Why Hackers Become Crackers

– An Analysis of Conflicts Faced by Hackers

Boyu Guo[1]

[1] WHBC of Wuhan Foreign Languages School, Wuhan, Hubei, China

Correspondence: Boyu Guo, WHBC of Wuhan Foreign Languages School, Wuhan, Hubei, China. Tel: 86-130-0719-4068. E-mail: BoyuGuo@outlook.com

Received: December 15, 2015 Accepted: January 22, 2016 Online Published: April 28, 2016
doi:10.5539/par.v5n1p29 URL: http://dx.doi.org/10.5539/par.v5n1p29

Abstract

Hacker culture is generally regarded as a subculture, and the public has a high degree of misunderstanding towards hackers. The media reports sometimes depict hackers overly negatively, possibly because hackers could gain a dominant position in the age of information and, therefore, threaten the existing balance of social power distribution. Moreover, those reports, whether intentionally or not, misunderstand the meaning of “hackers”: “Hackers” are people who want to identify and solve problems directly and effectively, but “crackers” are those who cause problems for society.

However, it is not merely a problem of media’s misnomer. This research shows that apart from the media distortion of hacker identity, even the hackers with positive intentions still have real potential to become crackers. Therefore, the aim of this paper is to understand why the transition from “hackers” to “crackers” takes place by identifying crucial factors that influence hackers’ behaviors. Specifically, the inherent conflicts between cyberspace and the real world can turn hackers into crackers. Through the research, two major conflicts are identified: the conflict between freedom and responsibility and the conflict between individuality and authority. To support the arguments, the history of hacker culture and specific cases of hacking events are studied and discussed. The research also brings a crucial issue: how do we co-exist with information technology in a society that is increasingly computerized and digitalized? To face this problem, we need to comprehensively understand situations faced by human civilization in the information era. Hacker culture is, therefore, a practical perspective of studying social transformations in the development of technology.

Keywords: hacker, cracker, hacker culture

1. How the Media Depicts Hackers

Computerization’s enormous capacity for interaction allows different users, from online gamers to professional programmers, to create their own virtual space beyond physical restrictions. Just like actual society, cyberspace has a high degree of complexity;[1] the diverse interpersonal relationships of cyberspace users, the multiple identities of an individual user,[2] the different patterns of logic employed by users with various backgrounds and the imbalanced degrees of IT know-how lead to a huge disparity among cyberspace groups of users. Among all of them, one of the most special groups is hackers.

Nowadays, many people might have difficulty answering this question: who are hackers? Are they the targets of Operation Sundevil (a nationwide United States Secret Service crackdown on "illegal computer hacking activities" in 1990),[3] the arrogant and zealous computer nerds in hacker movies,[4] or the Chinese Honker union which launched attacks on other countries' networks for patriotic reasons?[5] It seems like media has presented hackers in various but uniformly negative ways, depicting them as dreadful dangers to national security, self-important eggheads or global terrorists (Halbert 361).[6] News reporters employ slanderous narratives when

[1] For more information about complexity of cyberspace’s formation, see “The Hacker's Challenge: Active Access to Information, Visceral Democracy and Discursive Practice” P269 by Kirsty.

[2] For more information about identity, see “‘Education in Disguise’: Culture of a Hacker and Maker Space” by Schrock.

[3] For more information about Operation Sundevil, see http://www.sjgames.com/SS/topten.html.

describing hackers because many societal groups in the real world, including the public, firms and the government, feel greatly threatened by hackers. Even though IT knowledge, programming skills and technical knacks ensure the dominant power of hackers in and only in virtual space, the potential damage to real society can be tremendous because almost everything in the information age is digitalized, or computerized .[7] The digital space is no longer merely a derivation of the physical world. Rather, it has become so ubiquitous that modern society relies heavily on it in order to function. Hence, people ask for greater protection from "shrewd" hackers who can get access to their possessions and violate their privacy more and more easily.[8]

The sensationalism of the media also reflects increasing alarm towards Internet security, because the development of media is always in pace with the changing informational platforms.[9] Nowadays, while chasing the exploding speed of digitalization, media itself is undergoing a profound shift in its original definition—from "media" to "new media." Even though we are just experiencing the initial effects of computerization, unlike other effects of changes in platforms, "the computer media revolution affects all stages of communication, including acquisition, manipulation, storage, and distribution; it also affects all types of media—texts, still images, moving images, sound, and special constructions (Manovich 19)." The opinions expressed through media platforms represent not only public concerns but also those of media corporations. The notorious DDoS attack in July 2009, launched by unknown hackers, shows the vulnerability of Internet-based media platforms:

> The websites of South Korea's largest daily newspaper, a large-scale online auction house, a bank, the country's president, the White House, the Pentagon and U.S. Forces Korea—to name a few—came under DDoS attack as upwards of 166,000 computers in a botnet unleashed wave after wave after wave of a data-powered onslaught. Some believed operatives at North Korea's telecommunications ministry were to blame, using a backdoor for the infamous Mydoom worm of 2004, but this has never been proven (stealtheworld.html).

The control over information and computer technology foster hackers' pride and passion. The mass media and the general public also help to maintain the vitality of hacker culture to some extent, even promoting refreshing features that sometimes greatly inspire hackers with new excitement. For instance, "in the early to mid-1990s, cyberspace was marked as a heterotopia of compensation—as space for economic, social, or sexual redress (Wendy Chun, 245)." In the turbulent and uncertain periods of social reform, hackers' potential for creating and renovating is fully released; a strong sense of mission drives them to participate in the information revolution through cyberspace .[10] Although the relationship between hacking and crime is controversial, hacker activity can be very hard to categorize as "subversive" or "progressive." Despite the myriad mainstream reports of tremendous financial loss and the destructive aftermath for the companies being hacked, cases related to the protection of human rights by hackers also prevailed:

> Hacking becomes most overtly politicized when hackers join coordinated political action in groups, integrating their distilled democratic sentiments with their technological skill-set. Recent examples include hacking interventions in relation to human rights violations in Kosovo and China, as well as ongoing pressure from the hacker-founded Electronic Freedom Frontier on American Internet-related policy, such as overthrowing the Communications Decency Act. Here, hackers move beyond the mere signification of resistance to actual political practice, thereby reaching out to wrap hacking around democracy through the facility of technology (Best 263).

With contingency, randomness, diversity and entertainment replacing inevitability, determinacy, homogeny and seriousness, the trend of "informationizing society" and "symbolizing knowledge" of this century coincides with hackers' passion for constructing a community where information sharing is as easy and free as possible. [11] However, if both hacker ethics and the Internet age spirit have positive and social-friendly aims, what can

[4] For more discussion, see "Education in Disguise: Culture of a Hacker and Maker Space" P11 by Schrock.

[5] For more information about the Honker Union, see http://news.bbc.co.uk/2/hi/science/nature/1306591.stm.

[6] For more about media behaviors, see "Discourses of Danger and the Computer Hacker" by Halbert.

[7] For more about the trend of digitalization, see "More Than a Mouse Trap: Effective Business Models in a Digital World" P42 on International Journal of Media Management by Lawson.

[8] For more about media report, see "Discourses of Danger and the Computer Hacker" P363 by Halbert.

[9] For more explanation of "the development of media is always in pace with the changing of information platforms", see *The Language of New Media* P19 by Manovich.

[10] For more explanation of "heterotopia of compensation", see "Othering Space" P245 by Wendy.

[11] For more about information sharing, diversity and anti-tradition, see "Education in Disguise: Culture of a Hacker and Maker Space" P4 by Schrock.

account for all of the destruction caused by hackers? What can explain the increase in both the seriousness and quantity of Internet crimes?

2. Who Are the Hackers and Crackers

If demonized images of hackers proliferate through the media, how, then, do hackers identify themselves? According to Pekka Himanen, the following qualities characterize "the hacker ethic and the spirit of the information age":

- enthusiastic about this interesting thing
- passionate relationship to work
- wish to share one's skills with a community having common goals (nytimes.com)

It is worth emphasizing that once the concept "hacker" refers to any group of people who have the same characteristics named above, the array of hackers might be too large to study. The following discussion will be focused narrowly on hackers in cyberspace, whose culture nourishes itself from the rapid, exciting, intellectual history of technology development.

Another crucial qualification is the terminology of "hackers" and "crackers." Pekka Himanen briefly states the difference between hackers and crackers in the preface of The Hacker Ethic and The Spirit of Information Age:[12]

> …passionate programmers started calling themselves hackers in the early sixties. Later, in the mid-eighties, the media started applying the term to computer criminals. In order to avoid the confusion with virus writers and intruders into information systems, hackers began calling these destructive computer users crackers (Pekka Himanen Preface Viii.) …

Furthermore, Eric Raymond states hackers' opinion to crackers: [13]

> 'Real hackers call these people "crackers" and want nothing to do with them ... being able to break security doesn't make you a hacker any more than being able to hotwire cars makes you an automotive engineer' (Raymond 1996) …Moreover, many new school hackers would contend that a hacker who engages in criminal acts 'ceases being a hacker and commences being a criminal' (Best 266).

Indeed, hackers can be differentiated from crackers by their intentions. Hackers are building; crackers are breaking. Even though news reports generally fail to specify the difference, they refer to crackers instead of hackers when describing the criminals. However, the subject of this essay is hackers who might become crackers even without negative motivations. This essay is aimed to explore several internal and external causes for hackers to become crackers in a transformative media context.

3. Freedom Without Responsibility

This section will explain "why hackers become crackers" in terms of the unique relationship between hackers' freedom and their responsibility. Before the discussion begins, it is important to clarify the standard used to evaluate "freedom and responsibility" in hackers' behaviors. Jean-Paul Sartre has defined the relationship between freedom and responsibility in the following way:

> Another aspect of existential freedom is that one can change one's values. Thus, one is responsible for one's values, regardless of society's values. … The relationship between freedom and responsibility is one of interdependency, and a clarification of freedom also clarifies that for which one is responsible (stanford.edu).

This view can be applied as a criterion to study some problematic phenomena when people are interacting with each other in virtual space. Because cyberspace preserves anonymity, users perceive that they are "free" and perhaps not responsible for their actions.[14] The imbalance between personal freedom and responsibility is allowed in cyberspace but not so much in reality, where laws and regulations assign people obligations. Therefore, hackers might escape the consequences of their actions. The hacker spirit guarantees hackers' freedom by treating free information access and free opinion discussion as gifts of carrying out hackers' duties in the virtual world.[15] To fully explain this point, I will start by elaborating the origin of hackers' freedom, followed by the identification of potential elements that could become Internet crimes, and will end by explaining how the

[12] For more about hacker culture, see "The Hacker Ethic and the Spirit of the Information Age" by Himanen.

[13] For more about hackers' attitude towards crackers, see "The Hacker's Challenge: Active Access to Information, Visceral Democracy and Discursive Practice" P266 by Best.

transition from hackers to crackers takes place.

By refusing to become a part of society's assembly line, hackers prefer to stand outside of social restrictions and maximize their personal freedom in cyberspace. Between 1980 and 2000, hacker activists, like Richard Stallman, wrote a series of manifestos to support software sharing and freedom of programming: GNU ("GNU's Not Unix!") and Free Software Foundation (FSF) in 1985, GNU General Public License (GNU GPL or GPL) in 1989, etc. As every hacker can operate, revise, reproduce and release codes without restrictions, freedom of cyberspace is expanded to benefit those common users of the amended software, which should be among the hackers' foremost concerns.[16] Through actively directing the growth of cyberspace and the information technology market, hackers have cultivated a culture which is entwined with technology sharing, free discussion, international cooperation, non-restricted access to software, and which cultivate a democratic atmosphere:

> It suggests that hacking, as a culturally formed and informed practice, is involved in struggles over the signification and significance of democracy. In particular, hacking is associated with an ethics and practice of active access to information. However, after tracing historical and cultural shifts in practices, discourses and representations of hacking, the paper also suggests that hacking is becoming increasingly dissociated from its founding cultures and their ethics, as computer technology and technological skill sets become more widely available, networked and encoded. As such, hackers' overall relationship to the active access of information, and therefore to democracy, remains ambivalent and uncertain (Best 263).

However, they also face a choice between freedom and responsibility. The example below can illustrate how a hacker's personal interest might have a destructive effect on society. Such behavior - of avoiding to pay the price of freedom - is an evasion of responsibility. Those hackers whose understanding of freedom is romantic and arbitrary will be at odds with the interests of other people, as demonstrated by the invention of "Melissa" virus:

> In 1999, New Jersey resident David L. Smith gave a stripper in Florida the ultimate gift: a computer virus that bore her name. Using a stolen America Online account, Smith posted a Word document infected with "Melissa" to Alt.Sex, a discussion group on America Online, purporting it to be a list of usable log-in information to pornography sites. Smith's virus spread via email, forwarding itself to fifty email accounts in Microsoft Outlook on every infected computer, and which, over time, overloaded email servers and forced companies such as Microsoft, Intel, Lockheed Martin (a private military contractor—and weaponry producer), and Lucent Technologies to shut down their email networks. In the end, Melissa performed viral lap dances on upwards of one million infected PC's and caused $80 million in damages. For unleashing the virus, Smith faced 10 years in jail and $5,000 in fines but served just 20 months behind bars (the daily beast.com).

What is the origin of this willful disobedience? The answer might hide in the hackers' special cultural values. Hacker ethics originates from a property of "liberty, equality, and fraternity," whose universality minimizes differential treatment.[17] To hackers, sharing and publishing information are the necessary steps to obtain the absolute freedom of cyberspace. However, when a hacker tries to restore a bug to improve the safety of the Internet and appeals to collective solutions for problems, he or she might unintentionally publish some personal information of Internet users. This kind of transformation from private information to public information is a typical contradiction in hacking: even though hackers firmly protect their own freedom and interests, they fail to maintain those of vulnerable users. Once private information is posted on cyberspace by hackers, it will be exposed to millions of other profit-oriented parties on the Internet who might have an interest in collecting this kind of profitable data. As those potentially dangerous parties in cyberspace take advantage of the open information from hackers, they seriously threaten the privacy of common users. Therefore, those users express fear and uneasiness and form a negative stereotype of hackers. Some victims describe crackers as "rapists" [18]:

> Labeling hackers as victimizers also helps create the enemy…In the victim/victimizer narrative, companies are afraid to disclose their victim status for fear of embarrassment, loss of confidence in

15. For more about hackers' freedom, see "The Hacker's Challenge: Active Access to Information, Visceral Democracy, and Discursive Practice".

16. For more about hackers who want to bring freedom to other people, see "The Hacker's Challenge: Active Access to Information, Visceral Democracy and Discursive Practice" P275-276 by Best.

17. For more about "liberty, equality, and fraternity", see "Free as in Freedom 2.0: Richard Stallman and the Free Software Revolution" P9 by Stallman.

18. For more about hackers and crimes, see "Discourses of Danger and the Computer Hacker" by Halbert.

> their company, and fear that making their vulnerability public will only increase the chances of invasion—all images that help align the hacker with a rapist. One programmer, tired of hackers entering their system, makes the victim status of their company explicit: 'We seem to be totally defenseless against these people. We have repeatedly rebuilt system after system and finally management has told the system support group to ignore the problem. As a good network citizen, I want to make sure someone at network security knows that we are being raped in broad daylight. These people freely walk into our systems and are taking restricted, confidential and proprietary information (Halbert 364)'.

Can the ideal hacker spirit still guarantee hackers freedom and allow them to ignore their responsibility outside virtual space? After all, reality itself is not ideal. Some hackers might "naturally" become crackers on their way to obtaining individuality, and suddenly their career is brought to an end with an accusation of criminality. This conflict presents a paradox to both hackers and society because it is usually hard to find a balance between freedom and responsibility.

4. A Paradox – Individuality and Authority

This section, based on the previous discussion, will broaden the potential conflicts by including some political attributes of hackers, especially the conflict between individuality and authority. It will start with illustrating the hacker's individuality from the specific disparity of the hacker identity and "gawker" identity. After exploring the origins of the anti-authoritarian and skeptical ideas in the hacker ethic, this section will end by pointing out the paradox between individuality and authority in the technical age.

Some scholars use "gawkers" to refer to common Internet users. According to Chun, gawkers, or rubbernecks, do not have individuality: "Under the influence of the spectacle, the rubberneck becomes impersonal being. He is no longer a man—he is the public; he is the crowd" (Wendy Chun 248). The lack of individuality ties every user into the web of information, hence adjusting each user's vision only to the spectacles around him; the spectacles, moreover, are built up by millions of other similar, unintentional gawkers who form a compact atmosphere of unawareness. Flowing in the ocean of finished information, gawkers fail to realize not only their own positions but the formation of information as well.[19] The overemphasis on the final appearance of information directly presented by the Internet pages hampers gawkers from denaturalizing the process of producing knowledge or understanding the process of programing from a hacker's perspective. Hackers, on the other hand, enjoy a much more fragmented beauty of cyberspace. This appreciation results from their understanding of how to produce the information. The following is a quote from a classic cyberpunk literature Snow Crash, which vividly expressed hackers' method of interpreting cyberspace:[20]

> The number 65,536 is an awkward figure to everyone except a hacker, who recognizes it more readily than his own mother's date of birth: It happens to be a power of 2—the 216th power to be exact—and even the exponent 16 is equal to 24, and 4 is equal to 22. Along with 256; 32,768; and 2,147,483,648; 65,536 is one of the foundation stones of the hacker universe, in which 2 is the only really important number because that's how many digits a computer can recognize. One of those digits is 0, and the other is 1. Any number that can be created by fetishistically multiplying 2s by each other, and subtracting the occasional 1, will be instantly recognizable to a hacker (*Snow Crash* chapter 3).

Due to the secular bias towards hacking behavior, people hardly relate hackers to art, beauty, or even culture. However, just like Eric Steven Raymond's belief in the beauty of "Unix," which can be proved by his book *The Art of Unix Programming:*[21]

> If you are not a programmer, or you are a programmer who has little contact with the Unix world, this may seem strange. But Unix has a culture; it has a distinctive art of programming, and it carries with it a powerful design philosophy (Raymond chapter 1).

The difference of aesthetic habits is only one difference between hackers and common people. The aesthetics difference of hackers mentioned above reflects, at least, one problem: hacker culture is a subculture with a highly self-oriented spirit. Moreover, gawkers' "ignorance" and the public's misunderstanding further enhance the hackers' specialty. The above elaboration of hackers' enthusiasm in their own works might sound friendly and proper, even creative and progressive, but this might contain hidden dangers.

[19] For more about "gawkers", see "Othering Space" by Chun and "Visual Culture Reader 2.0ed." P241-254 by Nick.

[20] For more about hackers in cyberpunk literature, see "Snow Crash" by Stephenson.

[21] For more about the beauty of programming, "The Art of UNIX Programming" by Raymond.

Can we also trace back to the original hacker's spirit to find out what is responsible for this negative outcome? Hackers have been utilizing their freedom to fight against any form of restrictions for a long time: patents, copyrights, private ownership and unobtainable source code.[22] Indeed, the ability to manipulate information provides an enjoyment so compelling and unusual that hackers cannot hold back blurring the violation of privacy and the championship of personal freedom. They treat themselves like the authorities of cyberspace because of their ability to establish a distant, higher-level position from that of the community of gawkers, who actually make up of the majority of cyberspace users. Furthermore, hackers sometimes utilize their authoritative power off-line, hoping to correct real-life occasions whose motivation causes hackers skepticism. Organizations like Anonymous show such a high level of intolerance to groups with different ideologies that their reactions are direct subversion:

> In Anonymous's big "coming out party," the now infamous group of loosely-connected "hacktivist" computer users targeted the Church of Scientology in an operation dubbed "Project Chanology." The group's mass-DDoS attack, coordinated using the same software program used to fight for Wikileaks this week, targeted Scientology.org, momentarily knocking it offline. Their goal: to "save people from Scientology by reversing the brainwashing." At the time, a security expert monitoring the traffic generated by the DDoS attacks said it was "in the middle of attack sizes," noting "It's not just one or two guys hanging out in the university dorms doing this" (stealtheworld.html).

This case demonstrates the paradox of individuality and authority in hacker behaviors. While opposing the "brainwashing" activities of the Church of Scientology, whose behavior has already caused serious discussion in society, members of Anonymous are in line with the majority of citizens who detest thought control and want to protect personal freedom of thought. The hackers' goal also expresses their concern for preserving individuality and human rights. With this positive intention, hackers chose to show their anger and opposition to the Church of Scientology by launching net attacks, a method that displays their advantage and strength. As "authority" in cyberspace, hackers, equipped with collective intelligence and hacking ability, carry out "voluntary" Internet sanctions that reflected their stated values. The dilemma is that, in trying to preserve individuality, the action of "preserving" permitted hackers to take an authoritative position, further ensuring their power over other people. Like the concerns of existing governing organizations mentioned early in the paper, this new "governance" from hackers remains as a threat to the balance of power; as a result, they will use exaggerated depictions of hackers to maintain their positions in the game of power.

The conflict between individuality and authority is not merely a question about "govern" or "be governed," but we can further explain it in terms of the relationship between human beings and machines. Because of hackers' worship of technology, the technology-oriented logic reinforces the disregard for actuality in society. The problem is that when technology is sanctified, hackers will overvalue the importance of technology, regarding it as a solution to any kind of social problem in the digital world, or even in reality. The opposition to human leadership might indicate a support for technological authority. While trying to deal with the serious social situations with logic in virtual space, are hackers themselves becoming slaves of computer science, which is a restriction that should be opposed by hackers?

Acknowledgments

I would like to thank Professor Eva Woods for her time of supervising my research.

References

Best, K. (2010). *The Hacker's Challenge: Active Access to Information, Visceral Democracy, and Discursive Practice.* Social Semiotics. Ed. London: Routledge. p263-282.

Chun, W. (2003). "Othering Space." Visual Culture Reader 2.0. ED. Nick Mirzoeff. New York: Routledge. p241-254.

Chung, J., Linder, J., Liu, I., Seltzer, W., & Tse, M. (2015, June 29). Democratic Structures in Cyberspace.

Existentialism, S. (2015). Retrieved June 25, 2015 from http://plato.stanford.edu/entries/existentialism

Fsf.org, "Free Software Is a Matter Of Liberty, Not Price – Free Software Foundation – Working Together For Free Software". N.p., 2015. Web. 22 June 2015. http://www.fsf.org/about/

[22] For more about the history and fight against restrictions like copyrights, "Free as in Freedom 2.0: Richard Stallman and the Free Software Revolution" by Stallman.

Halbert, D. (2006). *Discourses of Danger and the Computer Hacker. The Information Society: An International Journal.* Ed. London: Routledge. p.361-374.

Himanen, P. (2001). *Preface. The Hacker Ethic and the Spirit of the Information Age.* By Himanen. New York & Toronto: Random House Trade Publishers. p.1-7.

Himanen, P. (2001). *The Hacker Ethic.* Retrieved June 15, 2015, from https://www.nytimes.com/books/first/h/himanen-hacker.html

J James, Jr Brown. (2008). *From Friday to Sunday: the hacker ethic and shifting notions of labor, leisure, and intellectual property, Leisure Studies. Leisure Studies.* Ed. London: Routledge. p.396-409.

Kelty, C. M. (2005). *Geeks, Internets, and Recursive Publics.* UCLA Previously Published Works.

Lawson, G.–B. (2010). More Than a Mouse Trap: Effective Business Models in a Digital World. *International Journal of Media Management.* Ed. London: Routledge. p41-45.

Lomie, L., Muchena, M., & Pierce, R. A. (2014). *Business Management.* Cambridge, Pearson Education.

Minovich, L. (2002). *The Language of New Media.* Cambridge: MA: MIT. p19-39.

News.bbc.co.uk. (2009). *BBC NEWS | Americas | China Denies Spying Allegations.* N.p. Retrieved June 17, 2015, from http://news.bbc.co.uk/2/hi/7972702.stm

Pekkahimanen.org. (n. d.). *Pekka Himanen - Biography.* Retrieved June 26, 2015, from http://www.pekkahimanen.org/?view=bio

Raymond, E. (2004). *The Art of UNIX Programming.* Crawfordsville: Pearson Education.

Ries, B. (2010). *Hackers' Most Destructive Attacks.* The Daily Beast. N.p. Retrieved June 21, 2015, from http://www.thedailybeast.com/articles/2010/12/11/hackers-10-most-famous-attacks-worms-and-ddos-takedowns.html

Schrock, A. R. (2014). Education in Disguise: Culture of a Hacker and Maker Space. *InterActions: UCLA Journal of Education and Information Studies, 10*(1).

Sjgames.com. (1994). *The Top Ten Media Errors about the SJ Games Raid.* N.p. Retrieved June 20, 2015, from http://www.sjgames.com/SS/topten.html

Skibell, R. (2010). *The Myth of the Computer Hacker.* Information, Communication & Society. Ed. London: Routledge. p336-356.

Stallman, R. (2010). *Free as in Freedom 2.0: Richard Stallman and the Free Soft- ware Revolution.* Boston: Free Software Foundation.

Stallman, R. (2014, May 14). *The GNU Project. gnu.* Retrieved June 23, 2015, from https://www.gnu.org/gnu/thegnuproject.html

Stephenson, N. (1992). *Snow Crash.* New York: Bantam Dell.

subcultureslist.com. (n. d.). *Hacker Culture.* Retrieved January 31, 2016 from http://subcultureslist.com/hacker-culture/

The 10 Most Destructive Hacker Attacks, Blogspot, Jul 2012. Retrieved June 20, 2015, from http://stealtheworld.blogspot.ca/2012/07/the-10-most-destructive-hacker-attacks.html

The Atlantic. (2015). *Technology.* N.p. Retrieved June 19, 2015, from http://www.theatlantic.com/technology/archive/2011/06/ibms-first-100-years-a-heavily-illustrated-timeline/240502/

Thomas, D. (2009). *Criminality on the electronic frontier: Corporality and the judicial construction of the hacker, Information.* Information, Communication & Society. Ed. London: Routledge. p382-400.

Walden, D. (2000). *Looking Back at The ARPANET Effort, 34 Years Later, Living internet.* Retrieved June 25, 2015, from http://www.livinginternet.com/i/ii_imp_walden.htm

Xun, X. (2013, May). Philosophy Thoughts of Hacker Phenomenon [D]. Taiyuan University of Science and Technology.

Copyrights