizations such as banks and criminal justice agencies. Any negative impacts resulting from these interactions can be labeled as secondary victimization. These include not being treated properly when reporting the incident, inappropriate disclosure of status information, careless handling of sensitive information, and poor functioning of criminal justice (Kunst & van Dijk, 2009). Secondary victimization is important to consider as it can worsen the harm felt by victims (Cross et al., 2016), and hinder the victims' recovery from crime (Wemmers, 2013).

Coping with victimization

After an individual has been victimized and experienced some of the effects as explained in the previous section, he or she has to invest effort to overcome the situation. For this study, we use the coping approach as a framework to describe these efforts. Lazarus and Folkman (1984, p. 141) defined coping as "constantly changing cognitive and behavioral efforts to manage specific external and/or internal demands that are appraised as taxing or exceeding the resources of the person." In other words, coping is a dynamic process of dealing with situations in which an individual is confronted with fear, stress, or threat. In the current context, we define coping as cognitive and behavioral responses against online

banking fraud and its impact, resulting in psychosocial adaptation to the stressful event. How stressful an event is depends on an individual's cognitive appraisal.

The coping process starts after two appraisal processes, which Lazarus and Folkman, (1984) referred to as primary appraisal and secondary appraisal. In short, appraisal processes comprise evaluations of the significance of what is happening in relation to one's well-being. These evaluations are affected by personal and situational factors and are often subjective in nature because individuals do not always have access to full information. Basic outcomes that are affected by appraisal and coping processes are functioning in work and social life, morale or life satisfaction, and somatic health (Lazarus & Folkman, 1984).

In the primary appraisal process, an individual evaluates why and to what extent the person-environment relationship is stressful (i.e., harm/loss, threat, and challenge). Note that a situation is not always evaluated as stressful; it can also be evaluated as irrelevant or benign-positive, respectively having no effect on or enhancing a person's psychological well-being (Lazarus & Folkman, 1984). When the situation is perceived stressful, an individual evaluates the options of how to deal with it in the secondary appraisal process. This is quite a complex process in which individuals not only need to consider coping responses, but also the efficacy of the coping response, one's self-efficacy related to performing the coping response, and the possible costs of the response (Lazarus & Folkman, 1984; Maddux & Rogers, 1983).

As our study deals with victims who are already confronted with a stressful situation, we are mainly interested in the coping process. Note that coping can take place before (threat anticipation), during, and after events (Beaudry & Pinsonneault, 2005). Frieze et al. (1987) divided coping strategies into cognitive and behavioral coping strategies. Another division that is made when dealing with stressful appraisal is problem-focused coping and emotion-focused coping (Lazarus & Folkman, 1984).

Problem-focused coping aims to solve an undesirable situation by tackling the direct cause of a problem or threat. Lai, Li, and Hsieh (2012) identify two types of problem-focused coping in the information systems context: technological and conventional coping. An example of the former is installing or updating anti-virus software to protect a device against future malware attacks. The latter deals with the behavior that an individual displays without using technology; for example, checking the account balance for inconsistencies. Lazarus and Folkman (1984) defined these as strategies directed at the environment and strategies directed at the self.

Emotion-focused coping aims to change undesirable feelings and emotions towards a problem or threat, such as stress, anger, fear, sadness, and helplessness without taking actions against the actual cause. Examples of emotion-focused coping include cognitive strategies such as avoidance, distancing, and selective attention, and behavioral strategies such as meditating, seeking emotional support, and having a drink (Lazarus & Folkman, 1984). Emotion-focused coping does not change the objective reality, but helps individuals to manage their emotions or control their emotional distress (Green et al., 2010), which is also important for effective coping (Lazarus & Folkman, 1984). However, such strategies can lead to a false perception of reality (Liang & Xue, 2009).

Emotion-focused coping is likely when an individual comes to the conclusion that nothing can be done about a situation, whereas problem-focused coping is more likely to be adopted when a situation is perceived to be changeable or controllable (Lazarus & Folkman, 1984). Liang and Xue (2009) stated that rational individuals are likely to use problem-focused

coping as a strategy because they probably have the required knowledge and the necessary skills to do so. However, if individuals do not find a solution to mitigate a threat or if they adopt an ineffective measure (e.g., anti-virus software that cannot detect new variants of malware), then they will have to use an emotion-focused strategy in order to maintain adequate levels of psychological well-being. Furthermore, these strategies are not opposites per se; they may also complement each other. For example, installing anti-virus software is a problem-focused strategy to mitigate malware attacks, but an emotion-focused strategy is applied as well, i.e., hoping that one will not contract a malware infection (Liang & Xue, 2009). Moreover, problem-focused and emotion-focused coping influence each other, which can be either facilitating or impeding (Lazarus & Folkman, 1984). Thus, although the problem-focused strategy appears to be the preferred one – since taking actions against a threat or harm seems more meaningful than changing relational meanings (Liang & Xue, 2009) – emotion-focused strategies are also very relevant for effective coping.

The extent to which a victim is able to regulate emotions can result in the victim denying, nullifying, or coping with victimization (Frieze et al., 1987). For coping to be effective, it is important that individuals (in time) move beyond seeing themselves as a victim. The extent to which victims perceive themselves as victims depends on whether the situation is cognitively evaluated as a harmful stressor or not. According to Matthieu and Ivanoff (2006), a stressful event becomes a stressor when it is perceived to have a negative impact on one's personal well-being. Thus, regardless of what is objectively defined as victimization, "victims" may not subjectively perceive themselves that way. Indeed, what some may consider stressful may not apply to others. This is primarily down to one's personal characteristics – some are more sensitive or vulnerable than others towards certain events – and the nature of the event (Lazarus & Folkman, 1984).

It is also important that victimization is recognized by others. However, this is not always obvious, because the offense itself might be evaluated as a victimless crime (Button et al., 2014a). Additionally, victimization might not be recognized because of the perceptions people hold about what constitutes being a victim. The "ideal victim," based on Nils Christie's definition, is likely to be female, sick, very young, very old, or disabled (or a combination of these attributes) (Dignan, 2005). When these attributes are not met, then the victim status will be less likely assigned, resulting in victims being given less recognition and/or being taken less seriously. In other words, the more innocent victims are perceived to be, the more likely it is for others to see them as victims. Similarly, if victims deviate from this image, i.e., when perceived to be not "ideal", this will be less likely.

Additionally, the circumstances play an important part in making an ideal victim according to Christie's typology. When victimization is perceived unavoidable, people are more easily assigned the victim status. This is also the case when it is believed that victims engaged in practices they thought were legitimate and, therefore, can be considered blameless for what had happened. An unknown attacker who is unambiguously evil is also of significance. Finally, victim status is more easily assigned when victims display the right combination of power, influence, and empathy (Dignan, 2005). The question is to what extent people believe online banking fraud victims to be truly innocent, as the victims – at least for phishing – adhered to what perpetrators demanded from them. However, the extent to which victims perceive themselves to be "victim" and their perceptions on how others viewed them is beyond the scope of the current study.

Coping efforts not only involve cognitive adjustments, but also taking action. Behavioral actions include locating the perpetrator (and demanding the stolen goods or

compensation for what was lost, but also retaliation for what was done), target hardening (e.g., self-defense lessons, being more cautious, installing alarm systems), avoiding social contacts (e.g., not leaving the home, moving to a new house, changing telephone number), seeking help from others (e.g., medical assistance, emotional support, assistance with physical tasks), and seeking help from the criminal justice system (Frieze et al., 1987).

Button et al. (2014a) reported changes in victims' behavior in a study of fraud. These included being more cautious when taking financial decisions, credit card usage and Internet purchases, and being less trusting of others. It also led to positive changes towards the threat because victims became more security aware and attentive to fraud prevention. Regarding behavioral coping, two effective strategies found in a study on identity theft by Sharp et al. (2003) were taking actions to resolve the issue and talking to family and friends. The latter was found to be an effective means of coping for victims of other types of offline crime as well (DeValve, 2005; Frieze et al., 1987; Lamet & Wittebrood, 2009). Frieze et al. (1987) argued that social support is effective in protecting victims from different pathological states, making it a vital aspect of successful coping. The extent to which online banking fraud victims use this and other coping strategies – as well as the effects and impact they have experienced – are inventoried by means of interviews, which are presented next.

METHOD

Semi-structured interviews were chosen as the research method to study the effects and impact of, and coping responses to, online banking fraud victimization. A topic list was developed based on a literature review. Although we tackled all of the topics in the interviews, the structure was modified in each interview to best fit the experience of the participant. The interviews were conducted face-to-face at a location decided by the interview participant. This was either at their home or at their working location.

Our aim was to identify the effects and impact of online banking fraud incidents and coping responses after the incident. The questions were newly developed for this study and included: What is your experience with online banking? What effects did the incident have on you? Did the incident result in emotional harm? Do you recall the amount that was stolen? Did your bank reimburse the financial damage? Have you taken new or additional precautionary measures since the incident? Furthermore, demographic characteristics of the participants were registered. During the interviews, participants were also asked about how the incident had unfolded, possible reasons for being targeted, and what protective measures they had in place. Outcomes of these particular questions are described in the work of Jansen and Leukfeldt (2016). The interviews lasted 52 minutes on average and were recorded using a digital voice recorder.

The participants were selected based on police reports and were contacted by a liaison officer working for the Dutch police to inform them about the study and to obtain their consent for voluntary participation in an anonymized interview. Of the 65 police reports selected from the Northern and Southern regions of the Netherlands, 29 participants agreed to be interviewed, nine declined the request, and 11 were not reached. Possible participants in the remaining 16 cases were not contacted because we obtained sufficient data to complete our study. One participant was recruited via a liaison officer at the Fraud Helpdesk, bringing the total number of participants to 30. The Fraud Helpdesk is a national organization for answering questions and collecting reports about fraud. The participants were interviewed between October 2014 and April 2015. The participants that were recruited based on police files were victimized in the year prior to the interview. The participant that was recruited via

the Fraud Helpdesk was victimized three years prior to the interview. In this study, participants were defined as victims when they actively or passively gave away their user credentials because of phishing or malware attacks. In addition, the reports were not made available to the researchers by these organizations, making it impossible to triangulate the data.

The ages of participants ranged from 23 to 89 years (M = 59, SD = 17). Thirteen women and 17 men were interviewed for this study. The distribution of their educational level – based on the grouping of Statistics Netherlands – was low (n = 3), medium (n = 15) and high (n = 12). The majority of participants were experienced users of online banking having used it for five years or more (n = 23) and using it at least once a week (n = 21). Their bank accounts were held at different banks in the Netherlands. In total, 17 phishing victims and 13 malware victims were interviewed – the cybercrimes of interest in this study.

The victim sample included private as well as corporate customers. For phishing, the distribution was 16 to 1. For malware, the distribution was 1 to 12. The corporate customers were primarily self-employed entrepreneurs and small and medium-sized enterprises. Two of the malware participants were not the actual victims. Instead, we spoke with the partner of a victim and a supervisor of an employee who was victimized. We decided to include their input in the analysis because their stories contained relevant information, such as the financial impact and changes due to the incident.

After the interviews were conducted, the recordings were transcribed and sorted into conceptual themes that we defined prior to the study. These were based on the research and interview questions, derived from general theoretical concepts, and include, for example, effects and impact. The interview data were analyzed using QualiCoder (Version 0.5), a type of computer-assisted qualitative data analysis software. Using this tool, we labeled the written information with analytical codes, which gave us the opportunity to separate the themes into more detailed categories (Ritchie, Lewis, McNaughton-Nicholls, & Ormston, 2014), such as psychological and emotional effects. Thereafter, the content within these categories was gradually specified into codes, including, feeling awful, stupid, and disbelief. Finally, the output was manually recorded in a Microsoft Excel file (which can be requested from the authors). A short summary of the interviews is provided in Table 1 of the Appendix.

RESULTS

In the following sections, we present damage amounts (rounded up to hundreds of euros) and incidence of particular views or experiences of participants. We do not claim that we are providing a representative reflection of online banking fraud incidents. That is not possible using this interview method nor was it the objective of our study. Rather, the study aims to provide insight into how coping phenomena vary among participants. Where possible, we make a distinction between the phishing and malware cases. Differences between phishing and malware are mentioned only when certain outcomes were reported for either one of the two fraudulent schemes. If only one participant mentioned a certain outcome, the response is not quantified, i.e., no “n” is indicated. Before we continue with the results, we provide a summary of a phishing and a malware case, because these give a good impression of what the interview participants have experienced.

Phishing attack – A participant received a deceptive e-mail containing a message to execute a security update for online banking. She clicked on the hyperlink that was included in the e-mail, which redirected her to a false website where she entered some personal details.

About two weeks later, she received a fraudulent phone call. During the telephone conversation, she followed the instructions of the caller and passed on user credentials by which the fraudster used to log in and make illegitimate bank transfers.

Malware attack – A participant noticed at some point that the online banking screen "shook" briefly when being used (interview 30). At a later date, the participant wanted to transfer money to the Dutch Tax and Customs Administration. However, in the background, the transfer was split into two transfers (adding up to the same amount), of which the largest amount was sent to an unknown account and a smaller amount to the administration service. During the execution of that particular money transfer, the participant noticed nothing out of the ordinary. The split-up money transfer was not visible in the payment summary screen when using the compromised device. Based on an investigation carried out by the Dutch police, we know that the malware was automatically installed on that particular device when visiting an infected website (Leukfeldt, Kleemans, & Stol, 2016).

Financial impact

Fifteen out of 17 phishing victims reported that the incident caused financial damage. The total damage that these 15 reported was 181,300 euros (M = 12,100; Min. = 900; Max. = 50,000). Seven of them were fully reimbursed by their bank. Three were fully reimbursed less a mandatory own risk excess of 150 euros, which one of the participants called a "fine" (interview 18). One participant received 1,000 euros from her bank, which was less than a third of the total damage of 3,600 euros. Four participants received no financial compensation, leaving a total damage of 58,700 euros. Two of the 17 participants reported no financial damage, as their banks were able to immediately stop the fraudulent transfer. The amounts that the fraudsters were attempting to steal were 2,000 and "over 10,000" euros.

We asked the participants who were not fully reimbursed about their opinion of this. The participant (interview 6) who got back 1,000 of 3,600 euros mentioned that, according to her emotional response, this amount was not proportionate. However, she thought that it may have been the maximum amount that could be refunded. In addition, she found the whole experience "a terrifying adventure," and so she made no further attempts to reclaim more money. "I was restless, frightened, tense. Maybe I should have stood up for myself?" Rationally, however, the participant stated that she understood why she was not fully compensated. "Not intentionally, but unintentionally, I was as stupid or as trusting as one could be." Because of the incident she had to cut her spending by not going on holiday for instance.

The participants who were not compensated at all expressed different views. Three of them respected the fact that they did not receive any compensation, stating that it was their own fault. One of them mentioned, "I did it to myself. So be it. I cannot turn things back. It is just silly, silly, silly" (interview 12). The second participant said, "It is the same as when you drive though a red traffic light. Then you get fined; it is your own fault. And that is also true in this case" (interview 13). She tried to minimize the impact by stating that, "It could have been more [money]." The third participant stated that he understood that he made the error, although he thought that the bank could have done more to trace the suspects.

The fourth participant (interview 15) who received no compensation was "very sorry" that she was not compensated, especially since "banks are so big." She felt that, because of the compulsory nature of online banking – "in particular for elderly people" – the bank could have shown more goodwill, also given the many years that she had been a customer of that

particular bank. However, her rationale was that the bank could not compensate her "because there are perhaps too many [phishing] cases." She also mentioned to have lost her security, i.e., having a monetary buffer, which affected her significantly. When talking about it with her husband, the impact was minimized for her because he made clear to her that they were still able to eat.

Twelve of the 13 malware victims reported that the incident caused financial damage. One participant did not mention the amount that was stolen. The other 11 participants reported a total damage of 52,800 euros (M = 4,800; Min. = 1,000; Max. = 10,000). All 12 participants were fully reimbursed by their bank. However, one participant claimed to have lost out on interest during the time that his money was not in his bank account. In one of the 13 cases, there was no financial damage because the bank was able to block the fraudulent transfer immediately. The participant explained that the amount that the fraudsters were attempting to steal was about a monthly wage.

Psychological and emotional impact

Most participants reported that the event had at least some psychological and/or emotional impact on them. However, four participants expressed no psychological or emotional impact. The supervisor of a malware victim stated, "It is all in the game. It is part of life, running those risks. […] And, besides, it is only money. If physical violence was involved, then it would have real impact" (interview 28). Three of these four participants indicated that they would probably have assessed the impact differently if they had not been compensated by their bank.

Eleven participants reported that the incident did have an impact, but that it was low. A malware victim mentioned that, "It is an administrative thing" (interview 21). Although he still felt "screwed," he did not worry about it, because he knew that the money would be back within a week. Another malware victim said, "You have a strange feeling, but nothing more. The intangible makes it difficult. With burglary, you see that things are broken and ransacked" (interview 23). Three phishing victims said that, although they did not experience any psychological or emotional impact or only to a small degree, they were annoyed by it.

Some participants compared online banking fraud with burglary (n = 2), while others believed that a comparison with burglary is not possible (n = 5). On the one hand, a phishing victim stated, "Strange people just enter your private life, and that is the most disgusting part of it. It does not matter if it is on your computer with money, or that people steal your belongings or are only sniffing around and turn things upside down. It just gets to you" (interview 2). On the other hand, the spouse of a malware victim indicated, "Hacking into your computer is a totally different experience. Burglary at home is a violation of your privacy. In this case, it is a technical thing" (interview 25).

Participants who experienced psychological and/or emotional effects said that, in general, they felt awful (n = 8), disbelief (n = 8), fear or shocked (n = 6), stressed or nervous (n = 6), cheated (n = 4), and insecure (n = 3). It also lowered their trust in banks and/or online banking (n = 8). Being misunderstood was an effect mentioned only by malware victims (n = 2). Effects that only phishing victims stated included feeling stupid (n = 8), shame or embarrassment (n = 5), angry (n = 2), devastated (n = 2), sadness, and feelings that things are deprived. Phishing victims also stated that the incident lowered their levels of trust in themselves (n = 3) and in people in general (n = 2). A participant pointed out that, "If you lose your trust, you lose more than your trust, you lose your certainties. […] I trust all people to be

honest and open. That trust has been given a big blow. When I say that I could cry again, since I find it that terrible. I still suffer from it" (interview 12).

Furthermore, phishing victims mentioned that the incident made them feel less safe online (n = 4) and offline. The participant who claimed feeling unsafe both online and offline said that these feelings were linked to a previous life event in which she was cheated. "Those feelings came back through this phishing incident. It really knocked me off balance. It certainly took a month. I was just really scared" (interview 6). She reported that the incident also affected her sense of safety in her home. She asked herself whether the criminals who had scammed her might have obtained her physical address. She indicated having had sleepless nights, wondering whether people would sneak into her home. "You don't know how far it may reach."

Other phishing victims also mentioned having suffered from physical effects. One participant (interview 17) spoke about having "a trauma" and indicated also having suffered from sleepless nights. "This was less about the money aspect, but more about the stupidity." The participant blamed himself that he fell for the scam. "You lose your self-confidence, because you can be so stupid." Contrary to this statement, four participants stated that the incident was something that befell them. A malware victim indicated that, "You must make sure that you don't blame yourself. You don't have control over it" (interview 30).

One of the phishing victims indicated that, "Its aftereffects are very bad. It has had a lot of impact and still makes me feel very sick" (interview 12). One aftereffect that she mentioned was that she experiences black outs from time to time. Another phishing victim claimed that she almost collapsed when the incident happened. She claimed having had heart palpitations when the bank e-mailed her with the message that she would not be compensated for her financial losses. She felt terrible and could not believe it. During the process of getting her money back, she became very insecure. "When I was using online banking for the first time after the incident, I was shaking all over" (interview 1). She reported being very anxious, mostly because she no longer felt in control. Furthermore, it influenced the work she was doing for a foundation. At the time of the interview, she was the treasurer of that particular foundation, but because of the incident she found it terrifying and wanted to resign from that role. "The idea that this [a successful phishing attack] would happen to me with other people's money makes me feel sick." Finally, a malware victim indicated that he was shivery using online banking after the incident, but that this feeling was subsiding as time passed.

The duration or timeframe of the effects was also mentioned in some of the other interviews. In total, four phishing victims stated that the effects were still (partly) present. For example, participants indicated that, although the incident had happened a while ago, feelings of uncertainty or distrust, especially with regard to digital payments, still existed. One participant claimed that she was trying to get over it, which she was confident about, as "time heals all wounds" (interview 6).

Seven participants reported that the impact goes away or at least goes into the background. A phishing victim reported that the impact lasted for two or three days. When things were back in order, she turned the page. Another phishing victim reported that feelings of shame and stupidity had subsided over time, but that it was not one of his favorite topics of conversation. "I don't talk about this topic at parties. It was quite an impactful experience" (interview 3). Two others also indicated not sharing the experience. However, some did (occasionally) talk about the incident within their social sphere (n = 13). Most did this for coping purposes, but five of them also did so to warn people about such schemes. In two out

of 13 cases, participants mentioned that the people they told about their experience tried to help them to get their money back and to locate the people responsible for the scam. Another participant indicated that the positive aspect was that her fellow residents from the elderly home and her family supported her really well, which helped her to cope with the incident.

Secondary impact

Some of the participants reported that the negative event also had secondary impact. This was often related to the handling of the incident. Obvious secondary effects were time loss due to reporting the incident to both the bank and the police, a blocked bank account and, consequently, not being able to having direct access to their own money. A malware victim indicated that the time between the incident and reimbursement of the bank was bothersome. “As a self-employed entrepreneur, you don’t feel like spending hours on phone calls with your bank during the day” (interview 9). One phishing victim explained, “Especially as you get older, you don’t want to be bothered by such things” (interview 4). Although this section mainly deals with negative experiences, nine participants explicitly indicated adequate levels of expertise among staff at the bank and/or the police, and mentioned that they took it seriously and were understanding and helpful. One of them argued that this attitude was very reassuring.

Other types of secondary impacts that were mentioned by participants from both fraudulent schemes included feeling mistreated (n = 6), bad communication (n = 4), and an uncooperative attitude (n = 3) on the part of banks. A phishing victim felt mistreated by her bank when reporting the incident. She got the impression that the bank employee sitting across her was thinking, “‘Oh, you are so stupid.’ He made that very clear” (interview 1). Participants also felt that they were being treated like the guilty one, or felt as though they needed to prove their innocence.

All of the participants went to the police to file a report. In 19 cases, participants were obliged or advised to do so by their bank. Eight reported having done so on their own initiative. Of the remaining three cases, we do not know what motivated them. Secondary impact related to the police were reported as follows: The police initially did not want to (or did not have time to) file the report (n = 5), have to wait for a few days until it was possible to file a report (n = 3), have to drive far to a police station, and a lack of expertise that was displayed by the particular police officer. The participant of the latter case – a malware victim – stated, “The person who filed the report did not understand any of it. You cannot blame that person for not knowing everything, but the police can significantly improve in this regard” (interview 21).

Two phishing victims mentioned that they received many payment reminders during the time their bank account was blocked, which they found annoying. Two malware victims claimed having to settle things because of the fraudulent transfer. One of them needed to settle things with the Dutch Tax and Customs Administration, because the participant’s business received a formal warning. She had to rectify things by reporting that the late payment was unintentional, that it was due to a fraudulent attack. The other participant needed to settle things similarly with a do-it-yourself store.

Finally, five participants indicated that either the police or their bank updated them about the incident. In two instances, updates included a standard message that there were not enough leads to continue working on the case. In one instance, a malware victim mentioned being updated on the case by a police detective. This had a positive effect on the level of trust

that something was actually being done. Some of the participants that indicated that no updates made them feel that they were being left in the dark or gave them the impression that nothing was done about their case.

Behavioral change

We asked participants whether they had changed their behavior due to the incident in order to cope with the incident or to prevent future incidents. We have categorized behavioral change into three categories: 1) behavioral change related to devices used for online banking; 2) behavioral change related to online banking sessions; and 3) behavioral change beyond the online banking context. It is important to note that we have relied on self-reported behavioral change. We have no additional data that provides support for what the participants told us.

Behavioral change and devices. Seven participants told us that they had installed an additional anti-virus or anti-malware package, such as Malwarebytes and TDSSKiller. Four participants reported having changed their anti-virus software, of which one indicated that the device had no anti-virus software during the time of the incident. Another participant switched from a free package to a paid package, in order to prove to the bank that he is doing a good job. Three participants said that they updated their software more frequently. A phishing victim reported that her computer now updates every night and that she manually checks for updates once a week. This was not only due to the incident, she received messages from her bank stating that financial losses caused by phishing will not be reimbursed if software is out of date.

Other changes that were mentioned more than once were no longer using the device that was used during the incident (n = 2) and buying a new computer (n = 2). The latter was only reported by malware victims. One of them claimed that the police advised her to buy a new computer. This additionally led to the IT staff needing to reinstall all the (business) software. She indicated, “We have no insurance for that” (interview 30). Changes that were mentioned once included using a different web browser, switching from a Windows desktop to an Apple iPad (which was perceived to be safer), and replacing the hard drive of the compromised device with a new one.

Behavioral change and online banking. More than half of the participants indicated that they had become (extra) alert or more aware of phishing and malware attacks (n = 17). Participants also indicated that the incident was a good learning experience (n = 14). In addition, participants had changed their online banking practices. Both phishing and malware victims mentioned being more careful/meticulous or taking more time to properly check what they were doing during online banking and online purchases (n = 8), checking the account balance more regularly (n = 7), and checking the security certificate (n = 7, e.g., https, closed padlock).

Changes that were reported only by phishing victims include logging out of banking sessions instead of clicking away the window (n = 3), checking the web address (n = 2), using online banking less and traditional banking methods more when transferring money (n = 2), and not using online banking at home anymore. In this particular case, the participant visited a local bank once a month to conduct his banking activities. If he was not sure about something, he could ask a bank employee to help him.

A new online banking practice that only malware victims mentioned was taking screen shots of their online banking activities (n = 2). One of them indicated doing this, “To be able

to prove that you are doing the right thing" (interview 23). After about a year, both participants stopped doing this. Another participant explained that when she had to transfer large amounts of money, she would contact the bank by phone to find out if everything was in order. She attributed this to her insecurity that was caused by the incident. However, she soon stopped with this procedure because it was not practical.

Besides the duration of the new behaviors explained above, the timeframe of the new behavior was also mentioned in a few other cases. Three malware victims claimed that being extra alert or more careful was already waning. Two phishing victims who stated that they checked to see if there was a closed padlock revealed that they did this less frequently now or not at all during the time of the study. Finally, a phishing victim disclosed that she no longer checked the account balance regularly.

Behavioral change beyond online banking context. One frequently mentioned change in the behavior of phishing victims beyond the online banking context was that they became more suspicious about e-mails (n = 8); for example, not clicking on hyperlinks and checking whether e-mails are trustworthy. One also commented that it had become difficult to differentiate between legitimate and false e-mail messages. Other phishing victims indicated deleting all e-mails that were or seemed to be sent by banks (n = 4). Two also commented that if the message was important, the bank would have sent a letter.

Six phishing victims made changes to their bank accounts. Changes included removing the credit limit from the account (for overdraft protection), configuring the debit card so that it could not be used abroad; receiving a different bank account number from the bank (because fraudsters carried out new phishing attempts); closing a savings account (because that particular account was protected by a password only, which seemed to be unsecure); opening a savings account at another bank (since the checking and savings accounts had the same numbers, which was perceived to be unsafe); and opening several bank accounts (where specific amounts of money can be deposited, leaving only a smaller amount in the checking account). In this particular case, the participant commented, "In this way, third parties cannot get to the big money" (interview 16).

Four phishing victims said that they are more on guard when using mobile phones and receiving telephone calls. Three of them suggested that if the phone's display did not show a number, they picked up the phone without stating their name or they did not answer it at all. The other participant obtained a new phone number. Furthermore, two participants intended to leave their bank, but did not follow through.

Changes that were mentioned just once by phishing victims included not buying or signing anything anymore at the door, not writing down the PIN code in an agenda or on a piece of paper, not giving out their bank account number as readily as before, and not going on the computer when feeling sad (for this participant, safety was embedded in sadness). A participant who was phished while being the treasurer of a foundation indicated that the foundation had invested in making its website more secure.

Two malware victims commented that they had made changes beyond the online banking context. One of them indicated that business procedures and protocols were carefully reexamined in order to make sure that incidents would be adequately prevented or detected as soon as possible. Another indicated not sending information from business computers to the main business computer (used for online banking), i.e., not running any unnecessary risks.

DISCUSSION

Although we believe that our study provides a unique contribution to literature, it has its limitations. First, the results are not generalizable for all online fraud victims. We focused on victims who suffered from online banking fraud only. Furthermore, the participants were selected from police files. Therefore, we do not know what the effects are on victims who did not report the crime or how they cope with such events. Reasons for non-reporting include, for example, not knowing that they had been defrauded, feeling partly responsible, feeling embarrassed, and suffering low financial losses (Button, Lewis, & Tapley, 2009b). This limits generalizability as does low reporting rates.

For example, in 2015, 2% of all hacking cases, 20% of marketplace fraud cases, and 13% of identity fraud cases that Dutch people experienced were officially reported to the police (CBS, 2016). Perhaps in-depth interviews with respondents that follow a crime survey could be a way to address this limitation. Moreover, some potential participants declined the request to be interviewed. Perhaps these victims did not participate because they perceived higher or more problematic psychological and emotional impact than those in the sample. Another possibility is that these victims were not affected at all and therefore had no interest in participating. What becomes clear though is that victims vary in their characteristics and profiles. This concurs with previous research on fraud victimization (Button, Lewis, & Tapley, 2009a; Button et al., 2009b; Cross et al., 2016).

A possible limitation is related to the identification of psychological and emotional effects. Although we found that the participants talked openly about these and other subjects, the participants may have hidden some of these effects from the researchers because they felt too embarrassed about them. Dignan (2005) stressed that it is very difficult to measure such effects because the willingness and ability of people to talk about these issues, as well as about the experience itself, are highly subjective and partly cultural specific. This also counts for coping efforts because people are not always aware of what they are doing exactly (Lazarus & Folkman, 1984). The subjective nature of this study may therefore have led to the problem of method variance. However, Lazarus and Folkman (1984) nuanced the problems of validation by stating that subjective reports allow researchers to learn more about coping than any other single source. In order to make outcomes more comparable, regardless of their subjective nature, we recommend using other specific assessment tools in future studies; for instance, the “ways of coping” checklist (see Lazarus and Folkman [1984]). However, this would require a more quantitative research approach.

Finally, the current study adopts a retrospective approach, which has its limitations (Shapland & Hall, 2007). Participants may have forgotten certain details about the effects of online banking fraud and how they cope or coped with these. We have gained an impression of the short-term consequences, but we do not explicitly understand how victims’ coping strategies play out in the long term. For example, some participants mentioned that they were already using some behavioral coping measures less frequently. It would be interesting to find out whether individuals are consistent or variable in their coping strategies, and what their overall coping style is, as opposed to our more contextual focus on coping efforts (Lazarus & Folkman, 1984). Indeed, coping is not a one-off activity. Future studies could benefit from a longitudinal approach. Studying the effects and impact that victims perceive and their cognitive and behavioral responses at multiple points in time provide richer data with more potential. For instance, to understand how perceived effects develop and to better guide a victim through the coping process. Further research may also benefit from investigation of personal, psychological, and contextual factors that affect coping efforts.

The first research question we wanted to answer is: What are the financial, psychological and emotional effects of online banking fraud victimization? We start with the financial effects. Most participants experienced some financial damage – at least initially – from either phishing or malware victimization. Two thirds of the phishing victims and all malware victims whose bank accounts were affected were fully compensated for their financial losses. The fact that all malware victims were fully compensated probably has more to do with the type of the offense – that is the obscureness of the malware attack – than with the observation that most were corporate customers. Imaginably, the circumstances surrounding malware victimization appeal to the "ideal victim" typology.

Five participants – all phishing victims – were not or were to a minor extent compensated for their losses. Although the participants who suffered financial losses acknowledged that being victimized was to some extent due to their own wrongdoing, some expected more goodwill from their bank regarding compensation. Moreover, it would be interesting to investigate the banks' reimbursement policies on this matter: Why are some phishing victims compensated, be it in full or not, while others are not?

Besides the direct financial effects, indirect financial effects were also reported. These effects included loss of interest, buying a new device for online banking, and several types of loss of time that can be considered to have a monetary value, such as devoting more time to taking precautions (online) and going to a physical bank office to use banking services. Thus, the financial effects go further than only the (initial) damages caused by the fraudulent schemes.

We will now turn to the psychological and emotional effects. The participants that indicated that the event affected them psychologically and emotionally mentioned a range of effects, such as feeling awful, stupid, stressed, disbelief, and fear. It also affected their levels of trust, including trust in banks and/or online banking, people, and themselves. That such psychological and emotional effects follow victimization is consistent with other research on (online) fraud (Button et al., 2009a; Cross et al., 2016). Some participants even reported physical effects, such as having sleepless nights, getting heart palpitations, experiencing blackouts, and feeling shivery or shaky when using online banking.

We also found some evidence regarding the duration of the effects (Frieze et al., 1987). Most participants claimed that they had immediate reactions to the incident. The psychological and emotional effects were often at their most severe during this particular timeframe. Some of the participants indicated that the effects subsided after a few days. However, some reported that the effects or impact experienced lasted from about a month to still being present at the time of the interview. This is a similar pattern that is observed for (offline) violent crimes (Dignan, 2005), as well as for different types of online fraud (Cross et al., 2016).

The second research question was: To what extent do online banking fraud victims suffer from secondary victimization? Secondary victimization relates to negative effects other than those instigated by the incident itself. Negative effects often related to the way the incident was handled, such as time loss due to reporting the incident, not being able to access the bank account, and feeling mistreated. Feeling mistreated has a negative influence on coping because it does not address the victims' need for recognition.

In addition, most participants mentioned that they did not receive feedback from either the bank or the police on the incident and how it was being handled. Frieze et al. (1987)

argued that such information helps victims to relieve their fear and frustration, thus helping them in the coping process. In addition, victims may develop a positive attitude towards banks and the police instead of losing their trust and confidence in these organizations. The study of Button et al. (2009b) also found that fraud victims have a need for being held up-to-date on the process of the case. We believe that providing feedback, not only on the status but also on how the incident happened, can help victims to develop more effective defense strategies against future attacks.

Besides negative effects, some participants explicitly reported positive aspects in how their cases were handled. They mentioned that bank employees and police officers took them seriously, were understanding and helpful, and had adequate levels of expertise for the situation. Again, banks and the police stand to gain a lot if they respond in this way, not only reputation-wise, but also when it comes to helping victims to recover properly from online banking fraud victimization.

The third research question was: What impact does online banking fraud have on its victims? Although the financial *effects* of online banking fraud could objectively be defined as quite severe, the participants did not claim that the incident had a devastating financial *impact*, which is sometimes the case for other fraud victims (Button et al., 2014a). Therefore, we conclude that the direct financial impact of online banking fraud victims is low, most notably because the majority of victims were compensated for their losses. This differs from other types of fraud, where it is often more difficult or even unlikely to get restituted (Button et al., 2009b). Remarkably, some of the participants who were not compensated at all also felt that the impact was low. Three participants had no financial damage to begin with.

Regarding the psychological and emotional aspects, four participants said they felt no such impact. This was also mainly due to the fact that they were financially compensated for their losses, but also because online banking fraud was considered a technical or invisible phenomenon. These participants felt that their private lives had not been affected. About a third of the participants mentioned that the *impact* of the fraudulent attack was low, but did express some psychological and emotional *effects*.

Half of the respondents were – to some extent – overwhelmed by the situation. Thus, reimbursement could not prevent some of the participants from being psychologically or emotionally affected by the incident. Furthermore, we found some evidence that previous negative life events affected the impact of victimization. Our topic list, however, did not include questions about such events or prior victimization, which could be beneficial to add in future studies. Similarly, questions could be asked whether or not other accounts beyond banking were hacked, which may also have affected the impact experienced by participants.

The final research question was formulated as follows: What are the cognitive and behavioral coping responses to online banking fraud victimization? Regarding the participants who were not compensated or not fully compensated for their financial losses, we observed that they used a cognitive coping style of rationalizing it, thereby minimizing their victimization. They came up with an explanation that seemed to fit the situation in order to cope with the fact that they had lost their money.

Cognitive coping strategies were also observed regarding the psychological and emotional effects of becoming an online banking fraud victim. Examples include being at ease with the situation because reimbursement procedures were understood, and viewing an incident as being something that is part of life. Some participants tried to create a

"hypothetical, worse world" scenario in order to cope with victimization (Taylor, Wood, & Lichtman, 1983), for example, by thinking that the stolen amount could have been higher or that it would have been worse if it had involved physical violence. These strategies are effective for reducing emotional distress, but ineffective for tackling the actual problem.

Another cognitive coping response is that victims feel strengthened by the experience. Some indicated that the experience was a good lesson in that it made them wiser, which is also considered to be positive change in other studies (Button et al., 2014a; Whitty & Buchanan, 2016). Perhaps confronting online banking users with (controlled) phishing and malware attacks would be a good strategy as a way to teach them how to prevent such attacks.

A strategy that makes coping difficult was observed in a participant who blamed himself for being victimized (Whitty & Buchanan, 2016). Although self-blame can be considered a maladaptive response, which could for instance lead to hopelessness and depression, it can also be considered an adaptive response if self-blame is considered to be behavioral. If victims are able to link their own actions to victimization, they can avoid future victimization by adjusting these actions. On the other hand, if victimization is linked to character, it gives victims less confidence in their perceptions of avoiding future victimization because personality is hard to change (Frieze et al., 1987).

Some participants reported an opposite strategy towards self-blame, indicating that the incident was something that befell them, which helped them control their emotional state. In our opinion, this is not a strange – and perhaps the right – reaction, as the skills of fraudsters are often the reason why people fall for such scams. Individuals that are victimized are not stupid; they simply made a choice that was not a good one. For malware victims, it was out of their hands because their systems were infected automatically.[i] For these victims, the cases remained unsolved; they do not know how their systems were infected, nor how the fraudulent transfer(s) took place. They were surfing online in the wrong place at the wrong time. In general, this did not cause any distress, most probably because all were reimbursed – which might have strengthened their belief that they could not help it.

Respondents also applied behavioral coping mechanisms. The first behavioral coping mechanisms that they applied was reporting the incident to, and seeking support from, their bank. In addition, all participants filed a report with the police (which is logical given our selection procedure), either because the bank required them to or on their own initiative.

Some participants also sought support from their social environment, which was assessed as an effective means of coping. This is also identified in the literature as one of the most effective means for successful coping (Frieze et al., 1987). One of the participants mentioned after the interview that the conversation had a healing effect on her as she had not talked about it much. According to her, banks should provide aftercare in the form of having a conversation about the event after some time, helping victims to process it. Were banks to follow up on these incidents, it is essential that the person instigating the conversation adopts a supportive attitude, i.e., be unprejudiced, show empathy and understanding – not blame the victim, as the situation itself is difficult enough.

However, it can remain a difficult topic to address for some time. Perhaps these participants are assuming that others might find them stupid or that they would be angry with them because of the financial loss. Indeed, according to Cross (2015), there is a negative vibe surrounding online fraud victimization, although she found that phishing is a more acceptable type of fraud victimization, than, for instance, advance fee fraud and romance fraud. Whitty

and Buchanan (2016) argued that negative or non-supportive responses from the social environment can be harmful for recovery. We found no evidence that online banking fraud victimization affected social relationships, nor did we find any leads indicating indirect victimization by people within the victims' social environment. Perhaps this is the case, because the research participants were open to share these experiences with the people closest to them. Other fraud research has shown that when such events, for example, are kept secret, the impact on partners and family members can be more severe (Button et al., 2014a).

We also identified environmental strategies and strategies directed at the victims themselves. Environmental strategies included installing a different or additional anti-virus package and (more regularly) checking for software updates. A frequently mentioned strategy that was directed at the victims themselves was that participants became more alert to or aware of phishing and malware. Being more cautious after victimization is also found in the fraud studies of Button et al. (2009a; 2014a) and Cross et al. (2016). Online banking processes were also adjusted, such as being more meticulous or taking more time to check things, checking the security certificate, and checking the account balance more regularly. Furthermore, we observed that some participants adopted avoidance behavior, i.e., using (or wanting to use) online banking less and using traditional banking services more.

Some of the abovementioned strategies can be considered to be problem-focused coping as they are intended to prevent an online banking fraud incident from happening again. However, these strategies could also be adopted as a means to control emotions, for example, making them feel more confident about online banking. It is therefore difficult to determine whether certain responses belong to problem-focused and/or emotion-focused coping strategies (Lazarus & Folkman, 1984), so we have not labeled them as such. Follow-up research is required to clarify in greater detail how these strategies work.

Finally, we found that participants also performed behavioral coping strategies beyond the online banking context. One frequently mentioned example was that phishing victims reported being more concerned about or suspicious of e-mails. As a consequence, participants indicated that it was often difficult to differentiate between legitimate and false e-mail messages. This was also observed by Wang, Chen, Herath, and Rao (2009), who noted that phishing has a high impact on legitimate commercial e-mails. Other responses that phishing victims mentioned more than once included making changes or restrictions regarding bank accounts and being more on guard when taking telephone calls.

CONCLUSION

We agree with Button et al. (2014a) that, similar to other types of fraud, online banking fraud cannot be considered a *victimless* crime, not even when the stolen money is reimbursed (see also Whitty & Buchanan, 2016). The effects and impact of such fraudulent schemes on victims should not be underestimated. Regardless of the financial costs associated with online banking fraud, losing trust (e.g., in online commerce and people in general), and declining levels of safety and security are a much higher price to pay. However, the extent to which an individual perceives these effects and impact differs significantly. For some it was a temporary inconvenience only and they managed to get over it, whereas for the other it was (and sometimes still is) an overwhelming experience that changed them; they became more attentive, alert, and distrustful as a result. This means that individual differences should be acknowledged when helping victims to cope with their victimization. Hence, for help to be effective, one should take into account the interplay between personal characteristics and the environment (Lazarus & Folkman, 1984). They went on to state that effective help can only

be achieved if a process-oriented view is adopted. This would involve examining what happened and what is happening to that particular individual in terms of coping.

This conclusion has implications for banks and law enforcement agencies. Banks primarily have to deal with the incident and the damage resulting from the incident. Banks could probably improve their services by recruiting dedicated personnel who devote attention to the victims' coping process, employees who are able to assess how the victims' coping process is unfolding and who can support these victims in that process. These employees could have contact with the victim at multiple points in time depending on the specific needs of the victim. This may require a different set of skills than those that bank employees at fraud departments currently have.

Another strategy might be to cooperate with "victim support," a service that is provided to victims when they report a crime to the Dutch police. Another important implication for law enforcement agencies is that victims should be treated seriously as the impact they experience goes further than the money aspect only. It is crucial to do this right the first time victims come into contact with these agencies to report the incident because this might set the tone for the whole handling procedure. Moreover, as pointed out by Cross et al. (2016), a negative reporting experience can worsen the harm that victims already undergo. To evaluate whether this is done adequately, and to continually improve the support of victims, it is recommendable to map the customer experience in terms of fraud handling, which is already done by different banks in the Netherlands (personal communication, April 26, 2017).

Conclusively, we have contributed to the literature by increasing insight into the effects and impact of phishing and malware attacks and enhancing the understanding of adaption after online banking fraud victimization. These aspects are currently lacking in studies on cybercrime. More thorough analysis of coping strategies is required to deepen insight into the phenomena described in our study. This is not only needed to advance theoretical knowledge on this topic, but also to further shape the supporting role that banks and law enforcement agencies have, as presented in the recommendations above. We need more information about the factors that cause stress, how coping strategies are chosen, which strategies are effective and which are not, and how these function over time. Some coping efforts seem to work for awhile, but subside over time as they seem to hinder usability, cost too much time, and some perhaps do not work at all.

Acknowledgements

This study is part of the Dutch Research Program on Safety and Security of Online Banking.

This program is funded by the Dutch banking sector (represented by the Dutch Banking Association), the Police Academy, and the Dutch National Police. We would like to thank the participants for telling their stories and our liaison officers at the Dutch National Police and Fraud Helpdesk for establishing the first contact with the interview participants.

REFERENCES

Beaudry, A. & Pinsonneault, A. (2005). Understanding user responses to information technology: A coping model of user adaptation. *MIS Quarterly, 29*(3), 493–524.

Bossler, A.M. & Holt, T.J. (2009). On-line activities, guardianship, and malware infection: An examination of routine activities theory. *International Journal of Cyber Criminology, 3*(1), 400–420.

Button, M., Lewis, C. & Tapley, J. (2009a). *A better deal for fraud victims: Research into victims' needs and experiences.* London: National Fraud Authority.

Button, M., Lewis, C. & Tapley, J. (2009b). *Fraud typologies and the victims of fraud: Literature review.* London: National Fraud Authority.

Button, M., Lewis, C. & Tapley, J. (2014a). Not a victimless crime: The impact of fraud on individual victims and their families. *Security Journal*, *27*(1), 36–54.

Button, M., Nicholls, C.M., Kerr, J. & Owen, R. (2014b). Online frauds: Learning from victims why they fall for these scams. *Australian & New Zealand Journal of Criminology, 47*(3), 391–408.

CBS (2016). *Veiligheidsmonitor 2015 [Safety monitor 2015]*. The Hague: Statistics Netherlands.

Cross, C. (2015). No laughing matter: Blaming the victim of online fraud. *International Review of Victimology*, *21*(2), 187–204.

Cross, C., Richards, K. & Smith, R.G. (2016). The reporting experiences and support needs of victims of online fraud. *Trends and Issues in Crime and Criminal Justice, 518,* 1–14.

Denkers, A.J. & Winkel, F.W. (1998). Crime victims' well-being and fear in a prospective and longitudinal study. *International Review of Victimology*, *5*(2), 141–162.

DeValve, E.Q. (2005). A qualitative exploration of the effects of crime victimization for victims of personal crime. *Applied Psychology in Criminal Justice, 1*(2), 71–89.

Dignan, J. (2005). *Understanding victims and restorative justice*. Maidenhead: Open University Press.

Frieze, I.H., Hymer, S. & Greenberg, M.S. (1987). Describing the crime victim: Psychological reactions to victimization. *Professional Psychology: Research and Practice, 18*(4), 299.

Gale, J.-A. & Coupe, T. (2005). The behavioural, emotional and psychological effects of street robbery on victims. *International Review of Victimology*, *12*(1), 1–22.

Green, D.L., Choi, J.J. & Kane, M.N. (2010). Coping strategies for victims of crime: Effects of the use of emotion-focused, problem-focused, and avoidance-oriented coping. *Journal of Human Behavior in the Social Environment*, *20*(6), 732–743.

Hanslmaier, M. (2013). Crime, fear and subjective well-being: How victimization and street crime affect fear and life satisfaction. *European Journal of Criminology*, *10*(5), 515–533.

Jansen, J. & Leukfeldt, R. (2015). How people help fraudsters steal their money: An analysis of 600 online banking fraud cases. *Proceedings of the 2015 Workshop on Socio-Technical Aspects in Security and Trust*, Verona (Italy), pp. 24–31.

Jansen, J. & Leukfeldt, R. (2016). Phishing and malware attacks on online banking customers in the Netherlands: A qualitative analysis of factors leading to victimization. *International Journal of Cyber Criminology*, *10*(1), 79.

Kirlappos, I. & Sasse, M.A. (2012). Security education against phishing: A modest proposal for a major rethink. *IEEE Security & Privacy*, *2*, 24–32.

Kunst, M.J.J. & van Dijk, J.J.M. (2009). *Slachtofferschap van fraude: Een explorerend onderzoek naar de impact van diverse vormen van financieel-economische criminaliteit [Fraud victimization: An exploratory study into the impact of diverse forms of financial crime]*. International Victimology Institute Tilburg (INTERVICT).

Lai, F., Li, D. & Hsieh, C.-T. (2012). Fighting identity theft: The coping perspective. *Decision Support Systems*, *52*(2), 353–363.

Lamet, W. & Wittebrood, K. (2009). *Nooit meer dezelfde: Gevolgen van misdrijven voor slachtoffers [Never the same again: The consequences of crime for victims]*. The Hague: Sociaal Cultureel Planbureau.

Lastdrager, E.E. (2014). Achieving a consensual definition of phishing based on a systematic review of the literature. *Crime Science*, *3*(1), 1–10.

Lazarus, R.S. & Folkman, S. (1984). *Stress, appraisal, and coping*. New York: Springer Publishing Company.

Leukfeldt, E.R., Kleemans, E.R. & Stol, W.P. (2017). A typology of cybercriminal networks: From low-tech all-rounders to high-tech specialists. *Crime, Law and Social Change*, 21–37.

Liang, H. & Xue, Y. (2009). Avoidance of information technology threats: A theoretical perspective. *MIS Quarterly*, *33*(1), 71–90.

Maddux, J.E. & Rogers, R.W. (1983). Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. *Journal of Experimental Social Psychology*, *19*(5), 469–479.

Matthieu, M.M. & Ivanoff, A. (2006). Using stress, appraisal, and coping theories in clinical practice: Assessments of coping strategies after disasters. *Brief Treatment and Crisis Intervention*, *6*(4), 337.

ONS (2016). *Crime in England and Wales: Year ending Sept 2016*. London: Office for National Statistics.

Schoepfer, A. & Piquero, N.L. (2009). Studying the correlates of fraud victimization and reporting. *Journal of Criminal Justice*, *37*(2), 209–215.

Shapland, J. & Hall, M. (2007). What do we know about the effects of crime on victims? *International Review of Victimology*, *14*(2), 175–217.

Sharp, T., Shreve-Neiger, A., Fremouw, W., Kane, J. & Hutton, S. (2003). Exploring the psychological and somatic impact of identity theft. *Journal of Forensic Science*, *49*(1), 1–6.

Shover, N., Fox, G.L. & Mills, M. (1994). Long-term consequences of victimization by white-collar crime. *Justice Quarterly*, *11*(1), 75–98.

Taylor, S.E., Wood, J.V. & Lichtman, R.R. (1983). It could be worse: Selective evaluation as a response to victimization. *Journal of Social Issues*, *39*(2), 19–40.

Van Wilsem, J. (2011). Worlds tied together? Online and non-domestic routine activities and their impact on digital and traditional threat victimization. *European Journal of Criminology*, *8*(2), 115–127.

Wang, J., Chen, R., Herath, T. & Rao, H.R. (2009). Visual e-mail authentication and identification services: An investigation of the effects on e-mail use. *Decision Support Systems*, *48*(1), 92–102.

Wemmers, J.-A. (2013). Victims' experiences in the criminal justice system and their recovery from crime. *International Review of Victimology*, *19*(3), 221–233.

Whitty, M.T. & Buchanan, T. (2016). The online dating romance scam: The psychological impact on victims-both financial and non-financial. *Criminology and Criminal Justice*, *16*(2), 176–194.

Jurjen Jansen is a senior researcher at the Cybersafety Research Group of NHL Stenden University of Applied Sciences and the Dutch Police Academy. In 2018, he obtained his PhD in behavioural information security at the Open University of the Netherlands. His research interests include human aspects of information security, cybercrime, cognition and human-computer interaction.

Rutger Leukfeldt is senior researcher cybercrime and the cybercrime cluster coordinator at the Netherlands Institute for the Study of Crime and Law Enforcement (NSCR). Furthermore, Rutger is director ('lector') of the Cybersecurity & SMEs Research Group of the Hague University of Applied Sciences.

APPENDIX

Table 1: Short summary of the interviews

Interview	Gender	Age (years)	Level of education	Victim type	Fraud type	Damage (euros)	Reimbursed
01	Female	58	Medium	Private	Phishing	13,000	Yes
02	Female	79	Medium	Private	Phishing	2,000	Yes
03	Male	45	Medium	Private	Phishing	11,000	Yes
04	Male	89	High	Private	Phishing	2,000 (a)	N/a
05	Male	73	Medium	Private	Phishing	8,000	Yes
06	Female	59	High	Private	Phishing	3,600	1,000
07	Male	77	Low	Private	Phishing	10,000 (a)	N/a
08	Female	70	High	Private	Phishing	50,000	Yes
09	Male	36	Medium	Corporate	Malware	1,300	Yes
10	Male	68	Medium	Corporate	Phishing	900	Yes
11	Male	23	High	Private	Phishing	7,000	Yes
12	Female	74	Low	Private	Phishing	1,200	No
13	Female	73	Low	Private	Phishing	1,800	No
14	Male	80	High	Private	Phishing	4,800	Yes (-150)
15	Female	74	High	Private	Phishing	50,000	No
16	Male	67	Medium	Private	Phishing	2,500	Yes (-150)
17	Male	71	Medium	Private	Phishing	5,700	No
18	Female	61	High	Private	Phishing	20,000	Yes (-150)
19	Male	38	High	Corporate	Malware	M.w. (a)	N/a
20	Female	64	Medium	Corporate	Malware	6,900	Yes
21	Male	29	Medium	Corporate	Malware	10,00	Yes
22	Female	57	Medium	Corporate	Malware	5,000	Yes
23	Female	46	Medium	Corporate	Malware	4,700	Yes
24	Male	64	High	Corporate	Malware	3,000	Yes
25*	Female	56	High	Corporate	Malware	5,000	Yes
26	Male	31	Medium	Private	Malware	3,500	Yes
27	Male	30	Medium	Corporate	Malware	4,700	Yes
28*	Male	63	High	Corporate	Malware	5,000	Yes
29	Male	50	High	Corporate	Malware	3,700	Yes
30	Female	51	Medium	Corporate	Malware	N.t.	Yes

*Note. * = not the actual victim, a = attempt, m.w. = about a monthly wage, n.t. = not told, n/a = not applicable, -150 = minus mandatory own risk (i.e., 150 euros).*

[i] This articles includes both phishing and malware attacks, because they are basically two types of the same crime. Leukfeldt, Kleemans, and Stol (2017), for example, show that not only the goal of phishing and malware attacks is the same (i.e., to steal money from online bank accounts), but that the modus operandi of both attack types is quite similar too (intercepting login credentials, intercepting one time transaction authentication codes, wiring the money to money mule accounts and cashing the money). The biggest difference is that the malware victims in this study were not actively engaged in providing perpetrators their credentials. However, being fully responsible or not, it is still relevant to find out how the malware attacks affected participants and how they recovered from it. Furthermore, we had no information on how well the victims were protected against malware attacks before conducting the interviews. Personal responsibility could have been an issue when we had found that malware victims, for instance, had poor security protection installed. Moreover, in other malware cases, victims were more personally responsible, for example, by responding to a malicious pop-up window (see e.g., Jansen & Leukfeldt, 2015).

Seductive Events: A Critical Examination of Youth Sexting

KAREN HOLT
Michigan State University

Abstract

The social impact of technologies is evident among both teenagers and young people. Youth now experience and engage in most aspects of daily life "online" through the use of social media, mobile phones, and the Internet. This has led to a host of concerns, from parents, educators, advocates, and law enforcement regarding the ways in which this technology is being used, with the debate focused primarily on the issue of "sexting" or sharing of naked and semi-naked selfies. This paper explores sexting behavior from a critical perspective, examining the individual and institutional narratives that continue to shape and influence opinion and policy. Drawing from narrative criminology I argue that there are competing narratives surrounding the sexting debate that serve to amplify the deviance associated with these behaviors, resulting in the criminalization of youth and masking the more insidious social problems, such as gender-based violence.

Keywords: sexting, sexuality, moral panic

INTRODUCTION

Youth crime, specifically drug use and youth violence are often the focuses of societal concern and moral panics (Goode & Ben-Yehuda, 1994). One term used to describe this is "juvenoia" – a tendency to be easily alarmed about changing youth mores in a rapidly evolving society (Finkelhor, 2010; Mitchell, Finkelhor, Jones, & Wolack, 2012). Hayward (2002) described the emotional response to youth crime and deviance:

> There can be few subjects as effective at setting in motion the meter of public opinion as youth crime. For many, it betokens a general erosion of public standards, providing visceral and compelling evidence of an ever more 'permissive society'. For others, such contemporary fears about the increased seriousness of youth criminality represent little new: simply the continuation of a two-century old tendency to scapegoat and vilify the transgressions of the young (e.g., Pearson, 1983), yet another moment in a long series of moral panics. (p. 1)

Contemporary anxiety has been focused on the "sexting teen," or youth who send sexually explicit selfies using digital media, most often presented as a young, heterosexual female who lacks sexual agency but who bears the responsibility for the negative consequences of sharing these images (Albury, 2017; Albury & Crawford, 2012; Dobson & Ringrose, 2016). The term "sexting" is a portmanteau of the words "sex" and "texting" which first appeared in the

news media in the early 2000s (Weins, 2014). Sexting began simply enough – using a mobile device to send a text message to another device; however, with the development of new media which individuals use to communicate, the sext has been transformed and definitions of sexting ought to include any technologies that use the Internet (Walker, 2012). The term is evolving and describes a wide variety of behaviors. These range from the consensual sharing of images between partners, the recording of sexual crimes, the commission of manufacturing or distributing child sexually abusive images, to non-consensual distribution of images (Lee, Crofts, McGovern, & Milivojevic, 2015).

Concern about sexting is hardly novel, as Jewkes (2010) asserted that anxieties involving sex, risk, and children have been "well-rehearsed in this country for more than 100 years" (p. 8). New technologies have always resulted in apprehension surrounding youth, for example, the panics over radio, music, and television (Albury & Crawford, 2012; Crichter, 2003; Lumby & Fine, 2006). What has changed is the type of technology used in order to participate in negotiating sexual identity and relations – the rise of the mobile phone.

The development of the mobile phone, specifically the smart phone, has changed modern life as we know it. This is especially so for youth who are considered "digital natives," having grown up with this technology. Many teens use their mobile phones exclusively for Internet access and do the bulk of their socializing via mobile phone, chronicling their lives in a way that sets them apart from previous generations (King, 2012). The Pew Research Center (2015) conducted a series of surveys and focus groups which examined tech use by youth. The findings indicated that most of young people's communication and maintenance of relationships occurs through the use of technology – from the use of emojis to express emotions and feelings, to announcing relationship statuses via Facebook, to ending relationships via text. The Pew study asserted that technology has altered young people's relationships – from the expected frequency of communication, the types of communication, the presentation of the relationship, to the ways in which youth end relationships.

As a consequence, there appear to be two differing views on the practice: Youth who view sexting as an appropriate application of technology to romantic relationships, and adults and criminal justice practitioners who perceive it as a threat to safety or moral standards for behavior. This paper utilizes a critical framework to address these conflicting views through a narrative criminological approach (Presser & Sandberg, 2015) examining the individual and institutional narratives that drive public opinion and social policy. This analysis argues that the competing narratives regarding youth sexting only amplify the perceived deviance of the act, simultaneously criminalizing youth while hiding more insidious social problems such as gender-based violence.

SEXTING NARRATIVES

It is difficult to estimate the prevalence of sexting as there is a lack of consensus among researchers and the media. Most inquiries regarding sexting have used survey methodology – for example, the National Campaign to Prevent Youth and Unplanned Pregnancy (2008), the MTV, and Associated Press (2009) online surveys which focused on digital abuse, the YouthOnline and Wireless Safety Survey (2009), and the PEW Internet and American Life Project (2015). These surveys have yielded quantitative data on the prevalence of sexting, but there is variability among the results. The two main reasons for this are sampling techniques and a general lack of consensus of definitions (Lounsbury, Mitchell, & Finkelhor, 2011). Operational definitions, ages

of participants (for example, asking older teenagers will yield a higher percentage of sexters), social desirability bias, issues regarding participants' understanding of the questions or willingness to honestly respond to questions of a sensitive nature impact the findings. The various conceptualizations of key terminology (e.g., defining sexting), research designs, data collection methods, sampling populations, and survey administrations have all affected results (Lamphere, 2014).

That said, estimates for the incidence of sexting range from 15% of youth to 40% or more (Ringrose, Gill, Livingstone, & Harvey, 2012). There are many reasons that youths offer for why they might sext. Due to the influence of peers among this population, most reasons are social in nature, such as a way to demonstrate flirtation or romantic interest, to initiate sex, and as a result of peer pressure (Le, Temple, Peskin, Markham, & Tortolero, 2014).

There are several prominent narratives when it comes to the phenomena of youth sexting. Narratives provide a window into how individuals organize themselves and the worlds around them, as well as how individuals are constructed and construct themselves (Daly & Maher, 1998; Miller, Carbone-Lopez, & Gunderman, 2015; Orbuch, 1997). Narratives are not objective, rather they are subjective, biased, influenced by circumstance and audience, and labyrinthine in their non-linearity (Maruna, 2015). Narratives inspire and motivate action, action which is imbued with meaning and where power and agency are constituted discursively (Presser & Sandberg, 2015). Narratives are delivered by using frames. These are ways in which to help people understand new information by relating it to existing knowledge, providing analytic structures that impact public perception of issues (Kim & Vishak, 2008). Frames guide our cognitive processing of events as they occur, and the media framing of events directly affects our understanding and response to issues (Meikle, 2012). Information is deemed as "news" when a culturally authorized storyteller validates it as such by delivering the narrative (Meikle, 2012).

The predominant narratives have exclusively focused on negative effects, both the psychological and social consequences of this behavior. Issues surrounding sexting involve self-sexual exploitation of minors and the loss of moral innocence in a digital culture that is saturated with sexual images (Cornwell, 2013; Weins, 2014). In addition to these more serious consequences, some research asserts that sexting may result in other negative outcomes, such as embarrassment and mental health problems (Dake, Price, Maziraz, & Ward, 2012).

The two most prominent narratives surrounding sexting and youth are the victim narrative and the moral panic narrative. The victim narrative is used to discuss the harms that can result from youth sexting. These narratives include stories of tragedy, such as youth suicide and child pornography (Podlas, 2014). The victim narrative portrays sexting youth as a vulnerable population, at risk for both victimization and exploitation, as well as the potentiality of becoming a criminal. Alternatively, the moral panic narrative asserts that the reaction to sexting is disproportionate to the threats presented by engaging in this behavior, and that much of the focus has been solely on the negative consequences of sexting, which are statistical anomalies.

As a result, criminal justice policies are enacted that exaggerate actual dangers and amplify deviance. An overreliance on the victim narrative has led to punitive policy and public concern. There is an emergent third category, the narratives from youth themselves, which suggests that the majority of sexting occurs between trusted partners and without negative consequences (Lee, Crofts, McGovern, & Milivojevic, 2015). This paper argues that it should be the narratives of youth that guide criminal justice policy moving forward.

Victim narratives: Suicide and child pornography

Youth behaviors are typically socially constructed by the media in one of two ways – with youth as either the tragic victim or the evil monster (Jewkes, 2015). Sexting debates tend to dichotomously portray youth as either victims who should take better precautions to avoid the negative costs of engaging in this behavior, or as offenders who create and distribute child pornography. Media coverage of sexting is constructed as overwhelmingly harmful, with teenage girls being in particular danger of what is termed an "epidemic," and a "dangerous youth trend" that could result in tragic consequences such as sexual exploitation, sex offender registration, and suicide (Karaian, 2012).

When it comes to the tragic victim, the stories of "tragic consequences" serve as morality tales, warning of the negative and potentially fatal dangers, particularly to young women, should they send sexually suggestive photos or videos. Public awareness and prevention was the reasoning that 18-year-old Jessica Logan gave for appearing on a local television station to discuss the negative consequences of sexually suggestive pictures of herself that her ex-boyfriend distributed after their break up. These images resulted in daily bullying and harassment. She appeared on television to share her story in May. Two months later, she committed suicide (Celizic, 2009).

Thirteen-year-old Hope Whitsell sent a crush some sexually suggestive photos in order to gain romantic attention. Those photos were promptly distributed to her peers. Like the Logan case, harassment and bullying ensued. The young teenager hanged herself while her family sat downstairs in their living room. Her distraught and heartbroken mother had a message for parents: "It happened to my daughter, it can happen to yours too. No one is untouchable. No one is untouchable" (Kaye, 2010).

The suicide victim narrative focuses on the deleterious effects, specifically for young women, that sexting can have on social status and reputation (Henry & Powell, 2015). Concerns surround the emotional and reputational damage that sexting can have, as well as the potential for both cyberbullying and offline harassment (Lee & Crofts, 2015). The Logan and Whitsell stories both shared the same tragic elements – young girls, presented as naïve and eager to impress young men, who send images only to have them non-consensually distributed, resulting in shame, stigma, harassment, and bullying.

Educational and prevention campaigns, such as the Australian video entitled *Megan's Story*, present cautionary tales that place responsibility squarely on the victim. *Megan's Story* details a young girl named Megan who emerges from a public school bathroom after sending a sext to boy. Upon returning to class, we hear the boy's mobile phone message alert and then the entire classroom, including the teacher, begin to receive message alerts as the picture is forwarded to everyone in school. The onus is on the victim as the voice over moralizes: "Think you know what happens to your images? Who will see them? How will they affect you? Think again."

As Albury and Crawford (2012) asserted in their analysis of this public campaign, the message is clear – the consequences of sexting are serious, but for the one who sends the sext and the consequences of that choice are shame and humiliation. This gendered double standard, where young women are seen as responsible for their victimization, is a current theme within the victim narrative (Albury, Crawford, Byron, & Matthews, 2013; Albury, Funnell, & Noonan,

2010; Lee & Crofts, 2015; Ringrose, Gill, Livingstone, & Harvey, 2012). Not unlike the victim blaming that occurs in cases of sexual assault, and the prevalent rape myths surrounding responsibility, there are moral expectations of what "good girls" do and do not do (Lee & Crofts, 2015; Worthen, 2016). Placing the responsibility solely on the victim, who should have avoided these risks in the first place, allows for a denial of the victim that leads to harassment and bullying and "slut shaming." As the Logan and Whitsell cases demonstrate, this can have devastating consequences (Ryan, 2010).

Though young girls are most often seen as being responsible for prevention of victimization, there is another way in which the victim narrative functions, which is the youth as offender stories. The "youth as victims of child pornography" frame draws from our collective fear about youth as tragic victims of sexual violence. The less common "youth as producers and distributors" frame represents our fears about the premature sexualization of youth and the development of criminality. This victim narrative is fueled by the archetype of a real life monster, despised and feared by all – the child predator. Behind the monitor of our computers, the ghost of the potential child predator lurks, waiting to gain access to images of vulnerable youth in order to use them for sexual satisfaction. More concerning, perhaps, is the elusive nature of digital images as their weightless nature allows them to be distributed to other predators – the specter of the pedophile haunts child pornography's production and consumption (Karaian, 2012). The Internet offers an environment where fictitious personas can be developed and used in order to trap naïve individuals, and this environment is perfectly suited to act as the perfect lair for child predators (Mitchell, Finkelhor, Jones, & Wolak, 2010).

The fears and concerns regarding child pornography shape the discourse surrounding sexting. A troubling trend of prosecution via child pornography laws is evidence of the panic regarding youth as victims and offenders (Arcabascio, 2010; Calvert, 2009; Goldstein, 2009; Humbach, 2010; Karaian, 2012; Kimpel, 2010; Leary, 2008, 2010). Under United States Federal Law, it is a crime to knowingly produce, distribute, receive, or possess with intent to distribute, visual media that depicts a minor engaging in sexually explicit conduct and is obscene (Federal Law 18 U.S.C. 2252). Therefore, when minors engage in sexting, felony charges may result.

When it comes to the victim narratives, there is a sense of familiarity associated with these tragic cases and the dangers they represent, which may be inextricably linked to our conceptions of sexting. We all know these victim stories, even if we are not sure *how* we know them. The purported devastating and fatal consequences of sexting are engrained in our cultural imagination. Linnemann (2014) discussed true crime stories as ghost stories that take residence in the public imaginary – these stories shape public opinion and policy. He draws on Derrida's (2006) concept of the "hauntological," the figure of the ghost, neither absent nor present. This is ever present in our collective unconscious; these stories reside within us and are stored until a focusing event acts as a medium, conjuring up ghosts that linger in the social imagination, animating the social space with spectral power (Armstrong, 2010; Bell, 1997; Gordon, 2008; Linnemann, 2014). The spectral traces these cases leave behind incite public panic and outrage, which informs policy, resulting in punitive and ineffective measures and sanctions. We pull from those cultural narratives regarding the intersection of youth, sex, technology, and danger because those are the stories most readily available and which fit emotionally charged concerns.

The victim narrative, though extensively propagated through media coverage, is problematic for several reasons. Suicides are not common reactions to sexting gone bad, and in most cases, youth report that they do not experience any harm from sexting behaviors (Lee, Crofts, McGovern, & Milivojevic, 2015). The fear of child pornography is exaggerated as most youths' photos fail to meet the legal standard for sexually abusive materials involving minors (Duncan, 2014; Podlas, 2014). Despite the extensive focus on the dangers associated with sexting, there is not an epidemic of child pornographers, and there is much debate over whether any youth sexting should be considered child pornography, with many legislators arguing that these laws will be ineffective and completely unnecessary (Fredella & Galeste, 2011; Painter, 2011). In most instances, cases involving youth sexting are only prosecuted when adults are the recipients of photos (Worthen, 2016). It is because of the exaggerated dangers of sexting that a second narrative has emerged in the debate, which is the moral panic narrative.

The moral panic narrative

The perpetuation of the victim narratives, despite the evidence of the actual dangers of sexting, has led to claims that what has occurred is a moral panic, or a "fundamentally inappropriate" reaction to events or conditions where the seriousness or gravity of these events or conditions becomes distorted or amplified (Goode & Ben-Yehuda, 2009). The moral panic argument claims that the response to youth sexting is exaggerated and overly paternalistic, and asserts that sexting among youth as a normal behavior in the digital era, a modern-day form of streaking or skinny-dipping, simply moving from offline to online in a culture of digital natives (King, 2012; Shellenbarger, 2009).

This panic is media produced and exclusively focused on the prevalence and potential negative consequences of this behavior, framing it as an emerging social problem (Karaian, 2012; Lumby & Fennell, 2011). What is clear from the scholarly literature is that it is the minority of youth who engage in sexting behaviors, and that negative consequences are uncommon, which lends credence to the moral panic narrative (Berkman Center for Internet Safety; Salter, Crofts, & Lee, 2013). The anxiety and concern over sexting would seem to be disproportionate to the actual threat of danger.

It is this anxiety which fuels moral panics. Take a legitimate fear (adolescent sexual behavior and risk or harm), amplify the deviance associated with the behavior and distort the chances of risk (through the media), and convince an audience (parents, religious groups, politicians) that something must be done to protect the vulnerable victims (youth, especially young girls). The actors involved are always the press or media, the public, agents of formal social control, lawmakers and politicians, and action groups (Cohen, 1979).

Young (2009) described the moral panic process as a moral disturbance, which is then focused on by the media, experts, and moral entrepreneurs and targeted by formal agents of social control until eventually the panic extinguishes. Anxiety and emotion fuel a moral panic, creating a sense of chaos and uncertainty, a crisis that threatens established norms or values. The group or event chosen as the focus of moral panic is related to the source of anxiety and can be understood as a symptom of the underlying moral uneasiness, which explains why the reaction to the perceived threat is disproportionate to the actual risk. He noted that "if panics are 'successful,' they connect up to fundamental shifts in the tectonic plates of order, each occurrence like a volcanic atoll. It is their reappearance that confirms their status as moral

disturbances of any significant order" (p. 14). Thus, concern about youth and crime or deviance is a panic that resurfaces and reappears often, though the form of troubling behavior may change

Curnutt (2012) offered a rich cultural and institutional analysis of youth sexting where it can be understood as a "sometimes-private sometimes-public practice that relies on a level of reflexivity for its participants to remediate themselves in accordance with the institutional discourses and conventions that govern the media industry's production of sexual imagery for a heterosexual male audience" (p. 361). Youth sexting is simply a new form of production for a product that the culture has long been consuming and venerating, one that elicits anxiety regarding our own sexuality, which we attempt to cover in a veil of secrecy.

Sexting can be understood as simply a means of courtship for an age in which so much of our lives are online (Weins, 2014). The youth who participate in sexting are digital natives who have grown up in a culture of participation – a culture where their lives are recorded, "snapped," "shared," "liked," and lived collectively with "friends" online (Palfrey & Gasser, 2008). It is irrational to expect that their sexual behavior would somehow be separate from this culture. These youth have been raised on reality shows and YouTube – personal life is public life, possibly even stardom (Weins, 2014).

These digital natives are coming of age in an era where the privacy and secrecy older generations once enjoyed has become obsolete. The Internet has opened Pandora's Box and there is no way of closing it, yet there is good news "offline" – there have been declines in "real life" risky sexual behaviors – youth pregnancy has decreased, birth control usage has increased, and teens report waiting longer to have sex and having fewer sexual partners (Eaton et al., 2011.) Shifting from a risk model of youth deviance to one that focuses on these behaviors as part of normal adolescent development may be a more useful framework in understanding youth sexuality and technology, and allow for a more realistic portrayal of sexting and its most often relative and benign nature (Michaud, 2006).

In fact, there are many beneficial aspects of the Internet for youth, such as education, access, and support. The Internet can offer a positive means of sexual exploration for youth; for example, by providing information on sensitive topics that youth may not want to discuss with adults, such as sexual health information, initiating and maintaining dating relationships, opportunities for peer feedback, and safe forums for traditionally marginalized populations such as lesbian, gay, bisexual, and transgender youth (LGBT, Comartin, 2013). Those uncomfortable conversations with guardians about the "birds and the bees" are no longer necessary – young people have access to information regarding sexual health. For teens who suffer from social anxiety or are uncomfortable in real life settings, online support can be found with the click of a button in Facebook groups, forums, and chat rooms. And for vulnerable populations, such as LGBT youth, the Internet can be an invaluable resource for finding support, discussing hardships or struggles with likeminded others. While the Internet can be used to harm, it is just as readily available to be used to inform and to guide youth through the unfamiliar and often terrifying terrain that is youth sexual exploration.

The moral panic narrative attempts to quell fears surrounding youth and technology by reminding us that this is not a new phenomenon. Sexting can be understood as simply another example of normal teenage deviance (Johnston, O'Malley, Bachman, & Schulenberg, 2013; Temple, Le, Peskin, Markham, & Tortolero, 2014). Youth have always used emerging technologies for sexual communication with others (Fox & Potocki, 2014; Vybiral, Smahel, &

Divinova, 2004). As technology has changed, youth have simply adapted their sexual behavior. Despite the best efforts of agents of social control seeking to protect the vulnerable, youth have always engaged in "risky" behaviors, and participation in these behaviors represent the norm rather than statistical anomalies (Johnston, O'Malley, Bachman,& Schulenberg, 2013; Temple, Le, Peskin, Markham, & Tortolero, 2014).

Moral panics are reflexive and interactive events. As Young (2009) asserted, they are seductive events loaded with explosive power. In dissecting a moral panic, there is always a legitimate fear underlying the chaotic and exaggerated reaction. A moral panic is not senseless fear and paranoia nor a random selection of a target or enemy (Garland, 2008; Young, 2009). Rather, the focus of a panic poses a real threat, and it is important to recognize the actual dangers associated with the behavior rather than to make the oversimplification that all concern about sexting is a moral panic. There are true dangers inherent in youth sexual behavior that are cause for concern. Unprotected sex, sex without commitment, having multiple sexual partners, and engaging in sex while intoxicated or under the influence are all behaviors that can result in serious consequences. Individuals from ages 15-24 account for 25% of sexually active individuals in the United States, but they represent nearly half of the new sexually transmitted disease cases each year and young females account for the largest proportion of unplanned pregnancies (Centers for Disease Control and Prevention, 2008; Finer & Henshaw, 2006). Thus, due to the disproportionate number of adolescents who experience these negative health outcomes, youth sexual behavior is a public health concern (DeClemente, Salazar, & Crosby, 2007; Dir, Coskunpinar, & Cyders, 2014).

Recent research has challenged the notion of the "disproportionate response" citing that the moral panic is a reflexive event, and that initial overreaction may become proportionate depending on how "folk devils" react (David, Rohloff, Petley, & Hughes, 2011). To suggest that the concern is an exaggeration may serve to deny those who have suffered as a result of sexting gone wrong. No sufficient amount of evidence supporting the moral panic narrative emphasizing the actual potential of harm will comfort the grieving parent who has lost a child or the youth who is forced to register as a sexual offender. To these individuals, these issues do not represent a moral panic, rather an actual consequence that they must survive.

This problem is similar in nature to the effectiveness of sex offender policies – the punitive measures that are in place, such as registration and notification, result in net widening and wasted resources when the minority of offenders pose a danger to society (Letorneau, Levenson, Bandyopadhyay, Sinha, & Armstrong, 2010). The statistics and evidence do not make a difference in public perception or opinion. That a sexual predator could harm one of our children is too great to chance. And the hauntological is at work conjuring the ghosts of those who were innocent victims of sexual crimes, such as Megan Kanka, Jacob Wetterling, and Adam Walsh, who serve as reminders that statistics are meaningless to those who are affected.

The moral panic narrative may be seen as overly simplistic and in some ways victim-denying. A responsible approach to dealing with these issues is to first develop an understanding of how youth frame and experience their own behaviors.

THE EMERGING YOUTH NARRATIVES: PERCEPTIONS AND PRACTICE

Lee and Crofts (2015) claimed that "research on sexting often begins with an adult oriented moral agenda and unproblematically takes sexting on board as a negative risk," (p. 468). This approach denies youth the agency that must be afforded to them to understand young people and media technologies. An essential part of this would be to study practices and attitudes and situate them within meaning and context so as to give youth an active voice, and place social fears and panics into perspective (Albury & Crawford, 2012; Crawford & Goggin, 2011). Narratives must come from those who engage in these behaviors – the stories they tell others, the stories they tell themselves,

Knowledge of the actual practices and perspectives of youth who sext is limited despite the media attention and public concern (Lee & Crofts, 2015). There have been qualitative examinations of sexting which aimed to provide a richer and more descriptive account of the behavior and those who engage in it (Phippen, 2012; Ringrose, Gill, Livingstone, & Harvey, 2012). These explorations represent unique attempts to directly engage with and listen to youth who sext rather than to administer surveys or test theories in the tradition of previous sexting research.

What emerges from the existing data is clear: It is the minority of youth who engage in sexting, and most sexting occurs among older youth (Lenhart, 2009). Most young people who engage in sexting do so within the confines of an existing relationship with a partner that they trust and appear to minimize harm and risks by doing so (Lee, Crofts, McGivern, & Milvojevic, 2015; Mitchell, Finkelhor, Jones, & Wolak, 2012). Harm and negative consequences represent the minority of cases (Lee & Crofts, 2015; Phippen, 2009). Youth who actually engage in sexting are less likely to construct it as a negative behavior, and there is little evidence to conclude that most girls feel especially coerced or pressured to sext (Lee & Crofts, 2015; Strassberg, McKinnon, Sustaita, & Rullo, 2013).

Young people, similarly to adults, represent and embody sensuality and sexuality and attempt to negotiate conventions that are sexed, gendered, and classed (Albury, 2015). Examining their negotiations through an adult gaze can lead to misreadings and misinterpretations of behaviors. The need for examination that focuses on sexting youth narratives and the intersection with dominant cultural and institutional narratives will provide for a comprehensive understanding of the lived meaning for participants as well as the actual dangers involved.

The real dangers: Gender-based violence, coercion

The exclusive focus on youth sexuality and sexting masks more insidious social issues. These issues fail to receive the necessary attention and resources due to the emphasis on victim narratives and moral panic surrounding youth. The real and significant harm centers on gender-based violence and the nature of coercion, not only among youth but also adult women.

Much like any other sexual behavior, there is a gender based double standard placed on sexting. The fact that females have more to lose, are publicly shamed, and are more often pressured to engage in sexting than their male counterparts, is troubling and has several possible repercussions (Lee, Crofts, McGivern, & Milvojevic, 2015; Ringrose, Harvey, Gill, &

Livingstone, 2013). Placing the blame on the victim may deter victims from reporting instances where negative instances do occur. Like many other educational and awareness campaigns regarding sexual assault, the message youth receive is that the onus is on females to minimize risk by abstaining from the behavior, rather than focusing on the actual issue, which is the non-consensual distribution of images that the victim sent to a primary recipient. Girls are typically misrepresented in media, and popular culture as lacking in sexual agency – their decisions to send images proof of victimization resulting from the "pornification" of a generation (Durham, 2008; Levine & Kilbourne, 2009; Scott & Sarracino, 2008). This essentialist construction is problematic and serves to reinforce the panic surrounding risks, youth sexting, and vulnerable populations.

Despite the misrepresentations, there is evidence that coercion is a valid concern for a subset of young girls. Prevalent in the literature is the argument that pressure and/or coercion is the reason why some young females send sexually explicit images of themselves to others, and most often the recipients are young males (Englander, 2012). Lee and Crofts (2015) further articulated this idea of "pressure," developing three categories of pressure that young females might experience: individual pressure, peer group pressure, and sociocultural pressure. Due to these pressures, each operating at different levels, the authors questioned whether young women in some instances are able to fully and freely "consent" to sexting, even where it would seem that images are produced and sent "consensually." Their findings were consistent with the notion of peer pressure and coercion being an important factor – many youth engaged "voluntarily under pressure." This is an important concept, an almost consensual non-consent that becomes problematic when discussing youth agency.

Some argue that the problem of coercion is structural. American society sexualizes adolescents and profits from doing so, and the vilification of youth sexting is one way to neutralize and displace blame (King, 2012). This is consistent with objectification theory, which focuses on the ways in which a sexually objectifying culture affects the experiences of young girls and women (Dir, Coskunpinar, Stenier, & Cyders, 2013). Society places greater emphasis on appearance for females and they are socialized to have a preoccupation with how they look (Fox & Potocki, 2014). Sexting mirrors a society that sexualizes and objectifies young women, partially evidenced by the finding that more females report sending images than males (Englander, 2012; Lamphere, 2014; Mitchell, Finkelhor, Jones, & Wolak, 2012; MTV Associated Press, 2009). Thus, because of internalized expectations about their appearance and sexuality, young girls may in fact be vulnerable, and these structural theories lead to questions regarding the nature of "consensual" images.

Henry and Powell (2015) argued that one of the unintended consequences of the focus on youth sexting is the reluctance or reticence to understand non-consensual creation and distribution of images as gender-based violence. As a result, there is a failure to respond to the harms that are caused and a lack of recourse for victims, which leads to an underreporting of these crimes. There is extant research that claims a continuum of abusive behaviors beginning in childhood and persisting into adulthood of which includes sexting (Lee & Crofts, 2015; Powell, 2007; Salter, Crofts, & Lee, 2013). Sexting as a youth may indicate a propensity for future interpersonal violence, particularly against adult women.

There is a dearth of research that examines how these technologies are used to facilitate violence against adult women who are more often victimized as adults and tend to engage in

sexting more regularly than young people (Henry & Powell, 2015; Lee & Crofts, 2015). The Internet and associated technologies have facilitated crimes against women such as stalking, harassment, and coercion (Crisafi, Mullins, & Jasinski, 2016; Spitzberg & Hoober, 2002; Woodlock, 2014). The non-consensual distribution of sexually explicit images with the intent to humiliate or cause shame is a common tactic among domestic violence offenders, who use technology in order to threaten, control, manipulate, and punish their partners or ex-partners (Diamond, Fisher, & Bruckman, 2011; Hand, Chung, & Peters, 2009; Southworth, Finn, Dawson, Fraser, & Tucker, 2007). Victimization through online media, including cyberstalking, cyber harassment, and sexual victimization most often occurs between intimate partners (Black et al., 2011). Much like other "offline" gender based violence, the real threat is often from those to whom we are closest and with who we are most intimate, a fact lacking from the prominent narratives.

A NEED FOR INQUIRY

The existing narratives regarding sexting, the victim narrative, and the moral panic narrative, are heavily media driven. The reaction from the criminal justice system has been primarily concerned with the victim narrative due to the tragic nature of celebrated cases, which has resulted in over-regulation or the criminalization of youth. Criminalization of these behaviors and the prominent narratives regarding sexting are consistent with the tendency to focus on normative frameworks concerned with risky behaviors and the agency and blameworthiness of victims (Albury & Crawford, 2012; Albury, Funnell, & Noonan, 2010; Henry & Powell, 2015, Salter, Crofts & Lee, 2013). The current fixation on the dangers of sexting reinforces problematic notions and assumptions regarding youth sexuality and technology, and deflects attention from real dangers, such as gender-based violence and technology assisted sexual violence (Henry & Powell, 2015). Therefore, policy responses by the legal and justice system, public education and awareness campaigns, and the public concern, will be ineffective at addressing the most serious consequences.

The youth narratives can inform the discourse moving forward and hopefully toward the process of change. Not only do narratives describe past actions, but it is argued that they can inspire future action by providing a legitimate path (Presser & Sandberg, 2015). Topics involving technology often takes time to "catch up" to the actual behaviors that are under study (Lamphere, 2012). A narrative criminological approach can elucidate the lived experiences of participants, and the emphasis on stories as influenced and biased can expose patterns of thought, attitudes, and behaviors in a way that traditional methodologies have not (Presser & Sandberg, 2015).

The emotions surrounding topics involving sex, youth, and harm are likely to remain a subjective and normative decision, with no quantity or quality of research and information able to definitively answer the question of whether sexting is, in fact, good or bad (Simpson, 2013; Weins, 2014). We must critically examine the narratives surrounding this issue, explore the fears that fuel panic, give serious consideration to the voices of those who have been directly affected by the consequences of sexting, and continue to evaluate sexting using a confluence of research methodologies in order to fully understand the potential risks associated with this behavior.

REFERENCES

Albury, K. (2017). Just because its public doesn't mean it's any of your business: Adults' and children's rights in digitally mediated spaces. *New Media and Society, 19*(5), 713-725.

Albury, K. (2015). Selfies, sexts, and sneaky hats: Young people's understandings of gendered practices of self-representation. *International Journal of Communication, 9*, 1734-1745.

Albury, K. & Crawford, K. (2012). Sexting, consent, and young people's ethics: *Beyond Megan's Story*. *Continuum: Journal of Media and Cultural Studies*, *26*(3), 463-473.

Albury, K. & Lumby, C. (2010). Too much? Too young? The sexualization of children debate in Australia. *Media International Australia, incorporating Culture and Policy*, 135, 141-152.

Albury, K., Funnell, N., & Noonan, E. (2010). The politics of sexting: Young people, self-presentation, and citizenship. Paper presented at the Australian and New Zealand Communication Association Conference: Media, Democracy, Change, Old Parliament House.

Arcabascio C. (2010) Sexting and teenagers: OMG R U going 2 jail??? *Richmond Journal of Law and Technology XVI* (3): 1–42.

Bell, M. (1997). The ghosts of place. *Theory and Society*, 26, 813-836.

Black, M.C., Basile, K.C., Breiding, M., Smith, S.G., Walter, M.L., Merrick, M.T., Chen, J. & Stevens, M.R. (2011). The national intimate partner and sexual violence survey. 2010 Summary Report. Atlanta, GA. National Center for Injury Prevention and Control, Centers for Disease Control and Prevention.

Bogle, K.A. (2008). Hooking up: Sex, dating, and relationships on campus. NYU Press: New York, NY.

Calvert C. (2009) Sex, mobile phones, privacy and the First Amendment: When children become child pornographers and the Lolita Effect undermines the law. *Catholic University of America Comm Law Conspectus* 18: 1–72.

Campbell, W.J. (2015). *1995: The year the future began*. University of California Press.

Celizic, M. (2009). Her teen committed suicide over sexting. Today.com. Retrieved from https://www.today.com/parents/her-teen-committed-suicide-over-sexting-2D80555048.

Centers for Disease Control and Prevention. (2008). Sexually transmitted disease surveillance, 2007. Division of STD prevention, U.S. Department of Health and Human Services, Atlanta, GA.

Comartin, E. (2013). Sexting and sex offender registration: Do age, gender, and sexual orientation matter? *Deviant Behavior*, 34(1), 38-52.

Cornwell, J.K. (2013). Sexting: 21st century statutory rape. *Southern Methodist Law Review*, 66, 111-155.

Crichter, C. (2003). *Moral panics and the media*. Buckingham: Open University Press.

Crisafi D. N., Mullins A. R., & Jasinski J. L. (2016). The rise of the "virtual predator": Technology and the expanding reach of intimate partner abuse. In Navarro J. N., Clevenger S., & Marcum C. D. (Eds.), *The intersection between intimate partner abuse, technology, and cybercrime: Examining the virtual enemy* (pp. 95–123). Durham, NC: Carolina University Press.

Curnutt, H. (2012). Flashing your phone: Texting and the remediation of youth sexuality. *Communication Quarterly*, *60*(3), 353-369.

Crawford, K. & Goggin, D. (2008). Handsome devils: Mobile imaginings of youth culture. *Global Media Journal*, Australian Edition, *1*(1), 1-12.

Dake, J.A., Price, J., Maziarz, L. & Ward, B. (2012). Prevalence and correlates of sexting behavior in adolescents. *American Journal of Sexuality Education, 7*(1), 1-15.

Daly, K. & Mahr, L. (1998). Crossroads and intersections: Building from the feminist critique. In K. Daly & L. Mahr (Eds.). *Criminology at the crossroads: Feminist readings in crime and Justice*, Oxford: Oxford University Press.

David, M., Rohloff, A. Petley, J., & Hughes, J. (2011). The idea of moral panic – ten dimensions of dispute. *Crime, Media and Culture, 7(*3), 215-228.

Davis, M.J., Powell, A., Gordon, D., & Kershaw, T. (2016). I want your sext: Sexting risk in emerging adult minority men. *Education and Prevention*, *28*(2), 138-152.

DeClemente, Salazar, & Crosby. (2007). A review of STD/HIV preventive interventions for adolescents: Sustaining effects using an ecological approach. *Journal of Pediatric Psychology, 32*, 888-906.

Derrida, J. (2006). *Specters of Marx: The state of the debt, the work of mourning, and the new international*. Routledge.

Diamond, J.P., Fiesler, C. & Bruckman, A.S. (2011). Domestic violence and information communication technologies. *Interacting with Computers,* 23, 413-421.

Dir, A.L., Coskunpinar, A., & Cyders, M.A. (2014). A meta-analytic review of the relationship between adolescent risky sexual behavior and impulsivity across gender, age, and race. Clinical Psychology Review, 34(7), 551-562.

Dir, A.L., Coskunpinar, A., J.L., Stenier, & Cyders, M.A. (2013). Understanding differences in sexting behaviors across gender, relationship status, and sexual identity, and the role of experiences in sexting. *Cyberpsychology, Behavior, and Social Networking*, *16*(18), 568-574.

Durham M.G. (2008) The Lolita Effect: *The Media Sexualization of Young Girls and What We Can Do About It.* New York: Penguin Group.

Eaton, D.K., Lowry, R., Brener, N.D., Kann, L., Romero, L., & Wechsler, H. (2011). Trends in human immunodeficiency virus and sexually transmitted disease – related risk behaviors among U.S. high school students 1991- 2009. *American Journal of Preventative Medicine*, *40*(4), 427-433.

Englander, E. (2012), 'Low risk associated with most teenage sexting: A study of 617 18-year olds'. Massachusetts Aggression Reduction Center, Bridgewater State University.

Finer, L.B. & Henshaw, S.K. (2006). Disparities in rates of unintended pregnancy in the United States, 1994 and 2001. *Perspectives on Sexual and Reproductive Health, 38*, 90-96.

Finkelhor D. (2010). The Internet, youth deviance, and the problem of juvenoia. Presentation: 2010.

Finn, J., & Atkinson, T. (2009). Promoting the safe and strategic use of technology for victims of intimate partner violence: Evaluation of the technology safety project. *Journal of Family Violence, 24*(1), 53-59.

Fox, J. & Potocki, B. (2014). Technology and culture. In T.C. Hiestand and W.J. Weins (Eds.). *Sexting and youth: A multidisciplinary examination of research, theory, and law*. Durham, NC: Carolina Academic Press.

Fredella. H.F. & Galeste, M.A. (2010). Sexting: the misguided penal social control of teenage sexual behavior in the digital age. *Criminal Law Bulletin, 47*, 438-473.

Garland, D. (2008). On the concept of a moral panic. *Crime, Media, Culture, 4*(9): 9–30.

Goldstein L. (2009) Documentation and denial: Discourses of sexual self-exploitation. Jump Cut: A Review of Contemporary Media, Spring (no. 51).

Goode, E. & Ben-Yehuda, B. (1994). *On moral panics.* Oxford: Blackwell.

Gordon, A. (2008). *Ghostly matters: Haunting and the sociological imagination*. University of Minnesota Press.

Hand, T., Chung, D., & Peters, M. (2009). The use of information and communication technologies to coerce and control in domestic violence and following separation. Stakeholder Paper Number 6, Australian Domestic and Family Violence Clearinghouse.

Hayward, K. (2002). The vilification and pleasures of youth transgressions. In Muncie, J., Hughes, G., and McLaughlin, E. (Eds.). *Youth Justice: Critical Readings*. London: Sage.

Humbach J.A. (2010) "Sexting" and the First Amendment. *Hastings Constitutional Law Quarterly 37*, 433–467.

Jewkes, Y. (2010). Much ado about nothing: representations and realities of the online solicitation of children. *Journal of Sexual Aggression, 16*(1), 5-18.

Ito, M., Horst, H., Bittanti, M., Boyd, D., Herr-Stephenson, B., Lange, P., . . . Robinson, L. (2008). Living and learning with new media: Summary of findings from the Digital Youth Project. (The John D. and Catherine T. MacArthur Foundation Reports on Digital Media and Learning). Retrieved from www.digitalyouth.ischool.berkeley.edu.

Johnston, D., O'Malley, P., Bachman, J.G., & Schulenberg, J.E. (2013). Monitoring the future: National survey results on drug abuse. *The National Institute on Drug Abuse*.

Karain, L. (2012) Lolita speaks: 'Sexting,' teenage girls and the law. *Crime Media Culture 8*(1): 57–73.

Kaye. R. (2010). How a mobile phone picture led to a girl's suicide. CNN.com.

Kim, Y.M. & Vishak, J. (2008). Just laugh: You don't need to remember. *Journal of Communication, 58,* 338-360.

Kimpel A.F. (2010) Using laws designed to protect as a weapon: Prosecuting minors under child pornography laws. *New York University Review of Law and Social Change 34,* 299–338.

King, B. (2012). How much is too much? Limit setting and sexual acting out in the digital era. *Journal of Clinical Psychology: In Session, 68,* 1196-1204.

Lamphere, R, (2012). TXT NOW, PAY L8R: An exploratory study of teenage participation in sexting. Ph.D. dissertation, Indiana University of Pennsylvania.

Lamphere, R. (2014). Prevalence and research methodology. In T.C. Hiestand and W.J. Weins (Eds.). *Sexting and youth: A multidisciplinary examination of research, theory, and law*. Durham, NC: Carolina Academic Press.

Leary M. (2008) Self-produced child pornography: The appropriate societal response to juvenile self-sexual exploitation. *Virginia Journal of Social Policy and the Law, 15*(1).

Lee, M. & Crofts, T. (2015). Gender, pressure, coercion, and pleasure: Untangling motivations for sexting among young people. *British Journal of Criminology*, 55, 454-473.

Lenhart, A. Purcell, K., Smith, A. & Zickhur, K. (2010). Social media and young adults. Pew Internet. Retrieved from http://www.pewinternet.org/2010/02/03/social-media-and-young-adults/

Letorneau, E. J., Levenson, J.S., Bandyopadhyay, D., Sinha, D., & Armstrong, K.S. (2010). Evaluating the effectiveness of sex offender registration and notification policies for reducing sexual violence against women. A report to the United States Department of Justice.

Levine D.E., Kilbourne J. (2009) *So sexy, so soon: The new sexualized childhood and what parents can do to protect their kids*. New York: Random House.

Lewis, P. (1995). Tech on the net: The Internet battles a much-disputed study on selling pornography on line. *The New York Times*.

Linnemann, T. (2014). Capote's Ghosts: Violence, media, and the spectre of suspicion. *British Journal of Criminology*, 1-20.

Lounsbury, K., Mitchell, K. & Finkelhor, D. (2011) 'The true prevalence of "sexting"'. Crimes against children research Centre.

Lumby, C. & Fine, D. (2006). *Why TV is good for kids: Raising 21st century children*. Pan MacMillan.

Lumby, C. & Fennell, N. (2011). Between heat and light: The opportunity in moral panics. *Crime, Media, and Culture*, 7(3), 277-291.

Meikle, G. (2012). Find out exactly what to think – next! Chris Morris, brass eye, and journalistic authority, *Popular Communication, 10*, 14.

Michaud, P-A. (2006). Adolescents and risks: Why not change our paradigm? *Journal of Adolescent Health, 38*(5), 482.

Miller, J. Carbone-Lopez, K., & Gunderman, M. (2015). "Gendered narratives." In L. Presser & S.Sandberg (Eds). *Narrative Criminology: Understanding Stories of Crime*. New York, NY: NYU Press.

Mitchell, K.J., Finkelhor, D., Jones, L. & Wolak, J. (2012). Prevalence and characteristics of youth sexting: A national study. *Pediatrics*, *129*(1), 13-20.

MTV Associated Press. (2011). The digital abuse study: A survey from MTV and the Associated Press- NORC Center for Public Affairs. Retrieved from http://www.athinline.org/pdfs/2013-MTV-AP-NORC%20Center_Digital_Abuse_Study_Full.pdf

Orbuch, T.L. (1997). People's accounts count: The sociology of accounts. *Annual Review of Sociology*, 23, 455-478.

Painter, K. (2011). *Sexting numbers among teens lower than thought*. USA Today.

Pearson, G., (1983) *Hooligan: A history of respectable fears*. London: Macmillan.

Pew Research Center. (2015). Retrieved from http://www.pewinternet.org/online-romance/

Phippen, A. (2009). Sharing personal images and videos among young people. South West Grid for Learning.

Phippen, A. (2012). Sexting: An exploration of practices, attitudes and influences. Report for the NSPCC.

Podlas, K. (2014). Media activity and its impact. In In T.C. Hiestand and W.J. Weins (Eds). *Sexting and youth: A multidisciplinary examination of research, theory, and law*. Durham, NC: Carolina Academic Press.

Powell, A. (2007). Sexual pressure and young people's negotiation of consent. ACSSA Newsletter, 14, 8-16.

Presser, L. & Sandberg, S. (2015). *Narrative criminology: Understanding stories of crime.* New York: NYU Press.

Ringrose, J., Gill, R., Livingstone, S., & Harvey, L. (2012). A qualitative study of children, young people and 'sexting': a report prepared for the NSPCC. National Society for the Prevention of Cruelty to Children, London, UK.

Ryan, E.M. (2010). Sexting: How the state can prevent a moment of indiscretion from leading to a lifetime of unintended consequences for minors and young adults. *Iowa Law Review*, 96, 357-383.

Salter, M. Crofts, T., & Lee, M. (2013). Beyond criminalization and responsibilisation: Sexting, gender, and young people. *Current Issues In Criminal Justice*, *24*, 301-316.

Scott K. & Sarracino C. (2008). *The porning of America: The rise of porn culture, what it means, and where we go from here*. Boston, MA: Beacon Press.

Shellenbarger, S. (2009, June 15). Why do teens engage in ‘‘sexting?’’ [Web log post]. Retrieved from http://blogs.wsj.com/juggle/2009/06/15/why-do-teens-engage-in-sexting/

Simpson, B. (2013). Challenging childhood, challenging children: Children’s right and sexting. *Sexualities*, *16*, 690-709.

Southworth, C., Finn, J., Dawson, S., Fraser, C., & Tucker, S. (2007). Intimate partner violence, technology and stalking. *Violence Against Women*, *13*, 842-856.

Spitzberg B.H. & Hoober, G. (2002). Cyberstalking and the technologies of interpersonal terrorism. *New Media and Society*, *4*(1), 71-92.

Strassberg, D., McKinnon, R., Sustaita, M., & Rullo, J. (2013). Sexting by high school students: An exploratory and descriptive study. *Archives of Sexual Behavior*, 42, 15-21.

Temple, J.R., Le, V.D. Peskin, M., Markham, C., & Tortolero, S. (2014). Risky behavior and adolescent development. In T.C. Hiestand & W.J. Weins (Eds). *Sexting and youth: A multidisciplinary examination of research, theory, and law*. Durham, NC: Carolina Academic Press.

Vybiral, Z., Smahel, D., & Divinova, R. (2004). Growing up in virtual reality: Adolescents and the Internet. In P. Mares (Ed). *Society, reproduction, and contemporary culture*. Czech Republic: Barrister and Principal.

Weins, J. (2014). Concepts and context: In Hiestand and W. Jesse Weins (ed.), *Sexting and youth: A multidisciplinary examination of research, theory and law*. Carolina Academic Press.

Woodlock, D. (2014). Technology-assisted stalking: Findings and research from the Smartsafe project Domestic Violence Resource Centre Victoria, Collingwood.

Worthen, M. (2016). *Sexual deviance and society: A sociological examination*. Routledge.

Karen Holt is an Assistant Professor in the School of Criminal Justice at Michigan State University. Broadly, her research focuses on sexual deviance and sexual offending. Her work has been published in *Sexual Abuse: A Journal of Research and Treatment, Violence and Victims,* and *Deviant Behavior*. Dr. Holt is the faculty adviser for S.T.R.I.V.E., a mentorship program that works with juveniles who commit sexual offenses.