SOCIOLOGICAL ASPECTS OF CYBERCRIME AND HACKING

by Greg S. Weaver
Department of Sociology, Anthropology, and Social Work
Auburn University

INTRODUCTION

Cyber is simultaneously a "place" and a tool that has become an increasingly important part of our identity. Its impact on the average person and his or her social relations cannot be understated. The typical smart-phone, essentially a hand-held computer, can be used for communication and a host of other activities such as online purchasing. Having the latest iPhone has become a status symbol of sorts. The advent and popularity of social media such as Facebook has influenced the definition of what constitutes a "friend." These examples reflect how the typical individual is increasingly reliant upon computer technology and the accessibility and convenience it affords; however, at the same time he or she is more fearful of that technology (Thomas, 2013, p. vii). We knowingly provide personal, financial, and medical information while supposedly being aware of the risks of doing so. To the extent the potential exists to capture, store, and redistribute personal data – particularly when coupled with increased video and electronic surveillance – it is not out of the question to suggest that computer technology is increasingly becoming a means of social control, given the extent of the potential to capture, store, and redistribute personal data – particularly when coupled with increased video

[1] Thomas Rid, *Cyber War Will Not Take Place*, (London: Oxford University Press, 2013), vii.

Formatted: Title, Left, Add space between paragraphs of the same style

Formatted: Font: Italic

Formatted: Left

Formatted: Space After: 0 pt, Don't add space between paragraphs of the same style

Formatted: Not Superscript/ Subscript

and electronic surveillance (Duff & Gardiner, ~~2~~1996, p. 212). At the same ~~time~~time, we are increasingly at risk of the cybercriminal (Hunton~~3~~, 2012, p. 201).

There are many typologies and categories of cybercrime, and there is lack of consensus in terms of what type(s) of acts constitute it. Some offenses have occurred long prior to the advent of computer technology, whereas others would not be possible apart from it (Yar~~4~~, 2013, p. 9). Cybercrime encompasses much more than simply using a computer to commit a crime or being able to do so more efficiently. Types of cybercrime vary based on intent, means, and opportunity, and include crimes against the person, production and distribution of illicit (sexual) material, financial crimes, computer misuse, intellectual property theft, and industrial espionage. Furthermore, these offenses are continuously evolving in relation to technology and are contained within what can be thought of as a cybercrime ecosystem, which includes many legitimate businesses and enterprises along with the criminal justice system and offenders (Kraemer-Mbula, Tang, & Rush~~5~~, 2013, p. 543). Cybercrime has evolved from the stereotypical hacker to organized crime networks that mirror legitimate enterprises (Hunton, 2012, ~~6~~p. 203). It is here where one can observe how cybercrime may begin to "touch" elements of ~~the~~ critical infrastructure (e.g. utilities, transportation, public health, etc.), thereby situating it within the somewhat clouded yet overlapping boundaries associated with crime, ~~inal versus terrorism~~terrorism, and ~~versus~~ national security interests.

Commented [J1]: AQ: I rearranged the sentence here; do you like the flow of this sentence?

Formatted: Not Superscript/ Subscript

Formatted: Not Superscript/ Subscript

Formatted: Not Superscript/ Subscript

Formatted: Not Superscript/ Subscript

Formatted: Not Superscript/ Subscript

[2] Liz Duff and Simon Gardiner, "Computer Crime in the Global Village: Strategies for Control and Regulation – in Defence of the Hacker." *International Journal of the Sociology of Law* 24 (1996):212.
[3] Paul Hunton, "Data Attack of the Cybercriminal: Investigating the Digital Currency of Cybercrime." *Computer Law and Security Review* 28, (2012): 201.

[4] Majid Yar. *Cybercrime and Society* (Thousand Oaks CA, 2013), 9.
[5] Erika Kraemer-Mbula, Puay Tang, and Howard Rush, "The Cybercrime Ecosystem: Online Innovation in the Shadows?" *Technological Forecasting and Social Change* 80 (2013): 543.
[6] Hunton (2012): 203.

~~Within the larger framework of cybercrime, T~~this essay focuses on one category within the larger framework of cybercrime – hacking – and particularly upon ~~the~~ its social aspects ~~of it~~. ~~In doing so, the~~The definition and context of hacking will be explored from a sociological perspective. In the early 1990s it was suggested that advances in computer security capabilities would render hacking obsolete, even though access to and use of computers would greatly expand (Hoath & Mulhall,~~7~~ 1998, p. 16). To borrow the catchphrase of a well-known sports commentator: "Not so fast..." Today, it is not uncommon for hacking to be referred to as an epidemic.~~8~~ (Xu, Hu, & Zhang, 2013, p. 64). These sentiments reflect important elements of the complex relationship between individuals (and for that matter, societies) with technology.

WHAT IS HACKING?

In the simplest of terms, hacking can be thought of as gaining unauthorized access to a computer or a computer system (Jordan & Taylor, 1998, p. 759).~~9~~ Gaining access to a computer (or a computer system or network) ~~is to~~ demonstrates talent and expertise, even though the hack may consist of nothing more than guessing the password of another individual. For the hacker, unauthorized access does not necessarily mean it is illegitimate;~~10~~ ~~h~~However, hacking – regardless of motivation – is generally considered to be a legal concern (Duff & Gardiner, 1996, p. 215; ~~11~~Yar, 2013, p. 23).

To better understand the phenomenon and dynamics of hacking, it seems reasonable to rely on a sociological axiom, the Thomas Theorem, which basically states that whatever is

~~[7] Cited in Peter Hoath and Tom Mulhall, "Hacking: Motivation and Deterrence, Part I." *Computer Fraud & Security* 1998 Issue 4 (1998): 16.~~
~~[8] Zhengchuan Xu, Qing Hu, and Chenghong Zhang, "Why Computer Talents Become Computer Hackers." *Communications of the ACM* 56 Issue 4 (2013): 64.~~
~~Zhengchuan Xu, Qing Hu, and Chenghong Zhang, "Why Computer Talents Become Computer Hackers." *Communications of the ACM* 56 Issue 4 (2013): 64.~~
~~013), 23.~~

Commented [J2]: AQ: I think we can delete this sentence, and jump right into the discussion of hacking.

Formatted: Not Superscript/ Subscript

Commented [J3]: We should probably cite this quote, or just delete the sentence. I do appreciate the style it adds, though.

Formatted: Not Superscript/ Subscript

Formatted: Heading 1, Line spacing: single

Formatted: Space After: 0 pt, Don't add space between paragraphs of the same style

Formatted: Not Superscript/ Subscript

Commented [J4]: AQ: Is this last piece necessary? It may come across as a bit redundant.

Formatted: Not Superscript/ Subscript

Formatted: Not Superscript/ Subscript

defined as true and real becomes real in its consequences. At the same time, shifts in these definitions result in changes in attitudes and behavior (Collins, 1985, p. 199).[12] In this context, changes in the nature and consequences of hacking are most interesting. Is hacking harmless fun; a way to support a cause; criminal behavior; a tactic of terrorism; or possibly even an act of war? Depending on the situation and who is asked, in each instance the answer could be "yes." Similarly, many are familiar with the hacking group Anonymous, if for no other reason than the imagery and symbolism associated with the Guy Fawkes mask. Are the actions of Anonymous "hacktivism" – activism employing computer technology – or are they criminal? Again, the answer to this question depends on a number of considerations.

The definitions of – as well as the individual and collective reactions to – cybercrime and hacking cannot be understood separately from the socially created and negotiated meanings attached to them. In this sense, cybercrime and hacking are social constructs (Yar, 2013, p. 23).[13] Whereas hacking was originally viewed in the broadest sense of exploration, open access to information, identifying new and innovative ways to use technology, etc., today the term is almost synonymous with deviant or criminal activity. This evolution possibly reflects the increased emphasis on how technology can be misused, recognizing that "computers and the Internet now serve as the backbone for virtually all facets of modern life" (Holt & Bossler, 2014, p. 20)."[14]

EVOLUTION OF HACKING

The definition of what constitutes hacking has evolved over time. Depending on the period, hackers have been viewed as being part of a legitimate profession, a cowboy of sorts on

[12] Randall Collins. *Three Sociological Traditions* (London: Oxford University Press, 1985), 199.
[13] Yar (2013), 23.
[14] Thomas J. Holt and Adam M. Bossler, "An Assessment of the Current State of Cybercrime Scholarship." *Deviant Behavior* 35 (2014):20.

Formatted: Not Superscript/ Subscript

Formatted: Not Superscript/ Subscript

Formatted: Not Superscript/ Subscript

Formatted: Heading 1, Line spacing: single

Formatted: Space After: 0 pt, Don't add space between paragraphs of the same style

the cyber ~~"~~frontier~~"~~, a mischievous yet intellectual joyrider or vandal, or a criminal. In recent years, the notion of the hacker as a criminal has expanded even further to include terrorism and national security. While it is true that a new generation of hackers follows every generation of computers~~15~~, we must be cautious of allowing the emphasis on technology to cloud our recognition of the social aspects of hacking, particularly the relationships between offenders, victims, and targets (Chandler, 1996, p. 230; ~~-~~Yar, 2013, p. 10).~~16~~

Formatted: Not Superscript/ Subscript

Formatted: Not Superscript/ Subscript

The first generation of hackers (until the 1970s) viewed their craft as both a passion and a profession fueled by the desire to learn as much as possible about computers, stretching them to their limits and also identifying new and innovative uses of computer technology. At the most basic level, hacking was defined as using a device or apparatus for any reason other than for which it was intended. The ethos of this generation included the ideas that information should be freely shared and that hacking should cause no harm. This generation contributed to the development of the personal computer, which signals the onset of the second generation of hackers. During the second~~is~~ generation~~period~~ (1980s), hackers and hacking were~~a~~re associated with themes of the 1960s counterculture, espousing the power and liberating potential of computer technology. The late Steve Jobs and Stephen Wozniak, developers of the Apple computer, are considered among this group.

It is with the third generation (1990s) that hackers began~~i~~n to be viewed in deviant/criminal terms. Typically, hacking was viewed as a form of online mischief, with terms such as "intellectual joyrider" used to describe these activities. The fourth generation of hacking (2000 to present) is characterized primarily by the idea that the activity is deviant or criminal. In

~~[15] Amanda Chandler, "The Changing Definition and Image of Hackers in Popular Discourse," *International Journal of the Sociology of Law* 24 (1996): 230.~~
~~[16] Yar (2013), 10.~~

this era the economic, political, and even religious aspects of motivation and intent are even more pronounced (Yar, 2013, p. 229-232; Heinsbroek, 2012, p. 6).[17]

HACKERS AND THEIR ACCOUNTS

For some, the term hacker brings to mind the Lisbeth Salander character in the novels of the late Stieg Larsson. The stereotypical imagery of the young, socially awkward and loner cyberpunk notwithstanding, the overwhelming majority of hackers are male. While a hacker may typically act alone,[18] hacking is first and foremost a social activity (Holt, Strumsky, Smirnova, & Kilger, 2012, p. 12; Vainio & Vadén, 2007, p. 2).[19] Hacking is a young person's "game," in part because of their greater familiarity with using computers. They frequently report becoming involved at a relatively young age (teenage years) and begin to develop associations with others at school or through online communities. One author suggests that hackers are "the middle class equivalent to the street gang." (Duff & Gardiner, 1996, p. 216).[20] Hacker forums and similar groups also serve as a repository of information. Generally speaking, formal training and academic credentials are not valued in this community. While many of the tools are available to anyone with a computer and access to the Internet,[21] expertise and status within the group is based in large part on demonstrating one's skill via the hack (Yar, 2013, p. 33). Not surprisingly, the largest portion of hackers possess little skill (relative to peers), but the relatively small percentage of highly skilled individuals pose the greatest threat, and

[17] Ibid, 229-232. See also T.L.P. Heinsbroek. *Hacking Revealed*, ver. 2.1, (Maasland, Netherlands: SeKuRiGo, 2012):6.
[18] Thomas J. Holt, Deborah Strumsky, Olga Smirnova, and Max Kilger, "Examining the Social Networks of Malware Writers and Hackers." *International Journal of Cyber Criminology* 6, no. 1, (2012):12.
[19] Niklas Vainio and Tere Vaden, "Free Software Philosophy and Open Source," in *Handbook of Research on Open Source Software: Technological, Economic, and Social Perspectives* (2007):2.
[20] Duff and Gardiner (1996): 216.
[21] Yar (2013), 33.

Formatted: Not Superscript/ Subscript
Formatted: Heading 1, Line spacing: single
Formatted: Space After: 0 pt, Don't add space between paragraphs of the same style
Formatted: Not Superscript/ Subscript
Formatted: Not Superscript/ Subscript
Formatted: Not Superscript/ Subscript
Formatted: Not Superscript/ Subscript

sometimes utilize the assistance (knowingly or unknowingly) of other hackers (Holt & Kilger, 2012, p. 892-893).[22]

An intriguing relationship exists between hackers and businesses, organizations, agencies, and the computer security industry. It is in many ways antagonistic, but not exclusively so. A business or organization may want to utilize the innovative talents of a hacker (hopefully for legitimate purposes) but at the same time recognize the inherent risks of doing so. A major source of validation for hackers comes from those entities charged with thwarting the hack. Furthermore, some hackers could be described as "wannabes," in that they desire to become part of the computer security industry. In this sense, hacking provides evidence of skills and expertise, and also identifies problems and security flaws that should be addressed. These elements help in understanding the white/gray/black hat distinction among hackers, which characterizes the nature of hacking based on intent, motivation, and possible harm. Interestingly, Microsoft periodically sponsors "blue hat" colloquia to bring together high level company employees with prominent hackers (Auray & Kaminsky, 2007 p. 1313-1319).[23] Of course, one must wonder if hackers consider the implications of their activities when viewed in the context of, for example, obtaining a security clearance, or the consequences of arrest/conviction on employment. While anecdotal, this author has heard more than one law enforcement professional lament that some of the most qualified persons could never be hired by their agency (Jordan & Taylor, 1998, p. 770).[24]

ACCOUNTS OF HACKERS

[22] Thomas J. Holt and Max Kilger, "Know Your Enemy: The Social Dynamics of Hacking." Honeynet Project KYE Paper (2012): 4; Holt et al. (2012):892-3.
[23] Auray and Kaminski (2007): 1313-1319.
[24] Jordan and Taylor (2012):770.

Formatted: Not Superscript/ Subscript

Commented [J5]: AQ: The wording here is a bit unclear to me. Maybe we could focus on the idea that hackers feel validated knowing that entities are charged with thwarting?

Formatted: Not Superscript/ Subscript

Formatted: Not Superscript/ Subscript

Formatted: Heading 1, Line spacing: single

As previously discussed, hacking was not originally considered criminal. Skilled hackers are generally thought of as celebrities within their communities and to a lesser extent, in society-at-large. However, in recent years, this external perception has changed somewhat, in part a consequence of the criminalization of hacking and through negative media portrayals of individuals and groups associated with high profile incidents. Hackers continue to get support from within, but how do they justify their actions to a public who tends to view them in an increasingly negative manner? On one hand, they tend to view the benefits (success, recognition, monetary, political, religious, etc.) as exceeding the potential consequences, namely the low likelihood of being caught and subsequently punished. Hackers also employ a number of justifications to distance themselves from the negative consequences of their actions. For example, the notion that information should be freely available is well established in the hacker community. Also, some offenders engage in a form of victim blaming, suggesting that targets should improve security if they want to avoid being hacked (Young, Zhang, & Prybutok, 2007, p. 284).~~[25]~~

This example illustrates the "account," a statement or claim that is used to explain unanticipated or undesirable behavior. The study of accounts provides a better understanding of the culture and community associated with hacking (Turgemon-Goldschmidt, 2005, p. 10).~~[26]~~ The following table outlines common hacker accounts, which will then be described below.

ACCOUNT	JUSTIFICATION

~~[25] Randall Young, Lixuan Zhang, and Victor R. Prybutok, "Hacking into the Minds of Hackers." *Information Systems Management* 24 (2007):284.~~

~~[26] Orly Turgeman-Goldschmidt, "Hackers Accounts: Hacking as Social Entertainment." *Social Science Computer Review* 23, no. 1, (2005): 10.~~

Formatted: Space After: 0 pt, Don't add space between paragraphs of the same style

Formatted: Not Superscript/ Subscript

Commented [J6]: Changed from italics to quotes to follow the Auburn Speaks Style Guide

Formatted: Font: Not Italic

Formatted: Not Superscript/ Subscript

Formatted: Left

Fun and Excitement	Accomplishment Thrill of Risky Activities
Curiosity	Information and Knowledge
Virtuosity	Power/Dominance Over Machines and People
Economic	Monetary Gain or to Harm Target
Deterrence	Benefits Exceed Costs Low Likelihood (perceived) of Being Caught
No Malicious Intent	No Real Victim No Intent to Harm "No Harm -No Problem"

Formatted Table

Intangible	No Real Damage Information Is Not a Commodity
Curiosity	Discover and Obtain Unknown or Confidential Information
Revenge	Mischief Right a Perceived Wrong
Ease (of completing hack)	Infrequent (Diminishes Perceived Skill)

Table 1 (Turgemon-Goldschmidt, 2005, p. 12-18)

~~Source: Turgeman-Goldschmidt (2005): 12-18.~~

Fun, thrill, and excitement are the primary motivating factors and provide the basis for all other accounts. Typically, the hacker contends that he or she gains unauthorized access to a computer or computer system in order to show others that he or she can do so, not necessarily to disrupt, alter, or to copy or remove information. It should be clear how these accounts reflect key elements of the hacker culture. For the hacker, free inquiry and freedom of information is paramount. Information or data is not a commodity that can be owned, therefore accessing or copying it does not constitute theft. This "no harm, no foul" mentality falls in stark contrast to

Commented [J7]: AQ: Is this capitalized in the original source. Checking for consistency with the others here.

Formatted: Keep with next

Formatted: Font: (Default) Times New Roman, 12 pt, Not Italic, Font color: Auto

Formatted: Caption, Centered, Line spacing: single

Formatted: Font: (Default) Times New Roman, 12 pt, Not Italic, Font color: Auto

Formatted: Font: (Default) Times New Roman, 12 pt, Not Italic, Font color: Auto

Formatted: Space After: 0 pt, Don't add space between paragraphs of the same style

the characterization of hacking as criminal behavior. From the perspective of law enforcement, business, and the computer security industry, motivation is irrelevant. Any unauthorized access is problematic.

Hacker accounts also reflect an assessment of the perceived costs and benefits of a course of action, but do so in a broader sense that is not limited to financial gains and losses. Economic motivation typically plays a secondary role, even when the hacker realizes his or her actions will result in the target experiencing a financial loss. Economic-oriented accounts also tend to focus on the rationale that knowledge and information is not a commodity to be owned. Expressing the "hit them where it hurts…" mentality, the potential or real loss to the hacking target is given priority over financial gain for the hacker. In terms to potential costs or consequences of their actions, hackers recognize that the potential for being caught does exist but conclude it is an unlikely outcome (Turgemon-Goldschmidt, 2005, p. 12-18).~~[27]~~

Overall, these categories of accounts allow the hacker to distance him- or herself from the criminal label and also to emphasize values or positive attributes, such as virtuosity, curiosity, happiness, and the desire to seek knowledge (Turgemon-Goldschmidt, 2005, p. 12-21).~~[28]~~ Because these attributes are generally viewed as positive, hackers frequently incorporate them in rationalizing deviant or criminal behavior. At the same time, these accounts provide evidence for the idea that for the hacker, hacking is a form of play or entertainment. Similar to the typical adolescent or teenager, these examples reflect a desire to test social boundaries (Yar, 2013, p. 34).~~[29]~~

CONCLUDING REMARKS

~~[27] Turgeman-GoldSchmidt (2005): 12-18.~~
~~[28] Ibid, 12-21.~~
~~[29] Yar (2013), 34.~~

Formatted: Not Superscript/ Subscript

Formatted: Not Superscript/ Subscript

Formatted: Not Superscript/ Subscript

Formatted: Not Superscript/ Subscript

Formatted: Heading 1, Line spacing: single

The previous discussion shows how the relationship between individuals, technology, and society is no doubt a complex one. As we ~~utilize~~ use and become even more dependent upon computer technology, the potential for cybercrime and related activities increases as well. What is defined as cybercrime and hacking is a social construction and reveals that regardless of the stated motivations, intent, and accounts of hackers, the definitions of the behavior as well as the social responses to it are overwhelmingly couched in terms of hacking as a form of criminal activity. Consequently, it begs the question of whether the legal system is best equipped to address this issue. Technology advances at a faster pace than does the law and as part of a bureaucracy, law enforcement is reactive and continually playing "~~"~~catch up" to potential and actual threats. Interestingly, some authors draw from one of the previously discussed hacker accounts to suggest that non-legal approaches are more important, namely that potential targets should bear a greater responsibility for securing information and systems (Duff & Gardiner, 1996, p. 226).~~,30~~

~~30 Duff and Gardiner (1996): 226~~

Formatted: Space After: 0 pt, Don't add space between paragraphs of the same style

Commented [J8]: Edited to follow Auburn Speaks Style Guide

Commented [J9]: edited to follow Auburn Speaks Style Guide

Formatted: Not Superscript/ Subscript

References

Auray, Nicolas and Kaminsky, Danielle. "The Professionalization Paths of Hackers in IT Security: The Sociology of a Divided Identity." *Annales Des Télécommunications* 62 (2007): 1312-1326.

Chandler, Amanda. "The Changing Definition and Image of Hackers in Popular Discourse." *International Journal of the Sociology of Law* 24 (1996): 229-251.

Collins, Randall. *Three Sociological Traditions*. New York: Oxford University Press, 1985.

Duff, Liz and Gardiner, Simon. "Computer Crime in the Global Village: Strategies for Control And Regulation in Defence of the Hacker." *International Journal of the Sociology of Law* 26 (1996): 211-228.

Heinsbroek, T.L.P. *Hacking Revealed*. Ver. 2.1. Maasland, Netherlands: SeKuRiGo, 2012. http://www.sekurigo.nl/uploads/1/3/7/9/13790882/hacking_revealed_versie_2.1_uk.pdf

Hoath, Peter and Mulhall, Tom. "Hacking: Motivation and Deterrence, Part I." *Computer Fraud & Security* 1998, no. 4 (1998): 16-19.

Holt, Thomas J. and Bossler, Adam M. "An Assessment of the Current State of Cybercrime Scholarship." *Deviant Behavior* 35 (2014): 20-40.

Holt, Thomas J. and Kilger, Max. "Know Your Enemy: The Social Dynamics of Hacking." Honeynet Project KYE Paper (2012).

Holt, Thomas J., Strumsky, Deborah, Smirnova, Olga, and Kilger, Max. "Examining the Social Networks of Malware Writers and Hackers." *International Journal of Cyber Criminology* 6, no. 1 (2012): 891-903.

Hunton, Paul. "Data Attack of the Cybercriminal: Investigating the Digital Currency of Cybercrime." *Computer Law and Security Review* 28 (2012): 201-207.

Jordan, Tim and Taylor Paul. "A Sociology of Hackers." *The Sociological Review* 24, no. 4 (1998): 757-780.

Kraemer-Mbula, Erika, Tang, Puay, and Rush, Howard. "The Cybercrime Ecosystem: Online Innovation in the Shadows?" *Technological Forecasting and Social Change* 80 (2013): 541-555.

Rid, Thomas. *Cyber War Will Not Take Place*. London: Oxford University Press, 2013.

Turgemon-Goldschmidt, Orly. "Hackers' Accounts: Hacking as a Social Entertainment." *Social Science Computer Review* 23, no. 1 (2005): 8-23.

Formatted: Tab stops: 0.19", Left

~~Vanio, Niklas and Vadén, Tere. "Free Software Philosophy and Open Source," in *Handbook of Research on Open Source Software: Technological, Economic, and Social Perspectives*, edited by Kirk St. Amand and Brian Still, 1-11. Hershey NY: Information Science Reference, 2007.~~

~~Yar, Majid. *Cybercrime and Society*. 2nd ed. Thousand Oaks CA: Sage, 2013.~~

~~Young, Randall, Zhang, Lixuan, and Prybutok, Victor R. "Hacking into the Minds of Hackers." *Information Systems Management* 24 (2007): 281-7.~~

~~Xu, Zhengchuan, Hu, QAing, and Zhang, Chenghong. "Why Computer Talents Become Computer Hackers." *Communications of the ACM* 56, no. 4 (2013): 64-74.~~

WORKS CITED

Auray, N., & Kaminsky, D. (2007). The Professionalization Paths of Hackers in IT Security: The Sociology of a Divided Identity. *Annales Des Télécommunications*, *62*, 1312-1326.

Chandler, A. (1996). The Changing Definition and Image of Hackers in Popular Discourse. *International Journal of the Sociology of Law*, *24*, 229-251.

Collins, R. (1985). *Three Sociological Traditions.* New York: Oxford University Press.

Duff, L., & Gardiner, S. (1996). Computer Crime in the Global Village: Strategies for Control And Regulation – in Defence of the Hacker. *International Journal of the Sociology of Law*, *26*, 211-228.

Heinsbroek, T. (2012). *Hacking Revealed.* Retrieved from SeKuRiGo: http://www.sekurigo.nl/uploads/1/3/7/9/13790882/hacking_revealed_versie_2.1_uk.pdf

Hoath, P., & Mulhall, T. (1998). Hacking: Motivation and Deterrence, Part I. *Computer Fraud & Security 1998*, *4*, 16-19.

Holt, T. J., & Bossler, A. M. (2014). An Assessment of the Current State of Cybercrime Scholarship. *Deviant Behavior*, *35*, 20-40.

Holt, T. J., & Kilger, M. (2012). Know Your Enemy: The Social Dynamics of Hacking. *Honeynet Project KYE Paper*.

Holt, T. J., Strumsky, D., Smirnova, O., & Kilger, M. (2012). Examining the Social Networks of Malware Writers and Hackers. *International Journal of Cyber Criminology*, *6*(1), 891-903.

Hunton, P. (2012). Data Attack of the Cybercriminal: Investigating the Digital Currency of Cybercrime. *Computer Law and Security Review*, *28*, 201-207.

Jordan, T., & Taylor, P. (1998). A Sociology of Hackers. *The Sociological Review*, *24*(4), 757-780.

Formatted: Tab stops: 0.19", Left

Formatted: Not Superscript/ Subscript

Formatted: Font: (Default) Times New Roman, 12 pt

Kraemer-Mbula, E., Tang, P., & Rush, H. (2013). The Cybercrime Ecosystem: Online Innovation in the Shadows? *Technological Forecasting and Social Change, 80*, 541-555.

Rid, T. (2013). *Cyber War Will Not Take Place*. London: Oxford University Press.

Turgemon-Goldschmidt, O. (2005). Hackers' Accounts: Hacking as a Social Entertainment. *Social Science Computer Review, 23*(1), 8-23.

Vainio, N., & Vadén, T. (2007). Free Software Philosophy and Open Source. In K. St. Amand, & B. Still (Eds.), *Handbook of Research on Open Source Software: Technological, Economic, and Social Perspectives* (pp. 1-11). Hershey, New York: Information Science Reference.

Xu, Z. H. (2013). Why Computer Talents Become Computer Hackers. *Communications of the ACM, 56*(4), 64-74.

Yar, M. (2013). *Cybercrime and Society* (2nd ed.). Thousand Oaks, California: Sage.

Young, R., Zhang, L., & Prybutok, V. R. (2007). Hacking into the Minds of Hackers. *Information Systems Management, 24*, 281-287.

Formatted: Font: (Default) Times New Roman, 12 pt

Formatted: List Paragraph, Indent: Left: 0.19", Space After: 12 pt, Add space between paragraphs of the same style