HOW HACKERS THINK: A MIXED METHOD STUDY OF MENTAL MODELS AND COGNITIVE PATTERNS OF HIGH-TECH WIZARDS

by

TIMOTHY C. SUMMERS

Submitted in partial fulfillment of the requirements

For the degree of Doctor of Philosophy

Dissertation Committee:

Kalle Lyytinen, Ph.D., Case Western Reserve University (chair)

Mark Turner, Ph.D., Case Western Reserve University

Mikko Siponen, Ph.D., University of Jyväskylä

James Gaskin, Ph.D., Brigham Young University

Weatherhead School of Management

Designing Sustainable Systems

CASE WESTERN RESERVE UNIVESITY

May, 2015

CASE WESTERN RESERVE UNIVERSITY

SCHOOL OF GRADUATE STUDIES

We hereby approve the thesis/dissertation of

Timothy C. Summers

candidate for the Doctor of Philosophy degree*.

(signed) Kalle Lyytinen
(chair of the committee)

Mark Turner

Mikko Siponen

James Gaskin

(date) February 17, 2015

*We also certify that written approval has been obtained for any proprietary material contained therein.

Dedication

I am honored to dedicate this thesis to my parents, Dr. Gloria D. Frelix and Dr. Timothy Summers, who introduced me to excellence by example and practice. I am especially thankful to my mother for all of her relentless support. Thanks Mom.

DISCLAIMER

The views expressed in this dissertation are those of the author and do not reflect the official policy or position of the Department of Defense, the United States Government, or Booz Allen Hamilton.

Table of Contents

List of Tables

List of Figures

ACKNOWLEDGEMENTS

The development of this thesis has been a long journey. Its creation has been a substantial cognitive maturation process. I wish to first thank those who provided me the opportunity to make the observations which this work is based. I am grateful to my doctoral committee, the faculty and staff at the Weatherhead School of Management, and the stimulating environment of Case Western Reserve University. My dissertation chair and program director, Kalle Lyytinen, Ph.D., merits special recognition for taking a chance and allowing me to conduct my radical research under his guidance. Also, I am especially grateful to my guides, James Gaskin, Ph.D. and Tony Lingham, Ph.D. There were many other faculty members who were also instrumental in my development and the lens with which I now see the world.

My greatest debt is to my family and friends, especially my mom, Gloria D. Frelix, MD, who provided encouragement, unrelenting support, amazing meals, and brainstorming assistance. Thanks.

How Hackers Think: A Mixed Method Study of Mental Models and Cognitive Patterns of High-Tech Wizards

ABSTRACT

by

TIMOTHY C. SUMMERS

Hackers account for enormous costs associated with computer intrusion in a world increasingly reliant on computer and Internet-based technologies. In the general sense, a hacker is a technologist with a love for technology and a hack is an inventive solution executed through non-obvious means. They speak the language of code which propels the evolution of our information technology. This makes hackers the solvers of our largest, most complex issues. They seek out weaknesses in computers and networks that can be used to steal data or impact the functionality of the entire Internet. In consequence, they are experts at solving poorly understood and challenging problems in a variety of settings requiring deep understanding of technical details and imagination.

Hacking is an activity that requires exceptional cognitive abilities. Through explanatory, sequential mixed methods research completed over three empirical studies, I discover how the mental models and the cognitive skills and traits of skilled hackers affect the way they learn and perform forward thinking. Proficient hackers construct mental representations of complex systems and their components. As they learn and interact with the system, their mental models evolve and become more reliable. This

research reveals that hackers use these continuously evolving cognitive structures to conceive of future results through speculative forecasting. These models are instrumental in setting the hacker's expectations about effects of actions, planning of actions, and ways of interpreting feedback.

This dissertation makes theoretical and empirical contributions to the literature on the mental models and cognitive faculties of hackers and practice through the development of evidence-based and research-informed strategies for improving the cognitive mechanisms necessary for hacking. The findings will be useful for leaders and managers in private, government, and nonprofit sectors with an interest in the advanced thinking required for cybersecurity and innovation. Additionally, this research contributes to the development of strategies for developing and managing effective hackers and improving talent identification and recruitment performance. It can serve as the foundation for the development of a training platform that improves the cognitive abilities necessary for effective hacking.

Keywords: Hackers; cybersecurity; expertise; mental models; cognitive framework; cognition; psychology; sociology; problem solving; decision making; patterning; learning; forward thinking

INTRODUCTION

Over the years organizational investments in information systems and technologies have grown exponentially (Broos & Roe, 2006; Filos, 2006; Venkatesh, Morris, & Ackerman, 2000); almost to the point of becoming a commodity as ubiquitous as labor (Dewett & Jones, 2001). By 1991, information technology investments by U.S. companies were higher than any other form of corporate investments. In fact, total spending on computers and related services substantially increased from approximately $80 billion in 1984 to over $160 billion in 1998 (Taylor, 1998). Gartner reported that global IT spending topped $3.75 trillion in 2013 (Gordon & Lovelock, 2014). Information systems and technologies include many different types of software and hardware devices which enable and manage all major functions of the modern organization including but not limited to email, voice conferencing, voicemail, video conferencing, the Internet, corporate intranets, and so on. The proliferation of and reliance on this broad array of technologies has manifested a dependence on inquisitive technologists with a passion for fiddling with and learning technical systems, namely hackers. Weizenbaum (1976) was one of the first to describe this emergent group:

> "Whenever computer centers have become established, that is to say, in countless places in the United States, as well as in virtually all other industrial regions of the world, bright young men of disheveled appearance, often with sunken glowing eyes, can be seen sitting at computer consoles, their arms tensed and waiting to fire their fingers, already poised to strike, at the buttons and keys on which their attention seems to be as riveted as a gambler's on the rolling dice. When not so transfixed, they often sit at tables strewn with computer printouts over which they pore like possessed students of a cabalistic text. They work until they nearly drop, twenty, thirty hours at a time. Their food, if they arrange it, is brought to them: coffee, Cokes, sandwiches. If possible they sleep on cots near the computer. But only for a few hours – then back to the console or the printouts. Their rumpled clothes, their unwashed and unshaven faces, and their uncombed hair all testify that they are oblivious to their bodies and to the world in which

> they move. They exist, at least when so engaged, only through and for the computers. These are computer bums, compulsive programmers. They are an international phenomenon" (p. 116)

Computer hackers are an important social phenomenon today (Nikitina, 2012). However, our society is perplexed about what to make of them. From one perspective, they are the "heroes of the computer revolution" for their technological wizardry (Levy, 1984); however, from another perspective, they are "the demons of big companies and of folks whose credit card numbers they have cracked open". To echo societal confusion on hackers, most dictionaries have contradictory definitions for "hacker": (1) a person who is inexperienced or unskilled at a particular activity" and (2) "a person who is skilled in the use of computer systems, often one who illegally obtains access to private computer systems". In general, a hacker is a technologist with a proclivity for computing and a hack is a clever solution accomplished through non-obvious means (Levy, 1984; Turkle, 1984). My research relates to larger questions concerning the relationship between history, culture, and the socialization of the hacker. Specifically to questions concerning learning and forward thinking. This relationship is central to human development and, particularly, to the cognitive psychology approach.

To advance understanding of how hacker think using mental models, particularly in regard to how they learn and perform forward thinking, the following higher-level research questions are posed for my thesis: 1) what cognitive faculties are involved in the act of hacking?; 2) how do hackers use mental models?; and 3) how can the cognitive skills and traits of hackers improve their learning and forward thinking?

Learning is a large and complex field concerned with the study of a person's behavior and *how* they adapt it to the environment. Some researchers suggest that the

human mind, like a computer, accepts input through "perception, storing it in memory, processing it in thought, and acting on it in making decisions" (Leahey & Harris, 1989a: p.11). With each technological advancement comes an emphasis on different sets of skills, different developmental pathways, and different processes of adaption – learning and forward thinking (Staddon, 1975; Thomas, 2002). Since the beginning, the computer hacker has been inextricably linked to the cultural, social, and political history of the computer (Taylor, 1999). But this is a history filled with complexity, contradictions, and cultural anxieties about technology.

The History of Hacking

Before we begin to discuss the technologists – the hackers that Weizenbaum (1976) described, we must address the contradictory and conflictory discourse that surrounds the term. Some researchers (Chandler, 1996) suggest that, with every new generation of computer technology came a new generation of hacker. The term *hacker* has been applied to various groups, at various times, and across different generations (Cornwall, 1987). As stated by Thomas (2002), "even hackers themselves have trouble coming up with a definition that is satisfactory, usually falling back on broad generalizations about knowledge, curiosity, and the desire to grasp how things work" (p. 3). For the purposes of this study, borrowing from Thomas (2002) and making small adjustments, we want to think of hackers as a group of technology enthusiasts who operate in a space and manner that is defined by a sense of boundless creativity and curiosity and an endless desire to understand how things work, but who respect and value the cultural notion of secrecy. As suggested by Thomas (2002), "to understand today's

hackers, it is essential to understand the history of computers and computer culture" (p. 3).

> "The 'original' hackers were computer professionals who, in the mid-sixties, adopted the word 'hack' as a synonym for computer work, and particularly for computer work executed with a certain level of craftsmanship. …Then in the seventies, assorted techno-hippies emerged as the computerized faction of the counterculture of the day. …What characterized the second wave hackers was that they desperately wanted computers and computer systems designed to be useful and accessible to citizens. …Finally, in the second half of the eighties the so-called cu [computer underground] emerged, appropriated the terms 'hacker' and 'hacking' and partly changed their meaning. To the computer underground, 'to hack' meant to break into or sabotage a computer system, and a 'hacker' was the perpetrator of such activities" (Hannemyr, 1997a).

The most seminal work on hackers to date, Levy (1984), details the various generations of hackers, beginning with the first generation of pioneering enthusiasts at MIT laboratories in the 1950s and 1960s, the second generation involved with bringing computer hardware to the public through development of the earliest personal computers in the 1970s and 1980s, and the third generation programmers who became the leaders in the arrival of computer game architectures in the 1980s and 1990s. The fourth generation, whom the word *hacker* now almost exclusively describes, gain unauthorized access to other people's computer systems.

The First Generation Hackers

Although, it could be argued that there would be no hackers had President Dwight Eisenhower not created the Defense Advanced Research Projects Agency (DARPA) in the post-Sputnik consternation and observed technological prowess of the Soviet Union (Hafner, 1998; Rosenzweig, 1998); as we know it today, the beginnings of hacker culture started with the intelligent and curious students of the Massachusetts Institute of Technology (MIT) (Levy, 1984; Raymond, 1999; Taylor, 1999; Thomas, 2002; Turkle,

1984). In 1961, MIT acquired its first Programmed Data Processor-1 (PDP-1). The PDP-1[1] is credited with being one of the computer most instrumental in the creation and proliferation of hacker culture at MIT and other institutions (Flowers, 2008; Raymond, 2001). The Tech Model Railroad Club (TMRC), an MIT student social club, became fascinated with the PDP-1 and created programming tools, jargon, and a culture that still exists as part of today's hacker culture (Levy, 1984; Raymond, 1999). The computer culture at MIT was the first to embrace the term *hacker* and it was the hackers from the TMRC that formed the foundation for the MIT Artificial Intelligence Laboratory (Levy, 1984; MIT, 2014; Raymond, 1999).

Some researchers (Raymond, 1999) suggest that the influence of MIT's TMRC also spread further after 1969 with the development of the Advanced Research Projects Agency Network (ARPAnet), one of the world's first operational packet switching networks. The ARPAnet was built by DARPA to experiment with the capability of digital communications to link together the best and brightest minds. It enabled researchers to exchange information with speed and flexibility during a time when technological advancement through collaboration was most highly desired (Leiner et al., 2009; Segaller, 1999; Tronco, 2010). The importance of ARPAnet in hacker history is that it enabled hackers at universities and research laboratories all over the United States to interact - virtually. Although most the hacker culture began at MIT, through ARPAnet, it soon spread to many others including Stanford University and Carnegie

[1] The PDP-1 was the first computer in Digital Equipment Corporation's PDP series and was first produced in 1959.

Mellon University (Raymond, 1999). The emergent hacker culture was a hit within artificial intelligence labs and computer science departments.

The Digital Equipment Corporation, developer of the flexible and inexpensive PDP-1, pioneered the interactive computing and time-sharing operating systems (human-computer interaction set up so that computers can be used at the same time by multiple users) of the 1960s (Raymond, 1999). Some of the earliest *hacks* came as a result of MIT hackers desiring alternate ways to interact with the system. Many of the creatively, unusual innovations developed by these early hackers are still in use today. One example of this is the EMACS program editor (Raymond, 1999).

Early on, hackers were not comfortable with the establishment, as noted by (Rosenzweig, 1998):

> "ARPA money supported the "hackers" at MIT's Artificial Intelligence Lab, but some of their goals – the free sharing of information, for example – led to direct clashes. Richard Stallman, a systems programmer in the lab, carried on a guerrilla war against the use of passwords on the system. The lack of security encouraged by Stallman and others caused nervousness at the Defense Department, which threatened to cut the computer off the ARPAnet, since anyone could walk into the lab and connect to the rest of the network" (p. 1542).

Even though the government sought help from the universities to advance the study of computer sciences, engineering, and artificial intelligence; the notion of secrecy was a source of contention between the hackers and the Defense Department (Levy, 1984; Raymond, 1999; Rosenzweig, 1998; Segaller, 1999; Taylor, 1999; Thomas, 2002). Since the days of Caesar, military forces have valued the ability to keep their plans secret from adversaries. The hackers of the 1950s and 1960s were accustomed to the open learning environment on university campuses and despised the notion of keeping information secret (Raymond, 1999; Rosenzweig, 1998; Thomas, 2002). For these

hackers, secrecy was about sharing code, collaborating with others on code design, and dabbling with any and everything (Thomas, 2002). According to Thomas (2002), "it was, in large part, that distaste for secrecy that led to most of the major advances that hackers would later make in the computer labs of MIT and other universities" (p. 13). Supplementary to that point, Levy (1984) argued that "a free exchange of information, particularly when the information was in the form of a computer program, allowed for greater overall creativity" (.p 27). In this manner, collaboration and the continuous improvement of ideas and programming techniques, are core elements of the *hacker ethic* (Levy, 1984; Taylor, 1999; Thomas, 2002). For hackers, the goal is not only to write original programs but to contribute to the work of others (Coleman, 2013; Thomas, 2002). As stated by Thomas (2002), "the most skillful *hack* was not writing a new line of code but finding a way to do something in someone else's code that no one had seen before – to eliminate code, making the program run faster and more elegantly". A *hack* is an inventive solution executed through non-obvious means (Coleman & Golub, 2008; Levy, 1984; Turkle, 1984).

During this same time, there was another type of hacking, known as *phreaking*, which started with a radical political group called the Yippies. According to Sterling (1992), "the genuine roots of the modern hacker underground probably can be traced most successfully to a now much-obscured hippie anarchist movement known as the Yippies". Thomas (2002) states, "the modern underground, then, had its roots in a leftist political agenda that grew out of 1960s counterculture and was fueled by the antiwar protect movements of the 1960s and 1970s". The Yippies, officially known as the Youth International Party (YIP), were a group of phone phreaks that published a newsletter and

tip-line known as the Technical Assistance Program (TAP) informing people on "tips on such topics as lock picking, the manipulation of vending machines, do-it-yourself payphone slugs and free electricity" (Hafner & Markoff, 1995; Thomas, 2002). As Thomas (2002) states, "in the late 1960s and early 1970s, while the hackers of TAP were busily disseminating information, hackers at MIT were busy creating information".

Although the first generation hackers and the government had a contentious relationship, the military industrial complex was the primary funder of hacker culture and a core element to the beginnings of the Silicon Valley era (Leiner et al., 2009; Levy, 1984; Raymond, 1999; Rosenzweig, 1998; Segaller, 1999). As Thomas (2002) states:

> "On the one hand, the MIC [military industrial complex] was funding the projects that would create hacker culture. Partially out of naïveté and partially because of the novelty of computers, the hackers of the 1960s and 1970s were able to avoid the obvious contradiction between their highly antiauthoritarian mind-set ("Information wants to be free") and the fact that the people were designing systems and software for were not likely to respect that basic tenet. Because they were producing the vast majority of new technology, the old-school hackers were able to maintain the illusion that they were also controlling it. Within a decade, the "old school" had moved to the Silicon Valley and started to build an industry that would look and operate increasingly less like the labs at MIT and Harvard and more like the corporations and organizations against which the 1960s hackers had rebelled" (p. 17).

The Second Generation Hackers

The transition of the "old school" hackers from the open-learning university environments to the Silicon Valley of California marked the beginning of the computer industry as we know it today. As Thomas (2002) argues, "the computer industry has always been and in many ways continues to be the very antithesis of the hacker culture, which is also the reason that it plays an important role in the formation of hacker culture" (p. 17-18). In fact, the personal computer would never have existed without computer

hackers (Chandler, 1996). It was second generation hackers like Bill Gates, Steve Jobs, and Steve Wozniak that were instrumental in making the PC a household name (Leiner et al., 2009; Levy, 1984; Rosenzweig, 1998; Segaller, 1999; Taylor, 1999; Thomas, 2002; Tronco, 2010). For example, before selling computers, Apple Computer founders, Steve Jobs and Steve Wozniak sold devices used for hacking telephone systems (Clarke & Knake, 2011). Of course, most people do not realize that the founders of Apple Computer were phone phreaks[2], but it is the story of how their company was started that reveals the difference between first generation and second generation hackers.

One of the first phone phreaks was John Draper, who called himself Captain Crunch. He chose this name as a result of one of his most popular hacks, which included using a toy whistle from the Capt'n Crunch cereal to produce a 2600 Hz tone that enabled him bypass the phone control system requiring payment for long distance calls. As with most hacks, hackers[3] took advantage of this discovery and began building small devices called a "blue box" that would emulate the same 2600 Hz tone for free long distance calls (Hafner & Markoff, 1995; Kluepfel, 1989; Leiner et al., 2009; Levy, 1984; Raymond, 1999; Rosenzweig, 1998; Segaller, 1999; Sterling, 1992; Taylor, 1999; Thomas, 2002; Tronco, 2010).

---

[2] Phone phreak was a term used in "the early sixties to describe youthful experimenters who broke the control codes of national and international telephone networks to probe the system, invade privacy and perpetrate fraud" Kluepfel, H. 1989. ***Foiling the wiley hacker: more than analysis and containment***. Paper presented at the Security Technology, 1989. Proceedings. 1989 International Carnahan Conference on.. In essence, "phone phreaks are to telephones what hackers are to computers – they possess a basic understanding of how the phone system works and as a result can do things such as place long-distance calls for free" Thomas, D. 2002. ***Hacker culture***: U of Minnesota Press..

[3] Although the word phreak is most appropriate here, the author thought it advantageous to use the word hacker.

Steve Jobs and Steve Wozniak read about Draper's discovery in an *Esquire* article (Rosenbaum, 1971) and soon built their own "blue box" (Thomas, 2002). After copying Draper's work, Jobs and Wozniak began selling the devices to other students in the Berkeley dorms (Levy, 1984; Thomas, 2002). As Thomas (2002) states, "Jobs and Wozniak copied a device someone else had originated and then sold those copies…This is a pattern Jobs and Wozniak would follow in building the first Apple…In contrast to the long-standing hacker ethic that freely distributed information and knowledge resisted the impulse toward commodification, Jobs and Wozniak openly embraced it" (p. 18).

But on the other side of the table was the journey of Bill Gates and Paul Allen. Prior to the Apple Computer was the Altair, the very first PC (Levy, 1984; Thomas, 2002). Gates and Allen were computer enthusiasts who wrote the first language for the Altair. That language was Altair BASIC. Although Gates and Allen were not the inventors of BASIC, they are credited with taking a programming language meant for mainframe computers and bringing it to the PC platform. Consistent with the hacker culture, most of the software for the Altair was written by hobbyists and given away during computer club meetings (Leiner et al., 2009; Levy, 1984; Thomas, 2002). As previously stated, information sharing was a core element of the hacker ethic and as stated by Thomas (2002) "would be the central organizing principle of one of the first computer clubs, the Homebrew Computer Club of Menlo Park, California" (p. 19).

The commodification of technology changed everything. As stated by Thomas (2002), "With commodification, the earliest computer hackers, those who had built their computers themselves and shared every tidbit of information that might help to improve their machines or programs, were in competiiton with each other, fighting to create and

maintain market share. The result was dramatic – competition in the marketplace "retarded Homebrew's time-honored practice of sharing all techniques, refusing to recognize secrets, and keeping information going at an unencumbered flow….All of a sudden, they had secrets to keep. That transition marks the dividing point between the old-school hackers of the 1960s and 1970s and the new-school hackers of the 1980s and 1990s" (p. 19).

The Third Generation Hackers

> "If Jobs and Wozniak can be described as the second generation of 'hackers', then the third generation are "the kids who inherited the gift of the personal computer and were hacking out and selling the first computer games. Their motivation was often a fast buck and their instincts were entirely commercial" (Chandler, 1996; Clough & Mungo, 1992: p. 74)

It was with the third generation hackers that the term *hacking* became associated with criminal behavior. As described by Chandler (1996), "here, hacking could be defined as the breaking of copyright protection codes thus enabling the games programs to be refined or altered, or simply to facilitate the 'pirating' of the games" (p. 231). However, hacking also referred to "the time-consuming process of writing the definitive program, a process involving long hours in front of a computer de-bugging home written codes" (Chandler, 1996), a definition that was much more consistent with the original. Some researchers contend that the third generation of hackers were short-lived and quickly overtaken by the fourth and current generation of hackers (Chandler, 1996); however, others suggest that the third generation had a substantial hand in the development of the cyberpunk[4] and gaming aspects of hacker culture. With second

[4] As described by Anonymous. 2012. What is Cyberpunk?, Vol. 2014: Cyberpunkforums.com.: "The very word *cyberpunk* is a portmanteau of *cybernetics*, the science and technology of the system, and *punk*, the philosophy of rebellion against the system. Where they intend for order, we make disorder; as they say,

generation hackers making the PC a household item, the third generation had the advantage of direct access them. As argued by Clough and Mungo (1992), taking "'hacking' – previously an honorable trade – and made it into a form of breaking and entering".

The cyberpunk movement was made popular by books such as Neuromancer by William Gibson. The gaming aspect could be seen clearly in the film *War Games*, where David Lightman (played by Matthew Broderick), a curious teenager, begins exploring a computer game and unintentionally starts a war between the United States and the Soviet Union. As Thomas (2002) states, "the film demonstrates a tremendous anxiety about technology, represented both by the missiles that threaten to destroy the United States and the Soviet Union and by the machines that control those missiles" (p. 25). The film was the first time that we saw an intersection between hacker culture and popular culture which made it a cult classic among hackers (Thomas, 2002). Finally, hackers had a national audience.

Even though films like *War Games* introduced society to hacker culture, it was Robert Morris who struck fear into the population. In 1988, Robert Morris, a student at Cornell University, unleashed the first Internet worm[5]. The worm replicated itself at a rate higher than Morris intended, resulting in an Internet shut down. Morris became the first person to be indicted under the Computer Fraud and Abuse Act. According to the

"the street will find its own use for things." As a movement, we seek to see the world for what it is and look past the black and white to see the true shades of grey, blurring the lines between natural and artificial, organic and mechanical, real and virtue".

[5] According to Barwise, M. 2010. What is an internet worm?: BBC. Retrieved December 9, 2014 from http://www.bbc.co.uk/webwise/guides/internet-worms., "A computer program that copies itself to other computers across the Internet is called a worm. Worms are often used to infect large numbers of broadband-connected computers in remote-control software".

court records, Morris stated that his motive was "to demonstrate the inadequacies of current security measures on computer networks by exploiting the security defects he had discovered"[6]. The Morris worm was the first situation to spur societal fear and debate over the impact of hackers on society. As Hafner and Markoff (1995) stated, "it also engaged people who knew nothing about computers but were worried about how this new technology could be used for criminal ends" (Thomas, 2002).

Following *War Games* (1983), the 1990s saw a huge release of hacker films with *Sneakers* (1992), *Hackers* (1995), and *The Net* (1995). Interestingly, each of the films presents a theme seen throughout hacker culture: secrecy. As noted by Thomas (2002):

> "In *Sneakers* (1992), the confusion between corporate and government secrecy is complete when it is revealed that the only real governmental use for the "black box" agents have been sent to recover is to snoop on other U.S. governmental departments, rather than on foreign governments. …In the case of *Hackers*, two employees (one a former hacker) of a major corporation are running a "secret worm program" to steal millions of dollars from the corporation. They are discovered when a hacker unwittingly copies one of their "garbage files" that contains the code for the worm's program. The same plot is played out in *The Net*, but from a governmental point of view. Angela Bassett (played by Sandra Bullock) accidentally accesses and copies secret governmental files that reveal wrongdoing on the part of the governmental officials, again demonstrating the manner in which the culture of secrecy is able to hide and allow for a deeper sense of criminality to ferment and function. In both cases, hackers, by violating the institutions' secrecy, expose criminality by enacting criminality. The message from the later films is that secrecy creates a space for the worst kinds of criminality, which, because of the culture of secrecy, can only be exposed by another type of criminality – hacking" (p. 31).

Although the third generation shared the computer-driven obsession as their second generation ancestors, there were clear levels of distinction. It would seem that, if the significant contribution of the second generation was bringing computer technology

[6] The official documentation from the United States Court of Appeals, Second Circuit can be found here: http://scholar.google.com/scholar_case?case=551386241451639668.

to the masses, the third generation explored the boundaries and reach of that technology through seeking ways to exploit the hardware and software. Some members of the second generation have suggest that "the fourth generation hackers were 'underage and underdeveloped' and that they displayed 'negative social attitudes' and degenerated [hacking] from a collective mission of exploration into an orgy of self-indulgence" (Chandler, 1996; Clough & Mungo, 1992: p. 74). Some researchers argue (Chandler, 1996) that this view of the fourth generation was "particularly evidenced by a new aspect of computer programming, i.e. the writing of computer viruses" (p. 232).

Most importantly, it was the third generation that brought us hackers like Kevin Mitnick – considered by many to be "a legendary outlaw on the computer frontier" (Chandler, 1996) and Tsutomu Shimomura – the hacker who caught him (Shimomura & Markoff, 1995). It was with this generation that we began to see terms like *electronic cowboys*, *outlaws*, and *renegades* being used to describe hackers. This is further evidenced by Sterling (1992) asserting, "hackers long for recognition as a praiseworthy cultural archetype, the postmodern electronic equivalent of the cowboy and mountain man…many hackers actually attempt to live up to this techno-cowboy reputation" (p. 54). Similar to the lawless American Wild West, there was a lack of regulation in cyberspace which provided an opportunity for the first and second generation hackers to create their own code of conduct (Chandler, 1996; Levy, 1984; Sterling, 1992). As Sterling (1992) asserts about previous generations, "truly heavy-duty hackers, those with serious technical skills who had earned the respect of the underground, never stole money or abused credit cards" (as cited by Chandler, 1996). But their third generation descendants differed in this respect. It was this divergence of *ethic* that brought about the classifier

terms, such as *white hat* and *black hat*. Similar to the influence that Americans have had on the development of the Internet, American culture is scattered throughout various aspects of hacker culture – particularly in reference to the *electronic frontier* and the *techno-cowboys* that explore it, as stated by Chandler (1996):

> "…it would seem that both the legend and the reality of the cowboy and the frontier are useful to the hacker community as it provided a popular and positive image to which Americans can relate because, for Americans, they are central to the American way of life. In this way, hackers may be accepted as the 'guys in the white hats' who are carving out and protecting a new American territory. It is an image for which the Americans have a sneaky admiration and creates a useful counterbalance for other, more sinister images of hackers which are being perpetrated by the media, law enforcement agencies and the legal system" (p. 236).

It was in the 1990s that the media began to advance the notions of negativism directed at hackers. This is not to say that there cannot be any negative aspects of hacking, as Chandler (1996) explains "hacking may be regarded as negativistic in that it is potentially dangerous as data may be deliberately or unintentionally altered (whereas hackers may describe their activities as exploring the 'frontier' or system to its fully potential or ensuring that the power of the computer does not reside in the hands of the powerful few)". But in the late 1980s and 1990s, the media was dominated with stories from various industries being victims of hacking activity (Chandler, 1996). Chandler (1996) describes such stories:

> "On 25 May 1988, *The Times* quotes an article from Computer Weekly that hospital systems and therefore lives may be at risk ("Computer Hackers 'May Kill'"). This potential for killing came to the fore in media reports surrounding the Michelangelo virus in March 1992 which, it was warned, could be lurking in computers in hospitals and medical research institutes. Reports at that time warned that not only could viruses lose companies millions but that, in extreme cases, they could kill (*The Mail* 5 March 1992 – "A Plague on Your Computer"), a sentiment echoed in *The Mirror* (6 March 1992 – "Terminators: How the Whizzkids Set Up A Computer Wipeout"). Both reports contain details of the

> Ethiopia Water Drilling Case in which it is alleged that 1400 lives were lost due to a virus infecting the drill's computer system. This seems to be the only reported case where lives have been lost due to what may be described as computer misuse, though it is not alleged that the virus was introduced by a remote hacker" (p. 239).

Due to stories like these and many more since the 1980s and 1990s, hackers have become incredibly feared by the public. In fact, many companies in the computer security industry utilize this to their advantage and present the "standard nightmare scenario" as a reason why computer security requires substantial investments (Chandler, 1996; Sterling, 1992; Taylor, 1999; Thomas, 2002). As stated by Chandler (1996), "this 'nightmare scenario' conjures up the worst fears – not only the threat of drugs, but also the potential for blackmail and death that a computer system makes people vulnerable to".

The Fourth Generation Hackers

> "From the year 2000 until the present time there was usually at least one major security incident, sometimes two a year. Early in the 2000s there were massive worms that plagued the Internet such as MS Blaster, Slammer, and Code Red. These worms exploited service side vulnerabilities mostly on servers, but also on workstations as well. Starting around the year 2007 there was a paradigm shift in how attacks were taking place. Attacks began to leverage client side exploitation. The attack would often occur by email or a malicious web site. A user would unknowingly interact with the attack, creating an outbound connection, which would bypass network security controls such as firewalls. These attacks would also leverage elements of social engineering to entice the user to interact with the malicious elements. In some cases, the exploit that was run on the system via the client side exploit would add that system into a botnet. Botnets are used to send span, perpetrate click fraud, launch denial of service attacks, and other nefarious deeds" (Bowles, 2012: pgs. 6-7).

Between the end of the 1990s and the 2000s, the hacker community became sociologically separated into two groups – the *black hats* and the *white hats* with a 'fuzzy gray line that separated the two' (Bowles, 2012; Constantin, 2012; Nikitina, 2012; Schell

& Dodge, 2002; Summers, Lyytinen, Lingham, & Pierce, 2013; Thomas, 2002; Xu, Hu, & Zhang, 2013). Bowles (2012) describes the groups in detail:

> "The evil hacker group [black hat hackers] can be characterized as people, groups, criminal organizations, governments, and military with malicious intent. The white hat hacker group, who we will refer to as security professionals, is comprised of people, groups, organizations, and governments who are employed to protect their employers from the evil hackers. Both groups have been around for a while but were fairly small until this point in time. The distinction between the two groups is often characterized by security professional practicing information security within the legal limits, and evil hackers having no regard for what laws they break or who is hurt by their actions. There is also a group known as gray hat hackers, which live in the gray fuzzy line between the two groups, who typically say they "bend" the law without breaking it. The three groups operate in the evil industry or the business industry and sometimes both. The business industry has grown out of necessity due to the increase of malicious hacking activity on the Internet" (p. 7).

As technology has become an important component to the human way of life, hacking has manifested itself in the form of two industries – an underground industry that is based on greed, theft, chaos, and human trafficking, and a business industry that survives based on its ability to combat that of the underground (Bowles, 2012). The hackers of the underground consist of 'all sorts of deviants who troll the Internet looking for weaknesses that they can exploit to their gain', while the business industry consists of professionals who develop tools and products to keep the underground hackers out (Bowles, 2012; Summers et al., 2013; Xu et al., 2013).

Today, the most common hacks come in the form of web application attacks, denial of service, malware, advanced persistent threats (APT), and social engineering. Some researchers argue that these attacks, used for malicious reasons, are typically carried out driven by motives of reputation, political protest, and monetary gain (Bowles, 2012). Hacktivism has become a common way of protest, as can be seen with hacking

groups like Anonymous and Lulzsec[7]. Hacktivist groups usually target governments, corporations, or social groups that have wronged others.

Another aspect of today's hacking includes cyber warfare, which can be defined as "actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption" (Bowles, 2012; Clarke & Knake, 2011; Summers et al., 2013). An example of cyber warfare as described by Bowles (2012):

> "The Stuxnet computer worm was one of the most eye opening cases of what might be classified as cyber warfare or APT. While the authors of the worm are still in question, the target was definitely the Iranian nuclear program. The worm sabotaged centrifuges used to enrich uranium, causing them to behave erratically. It was not only a worm but also contained a rootkit to hide its presence on systems that it had infected. Stuxnet was the first threat of its kind which brought to light just how devastating an advanced focused attack can be" (p. 9).

On the other hand, the professional information security business involves using risk management, penetration testing, incident response, and intrusion detection to mitigate the risks of falling victim to attacks like web application attacks, denial of service, malware, advanced persistent threats (APT), and social engineering. An entire sub-industry has emerged around security products and services, consisting of information security professionals are tasked with defending against, tracking, and pursuing black hats – while staying within the rules of the law (Bowles, 2012; Clarke & Knake, 2011).

[7] As protest can be considered a legitimate mechanism for making one's political voice heard, this researcher attempts to refrain from referring to hacktivism as a part of the evil industry; however, it should be noted that hacktivist groups common utilize unauthorized access to computer systems as a mechanism of protest. This is a fuzzy gray line and it is not the intent of this paper to debate the legality of hacktivism Caltagirone, S. A Practical Ethical Assessment of Hacktivism, Jordan, T., & Taylor, P. A. 2004. ***Hacktivism and cyberwars: rebels with a cause?***: Psychology Press, Thomas, J. 2001. Ethics of Hacktivism. ***Information Security Reading Room***, 12..

Hackers are one of the great sources of creative innovation of our time (Murray, 1997) yet remain crudely understood and understudied in organizational management theory. Hence to alleviate this lack of knowledge, I seek in this thesis to understand the cognition of hackers, their mental models, the cognitive skills and traits involved, and particularly their effects on learning and forward thinking. My main focus is *not* on the technical implementation as an outcome of such learning and forward thinking. Rather, my focal point is the cognitive abilities present that enable hackers to dynamically construct advanced knowledge for enigmatic problem solving and transfer of learning (Jonassen, 1995). My approach is not to understand *what* is learned by hackers, but rather *how* learning and forward thinking are achieved. I define learning as a hacker's shift in mental models (Norman, 1983a; Piaget, 1973) and forward thinking as the predictive power of those mental models (Norman, 1983a). So my interest lies specifically in different ways intrinsic individual characteristics, perceived skills, and perception of environment influence potential shifts in mental models and develop their predictive power (Summers, Lyytinen, & Gaskin, 2014; Summers et al., 2013). My motivation for understanding the *how* element of this process comes from my life experience as a hacker, both as a black hat when I was young and as a white hat designing systems to protect the nation's critical infrastructure. I have experienced the obsessive exploration of technological puzzles, observed my peers do the same, and wondered what lie within the mind. I have been deeply concerned by how hackers have been recognized as an important entity within today's technologically-driven society; however, we struggle to reach a legitimate understanding of this population.

Due to a paucity of a body of empirical and theoretical literature on the topic, I reviewed the cognitive and educational psychology concerned with the development of higher mental functions necessary for such activities as computer programming. Due to the millions of people involved in the programming process (Boehm, 1977) and the complexity of the activities required, there has been ample interest in the cognitive psychology (Brooks, 1977). This interest has led to the development of a small, but growing body of studies (Brooks, 1977). The extant literature indicates that the mental activities engaged by programming a computer and hacking are comparable (Coleman, 2013; Graham, 2008; Hafner & Markoff, 1995; Lakhani & Wolf, 2005; von Krogh & Von Hippel, 2003). By building on this foundational knowledge, I pursued a multipronged research strategy: 1) analyzing the hacker thought processes; 2) identifying the cognitive skills and traits of the hacker; and 3) using a cognitive psychology lens – the concepts of intrinsic individual characteristics, perceived skills and perception of environment- to examine their joint effects on the hacker's learning and forward thinking. I used a mixed method approach, because combinations of qualitative and quantitative methods are best suited in situations where the phenomenon is poorly understood, where access to data sources in the past has been insufficient, where a novel theoretical stance is expected and where research needs to be carried out through multiple phases (Creswell, Klassen, Plano Clark, & Smith, 2011; Tashakkori & Teddlie, 1998).

There are elements of the hacker mind and culture, such as social problem solving, system beautification and code aesthetic, and the creation of inventive solutions to ambiguous problems that imply linkages between hackers and the developing fields of design thinking and design attitude. However, the intent of this thesis was not to explore

those linkages but, in the Future Research section, I provide thoughts and potential implications that could results from the exploration of the intersection of these areas of interest.

The remainder of the dissertation introduction is as follows. First, I review relevant research literature on learning, forward thinking, intrinsic individual characteristics, perception of environment and perceived skills. Next, I discuss a theoretical framework that articulates the sensemaking and construction of derivational linkages between mental models necessary for skilled hacking. Next, I discuss the research plan and research design. Lastly, I conclude with a summary of results of remaining chapters and discuss how the results inform the extant literature and can be integrated to create a theory of cognitive psychology for hackers, specifically in learning and forward thinking competence.

LITERATURE REVIEW

In this section, I review concepts of learning, forward thinking, intrinsic individual characteristics, perceived skills, and perception of environment. I begin my discussion by introducing theories of how we know and how we understand using mental models. I then define learning as shifts in individual mental models and forward thinking as the predictive power of those models, i.e., the dynamism of an individual's sensemaking for problem solving and then using those models to forecast potential scenarios. I discuss how learning and forward thinking occur and how they occur for skilled hackers. I conclude with a discussion of intrinsic individual characteristics, perceived skills, and perception of environment and why they are important for gleaning insights into how hackers learn and perform forward thinking under different conditions.

Pragmatism

I approach the world in this thesis through the philosophical lens of pragmatism (Teddlie & Tashakkori, 2009; Van de Ven, 2007). Two philosophical theories underpin my orientation toward learning and forward thinking: Peirce's pragmatism (Peirce, 1974, 1997) and Dewey's pragmatism (Dewey, 2004; Scheffler, 2013). Peirce's concept of pragmatism addresses how we use abduction to acquire knowledge. Pragmatism, as stated by Peirce (1974), is 'nothing else than the logic of abduction". He suggested that there were three core propositions: (1) everything in our minds is based on something generated by our senses; (2) perceptual judgments include generality, which enables us to produce general statements based on them; (3) the subconscious uses abduction to produce perceptual judgments; the conscious mind does not criticize those perceptual judgments (Campbell, 2011). We acquire new knowledge through observation of a phenomenon, considering it in relation to other phenomenon, and proposing practical consequential hypotheses. The core premise of this form of pragmatism is that we see how we do something with the intention of getting better at it (Campbell, 2011). The study of learning, as proposed by Dewey (2001), is always active. Kivinen and Ristela (2003) point out that "from a Deweyan perspective, transaction between an organism and its environment is the basis for understanding all kinds of action and learning, including thinking and knowing. For Dewey, we gain knowledge by acting and interacting with the environment.

These philosophical lenses of Peirce and Dewey provide the motivation for a focus on individual learning within a social context of a human enterprise where cognitive structures are used to learn and used to predict: how we, as individuals, perform

personal reflection, are connected to social structures, perform social exploration, how we learn, and how we understand complexity around us.

Learning

I next focus on learning and the role of mental models within the context of hacking. By 'mental model', I mean a cognitive representation of a system, its component parts, and their behaviors, constructed as a means for understanding (Halasz & Moran, 1983; Kieras & Bovair, 1984; Norman, 1983a; Young, 1981). When interacting with systems, hackers form internal representations or mental models which provide explanatory capabilities for understanding that system and others with which it interacts (Gentner & Stevens, 1983a; Norman, 1983a; Staggers & Norcio, 1993). These cognitive structures are instrumental to the ways in which a hacker learns a specific domain within the individual and social contexts. The cognitive structures of the individual improve and adapt through accessing the expertise, experiences, insights, and opinions of others (Gray & Meister, 2004). They enable individuals to organize their knowledge to guide perception and inference (Fiske & Taylor, 1991). Within the context of hacking, *learning* involves that point which an individual hacker's cognitive structures have improved over time.

Researchers have referred to learning as new insights or knowledge (Argyris & Schon, 1978; Hedberg, 1981); new structures (Chandler, 1962); new systems (Jelinek, 1979; Miles & Cameron, 1982); mere actions (Cyert & March, 1963; Miller & Friesen, 1980); or some combination of the above (Bartunek, 1984). These phenomena refer to the ability to change behavior to adapt to the environment. Learning, in this context, involves building cognitive structures as a key component of the adaptation process.

Throughout the literature is the belief that learning improvements lead to improved future performance (Fiol & Lyles, 1985). Learning enables the understanding and interpretation of the environment; but also enables the creation of possible strategies – going forward – resulting in associations, cognitive structures, and memories.

Anchored in cognitive psychology (Leahey & Harris, 1989a), this research is concerned with exploring the ways in which hackers gain an understanding of their world by dynamically constructing and maintaining their mental models for problem solving and decision making (Frederiksen, White, & Gutwill, 1999). These cognitive structures assist with information interpretation and retrieval; thereby facilitating the integration of knowledge, both new and previously know (Leahey & Harris, 1989a). A hacker's mental models reflect their beliefs, observations, and inferences about a system, their components, and user interaction. Within the context of hacking, mental model dynamism is instrumental to enabling hackers to pick up new programming languages, find and fix bugs in computer code, and analyze the behaviors of a system and its users (Coleman, 2013; Summers et al., 2014; Summers et al., 2013).

Hackers – considered the epitome of knowledge workers – engage in just-in-time learning of new skills and which they use to clarify and extend their knowledge (Brandt, Guo, Lewenstein, Dontcheva, & Klemmer, 2009). This opportunistic form of learning facilitates the *prototype, ideate, and discover* methodology used by programmers and hackers alike. This methodology is used when, as described by Brandt et al. (2009) they want to build a minimally viable prototype to explore ideas – similar to scientists writing code to control for laboratory experiments or entrepreneurs construct complex spreadsheets to better understand business operations. Like programmers, to create

applications or tools quickly, hackers will take a bricolage approach by modifying and mashing up existing systems or code (Lieberman, Paternò, Klann, & Wulf, 2006; MacLean, Carter, Lövstrand, & Moran, 1990; Turkle & Papert, 1990). As part of this process, they must learn on-the-fly. The literature indicates that this form of learning and cognitive scaffolding is instrumental to a hacker's success (Brandt, Guo, Lewenstein, & Klemmer, 2008; Hartmann, Doorley, & Klemmer, 2008).

Forward Thinking

Forward thinking, the predictive power or ability to generate testable predictions that mental models provide to people when understanding complexity and problem solving. Mental models provide people with predictive power in that they enable an individual to understand and anticipate the behaviors being observed (Norman, 1983). When a person runs a model in their mind - internal experiments (Rasmussen, 1983) - reflect on its emergent behaviors, and infer linkages with other models, it enables them to predict and understand future behaviors (Frederiksen, White, & Gutwill, 1999; Norman, 1983). Rasmussen (1979b) suggests that these models are instrumental in predicting system response based on knowledge of the input information, the intention/purpose of the system and the system designer. Based on this, he asserts that mental models are for predicting future events, finding causes of observed events, and determining appropriate actions to cause changes (as cited by Rouse & Morris, 1986).

Forward thinking - performing anticipatory thinking to impact oneself and/or their environment - can involve actively adapting to new environments (Ashford & Black, 1996; Kim, Cable, & Kim, 2005; Saks & Ashforth, 1996; Wanberg & Kammeyer-Mueller, 2000), acting in advance to influence environmental factors (i.e. other

individuals, groups, etc.) (Kipnis & Schmidt, 1988; Williams, 1976), and realizing ideas and solving problems (Parker, Williams, & Turner, 2006). Mental models enable hackers to be future-focused (Frese & Fay, 2001) and mindful (Langer, 1989; Sternberg, 2000; Weick & Roberts, 1993); thereby, being instrumental to the "thinking, deliberating, planning, calculating, and acting in advance with foresight about future events before they occur" (Grant & Ashford, 2008: p. 9). It relies on envisioning possible futures and mentally constructing a picture of an object, person, or event which may exist at some point forward in time (Beach, 1990; Karniol & Ross, 1996; Taylor, Pham, Rivkin, & Armor, 1998). According to Kosslyn (1987), this envisioning serves two key functions: (1) enabling hackers to *see* how events will unravel; and (2) enabling them to understand and process information (as cited in Grant & Ashford, 2008). Forward thinking enables hackers to construct a conceivable version of future events and see it unfold which arouses emotional reactions and inspires problem solving (Taylor et al., 1998). Another benefit of forward thinking is that it facilitates advanced preparation for an activity (Little, 1983; Nurmi, 1991) by constructing links between one's expectations and future goals to actionable outcomes (Ajzen, 1991; Frese & Fay, 2001). It is this thoughtful reasoning that enables hackers to act with foresight to consider future problems and identify future opportunities (Frese & Fay, 2001).

To our knowledge there are no studies which have examined forward thinking and the related cognitive skills, and traits of hackers. We will review what we know about these cognitive skills and traits.

Knowledge Acquisition and Transfer

The literature is abound with studies on learning and knowledge transfer; however, within the context of this research, there are three key elements instrumental in acquiring new knowledge and applying it (Baldwin & Ford, 1988). One element is the individual's underlying cognitive attributes, another is the individual's established skill and competence, and the other is their consciousness of the work-environment. In this section, I review research on intrinsic individual characteristics, perceived skills, and perception of environment.

***Intrinsic individual characteristics*.** In learning environments, such as the workplace, intrinsic individual characteristics including creativity (De Bono, 1992; Eskildsen, Dahlgaard, & Norgaard, 1999) and curiosity (Berlyne, 1978; Loewenstein, 1994) enable individuals to make sense of and use varying amounts of disparate information (Reio & Wiswell, 2000).

***Creativity*.** Research on creativity identifies it as a cognitive trait that enables people to see the detail of a subject, formulate solutions to problems, and generate novel ideas (Gurteen, 1998; Reid & Petocz, 2004). Hackers believe hacking computer systems to be a creative endeavor requiring inquisitiveness and adaptability. Carrying out a successful hack can necessitate writing novel code or identifying indirect methods of achieving a goal which relies heavily on the hacker's creativity (Summers et al., 2014; Summers et al., 2013; Tiwana & Mclean, 2003). Tiwana and Mclean (2003) propose that creativity facilitates the improvisational mental process where individuals, alone and within groups, develop relationships between ideas. Further, they suggest that this process plays an important role in the generation and evaluation of ideas, design, and

solutions (Summers et al., 2014; Summers et al., 2013; Tiwana & Mclean, 2003). **Ocker, Hiltz, Turoff, and Fjermestad (1995a)** proposed that creativity also enables hackers to conceive of multiple solutions to poorly-defined problems. Hackers are known for their propensity for finding creative solutions and making original discoveries; however, the creative element of the hacker mind is also evident in the way that they explore and ideate (Lakhani & Wolf, 2005; Nikitina, 2012).

***Curiosity*.** Research on curiosity defines it as a cognitive trait that drives the human desire to know, explore, see, and discover with the purpose of acquiring information (Berlyne, 1950; Berlyne, 1978; Litman, 2005; Loewenstein, 1994). More specifically, it is the driving force behind the exploration and probing of situations abound with uncertainty. Litman (2005) describes it as being an "appetitive desire", similar to that of food or sex and others where reward is experienced. This cognitive trait can be exhibited in two ways: (1) knowledge acquisition when an individual's curiosity has been aroused leading to an intrinsically rewarding and highly pleasurable experience (Day, 1971; Kashdan, Rose, & Fincham, 2004; Peterson & Seligman, 2003) and (2) elimination of undesirable states of uncertainty and ignorance (Berlyne, 1950; Berlyne, 1978; Litman, 2005; Loewenstein, 1994). When hackers are faced with problems that they have never seen before, it is their curiosity that drives their desire to explore the situation. In fact, in some cases, hackers seek out these exploratory opportunities (Berlyne, 1950; Berlyne, 1978; Summers et al., 2014; Summers et al., 2013). Hebb (1955) explains that this curiosity-seeking behavior is driven by the pleasure of threats and puzzles. Further, the literature recognizes that hackers engage in intensive and focused activities to explore the nature of problems with which they are faced (Coleman,

2013; Jordan & Taylor, 1998; Levy, 1984; Summers et al., 2014; Summers et al., 2013; Taylor, 1999; Thomas, 2002). In order for us to understand how a hacker learns or anticipates, we must understand the motivational components of the hacker mind such as curiosity – the enjoyment in finding out facts and learning new things (Schifreen, 1994).

Perceived Skills

The research indicates that the teleonomy of self is characterized through two variables: (1) perceived challenges (intrinsic demands); and (2) perceived skills (self-perceived capacity to meet demands) (Massimini, Csikszentmihalyi, & Carli, 1987; Moneta & Csikszentmihalyi, 1996). In terms of this research, I will focus on the latter since *intrinsic individual characteristics* address much of the intrinsic demand via *curiosity* and *creativity* experienced by hackers. There is a direct correlation between a person's perceived skills and the quality of their work, learning and knowledge transferability (Baldwin & Ford, 1988; Lim & Johnson, 2002). Within hacker-centric environments, an individual's domain knowledge and comprehension techniques are instrumental in facilitating their ability to understand complex problems.

Domain expertise. There is an abundance of research on domain expertise; however, our review of the empirical research recognizes Dreyfus, Dreyfus, and Zadeh (1987b) and Benner (1983) who both found that expertise is not innate and that human beings must learn to become masterfully proficient at a skill. Learning takes place through trial and error and is sometimes guided by imitating others who are more proficient (Dreyfus et al., 1987b). A person has reached the expert level when they no longer have to rely on principles to connect their understanding of a situation to the appropriate response (Benner, 1983). There has been extensive research on expertise in

software design and programming exploring how experts differ from novices (Adelson, 1984; Jeffries, Turner, Polson, & Atwood, 1981; Sonnentag, Niessen, & Volmer, 2006). This body of research provides scientific insights into the processes associated with expertise within this complex domain. Similarly, the domain of hacking consists of specific tasks such as requirement analysis, software design, programming, testing, and debugging which are recognized in the literature as being ill-defined (Simon, 1977; Sonnentag et al., 2006). In their review of programming expertise, Campbell, Brown, and DiBello (1992) argued that due to the non-unitary nature of programming, the prevailing binary novice-expert comparisons provided little explanation of the psychology of programming. They found that when learning a new technology or new programming language expert programmers "become novices again". As a result, they concluded that for expert programmers, there is an evolutionary progress from "cookbook" to "intuition" as described by Dreyfus & Dreyfus (1986). Throughout the literature and history of hackers, technical expertise has been one of the consistent themes discussed in regard to hacking performance and abilities; therefore, we found it advantageous to understand the true reach and extent to which expertise could be developed and utilized in the hacker mind.(Coleman, 2013; Mayer, 1981; Taylor, 1999; Thomas, 2002).

Diagramming. The literature is abound with research on metacognitive methods and techniques to provide scaffolding for learners complex tasks and to assist with enabling them to deal with complex content and complicated skill demands (Davis, 2000; Edelson, Gordin, & Pea, 1999; Guzdial, 1994; Quintana, Eng, Carra, Wu, & Soloway, 1999; Reiser, 2004). For example, researchers propose that graphical representations are

instrumental in helping learner plan and organize their problem solving (Quintana et al., 1999) and assist learners with keeping track of steps taken to solve the problem at hand (Collins & Brown, 1988; Koedinger & Anderson, 1993). Several researchers have suggested that when a learner sees a visual stimulus such a diagram or concept map, a procedure called perceptual organization occurs (Henderson, 1999; Navon, 1977; Pylyshyn, 1984; Ullman, 1989). Winn (1993) proposed that perceptual organization involves the learner scanning for similarities and differences amongst the constructs represented and groups or connects them with lines and other visual artefacts. Metacognitive tools like concept mapping, mind mapping, network diagrams, and other graphical representations are recognized as influencing learning, especially in learning how to program (Ainsworth & Th Loizou, 2003; Henderson, 1999; Novak, 1990a, b; Novak, Bob Gowin, & Johansen, 1983). I refer to this type of metacognitive learning as diagramming. Diagramming represents visualization techniques used by hackers to create technical drawings to explore and understand associations and relationships between concepts (Summers et al., 2013). Utilization of these techniques enables hackers to represent and manipulate complex problems and have a better understanding of relationships and more thoroughly analyze each component (Davies, 2011). Researchers have suggested that diagramming promotes deep learning of a problem (Entwistle, 1981b; Marton & Säljö, 1976c; Novak, 1990b). Scaife and Rogers (1996) argue that diagramming offers three substantial advantages for learning: (1) computational offloading, the extent to which different representations reduce the amount of cognitive effort required to solve problems; (2) re-representation, the way that alternative external representations that have the same abstract structure, differentially influence problem

solving; and (3) graphical constraining, describing the limits on the range of inferences that can be made about the represented concept (Ainsworth & Th Loizou, 2003). Cox (1999) argues that diagramming is instrumental in constraining interpretation by limiting abstraction and providing learners with important and powerful feedback to perform comparative analysis with their explanations. For hackers, diagramming not only assist with associating ideas, but it is also important for mental model construction and maintenance (Davies, 2011). Diagramming promotes innovative thinking and brainstorming because of its ability to enable hackers to conceive of linkages between concepts (Novak & Cañas, 2006b). This is key for new learning and forecasting (Davies, 2011). In fact, I presume that there may be a correlation between the effectiveness of a hacker and their use of diagramming; however, it is not the aim of this paper to explore this subject. Understanding how hackers use diagramming provides insights into how they interact with graphical representations when learning, solving problems, and making inferences. This involves advanced specification of the cognitive mechanisms that I allude to throughout this body of work, but also introduces some sensitivities of the behavioral aspects of hacking as an activity.

Perception of Environment

Within any organizational construct, including that which includes hackers, it is important to understand the ways in which environmental factors constrain the structure of the organization and the behavior of its participants (Dill, 1958). The literature is abound with research on the central concepts of uncertainty and the perception of it, particularly as they relate to theories that seek to explain the nature of organizations and their perception of the environment (Dill, 1958; Duncan, 1972; Lawrence & Lorsch,

1967; Thompson, 1967). By identifying and understanding the relevant environmental factors and their impact on behaviors, we gain insights into the *demands* that participants are subjected to in order to be successful within that environment. Organizational theorists have particular focused on one environment factor that has become recognized as perceived environmental uncertainty (Milliken, 1987). Milliken (1987) describes perceived environmental uncertainty as being experienced by organizational participants as they try to understand, make sense of and respond to conditions in the external environment. I refer to this participant awareness of the environment as *perception of environment*. Hackers operate within environments abound with uncertainty and ambiguity (Summers et al., 2013) which brings with it various demands (Dill, 1958), namely *ambiguity tolerance*. In such environments, hackers engage in daily challenges in a constantly changing work environment and therefore continuously constructing new meanings and knowledge; thereby learning (Kozlowski & Bell, 2008; Senge & Suzuki, 1994). They frequently encounter ambiguous specifications and problem statements. Often they are faced with situations where cues are nonexistent or insufficient, too numerous, or contradictory (Owen & Sweeney, 2002a). Hackers perceive themselves as not having enough information to predict all conceivable solutions to a problem; therefore, they must cope with this uncertainty (Summers et al., 2013).

Ambiguity tolerance. The topics of ambiguity tolerance has been explored extensively by theorists of various communities spanning from authoritarian syndrome to leadership (Mac Donald Jr, 1970). Mac Donald Jr (1970) suggests that "persons having high tolerance of ambiguity (a) seek out ambiguity, (b) enjoy ambiguity, and (c) excel in the performance of ambiguous tasks" (p. 791). An ambiguous situations is considered to

be one which is not adequately structured or characterized as lacking sufficient cues (Budner, 1962). Further, Norton (1975) argues that a problem can be considered ambiguous when there is variability in structure and understanding and when there is variability in the interpretations or potential responses. Hackers constantly handle problems that lack clarity, structure, and are abound with uncertainty (Summers et al., 2013). Whereas people who are intolerant of ambiguity tend to avoid or give up on learning in ambiguous situations, hackers are aroused by them (Coleman, 2013; Owen & Sweeney, 2002a; Summers et al., 2013). Hackers solve advanced technical problems under uncertainty and ambiguity – a central component of the management of technology and innovative thinking. Being able to function in this type of environment means that hackers are willing to question their current assumptions and solutions in search of a definitive solution. In this way, problem solving for hackers is about the reduction of ambiguity (Schrader, Riggs, & Smith, 1993).

THEORETICAL FRAMING

What is Known

What we know from extant research related to the mental models and cognitive skills and traits of hackers can be organized into three categories drawn from the literature review on computer programming: expertise, individual characteristics, and learning. Table 1 lists the key foundational knowledge salient to our study.

Table 1: What We Know Concerning Hackers and Their Mental Models

KNOWN	DESCRIPTION	SOURCE
Independent Variables (IVs)	Knowledge models of experts influence performance	Vessey, 1985
	Experts have better mental models than novices	Cañas et al., 1994
	Experts maintain mental models to fit problem demands	Davies, 1994
	Diagramming helps plan and organize problem solving	Quintana, et al., 1999
	Diagramming assists with understanding complexity	Davis, 2000

Mediators	Creativity influences coding performance Intrinsic characteristics influence performance Curiosity increases programming mastery motivation Ambiguity tolerance positively impacts critical thinking Creativity effects how well code is interpreted Curiosity is a driver for learning to code People who design code are psychologically unique Environmental uncertainty enables forward thinking	Gotterer & Stalnaker, 1964 Mayer & Stalnaker, 1968 Jennings, Connors, & Stegman, 1985 Facione, Facione, & Sanchez, 1994 Tilley, Paul, & Smith, 1996 Jenkins, 2001 Capretz, 2003 Grant & Ashford, 2008
Dependent Variables (DVs)	Mental models increase coding success Mental models facilitate meaningful learning Learning to code develops problem solving skills Learning to code develops higher mental functions Mental models improve code evaluation/generation Mental models improve code self-efficacy and performance Forward thinking improves problem solving Forward thinking improves adaptation in new environments	Brooks, 1977 Mayer, 1981 Adelson, 1983 Pea & Kurland, 1984 Shih & Alessi, 1993 Ramalingam, LaBelle, & Wiedenbeck, 2004 Grant & Ashford, 2008

What We Do Not Know

Three categories of unknowns challenge our understanding of the mental models and cognitive skills and traits of hackers: 1) factors that influence mental model dynamism; 2) cognitive faculties involved with hacking; 3) combined effects of individual characteristics; and 4) impact on learning and forward thinking. These unknowns, depicted in Table 2, provide the basis for articulating my research questions, as will be discussed next.

Table 2: Unknowns Concerning Hackers and Their Mental Models

UNKNOWN	DESCRIPTION	GUIDING RESEARCH
Independent Variables (IVs)	Is expertise the primary factor in learning and forward thinking? To what degree does expertise impact learning and forward thinking for hackers? To what degree does diagramming impact learning and forward thinking?	Dreyfus et al., 1987 Campbell et al, 1992 Tiwana & Mclean, 2003 Ainsworth & Th Loizu, 2003
Mediators	What are the characteristics of skilled hackers? What cognitive faculties are involved in the act of hacking? What are the cognitive skills and motivational traits of hackers? How are individual characteristics impacted by sociocultural issues?	Berlyne, 1978 De Bono, 1992 Loewenstein, 1994 Gurteen, 1998 Henderson, 1999 Owen & Sweeney, 2002 Novak & Cañas, 2006 Grant & Ashford, 2008

	What are the combined effects of creativity and curiosity on learning and forward thinking? How do changes in the environment impact hackers?	Nikitina, 2012
Dependent Variables (DVs)	What factors influence how hackers construct and maintain mental models? To what degree do cognitive skills and motivational traits influence mental model dynamism? How does forward thinking occur for hackers? To what degree is learning impacted by sociocultural issues?	Vygotsky, 1978 Bruner, 1978 Norman, 1983 Morecroft, 1984 Soloway & Ehrlich, 1984 Vandenbosch & Higgins, 1996 Dewey, 1997 Frederiksen et al., 1999 Grant & Ashford, 2008 Argote & Miron-Spektor, 2011

A Tentative Theoretical Framework

Given the nature and dispersion of gaps in the literature, no single body of empirical or theoretical research exists to build upon and guide the research. As a result, I have chosen to integrate five disparate, but related streams of research to frame my study: mental models, skill acquisition, self-efficacy, flow, and systems thinking. Some of the frameworks assume a different unit of analysis; however, they collectively serve my research goals by providing basic building blocks upon which I can proceed. The mental model framework of Gentner and Stevens (1983a) and Johnson-Laird (1983) assumes an individual as the unit of analysis, but it helps to understand how hackers describe, explain, and predict during the learning process. The skill acquisition framework of Dreyfus et al. (1987b) uses an individual unit of analysis and provides insight into understanding what a skill is and what the hacker acquires when they achieve expertise. The self-efficacy framework of Bandura (1993) and Compeau and Higgins (1995a) uses an individual unit of analysis. It helps to understand how a hacker's

perceptions of their own abilities and environment can influence the decisions that they make. The flow framework of Csikszentmihalyi (1991), Moneta and Csikszentmihalyi (1996), and Lakhani and Wolf (2005) uses an individual unit of analysis. It helps to understand the intrinsic individual emotions and motivations of interest, enjoyment, and control linked to the process of hacking. The systems thinking framework of Senge and Sterman (1992) uses the organizational unit of analysis. It helps to understand how hackers learn complex systems and perform creative problem solving within ambiguous environments.

Mental models. A mental model is defined as "*a small-scale model* of external reality and of its possible actions" which enable an individual to try out various alternatives, deduce the best of them react to potential future situations before they occur, utilize knowledge of past events, and react in a more competent manner to new situations as they happen (Craik, 1943a; Johnson-Laird, 1980). Mental models are constructed and maintained by individuals but are shared within groups and the broader organization (Denzau & North, 1994; Mathieu, Heffner, Goodwin, Salas, & Cannon-Bowers, 2000). Mental models provide a mechanism through which an individual can think of a situation and an internal review of components, operating rules, and other attributes (Cañas, Bajo, & Gonzalvo, 1994; Mayer, 1981). An individual with complete, effective mental models have the ability to make quick decisions based on experiential knowledge, intuitive judgment, and heuristics. They enable the individual to describe, explain, and predict system behaviors and serve as a mneumonic mechanism for remember relationships and events (Williams, Hollan, & Stevens, 1983b). The construction and maintenance of mental models enables the individual to create descriptions of the situational purpose and

form, explanations of function, observed states and conditions, and predictions of future states and conditions throughout the learning process (Rouse & Morris, 1986).

Skill acquisition. The work of Dreyfus et al. (1987b) on skill acquisition postulates that an individual acquires new skill through education and lived experience, i.e., how the individual goes through various stages of qualitatively different perceptions of his task and mode of decision making as his skills improves. The individual traverses multiple stages from the position of being a novice to being an expert (Dreyfus et al., 1987b; Dreyfus & Dreyfus, 1980). Once an expert, the individual does not require conscious deliberation to complete a task and their performance is on-going and non-reflective. Dreyfus et al. (1987b) suggest that at the crux of their skill acquisition framework is the belief that "there is more to intelligence than calculative rationality" (p. 36). Expertise contributes to the completeness, stability, and parsimonious nature of an individual's mental models (Gentner & Stevens, 1983a); however, it does not provide insights into the specific individual cognitive characteristics involved: what specific cognitive characteristics or skills are used and how do they affect learning.

Self-efficacy. The work by Bandura (1993) on self-efficacy postulates that an individual's belief that they have the capabilities to perform a particular behavior has a substantial influence on their decisions about what behaviors to undertake. According to Compeau and Higgins (1995a), an individual's self-efficacy influences their decisions making, the amount of effort to expend and persistence, emotional reactions while performing, and the actual performance outcomes. Recent studies have found strong correlation between self-efficacy and computing performance, adoption of new technology, innovativeness, and performing in learning new systems (Compeau &

Higgins, 1995a, b). Ramalingam, LaBelle, and Wiedenbeck (2004) suggest that self-efficacy for computer programming is heavily influenced by previous experience and the use of mental models.

Flow. Flow is defined as the feeling of effortlessness experienced when highly engaged in a particular activity in such a way that the individual disregards time and other things not directly involved in the activity (Csikszentmihalyi, 1991). Csikszentmihalyi studied the creative process and became interested in understanding why it was that "when working on a painting was going well, the artist persisted single-mindedly, disregarding hunger, fatigue, and discomfort – yet rapidly lost interest in the creation once it has been completed" (Nakamura & Csikszentmihalyi, 2002). This model provides insights into the intrinsic motivation and the pursuit of an activity for fun or challenge rather than because of external pressures and encouragement (Lakhani & Wolf, 2005). Nakamura and Csikszentmihalyi (2002) suggest that the two conditions of flow are "perceived challenges or opportunities for action that stretch existing skills; a sense that one is engaging challenges at a level appropriate to one's capacities" and "clear proximal goals and immediate feedback about the progress that is being made" (p. 90). Csikszentmihalyi (1991) suggests that when a person is engaged in an enjoyable activity, they have feelings of creativity discovery, a challenge conquered, and a problem solved. Programmers express similar feelings and describe a state of flow when they are writing software for challenging projects (Lakhani & Wolf, 2005). According to Trevino and Webster (1992), there are four dimensions of flow in human-computer interaction: (1) the user perceives a sense of control over the computer interaction; (2) the user perceives that his or her attention is focused on the interaction; (3) the user's curiosity is aroused during

the interaction; (4) the user finds the interaction intrinsically interesting (as cited inVan Beveren, 2000, p. 4). However, the model does not provide insights into the effects of intrinsic individual characteristics as inputs to the learning process; nor does the model tell us which of the perceived skills or environmental perception the individual would use given these inputs or a detailed model of such interactions.

Systems thinking. I will finally use an organizational systems thinking model by Senge and Sterman (1992); Senge and Suzuki (1994), because it includes a method of analysis that encourages one to consider how things influence on another within a whole rather than thinking exclusively about the individual components of the whole. This model suggests that in order for to understand a system and its components, the individual or organization must understand the relationships between those components and other systems rather than considering any one component in isolation (Senge & Sterman, 1992; Senge & Suzuki, 1994). The systems thinking model focuses on how the component being studied interacts with other components within and outside of the system (Senge & Sterman, 1992). This encourages the individual to consider interactions between the components and the behaviors produced as a fruit of that interaction. This body of work suggests that individuals and organizations must expand their view and consider the various component-based interactions and resulting behaviors to explain how the system works (Senge, 1990). However, the model does not provide insights into the degree to which cognitive skills and individual characteristics effect the learning process.

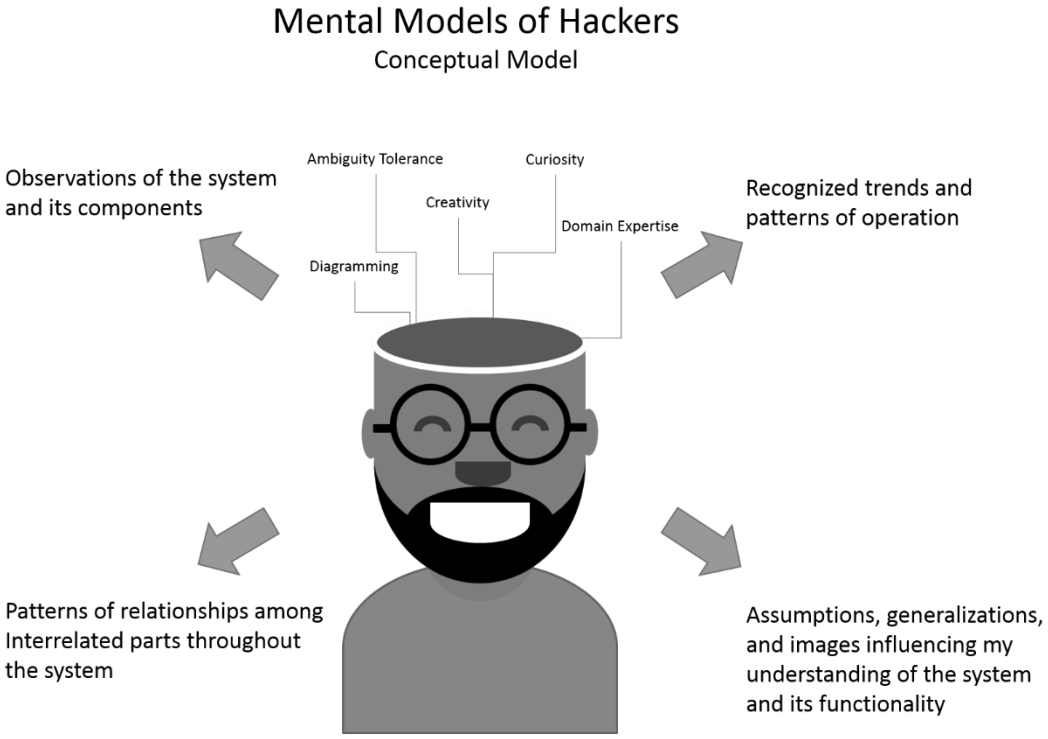
RESEARCH PLAN

Next, I will use these five frameworks to frame a study of the mental models of hackers within individual and social contexts – as to identify the cognitive factors – "the models that are the natural way in which the human mind constructs reality, conceives alternatives to it, and searches out the consequences of assumptions" that influence knowledge acquisition and use (Johnson-Laird, 1983; Johnson-Laird, 1980). I specifically seek to discover the hacker's cognitive skills and traits that are instrumental in the learning and forward thinking.

I will study the effects of such things as the user's technical expertise, previous experiences, and the structure of the human information processing system for the purpose of understanding how hackers learn – in terms of shifts in mental models – and how they perform forward thinking – building derivational linkages between models. Especially, I will try to understand how and understand under what conditions these shifts and linkages occur. The literature reveals that nearly all previous studies, at the individual and organizational unit of analysis, did not include an analysis of the cognitive structures or necessary cognitive skills and traits applicable to hackers. If I find that such structures, skills, and traits affect learning and forward thinking, then my research will provide an original and significant contribution to the fields of organizational learning, information systems, mental models, and information security. Figure 1 provides an overview of the high level conceptual model that informs my study. While I theorize that the mental models of hackers are affected by certain cognitive skills and traits, and how they impact the ways in which hackers acquire knowledge and perform speculative forecasting, my study focuses on hackers, their views of the world, of themselves, of their

own capabilities, and of the tasks that they are asked to perform, and topics they are asked to learn.

Figure 1: Conceptual Model of the Mental Models of Hackers



The three areas of unknowns noted above – expertise, individual characteristics, and learning- provide the motivation for my research questions. In Table 3, I map these unknowns to key research questions and specific theoretical frameworks that inform my subsequent attack on these research questions.

Table 3: Mapping Research Questions to Theoretical Frameworks

UNKNOWN	RESEARCH QUESTION	GUIDING FRAMEWORK(S)	REFERENCE(S)
Technical skills and hacking.	1. What effect do technical skills like domain expertise and diagramming have on the hacker's ability to learn and forward think – and their effect on the intrinsic individual characteristics?	Mental Models Skill Acquisition	Johnson-Laird, 1980 Norman, 1983 Dreyfus et al., 1987
Awareness of environmental requirements.	2. What is the effect of ambiguity tolerance on the learning and forward thinking of hackers? Is this effect impacted or facilitated by intrinsic individual characteristics?	Mental Models Systems Thinking Self-Efficacy	Johnson-Laird, 1980 Norman, 1983 Compeau & Higgins, 1995
Effects of creativity and curiosity on learning and forward thinking.	3. What are the effects of creativity and curiosity (combined and individually) on how hackers learn and perform forward thinking?	Mental Models Flow Self-Efficacy	Johnson-Laird, 1980 Norman, 1983 Csikszentmihalyi, 1991 Compeau & Higgins, 1995
Learning and Forward Thinking.	4. What impact do the cognitive skills and traits identified have on the mental model dynamism and anticipatory thinking of hackers?	Mental Models Skill Acquisition Systems Thinking	Johnson-Laird, 1980 Norman, 1983 Dreyfus et al., 1987 Senge & Suzuki, 1994

RESEARCH METHODOLOGY

I selected an open mixed method approach to address my research questions. The approach combines qualitative and quantitative research methods in an open ended sequence. The philosophical direction of pragmatism embraces both methods and serves as a reasonable foundation for my research design (Creswell et al., 2011; Teddlie & Tashakkori, 2009). When conducting mixed methods research, one must strongly consider the quality and validity of the research design (Bryman, 2007; Bryman, Becker, & Sempik, 2008). The researcher needs to have a sufficient reason as to why the specified mixed method design is used. The most commonly referenced reasons for combining research methods are triangulation, complementarity, development, initiation,

and expansion (Bryman et al., 2008; Creswell et al., 2011; Greene, Caracelli, & Graham, 1989).

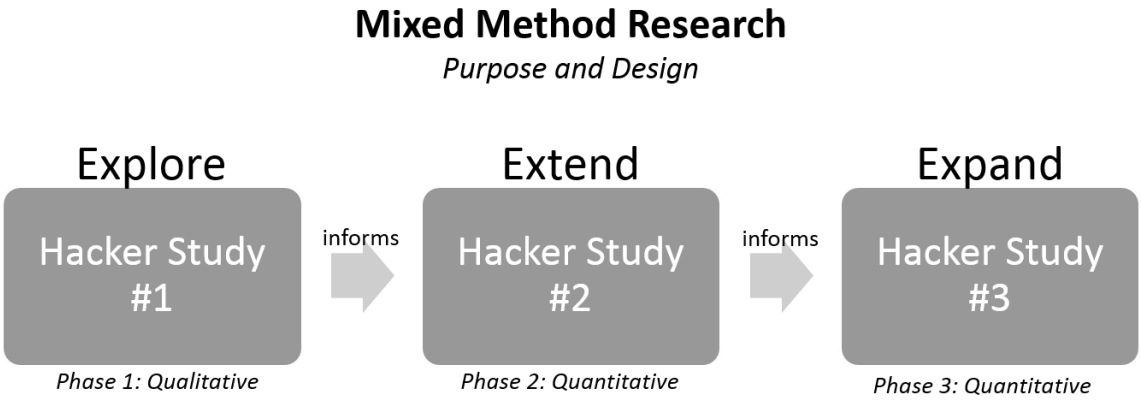
The purpose for my research is primarily expansion, which "…seeks to extend the breadth and range of inquiry by using different methods for different inquiry components" (Greene et al., 1989: 259). I intend to first use a qualitative/quantitative method to answer a research question about an unknown for which little or no prior research or knowledge exists, which then informs a subsequent research question about an unknown to be answered by another appropriate method to expand the depth of understanding from findings of prior methods, ensuring that the research design remains open.

The secondary reason is triangulation, which "…seeks convergence, corroboration, correspondence of results from the different methods" (Greene et al., 1989: 259). Collecting multiple types of data offers ways to validate findings about the data source across multiple methods and to a lesser degree, complementarity. Given the nascent level of theory and empirics in the study field, this combination of purposes is considered appropriate.

Since my primary purpose is expansion, an appropriate research design that builds upon the results of successive results demands a multiphase design (Creswell et al., 2011). A multiphase design sequentially combines multiple qualitative and quantitative studies. The reason for a multiphase design is "…to examine a topic through an interaction of connected quantitative and qualitative studies that are sequentially aligned with each new approach building on what is learned previously" (Creswell et al., 2011). As appropriate for my research questions, I will engage in the expansion three times:

from the 1st to 2nd research question; from 2nd to the 3rd research question. Figure 2 summarizes the key elements of research purpose and design. Decisions to connect the results within a multiphase design – creating meta-inferences – will be drawn from the collection of analysis results across multiple projects (Creswell et al., 2011).

Figure 2: Research Purpose and Design



Purpose for Expansion:
Seek to extend the breadth and range of inquiry by using different methods for different inquiry components. (Greene et al., 1989)

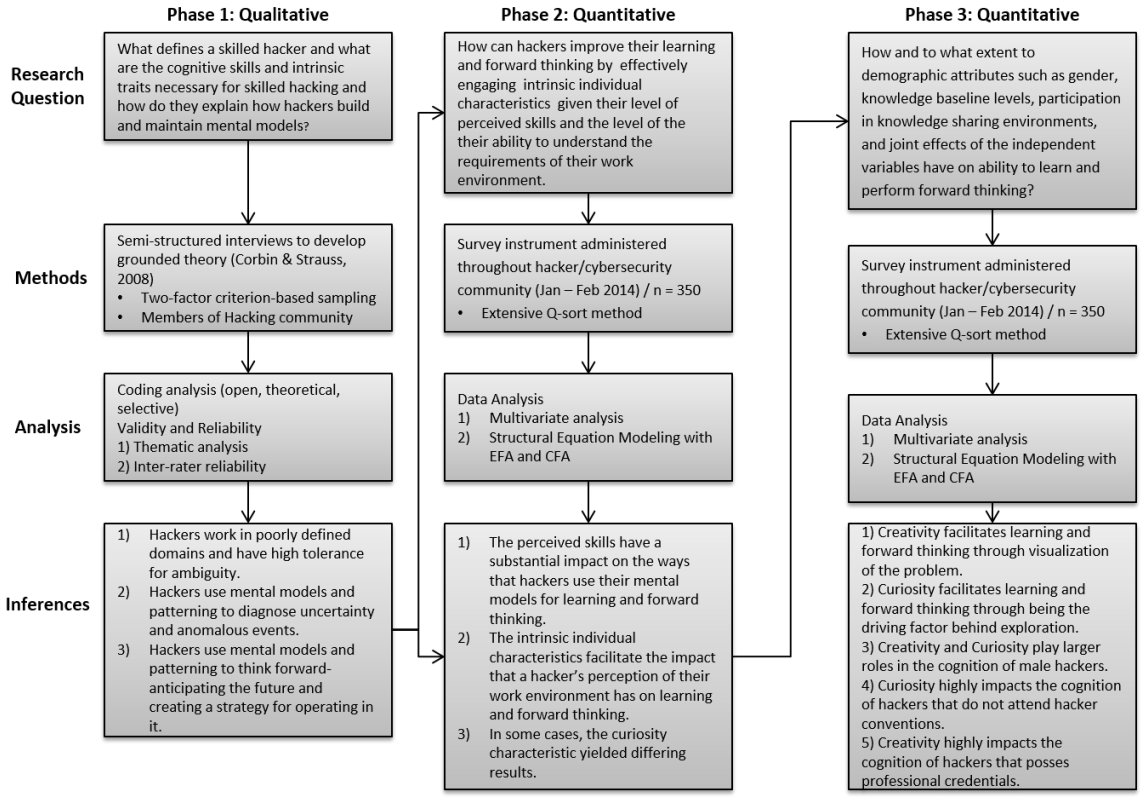
Reason for Multiphase:
To examine a topic through an interaction of connected quantitative and qualitative studies that are sequentially aligned with each new approach building on what is learned previously. (Creswell et al., 2011)

Since my first research question asks about uncovering the experience of hackers, I decided to deploy a qualitative method. The second and third questions seeks to understand the effects of causal mechanisms on hackers; hence I chose a quantitative method. The mixed method notation for my overall multiphase design is thus QUAL →QUAN → QUAN (Creswell et al., 2011).

My research answers three research questions over the course of three studies: Hacker Study #1; Hacker Study #2; and Hacker Study #3. Figure 3 organizes in more

detail the research questions and methods associated with each question as well as the overall flow of the study and related inferences. In the next section, I summarize respective results from each phase, and what subsequent research questions were informed by these results.

Figure 3: Multiphase Mixed Method Research Design



The first research question is: What defines a skilled hacker and what are the cognitive skills and intrinsic traits necessary for skilled hacking and how do they explain how hackers build and maintain mental models? Since little, if any, prior research provides insight into the cognitive structures, skills, or traits of hackers in individual or social contexts, I selected to elicit the lived experiences of hackers to derive cognitive theory of the hacker mind.

The research therefore studies, in an open ended manner, the structure and content of the mental models used by hackers and to what extent different factors are instrumental in shaping the acquisition, maintenance, and use of mental models critical for hacking. The research context mobilizes a host of individual and social cognitive mechanisms drawn from the experiences, feelings, and behaviors of active members of the black hat and white hat hacking communities (Strauss & Corbin, 1990b). Within this novel and complex community, I engage in a rich and naturalistic inquiry to gain a deeper understanding of the cognitive structures, skills, and learning attributable to these individual who are involved in this complex, cognition-intensive process. Therefore, to understand the perceptions, beliefs, and attitudes of the source (i.e. hackers) not only relevant to the activity of hacking, but also other social and cognitive interactions that occur leading up to and after the hacking activities, I use a qualitative, grounded theory study that draws upon semi—structured interviews. This resulted in the first paper, "How Hackers Think: A Qualitative Study of Cybersecurity Experts and Their Mental Models", which is next summarized and attached as a whole in Appendix A. It is important to note that due to the controversial nature of the hacking community, the identities of the study participants is not exposed.

The second research question is: How can hackers improve their learning and forward thinking by effectively engaging intrinsic individual characteristics given their level of perceived skills and the level of their ability to understand the requirements of their work? This question seeks to generalize some findings from the first study, apply them across the population. Using a number of key constructs identified in the first study, I explore the explanatory power of perceived skills (i.e., domain expertise and

diagramming), perception of environment (i.e., ambiguity tolerance), and intrinsic individual characteristics (i.e., creativity and curiosity). I seek to understand how the varying effects of perceived skills, perception of environment, and intrinsic individual characteristics hinder or strengthen the learning and forward thinking of hackers. To answer the second question, I use a quantitative survey-based study documented in the second paper, "How Hackers Think: Understanding the Mental Models and Cognitive Patterns of High-Tech Wizards". The study is summarized next and attached as Appendix B.

The third research question is: How and to what extent do sociocultural facets, such as gender, participation in intellectual capital sharing environments, and possession of professional credentials, impact the learning and forward thinking of hackers by effectively engaging their intrinsic individual characteristics given their level of perceived skills and their ability to understand the requirements of their work environment? I seek to understand how sociocultural factors effects how hackers utilize their cognitive skills and traits to make meaning of their environmental complexity. To answer the third question, I use a quantitative survey-based study documented in the third paper, "How Hackers Think: Sociocultural Facets and Understanding Their Impact on the Hacker Mind". The study is summarized next and attached as Appendix C.

Overall, I adopted an open multi-phase mixed method design where methods were sequentially deployed, each one designed to answer questions arising from previous studies. The multiphase design, I suggest, is also the best method to successively achieve a deeper understanding of a nascent research topic. Hence the primary purpose of the design is to expand our understanding of poorly understood phenomenon and the

secondary purpose of triangulation is to corroborate findings. Next, I discuss in detail the methods used in each research study.

Method – Hacker Study #1

As previously noted, this study used a qualitative method employing grounded theory (Glaser & Strauss, 1967a). Grounded theory is the discovery of theory from data systematically collected and analyzed within social research without making assumptions a priori (Glaser & Strauss, 1967a). Grounded theory is particularly advantageous when there is a dearth of refined theory and empirical studies on the research phenomenon. Additionally, since grounded theories are not tied to any preexisting theories, they often results fresh, innovative discoveries. Using semi-structured interviews, I interviewed eighteen hackers selected using a criterion-based sampling to ensure the collection of quality information (Turner, 2010). The final selected hackers were recognized within the community as experts and employed by foreign and domestic governments, private companies, or independent consultancies. I did not include hackers that were directly involved with organized crime groups for consideration of time and safety; however, some of the participants admitted to having consulted by such groups. The data was analyzed through an iterative process – involving constantly reviewing the data, the literature, field and observational notes, and the theory being development (Strauss & Corbin, 1990b). I carried out axial coding and thematic coding to discover systematically emergent interpretations (Corbin & Strauss, 2008). Based on this analysis, I developed a conceptual model of personal cognitive skills and social cognitive skills central to the task of hacking. The reader should note that these dimensions were not theorized

beforehand, but emerged from the data. The model was then used to generate a set of hypotheses that were tested in the second study using quantitative methods.

Method – Hacker Study #2

This study answered the second research question. I sought to validate a research model and associated set of hypotheses. We carried out an electronically disseminated, Internet-based, self-administered survey within a population of hackers and experts within the cybersecurity field. A total of 350 usable responses were collected during January – February 2014.

The hypothesized model involved seven constructs, all of which were measured with reflective scales. The model tested the direct effects of perceived skills and mediation effects of two intrinsic individual characteristics – creativity and curiosity – on hacker learning and forward thinking. I used structural equation modeling (SEM) to conduct the test as it allowed for the simultaneous evaluation of all of the construct and their potential causal effect on learning and forward thinking (Hair, Black, Babin, & Anderson, 2010a). I used techniques offered by SEM to evaluate the presence of mediating effects related to intrinsic individual characteristics. This led me to articulate new questions, which served as an impetus for the Hacker Study #3 discussed in the next section. The reader should note that in order to increase reliability, minimize measurement error, and improve the validity of my constructs, I pretested the scale items using a specialized Q methodology process which is detailed in the appendix of the second study.

Method – Hacker Study #3

This study answered the third research question. Once again, I sought to validate a research model and associated set of hypotheses. I used the same survey data from the second study. The hypothesized model tested the moderated mediation effects of three sociocultural facets – gender, participation in intellectual capital sharing environments, and possession of professional credentials – via the previously utilized constructs on hacker learning and forward thinking. Next, I will review the results of the three studies.

OVERVIEW OF RESULTS

Up until now, I have used a singular pronoun to reflect my single ownership of the research up to this point. While describing the overview of the results, I will change to use the plural pronoun of 'we' to reflect the joint co-authorship of these studies. I will switch back to first person pronoun in the discussion section to reflect my single authorship of this part of the dissertation.

Study I: How Hackers Think: A Study of Cybersecurity Experts and Their Mental Models

Summary of Findings

Finding #1: Hackers have a high tolerance for ambiguity in their work environment.

First, hackers have a high tolerance for ambiguity in their work environment. In order to effectively handle the risk, uncertainty, and vagueness associated with operating in ambiguous environments, hackers had to leverage their expert knowledge, creativity, curiosity, and interpretive schemas from across various technical and critical thinking disciplines. Within these poorly defined, ever-changing domains are many peculiar questions and issues which lack clarity and specification. Specifically, hackers express a

desire and interest in solving problems that lack definition and appear not to have a solution.

Finding #2: Skilled hackers exhibit elevated creativity and curiosity in their problem solving.

Second, skilled hackers exhibit elevated creativity and curiosity in their problem solving. There are two intrinsic individual characteristics that contribute substantially to the hacker's ability to build and maintain mental models necessary for dealing with uncertainty and ambiguity. Creativity is instrumental in running mental simulations against models to enable them to think through various hypothetical scenarios and events. Curiosity is the core driver behind the hacker's desire to explore and understand problems.

Finding #3: A hacker's effectiveness depends on their mental models.

Third, a hacker's effectiveness depends heavily on their ability to build and maintain mental models. Hackers are known to find novel and innovative solutions to problems within complex environments and situations. Constructing mental models based on these environments and situations enable the hacker to learn and predict future states and consequences of events.

Finding #4: Expertise and diagramming are instrumental for building effective mental models for hackers.

Fourth, domain expertise and diagramming are instrumental in building effective mental models. Domain expertise is a necessity in building effective mental models and improves the hacker's ability to deduce consequences of situations based on supplementary knowledge that only an expert would possess. This expert knowledge

spans across a variety of domains providing the ability to dynamically create new mental models and effectively maintain existing ones. Diagramming, in the ways of flows charts, mind maps, architectural drawings, and other visual aids help represent the problem being considered. It is instrumental for building and maintaining mental models.

Finding #5: Patterning is a key element of the hacker mind.

Fifth, hackers are adept at patterning. Patterning is important to hackers because it helps them diagnose sources of uncertainty and anomalous occurrences. Specifically, it is a key technique in recognizing everything from attack and defense patterns, data flow, system interactions, and behaviors – providing the foundational elements of forward thinking.

The study revealed personal cognitive skills and social cognitive skills central to the task of hacking, including: (1) using reflection to perform sense-making for building causal mental models; (2) using social exchanges – through argument and debate – to deal with uncertainty, make meaning, and maintain mental models; (3) using artifacts for personal reflection and social exploration to externalize their mental models for performing uncertainty-abduction; (4) using various mental patterns to identify new emergent patterns and predict potential future patterns and events through forward thinking. Performance of these activities depends heavily on, individual and collective, mental logic, technical expertise, creativity, curiosity, and substantial mental capacity to dynamically build and manipulate mental models inundated with complexity. This notion of mental models being instrumental to the uncertainty-abduction process is consistent with the well-established belief that mental models help humans understand the world within which they live.

Study II: How Hackers Think: Understanding the Mental Models and Cognitive Patterns of High-Tech Wizards

Summary of Findings

Finding #1: Expertise and diagramming are instrumental for learning and forward thinking.

First, domain expertise and diagramming has significant positive effects on learning and forward thinking. This finding was consistent with past research on expertise and the impact that diagramming has on construction and maintenance of mental models.

Finding #2: Curiosity facilitates the learning process for hackers.

Second, we found that curiosity is specifically important in terms of learning. Although, there was no evidence that curiosity assisted in the forward thinking process, it proved to be a central component in the learning process. We found that the consideration of new information requires the ability to discover and explore approaches. Finally, we found that curiosity plays a substantial role in the reduction of ambiguity within the hackers' work environment.

Finding #3: Creativity is everywhere.

Third, we discovered that creativity plays a mediation role between perceived skills and perception of environment and learning and forward thinking. This seems to be related to the hacker's willingness to think through the ideation and creation of new approaches. We conclude that creativity facilitates learning and forward thinking through the creation of new ideas and novel approaches; whereas curiosity facilitates learning through exploring the ideas.

Study III: How Hackers Think: Sociocultural Facets and Understanding Their Impact on the Hacker Mind

Finding #1: Hackers that do not attend conventions have more expertise.

First, domain expertise has a higher positive effect on learning for hackers that do not attend hacker conventions; whereas, diagramming has a mildly higher positive effect on learning for those that do attend conventions. These findings indicate that hackers that do not attend conventions have more pronounced domain expertise than those that do; however, hackers that do attend conventions are more adept as thinking toward the future.

Finding #2: Differences between credential holders and those that do not possess credentials.

Second, for hackers that possess professional credentials, creativity facilitates learning in environments abound with ambiguity; whereas, for those that do not possess professional credentials, it appears that curiosity is instrumental for learning in a similar environment.

DISCUSSION

Overall, the goal of my research was to generate theory on the cognitive psychology of hackers. That is to shed light on the mental models and "thinking practices", through which hackers create, change, and communicate their understanding of technology and the world within which it exists. I outlined a series of studies conducted in the promotion of an advanced understanding of a skillfully evasive human enterprise. What I hope to persuade the reader is that a deeper appreciation of the

cognitive processes of hackers provides new insights into organizational management and behavior.

The literature suggests that mental models are instrumental in learning and forward thinking for hackers, especially when acquiring new reasoning skills and understanding technical information (Cañas et al., 1994; Norman, 1983a; Rouse & Morris, 1986). Further, mental models are an effective mechanism for hackers to coordinate their actions and adapt their behavior to the demands of the task at hand (Cannon-Bowers & Salas, 2001). Hacking, like computer programming, is a complex, mixed skill cognitive activity that requires continuously incorporating new information (Cañas et al., 1994). This necessitates a number of abilities that interrelate with the hacker's knowledge base, memory, and processing capabilities, repertoire of comprehension strategies, and problem solving abilities involving inferencing and hypothesis generation (Pea & Kurland, 1984).

In general, hacking is a difficult but useful skill to master. In recent years, there has been an advancing body of research directed toward identifying and understanding the mental models, cognitive skills and traits that facilitate the acquisition of this skill (Summers et al., 2014; Summers et al., 2013). Our approach has been to focus on studying those factors that increase learning and forward thinking. For example, hacking requires having access to some sort of *mental* model of the system which acts as their mental representation of the components and operating rules of the system (Mayer, 1981). These models will vary depending on their completeness and accuracy; however, as hackers learn and interact with the system, their mental models evolve and become more reliable (Gentner & Stevens, 1983a; Jih & Reeves, 1992; Norman, 1983a). The

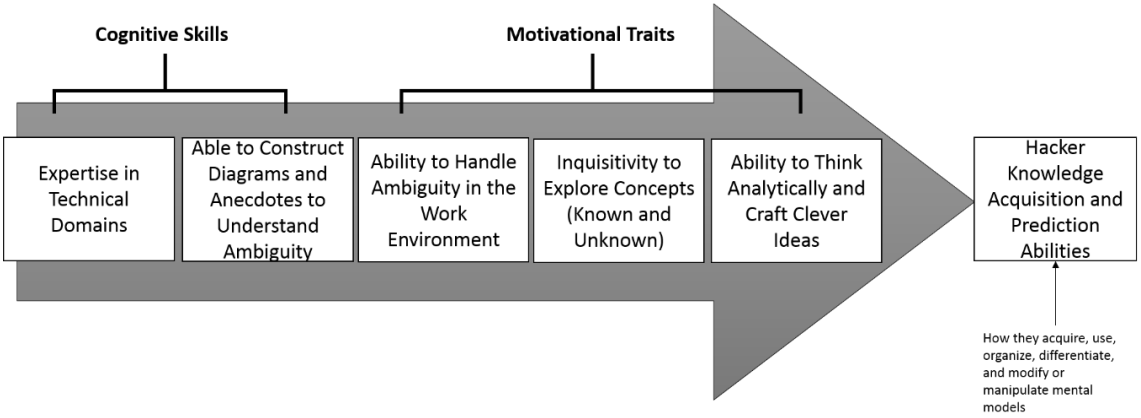
data revealed that hackers use these continuously evolving cognitive structures to conceive of future results through speculative forecasting (Adams, Murphy, & Clarke, 2009). These models are instrumental in setting the hacker's expectations about effects of actions, planning of actions, and ways of interpreting feedback (Jih & Reeves, 1992; Van der Veer, 1989).

As hackers work in ambiguous environments, they must use their mental models to learn the transactions of the computing platform and its components on both a physical and virtual level. More specifically, these transactions, as suggested by Mayer (1981) and Cañas et al. (1994), "involve a knowledge of how different components of the computer (i.e., input, memory, programs, output system, etc.) interact to produce a specific action". Essentially, proficient hackers are adept at constructing knowledge structures that contain an exceptional understanding of these systems and transactions. This is substantial considering that, in many cases, the hacker cannot *see* the virtual elements involved. To facilitate the acquisition of these mental models, hackers must make the computational states, operations, and transactions of the system externally visible. The data indicated that hackers externalize their mental models using diagrams (e.g., creating pictures representing the various components of the system) and narrative construction (e.g., constructing an anecdotal story to infer connections between actions and outcomes based on diagrams). This mental model externalization facilitates meaningful learning in which the hacker connected new knowledge with existing knowledge (Mayer, 1981). These diagrams and narratives represent how different transactions make use of components and operating rules of the system. The ability to collaborate with other hackers proved to be paramount to hacking success. More

importantly, hackers expressed externalizing their mental models as a key element in socially exploring a system and its behaviors. The literature indicates that individuals, within a hacker group, possess their own personally reflected mental models to actively conceptualize and process information about the system with their group (Cannon-Bowers & Salas, 2001; Levesque, Wilson, & Wholey, 2001).

To better understand the data in the qualitative study from a practical perspective, a model was developed that exhibits the cognitive skills and motivational traits that facilitate the learning and prediction abilities of high-performance skills, like hacking (Figure 1). As defined by Schneider (1985), high-performance skills, like hacking, involve those where: (1) the person involved spends considerable time and effort to achieve an acceptable mastery level, (2) there is a substantial number of individuals who fail to develop proficiency, and (3) there are qualitative differences in performance between novices and experts.

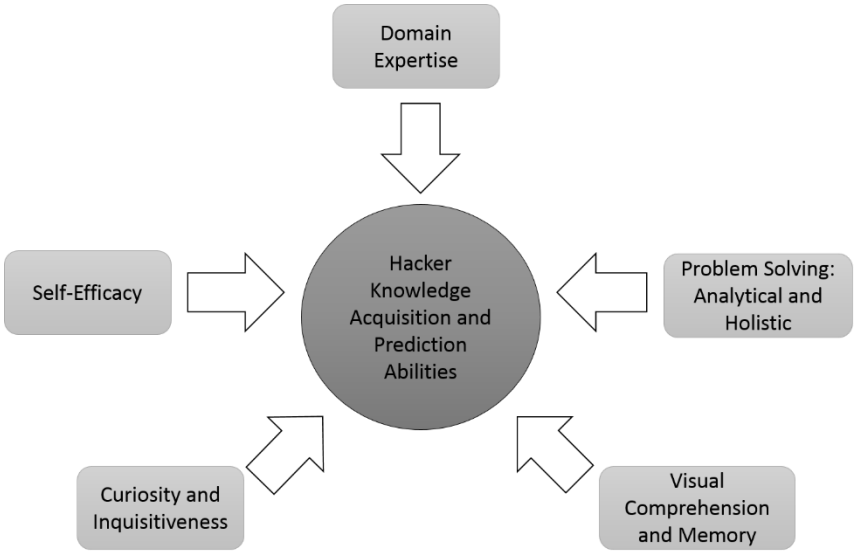
Figure 4: Cognitive Skills and Motivational Traits of Hacking



From a practical perspective, my qualitative research indicated that there are key elements necessary for hacker development. Based on the literature and study findings,

domain expertise, problem solving, visual comprehension and memory, curiosity, and self-efficacy were factors effecting the learning and anticipatory outcomes of hackers. This conceptual model from a practical perspective is illustrated in Figure 2.

Figure 5: The Five Elements of Hacker Development



The concepts from the qualitative study yielded emergent factors for quantitative analysis. Figure 3 illustrated the findings from the qualitative research (Study I) and the emergent factors examined in Study II and Study III.

A research model was then developed where the qualitative research (Study I) informed the quantitative analysis (Study II). The findings from Study II were significant and demonstrated the importance of perception of environment (i.e., ambiguity tolerance) (Krueger & Dickson, 1994), intrinsic individual characteristics (i.e., curiosity and creativity) (Berlyne, 1978; De Bono, 1992), and perceived skills (i.e., domain expertise and diagramming) (Lim & Johnson, 2002) as contributors to successful hacking. This

study empirically validates the impact of these five key elements on hacker learning and forward thinking performance.

The second quantitative analysis (Study III) builds upon Study II, by exploring the impact of sociocultural facets (i.e., gender, participation in hacker conventions, and possession of professional credentials) on hacking abilities. Study III also revealed that there are differences between sociocultural facets i.e., differences between genders and how they perform uncertainty-abduction, differences between how various sociocultural elements, such as convention attendance and possession of professional credentials, can impact how hackers address ambiguity. The research model from a theoretical perspective is illustrated in Figure 3.

Limitations

The quality of inferences within a mixed methods study can be discerned by evaluating qualitative and quantitative methods independently, as well as analyzing the combination of these inferences using an integrative framework that emphasizes design quality and interpretive rigor (Teddlie & Tashakkori, 2009). See Table 4 for a summary of criteria and how I have addressed each of these.

Table 4: Quality Criteria

Quality Criteria		
Method	Criteria	Address Through
Qualitative	Credibility Transferability Dependability Confirmability	Persistent observation and criteria-based selection Detailed descriptions Saturation of interviewees Interviewee review during analysis
Quantitative	Internal Validity External Validity Construct Validity Convergent Validity Discriminate Validity Reliability	Co-variance between independent and dependent variables Representative sample Instrument and item pretesting CR > AVE; AVE > 0.50 MSV < AVE, ASV < AVE

		CR > 0.70; Cronbach alpha > 0.50; factor loadings > 0.30
Mixed Method	**Design Quality**	Best effort at selection and implementation of appropriate procedures for answering research questions
	Interpretive Rigor	The quality of credible interpretations made on basis of results

Qualitative. In using qualitative method, I was concerned with credibility, transferability, dependability and confirmability. To address credibility, I reviewed and reflected upon interview data multiple times as part of the grounded theory process. I asked interviewees, after completion of my analysis, whether the analysis made sense to them; in every case it did. To reach transferability, to achieve the widest possible range of application, I documented the context and observational field notes yielding a detailed description of activities, events, and interactions (Teddlie & Tashakkori, 2009). To address dependability, I interviewed enough respondents until no new behaviors or patterns were detected. To mitigate concerns about confirmability, I discussed on-going analysis and results on a continuous basis with my principle investigators and wrote related memos and notes for discovery.

Quantitative. Threats to internal validity in the second and third studies were minimized by theoretical and empirical analyses suggesting statistically significant correlations between independent to dependent variables determined by covariance between those variables. Using a diverse population in terms of employer, industry, country, age, gender, education and experience reduced threats to external validity. I did not use a single rule as the determinant for validity assessment (Costello & Osborne, 2011) and chose to consider multiple measures for validity (Thompson & Daniel, 1996). To address face and content validity, I conducted pretesting using experts and a protocol analysis using Bolton's recommended methodology. I also piloted the survey instrument

with a small, separate group of respondents, ensuring initial convergent and divergent validity. Reliability was addressed by Cronbach alphas. Most constructs in both studies had construct reliability greater than 0.70.

Mixed method: Design quality. Concerns about design suitability were reduced as each research question used an appropriate method to answer the question. The open multiphase approach matched the expansion purpose of the entire study. The design adequancy of qualitative and quantitative procedures were met by obtaining a rich interview population for qualitative approaches and a rich data set for quantitative approaches resulting in a credible understanding of a complex phenomenon. Concerns about analytic adequacy were alleviated by the use of accepted and standard scholarly techniques: grounded theory for qualitative methods and structural equation modeling for quantitative analysis.

Mixed method: Interpretive rigor. For interpretive consistency in the first study, a grounded theory approach incorporating systematic coding protocol produced genuine insights into differences in underlying behaviors and helped answer the research questions. For interpretive consistency in the second and third study, causal inferences were made on statistically fit structural models with sufficient statistical power.

For theoretical consistency, the models in each successive Hacker study helped address new gaps in the literature. For the qualitative study, grounded theory findings builds upon the literature and enabled expansion in the second and third studies. For interpretive agreement, scholars evaluating the quantitative studies for their models and distinct results should arrive at similar results. For qualitative results in the first study, differences in interpretation are always possible even with the internal validity checks

discussed above. However, scholars will likely not reach contradictory conclusions. Having multiple interpretations it not a significant threat to consistency (Teddlie & Tashakkori, 2009). My long-term career and experience with the research domain should minimize possibility for non-faithful interpretations.

Implications for Practitioners

I began my research with a desire to solve the practitioner question, "How do hackers create innovative solutions and can we improve the thinking processes involved?" Using intrinsic individual characteristics, perceived skills, and perception of environment as key lenses to understand learning and forward thinking provided an excess of new results and implications for the existing body of knowledge. In this section, however, I will cover important contributions to practitioners.

This research contributes to the development of evidence-based and research informed practitioner tools and strategies for developing and managing effective hackers and improving talent identification and recruitment performance. This research can serve as the foundation for a training platform for individuals, companies, or governments interested in using cognitive development to improve hacker effectiveness. Within the cybersecurity industry, there has been a substantial manpower shortage; more specifically, there has been difficulty identifying qualified hackers (Libicki, Senty, & Pollak, 2014). In fact, Libicki et al. (2014) argue that this shortage has been devastating for the federal government thereby requiring the establishment of specialty scholarship programs, encouragement of hacker competitions, and other methods to motivate and entice talented individuals. To respond to this shortage, many larger organizations have resorted to internal promotion and education. Smaller organizations are more reluctant to

provide such expensive educational opportunities in fear that employees may take the new found skill elsewhere. Additionally, universities are beginning to train students to become cybersecurity specialists; however, finding qualified professors is another barrier that has hindered their success. According to Libicki et al. (2014), organizations have become "increasingly sophisticated in defining those personality characteristics that correlate well with cybersecurity requirements, notably an intense curiosity with how things work (and can be made to fail)". This shortage has driven organizations to seek unconventional methods to identify skilled hackers, such as hackathon participation, personalized job invitations, and other strategies to poach talent from other companies. One proposed solution to this challenge is to focus on hiring entry level workers and provide them with substantial levels of training (Libicki et al., 2014).

With organizations like Sony and Target being victims of the largest cyber-attacks in American history, it is no surprise that the demand for cybersecurity experts has risen substantially. However, the mechanisms for increasing the supply of these hacking experts such as education, recruitment, training, and talent identification have not caught up (Libicki et al., 2014). These difficulties have put a substantial amount of attention on the education and training of qualified people; however, the bulk of the current training provided is purely technical. There has been little to no focus, from an education and training perspective, on the *cognitive skills and traits* that correlate with cybersecurity requirements. This body of research successfully lends itself to this unaddressed space. The findings in this research provide substantial insights for the cybersecurity industry e.g., the specific cognitive and personality characteristics that correlate with cybersecurity, the impact of those characteristics on hacker effectiveness, and potential

cognitive development training mechanisms for improving hacking abilities. For example, cognitive training activities and assessments (e.g., computer-based games) could be utilized to improve the cognitive skills and traits necessary for skilled hacking.

The educational use of digital games is has been explored; however, the research has not been focused or well-defined (Gros, 2007). In general, digital games have become one of the most profitable and influential forms of entertainment in the world (Squire, 2003). In recent years, researchers have begun to consider the use of digital games as a tool for enhancing learning, production of knowledge and refinement of skills needed in a digital society (De Schutter, 2010; Gorriz & Medina, 2000; Gros, 2007; Lenhart et al., 2008; Squire, 2003). Some researchers fear that digital games can be detrimental by fostering violence, aggression, negative imagery, or social isolation (Provenzo Jr, 1991); however, other researchers consider games to be powerful motivation tools that can be integrated into instructional design (Bowman, 1982; Bracey, 1992; Driskell & Dwyer, 1984; Squire, 2003). In another study, Ricci, Salas, and Cannon-Bowers (1996) investigated the effects of a gaming approach on knowledge acquisition and retention in military trainees and found that participants that underwent game-based training scored significantly higher on tests than those that did not.

Based on the extant literature and this body of research, I propose a cognitive development platform that features activities and assessments (e.g., individual and social games, simulations, puzzles, etc.) designed to improve performance across a variety of cognitive functions. The activities and assessments within the platform would be designed to improve attention, working memory, processing speed, executive functioning, and the cognitive skills and traits of skilled hackers. Researchers have

experienced success in using web-based cognitive training activities and assessments in improving cognitive abilities (Guía, Lozano, & Penichet, 2014; Sarkar, Drescher, & Scanlon, 2007; Scanlon, Drescher, & Sarkar, 2007); however, due to a dearth of research on the cognitive abilities and mental characteristics of hackers, there is a lack of progress in cognitive training for them. The purpose of such a platform would be to provide rich digital learning environments that provide continuously advancing instruction to trainees in a way that addresses a practical need in a low-cost economical manner (Squire, 2003).

A cognitive development platform can provide situated cognition through rule-governed, goal-focused driven activities that incorporate gaming assisted instruction that target the learning of specific cognitive domains (e.g., domain expertise, diagramming, ambiguity tolerance, creativity, curiosity, etc.). Research has shown that gaming can be a powerful instrument for acquiring factual information and complex performance skills (Gee, 2003; Gros, 2007; Guía et al., 2014; Oblinger, 2006; Ricci et al., 1996). The literature also indicates that gaming is effective in knowledge maintenance, retention testing, and remediation. Many games enable the user to co-create the game world by building new scenarios, maps, or situations; thereby, exercising the user's mental visualization and creativity abilities through developing new perspectives and manipulating phenomena for learning (Barab, Hay, & Duffy, 1998; Gee, 2003; Hay, 1999; Squire, 2003). The exploratory nature of games and solving in-game situations has been proven to stimulate the curiosity of players and enrich learning opportunities (Malone, 1980).

Future Research

The proposed research provides a conceptual framework in an area where little prior research has been done. It is based on an integration and interpretation of both qualitative data generated through a number of in-depth interviews and quantitative data acquired through survey responses – a mixed method approach consistent with procedures recommended for management theory development. The conceptual model and propositions emerging from it imply a rich agenda for future research.

Hacker assessments. There is a need and an opportunity to develop an assessment to measure a hacker's existing cognitive skills and traits. The author's research revealed three dimensions (i.e. intrinsic individual characteristics, perceived skills, perception of environment) which transcend a variety of applications within the hacking domain. Research is now needed to generate activities or game-based tasks to flesh out these dimensions, to device appropriate rating scales to measure the cognitive skills and traits and to produce a reliable comprehensive but concise assessment. Further, the assessment generated should be such that with reasonable changes to wording, the same assessment can be used for a variety of domains.

Performance outcomes. Research is needed to examine the *nature* of the association between the hackers' cognitive skills and traits and performance outcomes. Specifically, are one or more of these cognitive skills and traits more critical than others in affecting hacker performance outcomes? Can effective training to one of these cognitive skills and traits create favorable performance outcomes? Are there differences across subfields (i.e. programming, system design, incident response, etc.) regarding relative use of the cognitive skills and traits and their impact on learning, forward

thinking, or performance? In addition to offering valuable managerial insights, answers to questions like these may suggest refinements to the proposed theory.

Comparison with other populations. The main thesis of the proposed theory is that a hackers' learning and forward thinking are influenced by a series of cognitive skills and traits. The author suggests that different populations can be studied to compare results within the hacking community. This would provide substantial insights into whether or not the findings expressed here are generalizable across other populations (i.e. programmers, financial traders, scientists).

Hackers as designers. Recent research (Boland & Collopy, 2004; Buchanan, 1992; Madden, 2015; Wiles, 2010; Yoo, Boland Jr, & Lyytinen, 2006) suggests that there may be some fascinating cognitive linkages between hackers and design thinking. The research presented here suggests that hackers are adept at creating inventive resolutions to ambiguous problems, using sensemaking to envision potential solutions, iterative idea generation, using visual artifacts to communicate, and never being satisfied with the way things are (Summers et al., 2014; Summers et al., 2013). Similar to these findings about hackers, Kimbell (2011) suggests that design thinking and the designers who practice it are "associated with having a human-centered approach to problem solving…[and] are seen as using an iterative process that moves from generating insights about end users, to idea generation and testing, to implementation…their visual artifacts and prototypes help multidisciplinary teams work together…they ask "what if?" questions to imagine future scenarios rather than accepting the way things are done now" (p. 287). In fact, Wiles (2010) suggests that "hacker culture has lurked at the edge of design discourse for years now, rich in potential, and its appeal seems to be growing".

Madden (2015) describes design as a comprehensive methodological problem solving approach with the intent of transformational outcomes with a focus on end-user centered research, prototyping, and creativity. In the hacker community, we see these sentiments expressed with the prevalence of hackerspaces – a community operated workspace where people with common interests can meet, socialize, and collaborate (Schlesinger, 2010). Wiles (2010) describes a similar occurrence happening within the design community, stating "there's the inexorable rise of the "hack lab", informal social events where people meet to collaboratively adapt and rework electronics and design objects". Artist and fashion theorist, Otto von Busch, suggests that "hacking is definitely catching on…as a lot of design takes on political and critical issues with the spread of the open source mindset it seems like hacking rhymes well with many of today's agendas" (Wiles, 2010). There appears to be a sensible relationship between how hackers think and how designers think. As suggested by Graham (2008), one thing that hackers and designers definitely have in common is that they are both makers.

The findings from this research and that of others discussed implies that the emergence of the use of design thinking within the hacker mindset is an additional area of study, where we may find that there is much to be discovered and explored. More specifically, the research indicates that hackers and designers are especially skilled at solving problems abound with ambiguity, capable of creating novel ideas, have a strong consideration for how their solution will be used by others, and a willingness to deep dive into these issues (Buchanan, 1992; Graham, 2013; Kimbell, 2011; Madden, 2015; Summers et al., 2014; Summers et al., 2013). It seems that exploratory research into the role that *design thinking* plays in the activity of hacking could provide further insights

into the hacker mind and possibly the mind of designers. By deepening our knowledge of the emergent field of hacker cognitive psychology and design for innovation, we may gain a further understanding of the hacker mind as a strategic organizational capability and as a source of potential social progress.

CONCLUSION

This thesis explored the mental models of hackers, in particular how they are used in individual and social cognitive environments. The resulting empirical findings reveal the cognitive and social cognitive processes that enabled hackers to be proficient at technical decision making and innovative thinking. The results of this research have revised our understanding of the role of mental models, cognitive frameworks, and the cognitive skills and traits of hackers. As our society becomes more reliant on digital technologies and nation states and corporations integrate hacking into their adversarial toolboxes, this theory of hacker cognition can provide substantial insights into understanding, not only how to protect ourselves, but also to innovate and develop the next generation of hackers.

Appendix A: How Hackers Think:
A Study of Cybersecurity Experts and Their Mental Models

By

Timothy C. Summers

Submitted in Partial Fulfillment of the Requirements of the Qualitative Research Report
in the Doctor of Management Program
at the Weatherhead School of Management

Advisors:
Kalle Lyytinen, Ph.D.
Richard Boland, Ph.D.
Tony Lingham, Ph.D.
Eugene Pierce, D.M.

CASE WESTERN RESERVE UNIVERSITY

June 2013

HOW HACKERS THINK: A STUDY OF CYBERSECURITY EXPERTS AND THEIR MENTAL MODELS

Abstract

Hackers account for enormous costs associated with computer intrusion in a world increasingly reliant on computer and Internet-based technologies. Within the hacker community, there are "good" hackers called *white hat hackers* and "bad" hackers called *black hat hackers*. Essentially, one identifies ways to protect information systems while the other identifies ways to exploit those information systems. Regardless of what type of hacker a person is, identifying system weaknesses requires logical reasoning and the ability to systematically think through possible actions, alternatives, and potential conclusions. This combination of reasoning and systematic thinking implies the use of mental models. Hacking is a cognitive activity that requires exceptional technical and reasoning abilities. In this domain, a mental model can be thought of as a hacker's internal representation of the components and operating rules of an extremely complex software and hardware system. Mental models help hackers describe, explain, and predict system attributes and behaviors. The literature is filled with analyses of motives and incentives to engage in hacking but lacks in explaining how hackers actually process knowledge and/or think about systems. It is the intent of this research to address this gap by analyzing how hackers identify and solve problems, make inferences as to reach decisions and implement solutions.

Key words: Hackers; cybersecurity; expertise; mental models; cognitive framework; cognition; psychology; sociology; problem solving; decision making; patterning

"We've broken into power systems, and we've broken into SCADA systems that control water supplies. We literally can shut off water. People will die. This is no bull shit. You know what I mean? That is incredibly important. That drove me to the tipping point at which I stopped liking [cyber] security as much. It stopped being a game and started being much more of a burden." - *Study Participant*

INTRODUCTION

Over the past few years, the list of hacking victims has included the International Monetary Fund (IMF), the United States Central Intelligence Agency (CIA), Sony, the Turkish government, the Estonian government, Citibank, and Visa. The cost of global cybercrime had grown to $388 billion annually[8] in 2011, costing about one-third more than the global black market of marijuana, cocaine, and heroin combined ($288 billion). It costs more than "$1.0 trillion to society, with billions of dollars being stolen from small, medium and large-sized enterprises, identity of millions of individuals compromised, and several governments across the world have already been targets of cyber-warfare" (Global Industry Analysts, Inc., 2011). Hacking is not limited, however, to hacking groups as nation states also leverage cyberwarfare against global and regional adversaries (Billo & Chang, 2004). Several countries, including the United States, China, India, Iran, North Korea, Pakistan, and Russia, have been working diligently to build the capabilities and requisite human resources to wage effective cyberwarfare campaigns against their adversaries (Hildreth, 2001). Such cyberattacks involve "intrusions into unprotected networks for the purpose of compromising data tables, degrading communications, interrupting commerce, or impairing critical infrastructures (such as

[8] Symantec Corp. 2011. *Norton Study Calculates Cost of Global Cybercrime: $114 Billion Annually* http://www.symantec.com/about/news/release/article.jsp?prid=20110907_02

transportation or medical and emergency services) in such a way that trust is undermined at the expense of a smoothly running economy and society" (Billo & Chang, 2004).

The primary executors of cyberwarfare are hackers—individuals with expertise in software programming and exploiting computer networks (Billo & Chang, 2004). For them, hacking is not the act of aimless, obsessed individuals, but that of a community with highly developed psychological and cognitive processes (Jordan & Taylor, 1998; Lakhani & Wolf, 2003; Levy, 2001). For example, Schneider (2006) characterizes hackers as:

> A hacker is someone who thinks outside of the box. It's someone who disregards conventional wisdom and does something else instead. It's someone who looks at the edge and wonders what's beyond. It's someone who sees a set of rules and wonders what happens if you don't follow them. A hacker is someone who experiments with the limitations of systems for intellectual curiousity (Schneier, 2006: 43–44).

Definition of a Hacker

> "The definitions I've always heard is the white hat hackers doing things with permission, with authorization and only does what he's allowed to, is ethical at handling information. The black hat, he's not getting permission. He's doing it for criminal or curious reasons and he's not constrained by any laws or ethics. He does what he wants." - Study Participant

Most people consider hackers to represent negative entities, whether in a group or individually. The media is fascinated with hackers, particularly individuals who have managed to steal identities and cause service disruption for companies and consumers (Hildreth, 2001; Marmon, 2011). Hackers are also members of a dynamic community and operate within social groups seeking and sharing expertise through various learning and engagement mechanisms, including training groups, scholarly journals, and conference presentations, like any other organized groups of professionals (Jordan & Taylor, 1998). Most studies on hacking have focused on the technological and sociological aspects of

the people and the activity (Jordan & Taylor, 1998; Lakhani & Wolf, 2003). Up to this point, most studies about hackers have focused on individual and social behavioral traits based on personality and motivation profiling. Currently, there is no research that has examined the mental processes that are instrumental to being a skilled hacker—especially in explaining their psychological development and cognitive processing. Our understanding of individual and social cognition, including the faculties for processing information, applying knowledge, changing preferences, and making decisions, is severely limited within hacker communities. From a theoretical standpoint, studying the mental processes of hackers enables us to have insight into their decision-making and learning. Taking this cognitive psychology approach offers us the opportunity to understand how the hacker mind inteprets reality, how hackers make decisions, and how the thoughts of hackers interact with language.

This paper is a qualitative study of skilled hackers in which we aimed to explore their minds as to understand how they use mental models to organize and interpret information as to aid in pattern matching, solving problems, and decision-making. We leveraged grounded theory to elicit their lived experiences—in all 18 experienced subjects—and subsequently analyzed their lived experience to understand their cognitive processes.

The purpose of this study is to explore the following research question(s):

1) What defines a skilled hacker? What are the necessary cognitive and social cognitive skills and motivational traits of a skilled hacker?

2) What factors can be said to influence or explain how skilled hackers acquire, maintain and use mental models instrumental for effective hacking?

3) How and to what extent do the traits, cognitive skills and motivational traits and motivational factors of a skilled hacker influence or explain how they use mental models?

Literature Review

Hacking is an activity for intellectuals with an enjoyment—and in some cases a compulsion—for problem solving[9]; therefore, it always requires higher level cognitive functions, including a combination of problem solving, reasoning, and systematic thinking. Although, we know this about hacking, there have been no studies to explore those cognitive functions. Generally, the literature on hacking refers to the technical knowledge necessary and makes the assumption that that is the most important element necessary for skilled hacking. We contend that an important function of the hacker mind is the building and maintenance of mental models. Such "[mental] models are the natural way in which the human mind constructs reality, conceives alternatives to it, and searches out the consequences of assumptions" (Craik, 1943b; Schaeken, Johnson-Laird, & d'Ydewalle, 1996). Comprehensively, all of these cognitive elements present themselves through identifying patterns, solving problems, and decision-making. Next, we will review the key elements of those cognitive functions that underlie hacking.

We were interested in understanding how personal and social cognition happens among hackers and how they build and maintain their mental models. In order to understand this, we conducted an extensive literature review which we used to frame the empirical inquiry presented in this paper. Initially, we began by reviewing all of the literature available on hackers and mental models; however, all of the literature regarding

[9] Reuters. 2011. *Hacking encouraged, even prized, at Vegas geek fest,* http://www.reuters.com/article/2011/08/07/us-usa-hackers-idUSTRE7760DC20110807 .

hackers studied the sociological and motivational aspects of hacking (Bratus, 2007; Jordan & Taylor, 1998; Lakhani & Wolf, 2003; Levy, 2001; Voiskounsky & Smyslova, 2003). We presume that this has much to do with the elusive nature of hackers. To get at the mental processes necessary for hacking, we began to explore literature on mental models and computer programming (Corritore & Wiedenbeck, 1991; Gomes & Mendes, 2007; Mayer, 1981; Soloway & Ehrlich, 1984). Although the literature on hacking was not comprehensive, we were able to find enough information to get to the cognitive functions and elements of hacking. After reviewing the literature, we synthesized the theories that could explain how hackers perform cognition using mental models. Those primary theoretical sources were mental model theory (Craik, 1943b; Rouse & Morris, 1986; Schaeken et al., 1996), skill acquisition theory (Dreyfus & Dreyfus, 2005), the theory of flow (Csiksczentmihalyi, 1991; Lakhani & Wolf, 2003), and self-efficacy theory (Bandura, 1977; Compeau & Higgins, 1995c). These theories were used as sensitizing devices to frame the domain and as a means to understand the hacker's congitive behaviors we observed in the field. Table 1 provides a brief overview of these theories.

TABLE 1
Sensitizing Theories of Hacking as Cognitive Activity

Theory	Contribution to the Research
Mental Model Theory	Mental models enable people to describe, predict, and explain system behavior and they serve as a mnemonic mechanism for remembering relations and events (Williams, Hollan, & Stevens, 1983a). They enable people to create descriptions of the system's purpose and form, explanations of system functions and observed system states and conditions, and predictions of future system states and conditions (Rouse & Morris, 1986). Mental model theory provides us an understanding of how hackers use mental models, i.e. how they are acquired, how they are used, how they are organized, how they are modified and refined, as well as how they are compared and contrasted. It provides additional insights into the visual comprehension and memory elements of the mental models of skilled hackers.
Skill Acquisition Theory	This theory helps us understand what a skill is and what the hacker acquires when he/she achieves expertise (Dreyfus & Dreyfus, 2005). It provides insights into discerning how years of experience, facts and heuristics, and cognitive bias can enable them to process information quickly and accurately. It provides insights into the domain expertise element of the mental models.
Self-Efficacy Theory	Self-efficacy can explain how a hacker's perceptions [of their own abilities] can influence the decisions that they make (Compeau & Higgins, 1995c) and thus offers insights into how hackers acquire, organize, and use their mental models.
Flow Theory	Flow theory helps us understand hacker's emotions of interest, enjoyment, and control linked with the process of hacking (Lakhani & Wolf, 2003). It provides insights into the hacker's need for intellectual stimulation, problem solving and mental model manipulation the drive for relentless curiosity and inquisitiveness of skilled hackers.

These theories identified factors such as expertise, curiosity and inquisitiveness, problem solving, systems thinking, self-efficacy, dialectic reasoning, visual comprehension and memory as major contributing factors that may influence how hackers acquire, maintain and use mental models.

Human beings acquire, maintain and use internal models to understand and manipulate complex systems or situations. Although first hypothesized by Charles Sanders Peirce in 1896, it was the Scottish psychologist Kenneth Craik (1943b) who

popularized the concept of mental models when he postulated that the mind creates a 'small-scale model' of reality that allows it to visualize possible events and various alternatives.

Hacking, as a cognitive activity, requires exceptional technical and reasoning abilities and the mental models can be thought of as a hacker's internal representation of the components and operating rules of software and hardware systems that enable them to explore and identify its vulnerabilities (Mayer, 1981). This gives insights into understanding how a system may function [or malfunction], how various components of that system interact, and how those interactions produce specific actions (Mayer, 1981). Therefore, the technical and reasoning abilities required for computer programming [in general] are required for engaging in hacking. Accordingly, mental models utilized in hacking include, but are not limited to, processes of writing code, debugging, and other systems and program comprehension-related tasks (Corritore & Wiedenbeck, 1991; Littman, Pinto, Letovsky, & Soloway, 1987; Nanja & Cook, 1987; Pennington, 1987; Soloway & Ehrlich, 1984; Wiedenbeck, Ramalingam, Sarasamma, & Corritore, 1999). These mental models help hackers describe, explain, and predict system attributes and behaviors. Specifically, they enable hackers to describe the system's purpose and form, explain observed states and system functionality, and predict future system states (Rasmussen, 1979a; Rouse & Morris, 1986).

It is apparent that well-developed mental models provide hackers with enormous insight about the system. We posit that mental models are dependent on a set of intrinsic cognitive skills and traits of a hacker—such as expertise, curiosity, and creativity. These

cognitive skills and traits enable a hacker to continually build and improve mental models and their ability to dynamically manipulate those models.

RESEARCH DESIGN

Methodology

The purpose of this study is to develop theory that explains the dynamism of the mental models of hackers, specifically addressing their content, how those mental models are built and how they are maintained. Due to the nascent nature of the theory development and minimal studies available on the topic, we decided to use a qualitative approach, letting "lived experience" expose the complex cognitive processes of hacking. We adopted an open-ended approach to allow "unplanned themes" to emerge from the data (Ibarra, 1999). We let the data inductively generate the theory to account for and explain the experiences and behaviors of the studied hackers. To do so, we needed to deeply investigate their experiences, accounts of their actions, and understand their local meaning (Charmaz, 2006). The methodological approach therefore followed grounded theory and was anchored in the experiences, feelings, and behaviors of active members of the hacking community (Charmaz, 2006; Glaser & Strauss, 1967b; Strauss & Corbin, 1990a). We used the hackers' self-reported behaviors and thought processes to examine the structure and content of their mental models and the extent to which specific factors (and/or other factors) are instrumental in shaping the acquisition, maintenance and/or use of mental models.

Semi-structured interviews were deployed as the main data collection method to ensure that the study captured the complexities of the hacker's behaviors and the meaning behind those behaviors (Glaser & Strauss, 1967b). These complexities included the

perceptions, beliefs, and attitudes of hackers as they responded to questions about the activity of hacking and other social and cognitive interactions that lead up to and or occur after the hacking activity. We also collected field notes through observing hackers in various social and working settings for triangulation and to understand their local activities and behaviors (Strauss & Corbin, 1990a).

Sample

Eighteen hackers were sampled for the study using purposive theory-driven sampling (Corbin & Strauss, 2008). Therefore, we sampled new interviewees until theoretical saturation was reached and no significant new information emerged during the interviews. The hackers were selected using a criterion-based sampling to ensure that qualified candidates were obtained and were able to provide quality information (Turner, 2010). All of the hackers had to meet two criteria: 1) enough years of experience (more than 2 years); and 2) validation of high level subject matter experience from colleagues[10]. They were identified through the researcher's personal and professional networks. The final selected hackers were also recognized hacking professionals within the cybersecurity community and they had participated in a variety of hacking projects, including development of complex security systems, protecting information systems, or finding ways to exploit security vulnerabilities through the employment of foreign and domestic governments, private companies, and/or independent consultancies. We did not include hackers that were directly involved in organized crime groups for consideration

[10] The goal was to identify key knowledgeable participants who 'see' the phenomenon from diverse perspectives – to ensure that there was variety in response and avoid convergence in retrospective sensemaking (Eisenhardt, K. M., & Graebner, M. E. 2007. Theory building from cases: Opportunities and challenges. ***Academy of Management Journal***, 50(1): 25–32.)

of time and safety; however, some of the participants have consulted for or admitted to being engaged with such groups.

Table 2 provides demographic information about the hackers. It is also a reasonably good representation of the community at large. It represents several age groups, backgrounds, industries, and participants from several domestic and international locales. The participants were composed of 17 men and 1 woman[11], aged between early 20s to mid-50s.

TABLE 2
Interview Participants

Gender/Age	Experience	Validation [12]	Face-to-Face/ Phone	Education	Industry[13]
M / 30s	5 – 10 years	Yes	Face-to-Face	Bachelor's degree or higher	Aerospace/Defense/ Government
M / 20s	5 – 10 years	Yes	Face-to-Face	Master's degree	Management Services/Defense
M / 30s	10 + years	Yes	Face-to-Face	Master's degree	Management Services/Defense
M / 30s	10 + years	Yes	Phone	Doctoral degree	Security Software & Services
M / 30s	10 + years	Yes	Phone	Master's degree	Security & Protection Services
M / 20s	10 + years	Yes	Face-to-Face	Bachelor's degree or higher	Security Software & Services
M / 30s	10 + years	Yes	Phone	Master's degree	Aerospace/Defense/ Government
M / 30s	10 + years	Yes	Phone	Master's degree	Aerospace/Defense/ Non-Profit
M / 30s	10 + years	Yes	Phone	Master's degree	Management Services/Defense
M / 40s	10 + years	Yes	Face-to-Face	Bachelor's degree or higher	Management Services/Defense

[11] The researcher made an extra effort to identify females to ensure that the experiences and mental models of men and women could be compared; however, since women are highly underrepresented in the industry, we were not able to identify a higher number of female hackers. It is recognized and accepted that the hacker community is predominately male. There are various reasons for this and Chiesa, Ducci, and Ciappi (2007) address male predominance as one of the identifying aspects of the hacker community. *Chiesa, R., Ducci, S., & Ciappi, S. 2008.* ***Profiling hackers: The science of criminal profiling as applied to the world of hacking****: CRC Press.*

[12] Validation [along with Experience] is a factor used for my criteria of selecting interview participants.

[13] Participant organizations/companies were cross-referenced with the industry list provided by the Yahoo! Finance Industry Browser at http://biz.yahoo.com/p/industries.html

F / 30s	10 + years	Yes	Face-to-Face	High School Diploma	Management Services/Defense
M / 30s	10 + years	Yes	Phone	Master's degree	Aerospace/Defense/ Non-profit
M / 50s	10 + years	Yes	Face-to-Face	Master's degree	Management Services/Defense
M / 20s	5 – 10 years	Yes	Face-to-Face	Bachelor's degree or higher	Management Services/Defense
M / 20s	Less than 5 years	Yes	Face-to-Face	Bachelor's degree or higher	Management Services/Defense
M / 30s	10 + years	Yes	Phone	High School Diploma	Management Services/ Security & Protection Services
M / 30s	10 + years	Yes	Phone	High School Diploma	Management Services/ Security & Protection Services
M / 30s	10 + years	Yes	Face-to-Face	Bachelor's degree or higher	Management Services/Defense

To protect the identities of the participants, the researcher created a list of one hundred codenames which were selected at random and assigned to each interview.

Instrument Development

The interview instrument was designed to reveal—at least broadly—the domain of topics covered in the Literature Review, including the content of the mental models. To this end, the interview instrument used open-ended questions that allowed the participants to respond with as much detailed information as they wished, while allowing the researcher to ask probing follow-up questions (Turner, 2010)[14]. The goal was to enable the participants to express their lived experiences and describe real examples of their hacking methodologies—mentally and socially. The instrument probed their analytical abilities and elements covered in the Literature Review, including questions about problems that participants faced, how they came up with solutions for those

[14] The interview protocol was developed using the following principles (Turner, 2010): (a) open-ended working to allow the respondent to answer the questions on their own terms; (b) using neutral questions that do not influence answers; (c) questions were asked one at a time; (d) the questions were worded clearly and accurately using terms that were recognized within the respondents' culture; (e) limited use of questions that ask 'why'.

problems, explanations of "trial-and-error" processing, and the results of their attempts to solve the problems.

Data Collection

The interviews were conducted between May 2012 and August 2012 and lasted between 60 minutes to well over two hours. The interviews were conducted face-to-face and/or by phone. In some cases where a face-to-face interviewing was not possible, phone-based interviews were performed, because it provided more time. No compensation was provided to the participants. All of the participants consented to being recorded. The interviews were transcribed verbatim. The research also collected observational field notes from various social interactions with hackers from professional, social or "unprofessional", and other out-of-band settings.

In the interviews, the participants were asked various questions regarding their background and experience, areas of expertise, their hacking activities, as well as any hacking problems or situations that they could recall and describe. We probed their cognitive processes about hacking and the problems that they could recall. We also probed their feelings about the hacking activities, relationships and communication with other hackers, opinions on using drawings, sketches, pictures, and other representations during hacking.

Data Analysis

The data was analyzed through an iterative process, involving constantly reviewing the data, the literature, field and observational notes, and the theory being developed (Strauss & Corbin, 1990a). Immediately after the interviews, the researcher would listen to the recordings so that he could ensure that he understood the experiences

being described. This provided the opportunity to listen for recurring themes. The researcher would re-listen to the recordings while reading the transcripts, enabling him to mentally revisit the interview. Overall, over 1,000 pages of interview transcripts were examined, which resulted in the final identification of eighteen codes and five themes.

The researcher performed open coding on the transcripts—creating categories using my "first-mind" intuition—based on the previous iterations of reviewing the data. After using techniques recommended by (Brown & Ryan, 2003)[15], we realized that there were five main themes: (1) cognitive patterns; (2) learning patterns; (3) comprehension patterns; (4) engaged patterns; and (5) predictive patterns (see Table 2 below). After identifying these themes, we iteratively went between the data, relevant literature, and my emerging theory to develop conceptual categories. To this end, we compared the emerging model, the data, and literature on mental models and personal and social cognitive development to guide decisions about the model (Charmaz, 2006; Strauss & Corbin, 1990a).

Once we were able to see prominence of the five themes, the researcher coded the transcripts for evidence of each—periodically discussing the themes and resulting codes with other colleagues to settle discrepancies. In Table 3, we present five themes that were identified.

[15] The researcher used techniques identified by Brown and Ryan (2003), including: (1) looking for word repetition for saliency; (2) observing indigenous categories or specialized vocabulary; (3) identifying key words and the ways in which they are used; (4) constantly comparing and contrasting interview passages; (5) observing evidence of social relationships, cultural descriptions, and individual and group problem solving; (6) seeking to identify and understand information missing from the interviews; (7) taking note of metaphors and analogies used by participants; (8) observing naturally occurring transitions in the participant's dialogue; (9) recognizing how the participant used words and phrases to connect concepts and establish relationships; (10) reading and re-reading passages that did not easily fall into the themes that were visible early on; (11) eyeballing and frequently handling the data; (12) cutting and sorting quotes of importance.

TABLE 3
Identified Themes[16]

Identified Themes	
Cognitive Patterns	Context specific mental models or logic concepts that serve as explanatory structures for the situation or problem.
Learning Patterns	Creating relationships between concepts, skill, people, experiences, and past mental logic to make meaning.
Comprehension Patterns	Using mental logic, learned relationships, and social discourse to make sense of the situation or problem.
Engaged Patterns	Interaction with others about ideas and concepts relative to the situation or problem.
Predictive Patterns	Using mental logic and understanding to posit alternatives and potential outcomes of a situation or problem prior to their occurrence.

FINDINGS

Hackers Have a High Tolerance for Ambiguity

Skilled hackers perform at the edge of the unknown within poorly defined domains. In order to effectively handle the risk, uncertainty, vagueness, and chaos associated with operating within such an environment, they had to leverage knowledge, creativity, curiosity, expertise, and interpretive schemes from various technical and critical thinking disciplines. Hackers accept ambiguity as a result of the accelerated technological changes that occur around them.

Within these poorly defined, ever-changing domains are many peculiar questions and issues that lack clarity and specification. To address these problems, skilled hackers use uncertainty-abduction[17] whereby they develop an interpretive scheme of how the

[16] For a detailed explanation of how hackers use these patterns, refer to the section entitled A Cognitive Framework of Hackers.

[17] According to Peirce, abduction consists of processes of thought capable of producing no conclusion more definite than a conjecture [or forming a hypothesis and deciding if it is worth testing] Fann, K. T. 1970.

environment works. This *sensemaking* enables the hacker to make meaning of the problem and craft a *vision* of potential solutions (Hill & Levenhagen, 1995).

70% of the respondents described being comfortable with or expressed a desire for the unknown and seeking to solve peculiar problems that lack considerable definition and understanding. Specifically, during interviews many respondents felt that they "operate in a very complex environment" and that "nothing is well defined." In discussing requirements for skilled hacking [from an evaluation perspective], some respondents stated that it was important to "find out if somebody [a hacker] has the acumen to really want to dig deeper into problems." From this point, skilled hackers not only have the ability to address complex problems, but that they also have a desire to explore those problems. Some respondents expressed this *relentless* nature explicitly. For example, one respondent stated "I take on something new, something that I haven't done before, and then I want to work on it until I understand it, until I'm happy with it." Skilled hackers also demonstrate competence to reduce ambiguity. 50% of respondents explicitly expressed this *desire of control* of a problem or domain. One respondent suggested that "the only time you fail is when you give up" and that "everything else is just a revision".

Constructing mental models of technology-based devices, systems, networks, and other environments of complexity was reported to be incredibly difficult. The more complicated it is to learn about an environment; the more difficult it will be to build mental models that represent that environment and its components (De Kleer & Brown,

---

Peirce's theory of abduction: Martinus Nijhoff La Haya. He considered abduction to be the first of stage of all inquiries and a foundational component of perception and memory.

1983; Vandenbosch & Higgins, 1996). These models not only have to represent the current state and functioning of the environment [being considered], but it must also be capable of predicting future states and consequences of events.

Hackers had to use reflective thinking and introspection to apply their personal mental logic and understanding to build a mental representation of the system or a physical *topology* of the system to help them *see* the structure and physical organization of it. 100% of respondents reported personal reflection as a means of building and maintaining their mental models. System architects, for example, had to construct topological models of a system and its components, external and dependent relationships, and potential behaviors between those components. These models usually addressed the situation in a way that assisted in making or formulating and articulating a decision or strategy. Once the hacker created a model that appeared to accurately reflect the situation with which they were faced, they began to make inferences about the system, *envisioning* its function and purpose. Successful envisioning enables them to build alternative or complementary models, further expanding their ability to make meaning of the environment. Depending on the completeness or depth of the model, a skilled hacker was able to deduce potential consequences [as related to the situation].

Hackers also reflected on the situation by *wrapping their head around* the topological structure and envisioning its function. By doing so, they were able to explore the causal mechanisms that underlie that structure. The causal model would "describe the functioning of the device (i.e., a description of how the device's behavior results from its constituent components which is stated in terms of how the components causally interact)" (Gentner & Stevens, 1983c: 158). This would enable the hacker to run mental

simulations against their models which would enable them to see how their constructed model holds up against hypothetical [or realistic] scenarios or events. For example, to analyze a system for vulnerabilities, the hacker would create a topological layout of the system, envision how it functions, understand its causal relationships and behaviors, and then test various attack methodologies against that model. Eighty-eight percent of the hackers suggested attributes like creativity and curiosity and stated that they directly contributed to their ability to build mental models to deal with uncertainty and ambiguity. One respondent stated, "I think people wildly underestimate the creativity of the bad guy." Another respondent said, "to do what I'm doing…your creativity and your skill is gonna have to outmatch all those people [referring to defending hackers]." This creativity was supplemented by an intense curiosity and desire to understand [and control]: "I have a lot of technical curiosity. I like to break things into lots of random technical pieces. But I don't do them maliciously, or for attack and defense purposes. I do it because I am interested in how things work and why they work and in making them better." Additionally, effective mental models assisted in articulating the strategy of influencing the system. Also, they assisted in the hacker's ability to communicate the strategy and their decisions to others.

Mitigating Uncertainty: Performing Mental Model Maintenance with Discourse

Strategizing and making decisions is a core part of being a hacker—how else can they find such novel and innovative ways to break into and protect systems in such complex environments and situations. However, no hacker does this in a vacuum. They use social interaction and exchanges—through discourse—to learn to identify the most probable outcomes, select the most advantageous strategies and make the best decisions.

One of the most common ways to evaluate a strategy or decision is through argument and debate (Morecroft, 1984). Hackers use discourse as a means of *sensegiving* to reduce the uncertainty, create meaning, and update their mental models. One hundred percent of the respondents used discourse as a way to comprehend [make meaning] and share their mental models. They used their models as vehicles for extending argument and debate…[and] brought them down from the pedestal of the infallible black box as a complement to the thinking and deducing powers (Morecroft, 1984). In a sense, hackers use their models as generators for opinions in group working sessions where they debated the strategies being proposed. These forums acted as knowledge transfer mechanisms whereby hackers could collectively [and dynamically] build and maintain their mental models—continuously changing, updating, reflecting upon, and testing them. Usually, these caffeine-fueled and intellectually rigorous sessions consisted of paper with hand-drawn doodles, dry-erase boards and walls full of flow charts, architectural drawings, and other visual aids to help represent the endless amounts of logic being verbally thrown around. One hundred percent of respondents reported using visual aids like diagrams, flow charts, "box-and-arrow" models, and other aids to externalize and augment their mental models and associated causality. Eighty-eight percent of respondents used narrative construction to help communicate their models, strategies, and decision. One respondent described the advantages of these sessions by stating "when you're sitting with a group of people…you have all these different, diverse ideas. It changes and usually gives…a better result." Another respondent stated, "I want to see the system network before I can understand why I'm looking at the security aspect. I want to see the network topology first."

Hackers also used group discussions to engage in social cognition and to jointly explore the problem or target system. Eighty-three percent of respondents used social discourse as a mechanism of knowledge transfer instrumental for understanding the environment and making meaning of the associated uncertainty. One respondent described these interactions of social exploration as, "a brainstorming session where you get everybody's experience." Hackers also construct stories and narratives to provide situational context for their models. One study respondent stated, "you know, I basically, I'm creating a story about the motivations of a hypothetical attacker…and using that straw man attacker as a model to describe ways in which a particular vulnerability could be exploited." Another respondent described using narratives by stating, "we create a narrative across the entire engagement…[we] saw this, and then looked at this, used this, and then here, so the idea of being able to kinda string together a story of how – here's where it started, and here's kinda the critical path to your [sensitive] data."

This process increased the hacker's ability to collect and process information and made them more adept at building effective mental models. Over time, this skill would offer the hacker the necessary domain expertise, and also the requisite mental capacity and cognitive abilities to be skilled in operating in that domain. It also improved the hacker's ability to deduce the consequences of a situation based on the supplemental mental models that had been created. The more complete these mental models were, the more likely the hacker would be able to recognize flaws and inconsistencies in the situation that might otherwise go unnoticed. Considering that skilled hackers possessed knowledge and expertise across a variety of domains, they also acquired the ability to dynamically create mental models that reflect that breadth.

Hackers externalized their mental models with diagrams and narrative construction. These diagrams and narratives became focal points for *working sessions* and helped hackers jointly explore internal and external linkages of the situation. They also enabled hackers to see emerging patterns. Patterning is incredibly important to hackers because it helps diagnose sources of uncertainty and anomalous events. Eighty-three percent of respondents described using patterning as a key technique in recognizing everything from attack and defense patterns, data flow, system interactions, and behavior (just to name a few). One respondent described how he witnessed a hacker breaking into a system by stating, "and so his attack pattern was he had to chain together 14 different attacks to get from Point A to winning the prize [breaking into the target system]…and you think wow, that guy's determined." Another respondent described using patterns by stating, "I mean I think that's why we go through the whole information gathering phase and system mapping at the beginning is because we are looking for what I would call… flaw patterns or attack patterns where I…know if you have this string in your code, you're a virus…I'm looking for similar type design flaws where I know from past experience that if I see this in your code, if you do certain things, you're probably gonna be vulnerable."

Although skilled hackers use patterning throughout much of their work, one of the most interesting uses is in their ability to perform *forward thinking*. Skilled hackers used patterning to assist them in anticipating future events and creating strategies for addressing those events before they occurred. Eighty-three percent of respondents described using patterning for forward thinking. Forward thinking enabled them to anticipate how their adversary would respond to their advances. One respondent

described how he attempted to anticipate the moves of his adversary by stating, "how can I predict, how can I anticipate what they're going to do? Where do I need to be in the network so that they can't see me?" Hackers used previous mental models and experiences to help them make assertions about future situations. One respondent described this by stating, "So the idea is that previous engagements are models for future ones. You can predict that if someone set up a product in this way, and you've seen this and this before, and you know for a fact that, for the most part, when people install Product X, they generally don't bother to change the password on this, you can basically say – if you've seen that five times before and you come across [a system] that has it installed, you can…[consider] a model of past behavior that says hey, I'll bet this is the same way. More often than not, you're right."

DISCUSSION

This study explored the mental models of hackers and how those mental models are built and maintained through the activity of hacking within complex systems, networks, and other ambiguous environments. The qualitative analysis revealed a model of personal cognitive skills and social cognitive skills central to the task of hacking including: 1) using reflection to perform sense-making for building a causal mental model; 2) using social exchanges—through argument and debate—to deal with uncertainty, make meaning, and maintain mental models; 3) using artifacts for personal reflection and social exploration to externalize the mental models [making it possible to use them] for performing uncertainty-abduction; and 4) using various mental patterns to identify new emergent patterns and predict potential future patterns and events through forward thinking. Performance of these activities depends heavily on [individual and

collective] mental logic, technical expertise, creativity and curiosity, and substantial mental capacity to dynamically build and manipulate mental models inundated with complexity. The notion that mental models are important in the use of uncertainty-abduction within hacking is consistent with the well-established idea that mental models help humans understand the world within which they live.

This investigatory endeavor contributes by applying mental model theory to the domain of hacking, which has been studied in a limited capacity. We took a grounded theoretical approach by interrogating skilled hackers to capture their lived experience and leveraging the resulting data extend the applicability of current mental model theory (e.g., Johnson-Laird (1983) and Norman (1986a)). This study extends mental model theory by exploring cognitively-intense processes involved in hacking and showing that there are cognitive skills, motivational traits, and social cognitive skills, such as expertise, creativity and curiosity, analytic and systems thinking, and visual comprehension abilities, that have a direct impact on the hacker's ability to build and dynamically manipulate mental models. Further, most discussions of mental models focus on simple physical systems and devices and not less tractable domains like hacking which involves highly dynamic phenomena (Stevens & Gentner, 1983). It reveals how skilled hackers use mental models, individually and socially, to *make sense* of uncertainty and ambiguity within highly complex situations that lack explicit normative models and in many cases are able to use this understanding to make predictions about future events. The study extends Norman's (1986a) ideas by showing how hackers use cognitive patterning to recognize nascent trends and patterns that can be indicative of future events or patterns.

The study also advances the knowledge of mechanisms that enable dynamic sharing and manipulation of mental models, such as diagramming, narrative construction, argument, and debate. Mental development is dependent on both personal reflection where one builds their internal mental models and social exploration where one shares and manipulates (or maintains) those models. For hackers, this is where the most important learning occurs (Vandenbosch & Higgins, 1996). Indeed, hackers were continuously *learning* through building new mental models and maintaining existing models.

The results of this study suggest that the hacker mind uses rich, varying, and evolving mental models to perform patterning [including creation and recognition]. Patterning enables them to effectively understand and observe complex system—as well as predict future states of those systems.

A Cognitive Framework of Hackers

In the beginning, it was our belief that mental models could explain, in a formulaic manner, how hackers approached decision-making and problem solving. Therefore, it only seemed logical that by interviewing hackers to capture their mental models, we would illuminate how they hack. However, our conceptual model (Figure 1) introduces rather a cognitive framework which integrates the various forms of patterning used by hackers via personal reflection and social exploration.

The framework reflects domains of critical thinking and cognitive presence: a) stimulation of a problem, event, or anomalous situation that initiates thinking (individually) [using cognitive patterns] and/or dialogue (collaboratively) [using engaged patterns] resulting in starting a new model(s) or adding a new reference point to a

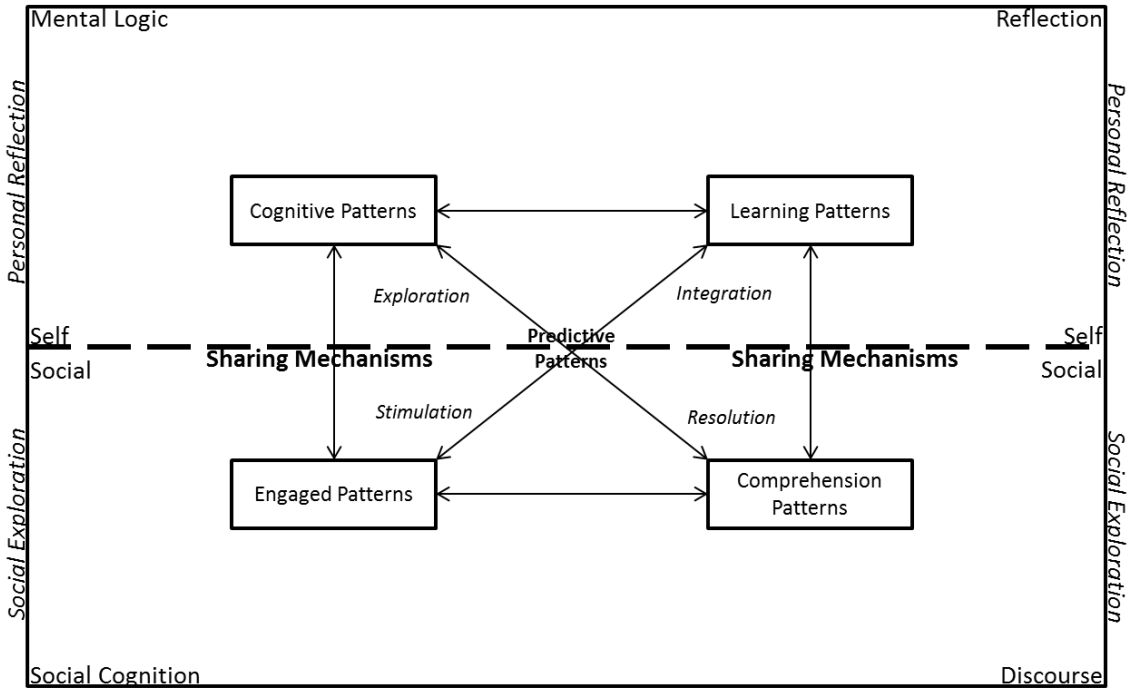
previously existing model; b) exploring the problem and resulting model(s) where the hacker transitions between personal reflection [using cognitive and learning patterns] (individually) and social exploration [using engaged and comprehension patterns] (collaboratively), continuously exchanging information about the problem [via sharing mechanisms - narrative construction, argument, and debate]; c) integrating new information and updating the model(s) and sometimes joining separate models into one when appropriate where hackers begin to use their mental logic and reflections [using cognitive and learning patterns] on the situation to *make sense* and come up with solutions from the ideas and concepts previously explored; d) resolving issues or discrepancies within the model(s) and searching for counterexamples where hackers feel that they have a sufficient understanding of the problem, potential solutions, and begin testing and challenging them [using cognitive, learning, comprehension, and engaged patterns]; and e) searching for examples that prove their model(s) and assist in anticipating future events where hackers use the constructed narratives, based on mental logic, methods of engagement, understanding of the domain, risk analysis, and alternative methodologies to predict the next possible outcome. There are bi-directional linkages between the patterns because they often work in congruence. For example, just because a hacker is engaged in personal reflection does not mean that it is happening independently or exclusively with or without social exploration.

Personal Reflection and Social Exploration

Within our cognitive framework, there are two *hemispheres* that represent the types of cognition in which a hacker engages: *personal reflection* and *social exploration*. The personal reflection is where the hacker performs introspection and internal cognitive processing; it includes using cognitive patterns which are context specific mental models or logic concepts that serve as explanatory structures for the situation or problem and using learning patterns which involves creating relationships between concepts, skills, people, experiences, and mental logic to begin making meaning. Social exploration is where the hacker performs collaborative analysis and social cognitive processing. It includes engaged patterns which involves interacting with others about ideas and concepts relative to the situation or problem and using comprehension patterns which involve using mental logic, learned relationships, and social discourse to make sense of the situation or problem. Predictive patterns are situated at the core of the other pattern types because they involve using mental logic and understanding to posit alternatives and potential outcomes of a situation or problem prior to their occurrence and leverage inputs from all of the other pattern types used by hackers. Personal reflection and social exploration are delineated by sharing mechanisms (like diagramming, narrative construction, argument, and debate) since hackers use them to develop and share mental concepts and cognitive awareness. Overall, it became apparent that cognition does not only occur within the individual hacker (Dewey, 2012; Hutchins, 1995; Vygotsky, 1986). In the same way that dentritic connections between neurons enable thinking for the *internal brain,* the same can be said for social cognition and the *external brain*. If we think of a hacker as being one processing unit within a larger computational machine, the

concept of an internal brain and an external brain helps make sense of the way that hackers make decisions and solve problems collaboratively (Hutchins, 1995).

FIGURE 1
Conceptual Model



LIMITATIONS

Potential limitations of this study are as follows:

- The sample size of 18 is relatively small.[18]
- The participants were drawn from the researcher's network of contacts and could have been skewed as a result.[19]

[18] The researcher continued interviewing participants until data saturation was reached.

[19] The initial participants were drawn from my network of contacts; however, the researcher continued identifying participants through referrals from the preceding participants.

- Participants were living in the United States during the time that interviewing took place and could have been skewed as a result.[20]

- The researcher is a member of the cybersecurity community and frequents hacking events which could have skewed the results.

- This study required the interview participants to recall experiences that may have taken place many years ago which could have been compromised by the effects of time on recalling those experiences.

- The Cognitive Framework of Hackers is preliminary and inadequately researched at this time; the researcher acknowledges that further research is necessary.

SUMMARY / CONTRIBUTIONS

"I think the results of your work are gonna be particularly interesting and applicable to our business because we're actually trying to hire, train and retain [hackers]; those that do nothing all day but hack. From our perspective, it's gonna be really interesting research, because we're building up our own profiles of ourselves on – because we're going to be doing – we do efficacy, we know who does well and we know who washes out." - Study Participant

"I will admit that I'm going to step out of this room, I think, with a little better understanding of myself." - Study Participant

This study explored the mental models of hackers, in particular their purpose and how they are created, acquired, and shared. The resulting empirical findings reveal the cognitive and social cognitive processes that enable skilled hackers to be proficient decision makers and problem solvers. The following are additional findings of this research:

- Skilled hackers are strategists.

[20] However, the researcher compared the results to the work being done by Chiesa, Ducci, and Ciappi (2007) in the Hacker Profiling Project, which is detailed in their book *Profiling Hackers*.

- Their strategies are based on many cognitive mechanisms, such as patterning and mental logic.
- In the mind of a hacker, a mental model is not a procedural flow of tasks, but a way of thinking about something specific.
- Hackers form their strategies through comparative analysis and patterning.
- Hackers look for anomalies because they are peculiar and warrant further investigation.
- Developing a strong strategy requires personal reflection and social exploration.
- Hackers construct narratives to help them understand their adversaries.
- Through narrative construction, hackers can use profiling and mental models of their opponents to conceptualize the opponent's potential strategies.

The results of this research have revised our understanding of the role of mental models and cognitive frameworks. As our society becomes more reliant on digital technologies and nation states and corporations integrate hacking into their adversarial toolboxes, a cognitive framework of hackers can provide substantial insights into understanding how to protect ourselves, innovate, and develop the next generation of hackers.

Appendix B: How Hackers Think:
Understanding the Mental Models and Cognitive Patterns of High-Tech Wizards

By

Timothy C. Summers

Submitted in Partial Fulfillment of the Requirements of the Quantitative Research Report
in the Doctor of Management Program
at the Weatherhead School of Management
DM Management Design Fellow

Advisors:
Kalle Lyytinen, Ph.D., Case Western Reserve University
James Gaskin, Ph.D., Brigham Young University

CASE WESTERN RESERVE UNIVERSITY

June 2014

HOW HACKERS THINK: UNDERSTANDING THE MENTAL MODELS AND COGNITIVE PATTERNS OF HIGH-TECH WIZARDS

Abstract

Hackers seek out weaknesses in computers and networks that can be used to steal data or impact the functionality of the Internet. In the general sense, a hacker is a technologist with a love for computers and a "hack" is an inventive solution executed through non-obvious means. Hackers speak the language of code which propels the evolution of our information technology. This makes hackers the solvers of our largest, most complex issues facing technological systems. In consequence, they are experts at solving poorly understood and challenging technical problems in a variety of settings requiring deep understanding of technical detail and imagination. This research aims to identify the brain-based skills needed to carry out hacking from the simplest to most complex levels to understand how the most impactful innovators of the technology age solve our most complicated problems.

Key words: hackers; cognition; mental models; learning; forward thinking

INTRODUCTION

Hackers seek out weaknesses in computers and networks that can be used to steal data or impact the functionality of the Internet. Many hackers are "white hats", meaning that they discover flaws in order to fix them and improve overall security. Others are "black hats", using their skills to commit crime. However, the term *hacker* does not always apply only to finding computer and network weaknesses. In the general sense, a hacker is a technologist with a love for computers and a "hack" is an inventive solution executed through non-obvious means (Coleman & Golub, 2008; Levy, 2001; Summers et al., 2013; Turkle, 2005). This research aims to identify the brain-based skills needed to carry out hacking from the simplest to most complex levels to understand how the most impactful innovators of the technology age solve our most complicated problems.

During the Facebook initial public offering, CEO Mark Zuckerberg distributed a letter to shareholders describing the company's *modus operandi* as 'the Hacker Way'. Hacking is the use of technical and analytical prowess to experiment with the limitations of systems for intellectual curiosity (Summers et al., 2013). He explained that this approach to building software was focused on excellence through continuous improvement and iteration and that it would drive the company's success (Rosoff, 2012). The reason for this belief is that hackers operate within a "maker culture" driven by playful cleverness, intellectual stimulation, problem solving, self and socially directed learning, and astute forward thinking (Summers et al., 2013). In short, hackers speak the language of code which propels the evolution of our information technology (Kastelein, 2014). This makes hackers the solvers of our largest, most complex issues facing technological systems. In consequence, they are experts at solving poorly understood and

challenging technical problems in a variety of settings requiring deep understanding of technical detail and imagination. This activity draws upon complex and diverse mental models (Jonassen, 1995) permitting sufficient synthesis of varied information that enables hackers to push the boundaries of technology and anticipate its future behaviors.

To stay abreast of technological evolutions, hackers must continuously construct advanced knowledge that will support their complex problem solving and transfer of learning (Jonassen, 1995). Such capacity often rests on their cognitive skills and traits such as, domain expertise, creativity, curiosity, diagramming or mind mapping, ambiguity tolerance, learning, and forward thinking. These cognitive skills and traits are major contributing factors to their mental models; thereby enabling hackers to learn their environment and see new, unseen emerging patterns.

What are the charactertistics of skilled hackers? What cognitive faculties are involved in the act of hacking? Recently, there has been an interest in questions such as these, and in hacking as a cognitive process. Cybercriminals, such as black hat hackers, cost society approximately $388 billion annually (Summers et al., 2013). In contrast, the effects of ethical hackers has yet to be quantified. However, the literature is remarkably scare on this highly impactful subculture.

Skilled hackers are adept at rigorous thinking, writing code, and debugging. They are able to recognize, use, and adapt patterns thereby obviating the need for extra, inefficient computation (Robins, Rountree, & Rountree, 2003). A hacker's success is largely dependent on their ability to learn by continuously maintaining and building their mental models of the environment and using those models to anticipate behaviors within that environment (Summers et al., 2013). In addition to maintaining existing mental

models and building new ones, some researchers suggest that learning involves the expert being able to continuously shift their mental models of the environment within which they operate (Weick, 1993; Wolfberg, 2014). Dynamically shifting those models and deriving conceptual linkages between them enables the expert to identify and reflect on emergent behaviors (Frederiksen et al., 1999).

A recent field study by Summers et al. (2013) investigated how skilled hackers use mental models to organize and interpret environmental information as to aid in pattern matching, solving problems, and decision making associated with hacking. The study found that hackers, when faced with a challenge or decision making opportunity, used several patterning mechanisms to make sense of the situation, craft potential solutions, and predict potential outcomes. The study also identified a complex array of interactions between the cognitive skills and traits, learning outcomes and forward thinking strategies. However, the detailed nature and specific effects of those mechanisms were not explored further. In this study, we will address this void. We recognize the information systems research body can benefit from a deeper understanding of how hackers use the knowledge structures related to hacking and how those knowledge structure assist with validating mental model content, acquiring new knowledge, perform planning activities, and applying the structures to define and solve problems (Robillard, 1999).

Our research question is: how can hackers improve their learning and forward thinking by engaging effectively intrinsic individual characteristics (such as creativity) given their level of perceived skills (such as domain expertise) and the level of the their ability to understand the requirements of their work environment (such as ambiguity

tolerance)? To investigate this question, we conduct a survey among hackers and cyber security professionals in various industries to detect the varying effects of intrinsic individual characteristics, perceived skills, and perception of environment in hindering or strengthening a hacker's learning and forward thinking. Understanding how hackers utilize their cognitive skills and traits to make meaning of their environment and complexity can provide important insights for improvements in information processing, knowledge production, decision making, organizational design, learning, anticipatory thinking and opportunity recognition in multiple complex technical tasks. The primary contribution of this research is to provide a deeper, richer understanding of innovative thinking employed hackers.

The remainder of the article is as follows. In the next section, we review how learning and forward thinking occur, and formulate a theoretical framework that articulates the sensemaking and construction of derivational linkages between mental models necessary for skilled hacking. More specifically, we discuss innate characteristics and recognized skills possessed by the hacker and review the varying effects of their understanding of the environment. We then articulate a research model and formulate a set of hypotheses between the intrinsic individual characteristics, perceived skills, perception of environment, and learning and forward thinking outcomes. In the next section, we discuss the research design and method followed by a review of the major findings. We conclude with a review of practical and theoretical implications and explore avenues for future research.

THEORETICAL FOUNDATION

Learning as the Dynamism of Mental Models

Learning has been studied from various perspectives including, problem solving (Bruner, 1978; Hayes, 1978), the use of metaphors and analogies to identify emerging behaviors (Lakoff & Johnson, 2003), using discourse to comprehend and share views of the world (Morecroft, 1984; Summers et al., 2013), and as the shifting of mental models (Norman, 1983b; Vandenbosch & Higgins, 1996; Wolfberg, 2014). In the following, we focus on the antecedents and their interactions that influence an individual's ability to dynamically shift their mental models to make meaning of the world.

Our research is anchored in cognitive psychology and concerned with how hackers can gain understanding of their world through dynamically constructing mental models and maintaining those mental models to solve problems (Frederiksen et al., 1999; Leahey & Harris, 1989b). In this context, a mental model is defined as a cognitive structure through which people perform information interpretation and information retrieval; thereby affecting how people process new information and (re)consider previously known information (Leahey & Harris, 1989b). This processing results in shifting mental models and is often facilitated by new experiences (Vosniadou & Brewer, 1992). Mental models provide hackers with the context necessary to view and interpret new information and guide them on how to store that information relevant to a specific situation (Kim, 1998).

In our context, a mental model reflects a hacker's beliefs about the domain of hacking—software, hardware, system and user behaviors. The factors that go into the construction of the mental model are acquired through observation, instruction, and

inference (Norman, 1983b). There is a direct correlation between the parameters and states of the thing being observed and the hacker's mental model. As situational context changes, the hacker dynamically shifts their mental models to reflect new understanding that covers both the prior and current information (Argote & Miron-Spektor, 2011). Here, we will focus primarily on the cognitive skill and traits that influence and enable the mental model shifting that hackers must do to solve the complex problems they face. We will next review the predictive nature of mental models.

Predictive Power of Mental Models

We are interested in the predictive power, which is the ability to generate testable predictions that mental models provide to people when understanding complexity and problem solving. We call this forward thinking. Mental models provide people with predictive power in that they enable an individual to understand and anticipate the behaviors being observed (Norman, 1983b). When a person runs a model in their mind, reflects on its emergent behaviors, and infers linkages with other models, it enables them to predict and understand future behaviors (Frederiksen et al., 1999; Norman, 1983b). To our knowledge, there are no studies which have examined forward thinking as an outcome of learning and related cognitive skills, and traits of hackers. We will review what we know about these cognitive skills and traits.

Intrinsic Individual Characteristics, Perceived Skills, and Perception of Environment

The literature is abound with studies on learning and knowledge transfer which consistently emphasize the importance of intrinsic individual characteristics, perceived skills, and perception of environment (Baldwin & Ford, 1988; Lim & Johnson, 2002) as transfer variables connecting learning and performance (Holton, 1996; Noe & Schmitt, 1986). After a review of the relevant literature, we define intrinsic individual characteristics to include factors such as creativity and curiosity (Berlyne, 1978; de Bono, 1995); perceived skills to include factors such as domain expertise and diagramming (Lim & Johnson, 2002); and perception of environment to include factors such as ambiguity tolerance.

Intrinsic Individual Characteristics

In learning environments such as the workplace, intrinsic individual characteristics including creativity (de Bono, 1995; Eskildsen et al., 1999; Evans & Lindsay, 1996) and curiosity (Berlyne, 1978; Loewenstein, 1994) enable individuals to make sense of and use varying amounts of disparate information (Reio & Wiswell, 2000).

Creativity. Hacking computer systems is a creative endeavor that requires expertise, inquisitiveness, adaptability, and technical skill. As hackers encounter the need to write novel code to implement an exceptional hack and face new problem domains, the need for creativity plays (Summers et al., 2013; Tiwana & Mclean, 2003). A review of the literature reveals that there have been few studies on creativity as a necessary cognitive skill and trait of hackers. Tiwana and McLean (2003) suggest that creativity exists at both the individual and team levels. They define creativity as an improvisational

process where team members work collaboratively to interrelate their ideas. These ideas are usually based on the unique perspectives and skills of the individuals involved. This process is important to the generation and evaluation of new ideas, designs, solutions, and artifacts required (Summers et al., 2013; Tiwana & Mclean, 2003). The work by Ocker, Hiltz, Turoff and Fjermestad (1995b) suggests that the problems faced by hackers rarely have one possible solution and that creativity would enable them to conceive of multiple possible solutions to the same problem.

Curiosity. In the literature, curiosity is recognized as a critical cognitive trait that influences human behavior. It is a key driving force behind learning and innovative discovery (Loewenstein, 1994). When hackers are faced with problems that they have never seen before, the cognitive trait of curiosity drives the desire to explore the situation. In fact, hackers seek out these exploratory opportunities (Loewenstein, 1994; Summers et al., 2013). Hebb (1955) explains that this curiosity-seeking behavior is driven by the pleasure of threats and puzzles. The literature recognizes that hackers engage in intensive and focused activities to explore the nature of problems with which they are faced (Jordan & Taylor, 1998; Summers et al., 2013).

Perceived Skills

Lim and Johnson (2002) suggest that perceived skills, such as technical competence and using technical techniques are highly influential to the degree of learning and knowledge transferability. Within hacker-centric environments, much focus is on the individual's technical skill and their ability to utilize technical methods to facilitate learning and transfer.

Domain Expertise

Our review of the empirical research on domain expertise recognizes Dreyfus and Dreyfus (Dreyfus, Dreyfus, & Athanasiou, 1987a; 1980) and Benner (1982) who both found that expertise is not innate and that human beings must learn to become masterfully proficient at a skill. Learning takes place through trial and error and is sometimes guided by imitating others who are more proficient (Dreyfus et al., 1987a). A person has reached the expert level when they no longer have to rely on principles to connect their understanding of a situation to the appropriate response (Benner, 1982). In their review of programming expertise, Campbell, Brown and DiBello (1992) argued that due to the non-unitary nature of programming[21], the prevailing binary novice-expert comparisons provided little explanation of the psychology of programming. They found that when learning a new technology or new programming language expert programmers "become novices again". As a result, they concluded that for expert programmers, there is an evolutionary progress from "cookbook" to "intuition" as described by Dreyfus and Dreyfus (1987a).

Diagramming

Diagramming is a visualization technique where hackers create technical drawings to explore and understand associations and relationships between concepts (Summers et al., 2013). Using this technique allows hackers to represent and manipulate a complex problem using a diagram and have a better understanding of the relationships, remember them, and more thoroughly analyze each part (Davies, 2011). Earlier studies

[21] Research on programmers is instrumental to understanding hackers because hackers are programmers who have a burning desire to write interesting software and for whom computers are a medium of expression (Graham, 2004).

suggest that diagramming promotes deep learning of a problem (Biggs, 1987; Entwistle, 1981a; Marton & Säljö, 1976a, b; Ramsden, 1992). Although diagramming helps hackers with associating ideas, it is also important for mental model construction and maintenance (Davies, 2011). It promotes innovative thinking and brainstorming thereby enabling hackers to conceive of linkages between disparate concepts (Novak & Cañas, 2006a). Using prior knowledge and conceptual brainstorming provides the scaffolding necessary for new learning (Davies, 2011).

Perception of Environment

From the time an employee considers a new position, to the time they engage in daily challenges in a constantly changing work environment, they are continuously constructing new meanings and new knowledge, thereby learning (Dixon, 1997; Kofman & Senge, 1993; Kozlowski et al., 2001; Reio & Wiswell, 2000). Within learning work environments, individuals can often feel psychological burdens imposed on them where they are continually expected to apply their new learning to their jobs (Lim & Johnson, 2002). The key factor that is included in these workplace psychological requirements is ambiguity tolerance (Summers et al., 2013).

Ambiguity Tolerance

Our review of the literature on ambiguity tolerance begins with McDougall (1926), Adorno, Frenkel-Brunswik, Levinson, and Sanford (1950) and MacDonald (1970). The literature describes tolerance of ambiguity as a person's ability to psychologically cope with ambiguous information and the affect it has on their perception, interpretation, and how they think about the situation. A problem can be considered ambiguous when (1) there is variability in structure and understanding, and

(2) there is variability in the interpretations or potential responses (Norton, 1975). As previously mentioned, hackers deal with problems that lack clarity, structure, and are abound with uncertainty. Whereas people who are intolerant of ambiguity tend to avoid or give up on learning in ambiguous situations, hackers are aroused by them (Owen & Sweeney, 2002b; Summers et al., 2013). Owen and Sweeney (2002b) demonstrated that being tolerant of ambiguity has a positive impact on learning and performance.

The relationship between the ambiguity tolerance factor and intrinsic individual characteristics, like creativity, has often been proposed but there have been few studies. Ambiguity tolerance is considered to be an essential element of creativity (Vernon, 1970) and curiosity (Summers et al., 2013). Ambiguity tolerance enables individuals to be dissatisfied with partial, non-optimal solutions to complex problems, thereby supporting creative, exploratory thinking and behaviors (Vernon, 1970). Individuals who tolerate ambiguity are able to be effective with large sets of stimuli and situations, ambiguous and non-ambiguous whereas intolerant individuals avoid such situations (Zenasni, Besançon, & Lubart, 2008). Zenasni et al. (2008) suggest that ambiguity tolerance enables individuals to optimize creative potential.

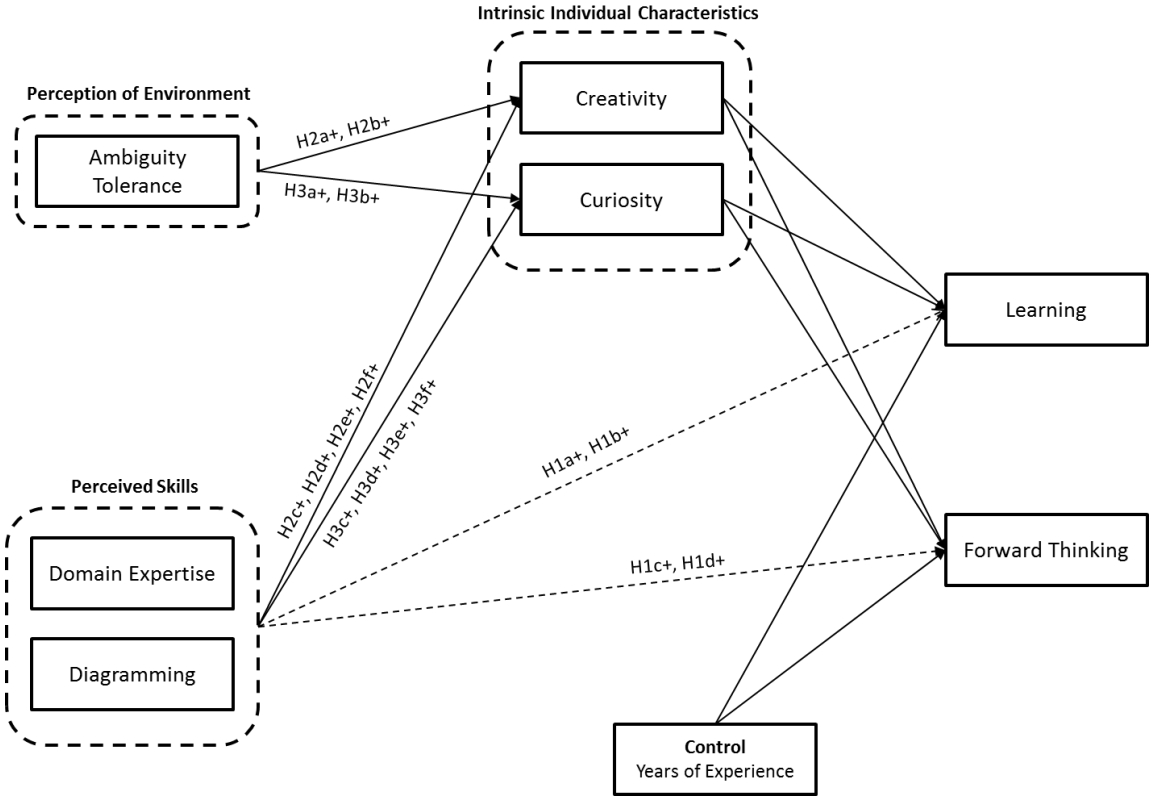
The literature indicates that there is a direct positive correlation between an individual's ambiguity tolerance and their creative, exploratory thinking (Barron & Harrington, 1981; Golann, 1963; Sternberg & Lubart, 1995; Zenasni et al., 2008). Situations that require creative, exploratory thinking often involve ambiguity (Zenasni et al., 2008). Stoycheva (1998; 2003) suggested that individuals tolerant of ambiguity are better suited to handle feelings of anxiety and psychological discomfort associated with unstructured complex situations. Urban (2003) proposed that ambiguity tolerance

contributes to creative problem solving because it enables the intrinsically motivated exploration of complex situations.

THEORETICAL MODEL AND HYPOTHESES DEVELOPMENT

Based on the constructs of intrinsic individual characteristics, perceived skills, and perception of environment we will next articulate a research model that posits how these elements influence learning and forward thinking within the hacker mind. In particular, we will analyze mechanisms that either strengthen or hinder a hacker's learning and forward thinking given the variation in intrinsic individual characteristics, perceived skills and perception of environment. We will argue for the presence of mediating effects of intrinsic individual characteristics in mitigating or enabling learning and forward thinking outcomes given the presence of certain elements of perception of environment, namely ambiguity tolerance. Because we assume a mediated model (Mathieu & Taylor, 2006), we will articulate the model by first stating direct effects assumed in the model and then developing a fully mediated model (Figure 1).

FIGURE 1
Research Model with Hypotheses



Direct Effects

Based on our theoretical framework, we will first formulate direct effects associated with the perception of environment and perceived skills on learning and forward thinking when intrinsic individual characteristics are absent. We posit that *ambiguity tolerance* decreases rigidity in thinking and increases willingness to accept and incorporate new knowledge (MacDonald Jr, 1970). The technology field is constantly changing and abound with ambiguous situations which generate substantial opportunities for learning and forward thinking (Owen & Sweeney, 2002b; Summers et al., 2013). *Domain expertise* enables a skilled hacker to intuitively respond in various situations without analytical principles needed by beginners. Whereas less skilled hackers may

require rules, guidelines, or definitive maxims to comprehend the situation before conceiving of a specific action, an expert hacker is more capable of intense absorption of the situation and utilize his mental energy to immediately conceive of potential actions and prepare for potential situational conditions (Dreyfus & Dreyfus, 1980). When learning, hackers adapt their knowledge and develop mental models that enable advanced thinking and problem solving. They interrogate, confront, error-check, and discover the rules and generalizations that influence their understanding of the situation thereby continuously testing and revising their mental models (Klahr & Kotovsky, 2013). This process of evaluating mental models involves the creation of new knowledge and enables hackers to break out of old patterns and discover new ones (Mylopoulos & Regehr, 2009). These new patterns address emerging problems thereby enhancing learning and forward thinking outcomes. *Diagramming* is used to create concept maps that represent meaning or ideational frameworks that are specific to a domain of knowledge. The diagrams used by hackers externalize their mental understandings of a situation using labeled constructs and propositional linkages between those constructs (Novak, 1990b; Summers et al., 2013). Visually seeing the knowledge structures before and after interacting with the environment generates learning and forward thinking opportunities (Novak, 1990b). Thus, we posit:

Hypothesis 1a. Domain expertise increases Learning.

Hypothesis 1b. Diagramming increases Learning.

Hypothesis 1c. Domain expertise increases Forward Thinking.

Hypothesis 1d. Diagramming increases Forward Thinking.

Mediation Effects

Next, we will articulate the effects of intrinsic individual characteristics in mediating the effects of perception of environment on learning and forward thinking.

Creativity. Past research identifies as a cognitive trait that enables a hacker to see the detail of a subject, formulate and solve problems, and question the connectedness of diverse topics, and generate new ideas (Gurteen, 1998; Reid & Petocz, 2004). This process is food for innovative thought and encourages hackers to push the boundaries of the environment. The creative process is instrumental to creating and applying new knowledge. This increases learning and forward thinking capabilities*; therefore we posit:*

Hypothesis 2a. Creativity positively fully mediates the relationship between Ambiguity Tolerance and Learning.
Hypothesis 2b. Creativity positively fully mediates the relationship between Ambiguity Tolerance and Forward Thinking.
Hypothesis 2c. Creativity positively partially mediates the relationship between Domain Expertise and Learning.
Hypothesis 2d. Creativity positively partially mediates the relationship between Domain Expertise and Forward Thinking.
Hypothesis 2e. Creativity positively partially mediates the relationship between Diagramming and Learning.
Hypothesis 2f. Creativity positively partially mediates the relationship between Diagramming and Forward Thinking.

Curiosity. *Curiosity* is a cognitive trait reached by the hacker when a situation contains subjective uncertainty. This uncertainty prompts the hacker's tendency to engage in exploratory behavior directed at resolving or mitigating the uncertainty thereby generating opportunities for learning and forward thinking (Berlyne, 1978). Overall, we posit:

Hypothesis 3a. Curiosity positive fully mediates the relationship between Ambiguity Tolerance and Learning.
Hypothesis 3b. Curiosity positively fully mediates the relationship between Ambiguity Tolerance and Forward Thinking.

Hypothesis 3c. Curiosity positively partially mediates the relationship between Domain Expertise and Learning.
Hypothesis 3d. Curiosity positively partially mediates the relationship between Domain Expertise and Forward Thinking.
Hypothesis 3e. Curiosity positively partially mediates the relationship between Diagramming and Learning.
Hypothesis 3f. Curiosity positively partially mediates the relationship between Diagramming and Forward Thinking.

RESEARCH DESIGN AND METHODS

To validate our research model and find support for related hypotheses, we designed and carried out an electronically disseminated, Internet-based, self-administered survey within a population of cyber security experts. The survey approach was appropriate for this research because cyber security experts value their anonymity and privacy. Specifics regarding the resulting sample of respondents are provided in a subsequent section. Scale items for the independent variables (learning and forward thinking), the dependent variables (domain expertise, creativity, curiosity, and diagramming), and mediators (ambiguity tolerance and flexibility) were adapted from existing literature. Data analysis was completed using IBM SPSS Statistics (v. 21) for initial statistical analysis and IBM SPSS AMOS (v. 21) for covariance based structural equation modeling. Our analyses were completed using the following staged approach: (1) confirm suitability of data for multivariate analysis; (2) a structural equation modeling strategy that included an exploratory factor analysis (EFA) and confirmatory factor analysis (CFA) to build the model.

Construct Operationalization

We adapted scales for our constructs from the extant literature. Due to the study context and lack of systematically developed scales in this domain, we carried out

significant modifications to construct operationalizations as explained below. All scales were defined as reflective (Jarvis, MacKenzie, & Podsakoff, 2003). The reliability of our constructs can be found in the Appendix. The Cronbach's alphas for all measures were above .700. The items in all of our scales were measured using a five-point Likert scale anchored by extremes of "strongly disagree" and "strongly agree".

Dependent Variables

Learning (Reflective). A four-item scale was adapted and significantly modified from (Wolfberg, 2014). Vandenbosch and Higgins (1996) and Norman (1986a) were also consulted for validity and adaptations. The construct measures whether hackers change their mental models to fit new situations and are responsive to disconfirming information or questioning the model.

Forward Thinking (Reflective). A five-item scale was adapted and modified from Greenglass et al. (1999). Norman (1983b) was also consulted for adaptations. The construct measures the extent a hacker feels that they utilize their mental models to anticipate future events. Another way to think about this construct is similar to what the entrepreneurship community refers to as opportunity recognition. It can be defined as "a motivated propensity of man to formulate an image of the future" (Kirzner, 1985: 56).

Independent Variables

Ambiguity Tolerance (Reflective). A five-item scale was adapted and modified from MacDonald (1970). The construct measures the relationship that a hacker has with ambiguous stimuli or events.

Domain Expertise (Reflective). A five-item scale was adapted and modified from Durcikova and Gray (2009). Sussman and Siegal (2003) was also consulted for

adaptations. The construct measures the extent to which a hacker feels that their years of experience, facts and heuristics, and highly developed repertoires of knowledge enables them to efficiently and effectively learn and perform forward thinking.

Diagramming (Reflective). A five-item scale was adapted and modified from Güven (2008). The construct measures whether a hacker utilizes diagrams or mind maps to understand relationships between concepts, ideas and other pieces of information.

Mediating Variables

Creativity (Reflective). A five-item scale was adapted and modified from Baer (2006). Zhou (2003) was also consulted for adaptations. The construct taps into the hacker's cognitive process of producing ideas that are novel and useful for solving problems.

Curiosity (Reflective). A five-item scale was adapted and modified from Jiang and Izak (2004). The construct taps into the hacker's cognitive process of using playful exploration to solve problems and make decisions.

Control variables. Research has shown that work experience is the most relevant predictor of job performance (Quiñones, Ford, & Teachout, 1995). The literature is abound by research showing a relationship between years of experience and job performance. More specifically, the research shows that years of experience is important for various human resource functions such as selection (Ash & Levine, 1985), training (Ford, Quiñones, Sego, & Sorra, 1992), and career development (Campion, Cheraskin, & Stevens, 1994; Mccall, Lombardo, & Morrison, 1988). Therefore, in order to further

assess the relationships between the independent variables and the dependent variables, we controlled for years of experience.[22]

Instrument Validation and Refinement

Scale development followed procedures and guidelines recommended by DeVellis (1991), Churchill (1979), and Dillman (2000). The constructs in the theoretical model were measured using multi-item scales to increase reliability, minimize measurement error, attempt greater variability among participants, and improve instrument validity (Churchill Jr, 1979). Each construct is operationalized using at least three items to effectively measure and analyze it using structural equation modeling (Churchill Jr, 1979). Our goal was to develop a survey instrument that was easy to answer and understand.

Once we made an informed decision on the survey items, the procedures suggested by Dillman (2000) for survey design were used. The overall objective of the design was to increase participant response rate and minimize measurement error. The variables of interest were estimated through respondent evaluation on a five-point Likert scale. The response categories for each item were anchored by 1 (strongly disagree) and 5 (strongly agree).

To increase reliability, minimize measurement error, and improve the validity of our constructs, we pretested the scale items (DeVellis, 1991; Dillman, 2000). The pretesting was broken down into two phases. The first phase focused on using the Q methodology to refine the instrument as most of the items measuring our constructs were

[22] We originally included additional controls, including gender, professional certifications, and participation in hacking conference; however, these control variables proved impotent.

adapted from previous studies (Thomas & Watson, 2002; Van Exel & de Graaf, 2005). The Q methodology is a cost effective and simple way to gain insight into the potential problem areas in the items being tested (Nahm, Rao, Solis-Galvan, & Ragu-Nathan, 2002)[23]. The second phase focused on instrument clarity and content validity using Bolton's methodology (Bolton, 1991).

Data Collection, Sampling, and Screening

To identify the appropriate sampling population, we used the researcher's personal networks and a Qualtrics panel because of access and the ability to acquire large numbers in an uninhibited way. We utilized a two-stage survey delivery method. First, we leveraged the contacts and social network of the researcher to identify hackers and experts in the cyber security field. These contacts were sent an email with a URL link to the survey. A similar email was also sent out to a carefully screened professional research panel provided by Qualtrics. The survey was sent out in January, 2014 and all results were received by the end of February, 2014.

Measurement Model

Exploratory factor analysis. We conducted an exploratory factor analysis (EFA) using the SPSS software package with Principal Axis Factoring (PAF) and oblique rotation (Direct Oblimin). This technique seemed appropriate since the factors were correlated and it is well-suited for large data sets (n=350). The factor loadings for two domain expertise items (DE4 and DE5), three flexibility items (FL1, FL2, FL3), two creativity items (CR1 and CR2), two curiosity items (CU1 and CU2), two forward thinking items (FT1 and FT2), and one learning item (LE1) were below the minimum

[23] In the Appendix, we provide a detailed explanation of the Q-sorting process designed by the researcher.

threshold (Hair et al., 2010) and therefore eliminated[24]. All of our items had communalities that exceeded 0.30 indicating adequacy for factoring (MacCallum, Widaman, Zhang, & Hong, 1999). The Kaiser-Meyer-Olkin (KMO) measure of sampling adequacy (MSA) was .928 and the Bartlett's Test of Sphericity was significant (x^2 = 4924.169, *df* =231, and $p < 0.000$) suggesting strong factorability (Hair, Black, Babin, & Anderson, 2010b). Cronbach's alphas (shown in Table 2) were greater than the lower limit of acceptability (> 0.70).

The EFA resulted in eight factors after a total of seventeen items and one construct were removed from the item pool. Sufficient convergent validity was achieved as factor loadings were above the minimum threshold of .40 for a sample size of 350 (Fornell & Larcker, 1981; Hair et al., 2010b). The model did not have strong cross-loadings greater than 0.250 and thus demonstrated sufficient discriminant validity (Fornell & Larcker, 1981). The final variance explained was 75.799%. Factor correlations were all less than 0.70 suggesting adequate initial convergent and discriminant validity and reliability.

[24] In order to achieve model fit, we had to remove flexibility as moving from the measurement model to the structural model introduced particular new relationships that caused flexibility to be overlapped with other variables. Flexibility dropped to two items which is known to cause stability issues. The ideal number of items for a latent factor is four Marsh, H. W., Hau, K.-T., Balla, J. R., & Grayson, D. 1998. Is more ever too much? The number of indicators per factor in confirmatory factor analysis. ***Multivariate Behavioral Research***, 33(2): 181-220..

TABLE 1
EFA Pattern Matrix

Pattern Matrix[a]

	Factor						
	1	2	3	4	5	6	7
de1	.681						
de2	.874						
de3	.455						
cr3						-.729	
cr4						-.783	
cr5						-.546	
cu3				-.439			
cu4				-.788			
cu5				-.781			
dg1			-.765				
dg2			-.765				
dg3			-.803				
dg4			-.794				
dg5			-.713				
at1		.791					
at2		.717					
at3		.847					
at4		.526					
at5		.835					
le2							.499
le3							.604
le4							.610
ft3					-.806		
ft4					-.802		
ft5					-.331		

Extraction Method: Principal Axis Factoring.

Rotation Method: Oblimin with Kaiser Normalization.

a. Rotation converged in 13 iterations.

Confirmatory factor analysis. A confirmatory factor analysis (CFA) was used to assess the statistical fit of the proposed measurement model. The factors demonstrate

convergent validity with diagonal values greater than the correlations (Fornell & Larcker, 1981). We reached a reasonable final fit (χ^2= 526.657, *df*=287, χ^2/df = 1.835, GFI=0.898; CFI= 0.960; RMSEA=0.049; PCLOSE=0.599). Composite reliability was also achieved with CR values above the 0.70 minimum threshold (see Table 3).

TABLE 2
Test for Discriminant Validity

	CR	AVE	MSV	ASV	FT	DG	AT	DE	CU	CR	LE
FT	0.824	0.611	0.554	0.421	0.782						
DG	0.898	0.639	0.379	0.322	0.598	0.799					
AT	0.876	0.592	0.331	0.193	0.417	0.492	0.769				
DE	0.874	0.699	0.549	0.395	0.720	0.515	0.306	0.836			
CU	0.844	0.645	0.513	0.420	0.659	0.616	0.575	0.636	0.803		
CR	0.862	0.677	0.554	0.433	0.744	0.556	0.425	0.741	0.676	0.823	
LE	0.822	0.607	0.551	0.434	0.697	0.615	0.373	0.735	0.716	0.742	0.779

Common method bias. Data collection for both the independent and dependent variables were completed using a single survey instrument. A test for common method bias (CMB) was facilitated to determine bias impacting the measurement model (Podsakoff, MacKenzie, Lee, & Podsakoff, 2003). A common latent factor (CLF) was introduced to the model. A comparison of the standardized regression weights with and without the CLF showed no common method bias. The difference in betas was no greater than 0.20 for any item, which implies that there is a limited threat of CMB (Podsakoff et al., 2003); therefore the CLF was not retained in the model.

Structural model. Our study seeks to understand the mediating mechanisms that influence perception of environment and perceived skills on learning and forward thinking (i.e. how the perception of the hacker environment and their perceived skills) are *mediated* by individual intrinsic characteristics (Baron & Kenny, 1986). Following the

guidance of Baron and Kenny (1986) and Mathieu and Taylor (2006), our model consisted of four independent variables (ambiguity tolerance, domain expertise, and diagramming)[25] and two dependent variables (learning and forward thinking) and one control variable (years of experience). With this model, we achieve the following model fit: χ^2= 472.258, *df*=156, χ^2/df = 3.027, GFI=0.895; CFI= 0.921; RMSEA=0.076 and PCLOSE=0.000. We added two mediating variables (creativity and curiosity) to produce a mediated model. We used bootstrapping to test statistical significance of the indirect effects by setting the sample size to 2000 (with return values) and used bias-corrected confidence intervals of 95%. With this structural model, we achieved the following model fit: χ^2= 532.704, *df*=269, χ^2/df = 1.980, GFI=0.895; CFI= 0.953; RMSEA=0.053 and PCLOSE=0.222. Following guidance from Hu and Bentler (1999), we agreed that these statistics were adequate.

We controlled with years of experience and tested for its effect on the mediator and the dependent variable. The control was found not to drive the current theory but was reported as a potential related variable.

Mediation. Mediation was tested using 2000 bias corrected bootstrapping resamples in AMOS (with 95% bias correct confidence intervals) to discover direct effects without mediation, then direct effects and indirect effects with mediation (Baron & Kenny, 1986).

[25] Our final SEM did not include Cognitive Flexibility due to its low reliability.

FINDINGS

Overall, our mediated model included sixteen hypotheses (see Table 5) of which twelve were supported and four were not. The final model and results are represented in Figure 2 along with the R^2 values of the endogenous variables. The results for all hypotheses tested are presented in Tables 5.[26]

Direct Paths

In the final mediated model, domain expertise has a significant positive effect on learning (β = .150**, p = .003), therefore providing evidence that ***H1a is supported***. Domain expertise also has a significant positive effect on forward thinking (β = .222***, p < .001), providing evidence that ***H1c is supported***. Diagramming has a significant positive effect on learning (β = .098**, p = .021) and forward thinking (β = .110***, p < .001) providing evidence that ***H1b and H1d are supported***.

TABLE 3
Direct Path Regression Results

Hypotheses	Direct Beta	Support?
H1a: DE --> LE	.150**, p = .003	Supported
H1b: DG --> LE	.098**, p = .021	Supported
H1c: DE --> FT	.222***, p < .001	Supported
H1d: DG --> FT	.110***, p < .001	Supported

[26] It is often recommended to use the Sobel test to test whether a mediator carries the influence of an IV to a DV. I decided not to do a Sobel test. According to Preacher & Hayes Preacher, K. J., & Hayes, A. F. 2004. SPSS and SAS procedures for estimating indirect effects in simple mediation models. ***Behavior Research Methods, Instruments, & Computers***, 36(4): 717-731, Preacher, K. J., & Hayes, A. F. 2008. Asymptotic and resampling strategies for assessing and comparing indirect effects in multiple mediator models. ***Behavior Research Methods***, 40(3): 879-891., the Sobel test works well only in large samples. They also suggest that if the user has access to the raw data, bootstrapping offers a much better alternative that imposes no distributional assumptions.

Mediation

We predicted that domain expertise (DE) and diagramming (DG) would increase learning (LE) and forward thinking (FT). We also predicted that both creativity (CR) and Curiosity (CU) would fully positively mediate the effect that ambiguity tolerance (AT) has on the outcome variables (learning and forward thinking) and that both would positively partially mediate the effects of domain expertise and diagramming on the outcome variables. Table 4 shows the results of our mediation analyses.

TABLE 4
Results for Mediated Hypotheses

Hypotheses	Direct Beta w/o Med	Direct Beta w/ Med	Indirect	Mediation
H2a: AT --> CR --> LE	-.048 (.271ns)	-.048 (.274ns)	.041*	Full mediation
H2b: AT --> CR --> FT	.020 (.660ns)	.016 (.726ns)	.044*	Full mediation
H2c: DE --> CR --> LE	.212 (***)	.303 (***)	.037*	Partial mediation
H2d: DE --> CR --> FT	.305 (***)	.403 (***)	.021**	Partial mediation
H2e: DG --> CR --> LE	.140 (***)	.188 (***)	.064as	Partial mediation
H2f: DG --> CR --> FT	.122 (.002**)	.157 (.005**)	.088as	Partial mediation
H3a: AT --> CU --> LE	-.048 (.271ns)	-.087 (.095)	.018*	Full mediation
H3b: AT --> CU --> FT	.020 (.660ns)	.014 (.793ns)	.287ns	No mediation
H3c: DE --> CU --> LE	.212 (***)	.249 (***)	.008**	Partial mediation
H3d: DE --> CU --> FT	.305 (***)	.435 (***)	.231ns	No mediation
H3e: DG --> CU --> LE	.140 (***)	.156 (.008**)	.002**	Partial mediation
H3f: DG --> CU --> FT	.122 (.002**)	.157 (.009**)	.174ns	No mediation
Notes: Standardized regression weights shown; *** p-value < 0.001; ** p-value < 0.01; * p-value < 0.05; ns=not significant				

Findings for the entire study are summarized in Table 5.

TABLE 5
Hypotheses Support

Hypotheses		Support?
H1a	Domain expertise (DE) increases Learning (LE).	**Supported**
H1b	Diagramming (DG) increases Learning (LE).	**Supported**
H1c	Domain expertise increases Forward Thinking (FT).	**Supported**
H1d	Diagramming (DG) increases Forward Thinking (FT).	**Supported**
H2a	Creativity (CR) positively fully mediates the relationship between Ambiguity Tolerance (AT) and Learning (LE).	**Supported**
H2b	Creativity (CR) positively fully mediates the relationship between Ambiguity Tolerance (AT) and Forward Thinking (FT).	**Supported**
H2c	Creativity (CR) positively partially mediates the relationship between Domain Expertise (DE) and Learning (LE).	**Supported**
H2d	Creativity (CR) positively partially mediates the relationship between Domain Expertise (DE) and Forward Thinking (FT).	**Supported**
H2e	Creativity (CR) positively partially mediates the relationship between Diagramming (DG) and Learning (LE).	**Supported**
H2f	Creativity (CR) positively partially mediates the relationship between Diagramming (DG) and Forward Thinking (FT).	**Supported**
H3a	Curiosity (CU) positively fully mediates the relationship between Ambiguity Tolerance (AT) and Learning (LE).	**Not Supported**
H3b	Curiosity (CU) positively fully mediates the relationship between Ambiguity Tolerance (AT) and Forward Thinking (FT).	**Not Supported**
H3c	Curiosity (CU) positively partially mediates the relationship between Domain Expertise (DE) and Learning (LE).	**Supported**
H3d	Curiosity (CU) positively partially mediates the relationship between Domain Expertise (DE) and Forward Thinking (FT).	**Not Supported**
H3e	Curiosity (CU) positively partially mediates the relationship between Diagramming (DG) and Learning (LE).	**Supported**
H3f	Curiosity (CU) positively partially mediates the relationship between Diagramming (DG) and Forward Thinking (FT).	**Not Supported**

DISCUSSION

Our study significantly extends the extant research on how hackers continuously construct advanced knowledge that will support their complex problem solving and transfer of learning and forward thinking. It integrates a more complete array of constructs and their interactions into a research model that accounts for changes in learning and forward thinking within the minds of hackers. Such interactions and the

need for learning and forward thinking have been identified as critical for skilled hacking (Summers et al., 2013). As noted in our literature review, past research has been lacking in focusing on the cognitive constructs presented in this model within the context of hackers. Our study, for the first time, examines these constructs in a more complete mediated model to determine the cognitive skills and traits that either mitigate negative effects or strengthen positive effects. We did not find any literature that has attempted to explore such interactions in the context of how hackers learn and perform anticipatory thinking which is incredibly important in today's organizations.

We found that in the direct paths model, domain expertise positively effects learning ($\beta = .150^{**}$, $p = .003$) and forward thinking ($\beta = .222^{***}$, $p < .001$) which was consistent with past research (Benner, 1982; Campbell et al., 1992; Dreyfus et al., 1987a). Also, as we expected, diagramming did have a significant positive effect on both learning ($\beta = .098^{**}$, $p = .021$) and forward thinking ($\beta = .110^{***}$, $p < .001$), consistent with the extant literature on the topic (Davies, 2011; Novak & Cañas, 2006a). We utilized past research to develop our mediated hypotheses where each the perception of environment of hackers was associated through two mediators (creativity and curiosity) to learning and forward thinking. Next, we will discuss the impact that our mediators had on the model.

Creativity

The effects of creativity have been examined in many ways in past research. We posited that creativity would be a substantial facilitating construct of the perception of environment (ambiguity tolerance) and perceived skills (domain expertise and diagramming) of skilled hackers on learning and forward thinking.

Mediated effect of creativity on the relationships between independent variables and outcome variables. When creativity was added to the relationship of the perception of environment (ambiguity tolerance) and the dependent variables (learning and forward thinking), it positively fully mediated the relationships. For example, the direct beta between ambiguity tolerance and learning was negative and not significant (β = -.048, p = .271ns). When we added creativity as a mediator to the relationship, we saw the direct beta effect of ambiguity tolerance on learning remained negative and decreased slightly in significance (β = -.048, p = .274ns). However, the indirect effect of this relationship was significant (p = .041*). The direct beta between ambiguity tolerance and forward thinking was positive and not significant (β = .020, p = .660ns) and when creativity is added to mediate the relationship we observed the direct beta decrease (β = .016, p = .726ns). The indirect effect of this relationship was significant (p = .044*). This provided evidence that creativity positively, fully mediates the relationship of ambiguity tolerance on forward thinking.

The direct beta between domain expertise and learning had a significant positive effect (β = .212***, p < .001) but when we added creativity, we observed a substantial increase in the strength of the relationship (β = .303***, p < .001). The indirect effect of this path was also significant (p = .037*), providing evidence that there was positive partial mediation. The direct beta between domain expertise and forward thinking also had a significant positive effect (β = .305***, p < .001). We observed that when creativity was included as a mediator, the strength of the relationship increased and remained significant (β = .403***, p < .001). The indirect effect of this path was also significant (p = .021**). This provided evidence that there was partial positive mediation.

The direct beta between diagramming and learning had a significant positive effect (β = .140***, p < .001) and when creativity was added, we observed an increase in the strength and continued significance of the effect (β = .188***, p < .001). The indirect effect of this path was approaching significance (p = .064), providing evidence that there was positive partial mediation. The direct beta between diagramming and forward thinking also had a significant positive effect (β = .122**, p = .002). We observed that when creativity was added there was an increase in strength but a slight decrease in significance (β = .157**, p = .005). The indirect effect was approaching significance (p = .088). This provided evidence that there was positive partial mediation.

Curiosity

We posited that curiosity would be a substantial facilitating construct of the perception of environment (ambiguity tolerance) and perceived skills (domain expertise and diagramming) of skilled hackers on learning and forward thinking.

Mediated effect of curiosity on the relationships between independent variables and outcome variables. When curiosity was added to the relationship of the perception of environment (ambiguity tolerance) and the dependent variables (learning and forward thinking), it positively fully mediated the relationship one relationship but not the other. For example, the direct beta between ambiguity tolerance and learning was negative and not significant (β = -.048, p = .271ns). When we added curiosity as a mediator to the relationship, we saw the strength of the effect decrease but the significance increased (β = -.087, p = .095). However, the indirect effect of this relationship was significant (p = .018*), providing evidence that there was positive full mediation. The direct beta between ambiguity tolerance and forward thinking was positive and not significant (β = .020, p =

.660ns). When curiosity was added to mediate the relationship, we observed the direct beta decrease in strength and significance (β = .014, p = .793ns). The indirect effect of this relationship was not significant (p = .287ns). This provided evidence that curiosity provided no mediation for the relationship between ambiguity tolerance and forward thinking.

The direct beta between domain expertise and learning had a significant positive effect (β = .212***, p < .001) but when we added curiosity, we observed a slight increase in strength of the relationship (β = .249***, p < .001). The indirect effect of this path was also significant (p = .008**), providing evidence that there was positive partial mediation. The direct beta between domain expertise and forward thinking also had a significant positive effect (β = .305***, p < .001). We observed that when curiosity was included as a mediator, the strength of the relationship substantially increased and remained significant (β = .435***, p < .001). The indirect effect of this path was not significant (p = .231ns). This provided evidence that there was no mediation.

The direct beta between diagramming and learning had a significant positive effect (β = .140***, p < .001) and when curiosity was added, we observed an increase in strength and a slight decrease in significance (β = .156**, p = .008). The indirect effect of this path was significant (p = .002**). This provided evidence that there was positive partial mediation. The direct beta between diagramming and forward thinking also had a significant positive effect (β = .122**, p = .002). We observed that when curiosity was added there was an increase in strength but a decrease in significance (β = .157**, p = .009). The indirect effect was not significant (p = .174ns). This provided evidence that there was no mediation.

LIMITATIONS

Our results may assist in better understanding the hacker population; however, we recognize that they cannot explain all hacker cognition. While our sample size was adequate with more than 350 surveys completed, there are limits to the generalizability of the findings. We did not test for all factors that may contribute to how a person hacks. Similarly, to the best of our knowledge, the scales used in the study have never been used in combination, in our context, and there are no acceptable tests for scale validity. Some caution should be acknowledged with regard to some of our measures. Specifically, we had low levels of reliability for *flexibility*, which calls for future instrumentation and measurement development. We recognize that as a mediator and given its low reliability this could increase type I and type II errors. It is our belief that the reason for this low reliability is that due to the nature of the construct itself. *Flexibility* can be seen from multiple viewpoints and refers to the individual's ability to shift focus from one concept to another which can be misinterpreted and complex to discern from other constructs used in this study. Finally, we could not assess response biases because we utilized third party collection.

IMPLICATIONS FOR PRACTICE AND FUTURE RESEARCH

Our research provided many insights about the building and maintenance of mental models for hackers, as well as the predictive nature of those mental models. More specifically, these findings help us understand how hackers use their playful cleverness, intellectual stimulation, problem solving, self- and socially-directed learning, and astute anticipatory thinking to make decisions and create solutions. This research may help managers of organizations by giving them additional indicators to explore when

interested in identifying the best innovative thinkers. Our study showed that perception of environment, perceived skills, and intrinsic individual characteristics are instrumental to the dynamism of mental models. One critical lesson for managers is that the cognitive skills and traits identified in this study provide the foundation for a hacker's ability to construct effective mental models.

Although there are tremendous individual differences among hackers and their abilities, this body of work provides us with an improved understanding of the dynamism of mental models necessary for skilled hacking and their predictive power which could have substantial implications on the way that hackers are trained. This research could provide organizations with insights into using cognitive training to improve the way that hackers assimilate, organize, and process information. This research could also be used to assist with classroom learning and employee assessments.

APPENDIX

Respondent Demographics and Comparisons with Previous Studies on Hackers

Since the literature is lacking in studies on the hacking community, we thought it advantageous to compare our respondent demographics to those of previous research. Schell and Melnychuk (2010a) conducted a study of hacker conference attendees. Based on the researcher's experiences, hacking conferences reasonably represent the demographics of the overall hacker community.

Male vs. Female. In the Schell and Melnychuk (2010a) study, the researchers had a small sample (n = 136) with a demographic breakdown of 49.5% males (n = 66) and 51.5% females (n = 70). When compared to the overall sample demographics of Schell and Melnychuk (2010a), the sample for this study is not consistent. This study had a higher sample (n = 350) with a demographic breakdown of 76.0% males (n = 266) and 24.0% females (n = 84). This inconsistency probably has much to do with the Schell et al. study being utilized exclusively at conferences. The researchers in the Schell et al. (2011) study admittedly made an extra effort to acquire female respondents due to the low numbers of female participants in the hacker community. An interview-driven study conducted by Summers et al. (2013) made a similar effort but this study did not.

TABLE A1
Sample Gender Demographics

Study	Schell et al. (2011)	Summers (2013)	Summers (2014)
Sample (Gender)	n = 136	n = 18	n = 350
Males	66 male (48.5%)	17 male (94.4%)	266 male (76.0%)
Females	70 female (51.5%)	1 female (5.6%)	84 female (24.0%)

Age. The age range for our study respondent sample was broad. The youngest male respondents were in the 20 or younger group (n = 5) and the oldest being in the 61 or older group (n = 18). The median male respondents were in the 31–40 group (n = 101). For females, the youngest respondents were in the 20 or younger group (n = 2) and the oldest were in the 61 or older group (n = 5). Similar to the male sample, the female median respondents were in the 31–40 age group (n = 29).

Schell and Melnychuk (2010a) reported a broad respondent age range with the youngest male being 18 years of age and the oldest being 56. The youngest female was 19 years of age and the eldest was 54. The respondents for this study was consistent with those of Schell et al. 2011; however, this study had respondents reporting to be within the 61 or older age group (n = 23; 6.6%). This appears to be reasonable because out of the respondents within the 61 or older age group, only 2.4% (n = 4) reported that they attend conferences. Of this same age group, 10.4% (n = 19) reported that they do not attend conferences. This could explain why the Schell and Melnychuk (2010a) study did not report anyone older than 56 years of age. This also indicates that this study had a more mature set of respondents than that obtained in Schell and Melnychuk (2010a).

Employment. In the Schell and Melnychuk (2010a) study, the researchers noted that the hacker conference attendees were usually gainfully employed. The results of this

study are consistent with those previous findings. All of the respondents in this study (n = 350) were gainfully employed within various sectors of industry. Most of the respondents reported to be within the For-Profit/Private sector (n = 258). The next most reported sector was Government/Quasi-Governmental Entities (n = 35). Followed by Higher Education (n = 34) and the Non-Profit sector (n = 23). Due to a negative perception held by the media and general public, it was historically believed that hackers tend not to be gainfully employed. These results show another picture.

Education. Gainful employment reflects reasonable economic and education status. This study had a large percentage of respondents who graduated from university programs. For example, 82.9% of the respondents reported having a college/university or post-graduate degree. The breakdown is as follows: 10.3% had a 2-year college degree (i.e. Associates degree), 40.6% had a 4-year college degree (i.e. Bachelor's degree), 28.3% had a Master's degree, 9% had a Doctoral degree, and 1.1% had a Professional degree (i.e. Medical Doctorate or Juris Doctorate). Of those that did not have a college or university associated degree, 11.7% of the respondents had completed some college, 4.6% had completed High School and .9% had less than High School.

The education breakdown for Schell et al. 2011 was as follows: 82% of respondents had a university or post-graduate degree, 57% had an undergraduate degree, 18% had a Master's degree, and 7% had a PhD. Previous research, like Schell and Melnychuk (2010a), had an overall consistent education breakdown; however, there were more university and post-graduate respondents in our study.

Initial Construct with Items

TABLE A2
Initial Constructs with Cronbach's Alphas

Measure	Items	Reliability (Cronbach's alphas)
Independent Variables		
Ambiguity Tolerance	AT1. I like problems that seem ambiguous. AT2. IT security problems always have ambiguous solutions. AT3. I like ambiguous security problems. AT4. I am willing to tolerate uncertain IT security problems. AT5. Ambiguous problems are appealing.	.867
Flexibility	FL1. I am able to communicate ideas in many different ways. FL2. I am willing to consider alternative solutions to problems. FL3. I am willing to consider solutions offered by others. FL4. I am willing to try different ways of solving problems. FL5. I am willing to be flexible in any given situation.	.871
Domain Expertise	DE1. I am good at solving technical problems. DE2. I am experienced at technical troubleshooting. DE3. My coworkers consider me to be an expert in technical issues. DE4. I am an expert at understanding technical issues. DE5. My technical skill has been acquired through experience.	.883
Diagramming	DG1. I create diagrams that map concepts, facts, and relationships between components. DG2. I arrange information into charts and tables. DG3. I draw diagrams that show relationships between concepts. DG4. I map out components and their attributes. DG5. I create diagrams to understand complexity.	.897
Mediating Constructs		
Creativity	CR1. I am a good source of creative ideas.	.888

	CR2. I suggest innovative ways of solving problems. CR3. I come up with creative solutions to problems. CR4. I suggest creative ideas that improve the outcome of work activities. CR5. I use my creativity to solve problems.	
Curiosity	CU1. I feel that IT security problems arouse my interest. CU2. I am always interested in solving IT security problems. CU3. IT security problems stimulate my curiosity. CU4. IT security problems are fun and interesting. CU5. IT security problems are interesting to me.	.887
Dependent Variables		
Learning	LE1. I learn by examining my perspective. LE2. I learn new skills when solving IT security problems. LE3. I learn by solving IT security problems. LE4. I acquire knowledge through solving IT security problems.	.842
Forward Thinking	FT1. I plan for future threats. FT2. I think that planning for future threats is important. FT3. I prepare for unfavorable events. FT4. I prepare for disastrous consequences. FT5. I plan my strategies before I act.	.871

Final Construct with Items

TABLE A3
Final Constructs with Cronbach's Alphas

Measure	Items	Reliability (Cronbach's alphas)
Independent Variables		
Ambiguity Tolerance	AT1. I like problems that seem ambiguous. AT2. IT security problems always have ambiguous solutions. AT3. I like ambiguous security problems. AT4. I am willing to tolerate uncertain IT security problems. AT5. Ambiguous problems are appealing.	.867
Flexibility	FL4. I am willing to try different ways of solving problems. FL5. I am willing to be flexible in any given situation.	.693
Domain Expertise	DE1. I am good at solving technical problems. DE2. I am experienced at technical troubleshooting. DE3. My coworkers consider me to be an expert in technical issues.	.864
Diagramming	DG1. I create diagrams that map concepts, facts, and relationships between components. DG2. I arrange information into charts and tables. DG3. I draw diagrams that show relationships between concepts. DG4. I map out components and their attributes. DG5. I create diagrams to understand complexity.	.897
Mediating Constructs		
Creativity	CR3. I come up with creative solutions to problems. CR4. I suggest creative ideas that improve the outcome of work activities. CR5. I use my creativity to solve problems.	.860
Curiosity	CU3. IT security problems stimulate my curiosity. CU4. IT security problems are fun and interesting.	.839

	CU5. IT security problems are interesting to me.	
Dependent Variables		
Learning	LE2. I learn new skills when solving IT security problems. LE3. I learn by solving IT security problems. LE4. I acquire knowledge through solving IT security problems.	.819
Forward Thinking	FT3. I prepare for unfavorable events. FT4. I prepare for disastrous consequences. FT5. I plan my strategies before I act.	.817

Detailed Q-Sort Process

The Q-sort is an iterative process where the degree of agreement between judges provides the foundation for assessing construct validity and improving the reliability of the constructs (Nahm et al., 2002). The Q-sort was conducted in two stages. First, our judges were asked to sort the survey items according to different constructs using an electronic instrument created within the Qualtrics online survey software platform. This allowed us to measure the amount of inter-judge agreement (Nahm et al., 2002; Van Exel & de Graaf, 2005). Although some argue that the Q-sorting procedure must be conducted in a face-to-face interview setting, due to our population's preference of communicating via computer and geographical distribution, an Internet-based Q-sort was appropriate (Van Exel & de Graaf, 2005). Research has shown that there are no differences in reliability or validity of administering the Q methodology via computer or in a face-to-face interview setting (Reber, Kaufman, & Cropp, 2000; Van Exel & de Graaf, 2005). Second, as a result of the first stage, we were able to recognize survey items that were identified as being too ambiguous. Those items were reworded or deleted. This process was carried out repeatedly until we reached a satisfactory level of agreement.

A personalized email with a link to the Q-sort was sent to a variety of cyber security experts and others from different industries. Each of these experts was selected based on their areas of expertise and experience in industry. The Q-sort contained 44 survey items for our 9 constructs[27], along with a definition for each. The 9 constructs were used to represent *categories* and the respondents were asked to place each item into the category they felt best represented the item (Gligor, Holcomb, & Stank, 2013). Additionally, the experts were asked to evaluate the items for face validity and provide qualitative feedback on the categories and items. Eighty percent of the experts responded. Based on the item placements and qualitative feedback received from the experts, some of the survey items were revised while others were selected for elimination. The purpose of this pretesting was to identity items that would perform poorly in the EFA and CFA. We conducted several rounds of Q-sorting.

For each round of the Q-sort, we utilized a systematic, technical procedure to analyze the results (Brown, 1980, 1986). First, we constructed a correlation matrix representing the level of agreement and disagreement between the ways that the respondents sorted each item (Van Exel & de Graaf, 2005). The correlation matrix enabled us to analyze the number of items placed by the judges within the target construct for each round. Our goal was to reach an 80% inter-judge agreement for each item and target construct. In our correlation matrix, we calculated the percentage of consensus relative to the number of responses received to provide insight on the degrees of similarities in viewpoints between each individual respondent (Van Exel & de Graaf,

[27] In our initial model, we had domain expertise, creativity, curiosity, diagramming, and flexibility as independent variables, ambiguity tolerance and reflection as mediators, and learning and forward thinking as dependent variables; however, we removed the reflection and flexibility constructs.

2005). Each item was included in a pool to measure the overall frequency with which the judges placed the items into the intended theoretical construct. The higher the percentage of items placed in the target construct, the higher the degree of inter-judge agreement (Nahm et al., 2002). Items placed in the pool were subjected to multiple rounds of sorting by independent judges. The judges sorted the items based on similarities and differences among items. The correlation matrix was used to produce a cluster analysis which enabled us to identity the natural groupings of Q-sort results to examine how respondents actually sorted the items compared to how we expected them to be sorted (Brown, 1980, 1986). The cluster analysis enabled us to see which items were problem areas and had unacceptable overlap and provided evidence necessary to see which items could be eliminated[28] or rewording.

In the first round, the inter-judge raw agreement scores averaged 54%. Feedback from the judges indicated that the items were ambiguous and seemed to overlap. The cluster analysis of the judge rating confirmed the overlap across items and the target constructs. Items that were considered ambiguous (fitting into more than one construct) were either reworded or deleted. Overall, we revised 36 items to pursue higher inter-judge agreement for the next round. In the second round, the inter-judge raw agreement scores averaged 67%. Seven out of nine of our constructs ("domain expertise", "cognitive flexibility", "creativity", "curiosity", "ambiguity tolerance", "reflection", and "learning") experienced an inter-judge agreement measure below 70%. On the other hand, the highest inter-judge agreement measures were 76% for "Diagramming" and 85% for "Forward Thinking" indicating a high degree of construct validity. Feedback from the

[28] We considered item elimination to be an absolute last resort and made every attempt to revise items.

judge indicated that the items across the problem constructs were better than in the first round; however, there still seemed to be overlap. The cluster analysis further confirmed the existing overlap and provided the insights necessary to distinguish items. For example, by using the cluster analysis, we were able to identify specific elements of the items that seemed to make them similar to items not within their target construct. Using this information, we were able to take a precision-based approach to revising the items. In the third round, the inter-judge agreement scores averaged 98%. For instance, the lowest inter-judge agreement was 92% for the "Learning" construct; however, this still met our threshold minimum of 80% consensus. On the other hand, six constructs obtained a 100% inter-judge agreement measure, indicating a high degree of construct validity.

Appendix C: How Hackers Think:
Sociocultural Facets and Understanding Their Impact on the Hacker Mind

By

Timothy C. Summers

Submitted in Partial Fulfillment of the Requirements of the Quantitative Research Report
in the Doctor of Management Program
at the Weatherhead School of Management
Doctor of Management Design Fellow

Advisors:
Kalle Lyytinen, Ph.D., Case Western Reserve University
Mark Turner, Ph.D., Case Western Reserve University
Mikko Siponen, Ph.D., University of Jyväskylä
James Gaskin, Ph.D., Brigham Young University

CASE WESTERN RESERVE UNIVERSITY

November 2014

HOW HACKERS THINK: SOCIOCULTURAL FACETS AND UNDERSTANDING THEIR IMPACT ON THE HACKER MIND

Abstract

Society's dependence on computer technology and the Internet has substantially increased the risks from computer hackers (Bachmann, 2010; Holt & Schell, 2010; Holt, Strumsky, Smirnova, & Kilger, 2012; Schell & Dodge, 2002; Summers et al., 2013; Wall, 2007). In general, a hacker is a technologist with a proclivity for computing and a hack is a clever solution accomplished through non-obvious means (Levy, 1984; Turkle, 1984). However, many hackers use their knowledge to craft hacks that provide unauthorized access to computer systems (Bowles, 2012; Holt & Schell, 2010; Peretti, 2008; Summers et al., 2013). A small body of research has explored the subculture and norms of hackers and malware writers which found that hackers value autodidacticism and sharing their knowledge with other hackers through online and offline social interactions (Gordon & Ma, 2003; Holt, Soles, & Leslie, 2008; Holt et al., 2012; Jordan & Taylor, 2004; Schell & Dodge, 2002; Summers et al., 2013; Thomas, 2002). In this research, we explore: how and to what extent sociocultural facets (i.e. gender, participation in intellectual capital sharing environments, and possession of professional credentials) of the hacker subculture improve their learning and forward thinking by effectively engaging intrinsic individual characteristics (i.e. creativity, curiosity) given their level of perceived skills (i.e. domain expertise, diagramming) and the level of their ability to understand the requirements of their work environment (i.e. ambiguity tolerance).

Key words: hackers; cognition; mental models; learning; forward thinking; gender; education; conventions.

INTRODUCTION

Society's dependence on computer technology and the Internet has substantially increased the risks from computer hackers (Bachmann, 2010; Holt & Schell, 2010; Holt et al., 2012; Schell & Dodge, 2002; Summers et al., 2013; Wall, 2007). In general, a hacker is a technologist with a proclivity for computing and a hack is a clever solution accomplished through non-obvious means (Levy, 1984; Turkle, 1984). However, many hackers use their knowledge to craft hacks that provide unauthorized access to computer systems (Bowles, 2012; Holt & Schell, 2010; Peretti, 2008; Summers et al., 2013). Recently, we have seen many high profile data breaches committed by hackers, individually and in groups. Researchers suggest that by studying hackers, we will have a better chance at protecting ourselves and the systems, which we have become so reliant (Chiesa et al., 2008; Clarke & Knake, 2011; Summers et al., 2013; Taylor, 1999; Thomas, 2002; Xu et al., 2013). We believe that by gaining a deeper understanding of how certain sociocultural facets of the hacker community influence the cognitive processes of process of hackers, we can development a richer understanding of learning and forward thinking within the hacker community.

A small body of research has explored the subculture and norms of hackers and malware writers which found that hackers value autodidacticism and sharing their knowledge with other hackers through online and offline social interactions (Gordon & Ma, 2003; Holt et al., 2008; Holt et al., 2012; Jordan & Taylor, 2004; Schell & Dodge, 2002; Summers et al., 2013; Thomas, 2002). The hacker community is a meritocracy that assesses individuals based on their skills and ability (Holt et al., 2012; Jordan & Taylor, 2004; Summers et al., 2013) and prides itself on being impartial when it comes to race,

gender, and other sociocultural characteristics (Wark, 2006). However, research indicates that there are substantial sociocultural gaps within the community that could potentially impact how hackers see themselves and engage with others, such as gender (Gressard & Loyd, 1987; Lockheed, 1985; Loyd & Gressard, 1984; Schell & Dodge, 2002; Schell & Melnychuk, 2010b; Schubert, Brown, Gysler, & Brachinger, 2000; Wilder, Mackie, & Cooper, 1985), participating in information sharing environments (like hacker conventions) (Levy, 1984; Poeter, 2012; Summers et al., 2013; Taylor, 1999; Thomas, 2002), and engaging in professional education (Bowles, 2012; Gabelhouse, 2002; Levy, 1984; Taylor, 1999; Thomas, 2002; Tittel, 2000). Summers et al. (2013) investigated how skilled hackers use mental models to organize and interpret environmental information as to aid in pattern matching, solving problems, and decision making associated with hacking. The research found that the hacker's ability to continuously construct advanced knowledge that support complex problem solving and learning transfer, rests on cognitive skills and traits such as domain expertise, creativity, curiosity, diagramming, ambiguity tolerance, learning and forward thinking. It also indicated that these cognitive skills and traits are major contributing factors to their mental models and enables them to learn their environment and emerging patterns. In another recent study, Summers et al. (2014) investigated how hackers can improve their learning and forward thinking outcomes by effectively engaging their intrinsic individual characteristics (such as creativity and curiosity) given their level of perceived skills (such as domain expertise and diagramming) and the level of their ability to understand the requirements of their work environment (such as ambiguity tolerance). The research found the intrinsic individual characteristics, perception of environment, and perceived skills are indeed instrumental to

the cognition of hackers; specifically calling attention to the roles of curiosity and creativity as facilitators for the innovative thinking commonly attributed to them.

Our research question is: How and to what extent do the sociocultural facets (such as gender) of the hacker subculture improve their learning and forward thinking by effectively engaging intrinsic individual characteristics (such as creativity) given their level of perceived skills (such as domain expertise) and the level of their ability to understand the requirements of their work environment (such as ambiguity tolerance)? To investigate this question, we conducted a survey among hackers and other security professions in various industries to detect the moderating effects of sociocultural facets (such as gender) on the varying effects of intrinsic individual characteristics, perceived skills, and perception of environment in hindering or strengthening a hacker's learning and forward thinking. Understanding how sociocultural facets, like gender, participation in hacker conventions, and possession of professional credentials changes how hackers utilize their cognitive skills and traits to make meaning of their environment and complexity can provide deeper insights in information processing, knowledge, production, decision making, organizational design, learning, and opportunity recognition in complex technical tasks and environments. The primary contribution of this research is to provide a richer, deeper understanding of individual cognition and innovative thinking employed by hackers and understanding how they can be impacted by naturally occurring sociocultural factors.

The remainder of the article is as follows. In the next section, we review the importance and occurrence of learning and forward thinking. Then we formulate a theoretical framework that articulates the sociocultural facets of the hacker community

and the implications of those facets on learning and forward thinking outcomes necessary for skilled hacking. More specifically, we discuss how gender differences, participation in hacker conventions, and the possession of professional credentials can have strengthening or hindering effects on hacking outcomes. We then articulate a research model and formulate a set of hypotheses between the intrinsic individual characteristics, perceived skills, perception of environment, and learning and forward thinking outcomes. In the next section, we discuss the research design and method followed by a review of the major findings. We conclude with a review of practical and theoretical implications and explore avenues for future research.

THEORETICAL FOUNDATION

In general, there is an abundance of literature on hackers as a social phenomenon (Chiesa et al., 2008; Clarke & Knake, 2011; Clough & Mungo, 1992; Coleman, 2013; Hafner & Markoff, 1995; Hannemyr, 1997b; Levy, 1984; Murray, 1997; Sterling, 1992; Taylor, 1999; Thomas, 2002; Turkle, 1984; Wark, 2006; Weizenbaum, 1976). Additionally, there has been research conducted on the sociology of hackers (Jordan & Taylor, 1998), their social networks (Holt & Schell, 2010; Holt et al., 2012), and potential psychological conditions (Schell & Dodge, 2002; Schell & Melnychuk, 2010b); however, there is a dearth of research that considers how some of those sociocultural dynamics impact their effectiveness. In this study, we address this void. We recognize that the information systems and security research body can benefit from a deeper understanding of sociocultural understanding of the hacker subculture and its participants (Holt et al., 2008; Holt & Schell, 2010; Holt et al., 2012). Although there are many sociocultural facets of the hacker subculture, we felt it prudent to explore three of the most commonly

mentioned: gender, professional education, and hacker conventions (Butler, 2000; Chiesa et al., 2008; Coleman, 2013; Poeter, 2012; Summers et al., 2013; Taylor, 1999; Thomas, 2002; Wilder et al., 1985).

Hacking Culture and Gender

For as long as most hackers can remember, there has always been an accepted but not well understood male dominance in the hacker subculture (Chiesa et al., 2008; Summers et al., 2013). This is surprising considering the valuable contributions made by women in the world of computing.[29] There has been much debate over reasons why computing and as a result, the hacking community, are largely male-dominated. A number of researchers propose that males inherently have more positive attitudes toward computers than females (Collis, 1985; Dambrot, Watkins-Malek, Silling, Marshall, & Garver, 1985; Nickell & Pinto, 1986; Wilder et al., 1985; as cited by Temple & Lips, 1989). In contrast, other researchers have reported no such findings regarding differences in computer attitudes (Gressard & Loyd, 1987; Loyd & Gressard, 1984; as cited by Temple & Lips, 1989). Some researchers attribute the male-dominance to three main factors: 1) societal factors, such as "the sexual stereotyping of young children, where boys are given technical playthings whilst girls are given cuddly toys and plastic tea-sets"; 2) the masculine computer science environment where the male dominance "creates a general 'locker room' climate in which women feel threatened or

[29] In fact, the world's first programmer, a woman named August Ada Lovelace, wrote code for Babbage's computing machine in the 1800s. In the 1940s, Adele Goldstein wrote some of the first programs for the Electronic Numerical Integrator and Computer (ENIAC). There was also Grace Hopper, one of the key figures in the development of the COBOL programming language and the first person to use the term *bug* to refer to a code malfunction Lockheed, M. E. 1985. Women, girls, and computers: A first look at the evidence. ***Sex Roles***, 13(3-4): 115-122.

uncomfortable"; and 3) gender in language evidenced by the "male gender bias in the language used in computer science" (Spertus, 1991; as cited in Taylor, 1999).

Researchers define key themes of hacking as relating to "exploration, obsession, and ingenuity/creativity" (Summers et al., 2013; Taylor, 1999; Thomas, 2002; Turkle, 1984). The literature suggests that perception of one's skills, such as technical competence and confidence, play an important part in the degree of technical learning and knowledge transferability (Lim & Johnson, 2002; Summers et al., 2013). Although, there is no research that reports a lack of computing competency among females, there is a stream of research that reports overall attitudinal differences between genders. In fact, some researchers have reported that women view themselves as being less comfortable, confident and competent with computing technology than men (Collis, 1985; Wilder et al., 1985). Temple and Lips (1989: 223) state that "these young women, while ideologically supporting beliefs that women are as capable as men, may be personally vulnerable to threats to their self-confidence that stem from a variety of sources." Some researchers suggest that these sources could be due to the their male counterparts having the stereotypical attitude that computers and sciences are male domains and/or due to a female lack of confidence in mathematics since many aspects of computing, such as programming, are associated with mathematics (Linn, 1985; as cited by Temple & Lips, 1989). A study conducted by Temple and Lips (1989) found that "women are just as interested in computers as men"; however, "they are scared off by uncertainty about their own abilities—an uncertainty that is apparently reinforced by, among other things, the attitudes of their male peers." More specifically, the researchers (Temple & Lips, 1989) state that "where they [females] lag behind males is in confidence."

Disregard of Professional and Academic Education

Levy (1984: 43) states that "part of the hacker ethic is the assertion that 'Hackers' should be judged by their hacking, not by bogus criteria such as degrees, age, race, or position" (Taylor, 1999). Hackers have a proclivity for exploration and curiosity and therefore have a low tolerance for boredom (Summers et al., 2013; Taylor, 1999; Thomas, 2002). A common complaint amongst hackers, when discussing traditional education, is how boring and unengaging courses are in formal professional and academic settings (Taylor, 1999; Wark, 2006). Some researchers suggest that these feelings of educational confinement result from a lack of cognitive stimulation in professional and academic computing courses and insufficient access to desirable computing facilities (Taylor, 1999; Thomas, 2002). Many hackers describe the professional and academic environment as not being challenging enough, boring, and discouraging (Taylor, 1999). In fact, many hackers usually describe their knowledge of computing technology and security as being self-taught or peer group-derived. As evidenced in an interview with Schifreen (Taylor, 1999):

> "I didn't go to university, I did computing at school until o-level and that was basically the only computing education I got, the rest of it was self-taught for enthusiasm … the knowledge you need for a computing job doesn't correspond to the course work you've done at University or College. They're not teaching the things that are right for jobs" (p. 76).

There is a standing contention within the information security community over professional credentials. Companies and governments value highly coveted certifications; however, the hacking community does not put weight into such social measures of knowledge. Typically, hackers find more significance in hand-on experience and exhibited technical skills. Most hackers would probably agree that the IT and security

industries have become obsessed with credentials and certifications. According to some researchers (Bartlett, 2002; Gabelhouse, 2002; Tittel, 2000), IT credentialing and certification, which includes IT training companies, publishing companies, testing vendors, certification governing authorities, online mentoring, and other resource providers, make up a multibillion dollar per year industry. As Bartlett (2002) describes, "the expanding variety and complexity of computer software, hardware products, and their related applications have created and will continue to create a specific demand for employees with unique combinations of IT skills, experience and industry knowledge" (p. 17). Many organizations rely on certifications to help them identify exceptional candidates with the requisite skills in hiring situations. Therefore, hackers that desire employment, which is usually quite lucrative, they must give in to the organizational demand of professional credentials. The general sentiment among hackers is that anyone can study for and take a test; however, real knowledge is gained through hands-on-keyboard experience. It is this deep passion for hacking that gives hackers the advantage over professional computer security consultants. As stated by Kevin Mitnick in Taylor (1999):

> "They've got the motivation and don't forget, computer security people go to their job from nine to five, for hackers it's a hobby. You dedicate more time to that hobby than you would a job, when you're done with your job, you want to get out of there, go home to your wife, play golf, go work out at the gym. You don't want to sit there and deal with it, usually. But hackers, on the other hand, devote hours and hours to learning, so a lot of them are more talented in maybe that narrow area of computers" (p. 79).

Sharing Environments and Collaborations

From the beginning, *sharing information with others* has been a core tenet of the hacker ethos (Coleman, 2013; Raymond, 1999; Rosenzweig, 1998; Sterling, 1992;

Summers et al., 2013; Taylor, 1999; Thomas, 2002; Turkle, 1984). For hackers, sharing one's *hack* builds credibility and prestige within social circles. As described by Thomas (2002):

> "In the 1980s and early 1990s there were several tried and true methods for a hacker to make his or her name. First, hackers gained a certain prominence by virtue of their affiliations. To be a member of an elite circle of hackers…ensured a certain credibility in hacking circles. It also provided hackers with access to resources and information that were not generally available. Within those small circles, hackers would learn from each other and generally develop their skills. Those circles also provided a network of information whereby hackers would learn the latest hacks or exploits" (p. 90).

Hacking groups, like those of the 1980s and 1990s, still exist[30]; however, they are more exposed. Whereas hacker groups of earlier years operated under anonymity and stealth, modern day groups publicize their attacks and conquests.

The favorite and most effective way to build prestige within the hacker community is through sharing information in public forums. Prior to the 1980s, when hackers wanted to share information in the public forum, they would either disseminate text files throughout the underground or publish in underground journals like *2600* or *Phrack* (Taylor, 1999; Thomas, 2002; Tronco, 2010). As Thomas (2002) describes:

> "Starting in the late 1980s, hackers began to gather informally in an effort to meet one another face-to-face and share information. They would smoke, drink, and hack into the wee hours of the morning in the rooms of some unsuspecting hotel. The gatherings, initially, would be small, a couple dozen hackers at most gatherings named SummerCon, PumpCon, HoHoCon (held over Christmas), and, perhaps most famously DefCon and HOPE (Hackers on Planet Earth)" (p. 92).

[30] Some of the most well-known hacker groups from the 1980s and 1990s include but are not limited to, the Chao Computer Club, Cult of the Dead Cow (cDc), L0pht, Masters of Deception (MOD), and Legion of Doom (LOD). Newer examples include groups such as Anonymous, LulzSec, the Syrian Electronic Army, and the Unknowns.

Conventions, or cons, provide hackers with an organized means to meet face-to-face in large numbers (Coleman, 2013; Coleman & Golub, 2008; Levy, 1984; Summers et al., 2013; Taylor, 1999; Thomas, 2002). Although the conventions of the 1980s only brought in a few dozen hackers, the conventions of the 1990s were large organized events. They have managed to get even larger, with over 10,000 people having converged in Las Vegas, for DefCon in 2010.

To date, DefCon is considered to be the most widely recognized hacker convention. DefCon, organized by Jeff Moss (also known as Dark Tangent), is a three-day event consisting of lectures, discussions and presentations among hackers, security experts, law enforcement, and industry specialists (Schell & Dodge, 2002; Taylor, 1999; Thomas, 2002). The attendees are typically male, in their early twenties, and referred to by their handles instead of their real names (Schell & Dodge, 2002; Taylor, 1999; Thomas, 2002). Also, the registration fee for the convention must be paid in cash. To outsiders, hacker cons seem incredibly novel and something representative of another world. As Thomas (2002) states:

> "Part of what makes DefCon unique is that it openly invites industry and law enforcement to the gathering. There are even good-natured games, such as "Spot the Fed", where conference goers are invited to identify someone they think is a federal agent or law enforcement personnel and bring them up to the stage. The hacker states his reasons for thinking the person is "the fed", and the audience votes. If a general consensus is reached (or the suspected individual "confesses"), the hacker receives an "I spotted the Fed" T-shirt, and the fed receives an "I am the Fed" T-shirt. The contest is held between each speaker, and there is generally no shortage of willing participants on either side. …While speakers talk on issues ranging from how to hack the Las Vegas gaming industry to how to con your way into first-class travel, there are a range of "games", including a hacker scavenger hunt, electronic "capture the flag", where hackers take over one another's systems, and Hacker Jeopardy" (p. 93).

In terms of sharing knowledge and information, hacker cons are the most popular choice. They give members of the community an opportunity to share their latest research, meeting "elite" hackers, and buy the latest hacker swag. But they also enable hackers to officially organize in a way not previously possible (Thomas, 2002). More recently, hackers are not the only ones finding value in hacker cons. In 2012, the Director of the National Security Agency (NSA), four-star General Keith Alexander, gave a keynote speech where he asked hackers to join the NSA (Constantin, 2012; Cowley, 2012; Poeter, 2012).

Hacker cons are instrumental to the development and evolution of this vibrant and ever-changing community. Although hacker cons occur infrequently and not on a set schedule, they are consistently attended. They play an important role in the continual evolution of hacker culture and further the collective knowledge of the community. Hacker cons enable, white hats, black hats and the other hats, to celebrate their latest conquests and share them with others who are equally excited. As described by Coleman (2013), "…hacker conferences are rituals of confirmation, liberation, celebration, and especially reenchantment, where the quotidian affairs of life, work, labor, and social interactions are ritualized, and thus experienced on fundamentally different terms." To hackers, the cons "allow for a series of personal transformations; and perhaps most significantly, reinforce group solidarity" (Coleman, 2013: 47). Unlike other conventions of the professional sort, hacker cons are informal and highly flexible where participants can self-organize, create new talking sessions that were not previously on the agenda, engage in copious eating and drinking, and hack anything of interest—including your girlfriend's smartphone (Coleman, 2013; Nikitina, 2012; Schell & Dodge, 2002;

Summers et al., 2013). Hacker cons are about finding other hackers that share passions, interests, and views on their favorite distributions of Linux or text editor. But the impact and value of the hacker con is most reasonably described by Coleman (2013):

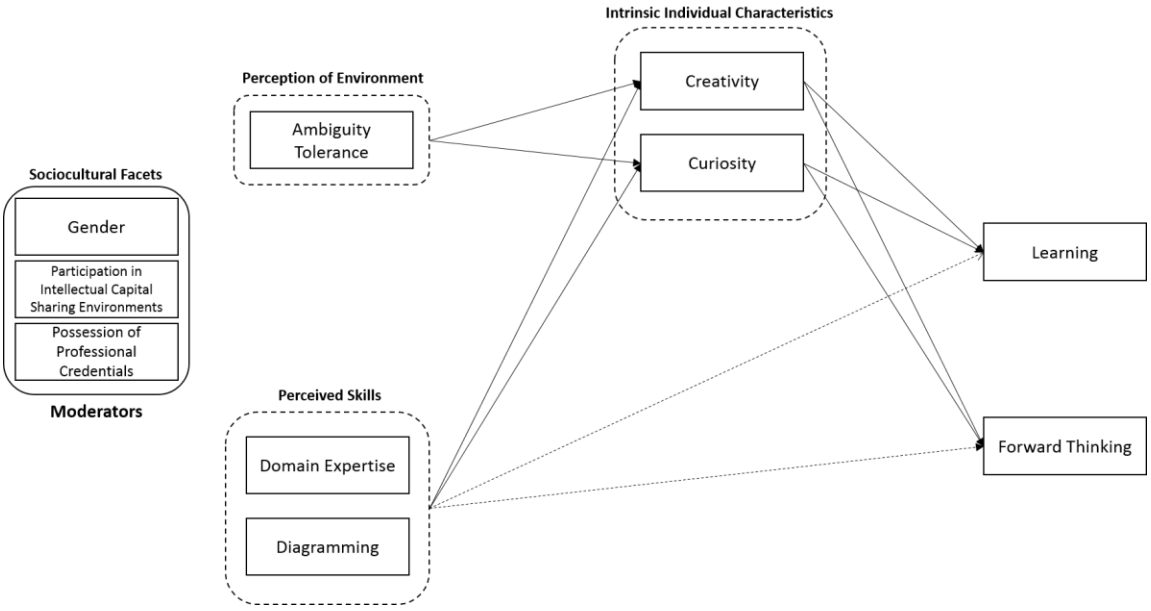
> "Sometimes, as one sits at their computer, coding feverishly for a project, thousands of miles away from some of their closest friends and interlocutors, one has to wonder, "Does this matter to others in the same way as it does to me? In what ways does this matter?" And more than any other event, the hacker conference answers such questions with lucidity and clarity. During the con, hackers see themselves. They are collectively performing a world that is an outgrowth of their practices, quotidian daily life, and deepest passions. The con powerfully states that this world, which us usually felt in unremarkable terms, is as important to others as it is to each hacker—a clear affirmation of the intersubjective basis by which we can conceptually posit any sort of lifeworld" (p. 60).

THEORETICAL MODEL AND HYPOTHESES

Based on the constructs of intrinsic individual characteristics, perceived skills, and perception of environment, we will next articulate a research model that posits how these elements influence learning and forward thinking across sociocultural facets of the hacker subculture. The sociocultural facets explored are gender, participation in organized education, and participation in intellectual capital sharing environments. In particular, we will analyze mechanisms that either moderate the strengthening or hindering of a hacker's learning and forward thinking given the variation in intrinsic individual characteristics, perceived skills and perception of environment across sociocultural facets. We posit that gender, professional education, and participation in intellectual capital sharing environments moderate the mediating effects of intrinsic individual characteristics in mitigating or enabling learning and forward thinking outcomes given the presence of perception of environment, namely ambiguity tolerance. Because we assume a mediated model (Mathieu & Taylor, 2006), we will articulate the

model by first stating direct effects assumed in the model and then developing a fully mediated model (Figure 1).

Figure 1: Moderated Mediation Model



Learning

Throughout the years, learning and development have been studied from various perspectives with the intention of gaining a better understanding of how the human mind performs active learning and constructs new knowledge based on prior knowledge (Bruner, 1996; Dewey, 1997; Huang, 2002; Piaget, 1973; Summers et al., 2014; Summers et al., 2013; Vygotsky, 1978). Our view of learning concerns a person's "involvement in a project or activity" (Ausubel, 1961: 19) in which they "become aware of either concepts or principles" (Hendrix, 1961: 296). We are particularly concerned with the role that mental models play in the learning processes of hackers. As hackers are constantly interacting with complex systems, we suspect that their learning capabilities are related to the dynamic nature of their cognitive structures. Rouse and Morris (1986) suggest that in

such cases, where humans interact with systems of complexity, "mental models are the mechanisms whereby humans are able to generate descriptions of system purpose and form, explanations of system functioning and observed system states, and predictions of future system states" (p. 351). Further, Williams et al. (1983b) claim that the purpose of mental models is to enable humans to explain and predict system behaviors as well as to serve as mnemonic devices for learning and remembering relations and events. The extant literature has provided the theoretical foundation necessary to understand the scaffolding process that enables the human mind to solve a problem, carry out a complicated task, or achieve a goal (Huang, 2002). For hackers, learning involves becoming acquainted with new programming languages, finding and fixing bugs in computer code, and researching the ins-and-outs of a system (Coleman, 2013; Summers et al., 2014; Summers et al., 2013). Hacking requires having access to some sort of *mental* model of the system which acts as their mental representation of the components and operating rules of the system (Mayer, 1981). These models will vary depending on their completeness and accuracy; however, as hackers learn and interact with the system, their mental models evolve and become more reliable (Gentner & Stevens, 1983b; Jih & Reeves, 1992; Norman, 1983a). We will here focus primarily on the cognitive skills and traits that influence and enable the learning that hackers must do to solve the complex problems they face. We will next review their forward thinking.

Forward Thinking

Forward thinking is the ability to generate testable predictions that mental models provide when understanding complexity and problem solving. It is a core element of the predictive power that enables an individual to understand and anticipate behaviors being

observed (Norman, 1986b) or as described by Pasquale (2015) "connecting the dots of past behavior to predict the future" (p. 20). When a hacker uses the knowledge learned, reflects on emergent behaviors, and infers linkages with other models, it enables them to predict and understand future behaviors (Frederiksen et al., 1999; Norman, 1986b; Summers et al., 2014; Summers et al., 2013). Hacking, like computer programming, is a complex, mixed skill cognitive activity that requires continuously incorporating new information (Cañas et al., 1994). This necessitates a number of abilities that interrelate with the hacker's knowledge base, memory, and processing capabilities, repertoire of comprehension strategies, and problem solving abilities involving inferencing and hypothesis generation (Pea & Kurland, 1984). Rasmussen (1979b) suggests that these models are instrumental in predicting system response based on knowledge of the input information, the intention/purpose of the system and the system designer. Based on this, he asserts that mental models are for predicting future events, finding causes of observed events, and determining appropriate actions to cause changes (as cited by Rouse & Morris, 1986). Hackers use these continuously evolving cognitive structures to conceive of future results through speculative forecasting (Adams et al., 2009). These models are instrumental in setting the hacker's expectations about effects of actions, planning of actions, and ways of interpreting feedback (Jih & Reeves, 1992; Van der Veer, 1989). Next, we will review our research model.

Direct Effects

Based on our theoretical framework, we will first formulate direct effects associated with the perception of environment and perceived skills on learning and

forward thinking across sociocultural facets when intrinsic individual characteristics are absent.

Domain expertise enables a skilled hacker to intuitively respond in various situations without analytical principles needed by beginners. Expert hackers are capable of intense absorption of a situation and able to utilize their mental energy to immediately conceive of potential actions and prepare for potential situations conditions (Dreyfus & Dreyfus, 1980). We propose that this would be true regardless of gender. However, we posit that domain expertise would have a distinguishable impact on learning and forward thinking across groups that participate/do not participate in professional education and those that attend/do not attend intellectual capital sharing environments. We have taken this position based on the abundant literature that indicates that hackers prefer informal, hands-on training over organized learning (Chiesa et al., 2008; Coleman, 2013; Levy, 1984; Nikitina, 2012; Rosenbaum, 1971; Rosenzweig, 1998; Sterling, 1992; Summers et al., 2013; Taylor, 1999; Thomas, 2002). Thus, we posit:

> *Hypothesis 1. Attending hacker conventions moderates the effect between domain expertise (H1a) and diagramming (H1b) with learning, such that the relationship will be weaker for those that do not attend hacker conventions.*
>
> *Hypothesis 2. Attending hacker conventions moderates the effect between domain expertise (H2a) and diagramming (H2b) with forward thinking, such that the relationship will be weaker for those that do not attend hacker conventions.*
>
> *Hypothesis 3. Professional credentials moderates the effect between domain expertise (H3a) and diagramming (H3b) with learning, such that the relationship will be weaker for those that do not possess professional credentials.*
>
> *Hypothesis 4. Professional credentials moderates the effect between domain expertise (H4a) and diagramming (H4b) with forward thinking, such that the relationship will be weaker for those that do not attend hacker conventions.*

Diagramming is used to create concept maps that represent meaning or ideational frameworks that are specific to a domain of knowledge. The diagrams used by hackers externalize their mental understandings of a situation using labeled constructs and propositional linkages between those constructs (Novak, 1990a; Summers et al., 2013). Visually seeing the knowledge structures before and after interacting with the environment generates learning and forward thinking opportunities (Novak, 1990a; Summers et al., 2013). Some researchers (Trahan & Quintana, 1990) suggest that males perform slightly better than females on measures of visual memory structures. Thus, we posit:

> *Hypothesis 5. Gender moderates the effect between diagramming with learning (H5a) and with forward thinking (H5b), such that the relationship will be weaker for females.*

Moderated Multi-Group Mediation Effects

We will next articulate the effects of intrinsic individual characteristics in mediating the effects of perception of environment on learning and forward thinking across sociocultural facets.

Ambiguity tolerance decreases rigidity in thinking and increases willingness to accept and incorporate new knowledge (MacDonald & Games, 1976; Summers et al., 2013). When considering gender, we posit that this would remain true for men but not so for women. Many researchers (Schubert, Brown, Gysler, & Brachinger, 1999; Schubert et al., 2000) have considered differences in decision making between the genders, finding that "women are more risk-averse than men." Also, this same stream of research indicates that personal perspectives on technical competence and confidence is important in the valuation of decision making in ambiguous situations. Based on this, we posit that there

will be distinguishable differences between males and females. We do not propose that there will be any distinguishable differences between those who participate in professional education or intellectual capital sharing environments.

Creativity. Past research identifies creativity as a cognitive trait that enables a hacker to see the detail of a subject, formulate and solve problems, and question the connectedness of diverse topics, and generate new ideas (Gurteen, 1998; Reid & Petocz, 2004). This process is food for innovative thought and encourages hackers to push the boundaries of the environment. The creative process is instrumental to creating and applying new knowledge. This increases learning and forward thinking capabilities.

***Curiosity*.** Curiosity is a cognitive trait reached by the hacker when a situation contains subjective uncertainty. This uncertainty prompts the hacker's tendency to engage in exploratory behavior directed at resolving or mitigating the uncertainty thereby generating opportunities for learning and forward thinking (Berlyne, 1978).

Thus, we posit:

Hypothesis 6. Gender moderates the effect of the mediated relationships between ambiguity tolerance (H6a), domain expertise (H6b), and diagramming (H6c) with learning via creativity, such that the mediated relationship will be weaker for females.

Hypothesis 7. Attending hacker conventions moderates the effect of the mediated relationships between ambiguity tolerance (H7a), domain expertise (H7b), and diagramming (H7c) with learning via creativity, such that the mediated relationship will be weaker for those that do not attend hacker conventions.

Hypothesis 8. Attending hacker conventions moderates the effect of the mediated relationships between ambiguity tolerance (H8a), domain expertise (H8b), and diagramming (H8c) with learning via curiosity, such that the mediated relationship will be weaker for those that do not attend hacker conventions.

Hypothesis 9. Professional credentials moderates the effect of the mediated relationships between ambiguity tolerance (H9a), domain expertise (H9b), and

diagramming (H9c) with learning via creativity, such that the mediated relationship will be weaker for those that do not possess professional credentials.

RESEARCH DESIGN AND METHODS

To validate our research model and find support for related hypotheses, we designed and carried out an electronically disseminated, Internet-based, self-administered survey within a population of cyber security experts. The survey approach was appropriate for this research because cyber security experts value their anonymity and privacy. Specifics regarding the resulting sample of respondents are provided in a subsequent section. Scale items for the independent variables (learning and forward thinking), the dependent variables (domain expertise, creativity, curiosity, and diagramming), and mediators (ambiguity tolerance and flexibility) were adapted from existing literature. Data analysis was completed using IBM SPSS Statistics (v. 21) for initial statistical analysis and IBM SPSS AMOS (v. 21) for covariance based structural equation modeling. Our analyses were completed using the following staged approach: 1) confirm suitability of data for multivariate analysis and 2) a structural equation modeling strategy that included an exploratory factor analysis (EFA) and confirmatory factor analysis (CFA) to build the model.

Construct Operationalization

We adapted scales for our constructs from the extant literature. Due to the study context and lack of systematically developed scales in this domain we carried out significant modifications to construct operationalizations as explained below. All scales were defined as reflective (Jarvis et al., 2003). The reliability of our constructs can be found in the Appendix. The Cronbach's alphas for all measures were above .700. The

items in all of our scales were measured using a five-point Likert scale anchored by extremes of "strongly disagree" and "strongly agree".

Dependent Variables

Learning (Reflective). A four-item scale was adapted and significantly modified from (Wolfberg, Boland et al., 2012). Vandenbosch and Higgins (1996) and Norman (1986a) were also consulted for validity and adaptations. The construct measures whether hackers change their mental models to fit new situations and are responsive to disconfirming information or questioning the model.

Forward thinking (Reflective). A five-item scale was adapted and modified from Greenglass et al. (1999). Norman (1983b) was also consulted for adaptations. The construct measures the extent a hacker feels that they utilize their mental models to anticipate future events. Another way to think about this construct is similar to what the entrepreneurship community refers to as opportunity recognition. It can be defined as "a motivated propensity of man to formulate an image of the future" (Kirzner, 1985: 56).

Independent Variables

Ambiguity tolerance (Reflective). A five-item scale was adapted and modified from MacDonald (1970). The construct measures the relationship that a hacker has with ambiguous stimuli or events.

Domain expertise (Reflective). A five-item scale was adapted and modified from Durcikova and Gray (2009). Sussman and Siegal (2003) was also consulted for adaptations. The construct measures the extent to which a hacker feels that their years of experience, facts and heuristics, and highly developed repertoires of knowledge enables them to efficiently and effectively learn and perform forward thinking.

Diagramming (Reflective). A five-item scale was adapted and modified from Güven (2008). The construct measures whether a hacker utilizes diagrams or mind maps to understand relationships between concepts, ideas and other pieces of information.

Mediating Variables

Creativity (Reflective). A five-item scale was adapted and modified from Baer (2006). Zhou (2003) was also consulted for adaptations. The construct taps into the hacker's cognitive process of producing ideas that are novel and useful for solving problems.

Curiosity (Reflective). A five-item scale was adapted and modified from Jiang and Izak (2004). The construct taps into the hacker's cognitive process of using playful exploration to solve problems and make decisions.

Control variables. Research has shown that work experience is the most relevant predictor of job performance (Quiñones et al., 1995). The literature is abound by research showing a relationship between years of experience and job performance. More specifically, the research shows that years of experience is important for various human resource functions such as selection (Ash & Levine, 1985), training (Ford et al., 1992), and career development (Campion et al., 1994; Mccall et al., 1988). Therefore, in order to further assess the relationships between the independent variables and the dependent variables, we controlled for years of experience.[31]

[31] We originally included additional controls, including gender, professional certifications, and participation in hacking conference. However, these control variables proved impotent.

Instrument Validation and Refinement

Scale development followed procedures and guidelines recommended by DeVellis (1991), Churchill (1979), and Dillman (2000). The constructs in the theoretical model were measured using multi-item scales to increase reliability, minimize measurement error, attempt greater variability among participants, and improve instrument validity (Churchill Jr, 1979). Each construct is operationalized using at least three items to effectively measure and analyze it using structural equation modeling (Churchill, 1979). Our goal was to develop a survey instrument that was easy to answer and understand.

Once we made an informed decision on the survey items, the procedures suggested by Dillman (2000) for survey design were used. The overall objective of the design was to increase participant response rate and minimize measurement error. The variables of interest were estimated through respondent evaluation on a five-point Likert scale. The response categories for each item were anchored by 1 (strongly disagree) and 5 (strongly agree).

To increase reliability, minimize measurement error, and improve the validity of our constructs, we pretested the scale items (DeVellis, 1991; Dillman, 2000). The pretesting was broken down into two phases. The first phase focused on using the Q methodology to refine the instrument as most of the items measuring our constructs were adapted from previous studies (Thomas & Watson, 2002; Van Exel & de Graaf, 2005). The Q methodology is a cost effective and simple way to gain insight into the potential

problem areas in the items being tested (Nahm et al., 2002).[32] The second phase focused on instrument clarity and content validity using Bolton's methodology (Bolton, 1991).

Data Collection, Sampling, and Screening

To identify the appropriate sampling population, we used the researcher's personal networks and a Qualtrics panel because of access and the ability to acquire large numbers in an uninhibited way. We utilized a two stage survey delivery method. First, we leveraged the contacts and social network of the researcher to identify hackers and experts in the cyber security field. These contacts were sent an email with a URL link to the survey. A similar email was also sent out to a carefully screened professional research panel provided by Qualtrics. The survey was sent out in January 2014 and all results were received by the end of February 2014.

Measurement Model

Exploratory factor analysis. We conducted an exploratory factor analysis (EFA) using the SPSS software package with Principal Axis Factoring (PAF) and oblique rotation (Direct Oblimin). This technique seemed appropriate since the factors were correlated and it is well-suited for large data sets (n=350). The factor loadings for two domain expertise items (DE4 and DE5), three flexibility items (FL1, FL2, FL3), two creativity items (CR1 and CR2), two curiosity items (CU1 and CU2), two forward thinking items (FT1 and FT2), and one learning item (LE1) were below the minimum threshold (Hair et al., 2010b) and therefore eliminated.[33] All of our items had

[32] In the Appendix, we provide a detailed explanation of the Q-sorting process designed by the researcher.

[33] In order to achieve model fit, we had to remove flexibility as moving from the measurement model to the structural model introduced particular new relationships that caused flexibility to be overlapped with other variables. Flexibility dropped to two items which is known to cause stability issues. The ideal number of items for a latent factor is four (Marsh, Hau, Balla, & Grayson, 1998).

communalities that exceeded 0.30 indicating adequacy for factoring (MacCallum et al., 1999). The Kaiser-Meyer-Olkin (KMO) measure of sampling adequacy (MSA) was .932 and the Bartlett's Test of Sphericity was significant (x^2 = 5688.316, *df* =300, and $p <$ 0.000) suggesting strong factorability (Hair et al., 2010b). Cronbach's alphas (shown in Table 2) were greater than the lower limit of acceptability (> 0.70).

The EFA resulted in eight factors after a total of seventeen items and one construct were removed from the item pool. Sufficient convergent validity was achieved as factor loadings were above the minimum threshold of .30 for a sample size of 350 (Fornell & Larcker, 1981; Hair et al., 2010b). The model did not have strong cross-loadings greater than 0.250 and thus demonstrated sufficient discriminant validity (Fornell & Larcker, 1981). The final variance explained was 74.643%. Factor correlations were all less than 0.70 suggesting adequate initial convergent and discriminant validity and reliability.

Table 1: EFA Pattern Matrix

Pattern Matrix[a]

	Factor						
	1	2	3	4	5	6	7
de1	.681						
de2	.874						
de3	.455						
cr3						-.729	
cr4						-.783	
cr5						-.546	
cu3				-.439			
cu4				-.788			
cu5				-.781			
dg1			-.765				
dg2			-.765				
dg3			-.803				
dg4			-.794				
dg5			-.713				
at1		.791					

at2		.717					
at3		.847					
at4		.526					
at5		.835					
le2							.499
le3							.604
le4							.610
ft3					-.806		
ft4					-.802		
ft5					-.331		

Extraction Method: Principal Axis Factoring.
Rotation Method: Oblimin with Kaiser Normalization.
a. Rotation converged in 13 iterations.

Confirmatory factor analysis. A confirmatory factor analysis (CFA) was used to assess the statistical fit of the proposed measurement model. The factors demonstrate convergent validity with diagonal values greater than the correlations (Fornell & Larcker, 1981). We reached a reasonable final fit (χ^2= 526.657, *df*=287, χ^2/df = 1.791, GFI=0.907; CFI= 0.965; RMSEA=0.048; PCLOSE=0.701).[34] Composite reliability was also achieved with CR values above the 0.70 minimum threshold (see Table 2).

Table 2: Test for Discriminant Validity

	CR	AVE	MSV	ASV	FT	DG	AT	DE	CU	CR	LE
FT	0.824	0.611	0.554	0.421	0.782						
DG	0.898	0.639	0.379	0.322	0.598	0.799					
AT	0.876	0.592	0.331	0.193	0.417	0.492	0.769				
DE	0.874	0.699	0.549	0.395	0.720	0.515	0.306	0.836			
CU	0.844	0.645	0.513	0.420	0.659	0.616	0.575	0.636	0.803		
CR	0.862	0.677	0.554	0.433	0.744	0.556	0.425	0.741	0.676	0.823	
LE	0.822	0.607	0.551	0.434	0.697	0.615	0.373	0.735	0.716	0.742	0.779

[34] We further fine-tuned our EFA and CFA which lead us to new fit statistics. Our previous fit statistics (χ^2= 526.657, *df*=287, χ^2/df = 1.835, GFI=0.898; CFI= 0.960; RMSEA=0.049; PCLOSE=0.599) were identified in Summers, T. C., Lyytinen, K. J., & Gaskin, J. 2014. How Hackers Think: Understanding the Mental Models and Cognitive Patterns of High-Tech Wizards: Case Western Reserve University..

Common method bias. Data collection for both the independent and dependent variables were completed using a single survey instrument. A test for common method bias (CMB) was facilitated to determine bias impacting the measurement model (Podsakoff et al., 2003). A common latent factor (CLF) was introduced to the model. A comparison of the standardized regression weights with and without the CLF showed no common method bias. For no item the difference in betas was greater than 0.20 which implies that there is a limited threat of CMB (Podsakoff et al., 2003); therefore the CLF was not retained in the model.

Structural model. Our study seeks to understand the mediating mechanisms that influence perception of environment and perceived skills on learning and forward thinking (i.e. how the perception of the hacker environment and their perceived skills) are *mediated* by individual intrinsic characteristics (Baron & Kenny, 1986). Following the guidance of Baron and Kenny (1986) and Mathieu and Taylor (2006), our model consisted of four independent variables (ambiguity tolerance, domain expertise, and diagramming)[35] and two dependent variables (learning and forward thinking) and one control variable (years of experience). With this model, we achieve the following model fit: χ^2= 472.258, *df*=156, χ^2/df = 3.027, GFI=0.895; CFI= 0.921; RMSEA=0.076 and PCLOSE=0.000. We added two mediating variables (creativity and curiosity) to produce a mediated model. We used bootstrapping to test statistical significance of the indirect effects by setting the sample size to 2000 (with return values) and used bias-corrected confidence intervals of 95%. With this structural model, we achieved the following model fit: χ^2= 532.704, *df*=269, χ^2/df = 1.980, GFI=0.895; CFI= 0.953; RMSEA=0.053

[35] Our final SEM did not include Cognitive Flexibility due to its low reliability.

and PCLOSE=0.222. Following guidance from Hu and Bentler (1999), we agreed that these statistics were adequate.

We controlled with years of experience and tested for its effect on the mediator and the dependent variable. The control was found not to drive the current theory but was reported as a potential related variable.

Mediation. Mediation was tested using 2000 bias corrected bootstrapping resamples in AMOS (with 95% bias correct confidence intervals) to discover direct effects without mediation, then direct effects and indirect effects with mediation (Baron & Kenny, 1986).

FINDINGS

Overall our mediated model included eleven hypotheses (see Table 12 for final results).

The Impact of Perceived Skills on the Outcome Variables for Convention Attendees

Hypothesis 1 proposed that attending hacker conventions would moderate the effect between domain expertise (H1a) and diagramming (H1b) with learning, such that the relationship will be weaker for those that do not attend hacker conventions. The regression results for the relationships are reported in Table 3. The results in Table 3 show that when using hacking convention attendance as a moderator, domain expertise had a stronger relationship with learning for those that do not attend hacker conventions (β =.478***, $p < .001$) as opposed to those that do attend conventions (β =.365***, $p < .001$). Whereas, diagramming had a stronger relationship with learning for those that do attend hacker conventions (β = .207**, $p = .005$) as opposed to those that do not attend

conventions (β =.181**, p = .002). Thus, **H1a was not supported**; **while H1b was supported**.

Hypothesis 2 proposed that attending hacker conventions would moderate the effect between domain expertise (H2a) and diagramming (H2b) with forward thinking, such that the relationship will be weaker for those that do not attend hacker conventions. Our regression results indicate that when using hacker convention attendance as a moderator, domain expertise had a stronger relationship with forward thinking for those that do not attend hacker conventions (β =.596***, p < .001) as opposed to those that do attend conventions (β =.321***, p < .001). On the other hand, when using hacker convention attendance as a moderator for the relationship between diagramming and forward thinking, we found that the relationship was weaker for those that do not attend conventions (β =.069, p = .200) as opposed to those that do attend conventions (β =.379***, p < .001). Thus, **H2a was not supported**; while **H2b was supported**.

Table 3: Regression Results for Attending Hacker Conventions

Hypotheses	**Direct Beta**		**Support?**
	Attend Cons	Do Not Attend Cons	
H1a: DE → LE	.365***, p < .001	.478***, p < .001	Not Supported
H1b: DG → LE	.207**, p = .005	.181**, p = .002	Supported
H2a: DE → FT	.321***, p < .001	.596***, p < .001	Not Supported
H2b: DG → FT	.379***, p < .001	.069, p = .200	Supported
Notes: Standardized regression weights shown; *** p-value < 0.001; ** p-value < 0.01; * p-value < 0.05; as = approaching significance; ns=not significant			

The Impact of Perceived Skills on Outcome Variables for Hackers with Professional Credentials

Hypothesis 3 proposed that professional credentials would moderate the effect between domain expertise (H3a) and diagramming (H3b) with learning, such that the relationship would be weaker for that that do not possess professional credentials. Our results show that when using professional credentials as a moderator, domain expertise had a stronger relationship with learning for those that have professional credentials (β =.452***, p < .001) over those that do not (β =.382***, p < .001). Diagramming had a slightly stronger relationship with learning for those that do not have professional credentials (β =.185**, p = .005) as opposed to those that do have professional credentials (β =.183**, p = .003). These results provide evidence that **H3a was not supported**; while **H3b was supported**.

Hypothesis 4 proposed that professional credentials would moderate the effect between domain expertise (H4a) and diagramming (H4b) with forward thinking, such that the relationship would weaker for those that do not attend hacker conventions. Our results show that when using professional credentials as a moderator, domain expertise had a stronger relationship with forward thinking for those that do not have professional credentials (β =.522***, p < .001) as opposed to that that do (β =.452***, p < .001). On the other hand, when using professional credentials as a moderator, diagramming had a stronger effect on forward thinking for those that have professional credentials (β =.210***, p < .001) over those that do not (β =.058, p = .381). Thus, **H4a was supported**; while **H4b was not supported**.

Table 4: Regression Results for Possessing Professional Credentials

Hypotheses	Direct Beta		Support?
	Professional Certs	No Professional Certs	
H3a: DE → LE	.452***, p < .001	.382***, p < .001	Not Supported
H3b: DG → LE	.183**, p = .003	.185**, p = .005	Supported
H4a: DE → FT	.452***, p < .001	.522***, p < .001	Supported
H4b: DG → FT	.210***, p < .001	.058, p = .381	Not Supported
Notes: Standardized regression weights shown; *** p-value < 0.001; ** p-value < 0.01; * p-value < 0.05; as = approaching significance; ns=not significant			

Gender Differences for Relationships between Perceived Skills on Outcome Variables

Hypothesis 5 proposed that gender would moderate the effect between diagramming with learning (H5a) and with forward thinking (H5b), such that the relationship will be weaker for females. Our results show that when using gender as a moderator, diagramming had a stronger relationship with learning for males (β =.166***, p < .001) than for females (β =.091(ns), p = .415). Also, we found that when using gender as a moderator, diagramming had a stronger relationship with forward thinking for males (β =.162***, p < .001) than for females (β =.013(ns), p = .909). Thus, providing evidence that **H5a and H5b were supported**.

Table 5: Regression Results for Impact of Perceived Skills on Outcome Variables when Moderating for Gender

Hypotheses	Direct Beta		Support?
	Males	Females	
H5a: DG → LE	.166***, p < .001	.091(ns), p = .415	Supported
H5b: DG → FT	.162***, p < .001	.013(ns), p = .909	Supported
Notes: Standardized regression weights shown; *** p-value < 0.001; ** p-value < 0.01; * p-value < 0.05; as = approaching significance; ns=not significant; NH = not hypothesized			

Moderated Mediation Findings

Hypothesis 6 proposed that gender would moderate the effect of the mediated relationships between ambiguity tolerance (H6a), domain expertise (H6b), and diagramming (H6c) with learning via creativity, such that the mediated relationship would be less significant for females. Our results can be seen in Tables 6 and 7.

The results show that when creativity was added to the relationship of ambiguity tolerance and learning; it did not mediate the relationship for males or females. For example, the direct betas between ambiguity tolerance and learning for males (β =.023ns, p = .725) and females (β =.058ns, p = .975) were both positive and not significant. When we added creativity as a mediator, we saw the direct betas for males (β =-.127as, p = .051) and females (β =.008ns, p = .901) drop and not reach significance. Although the negative relationship for males was approaching significance, the indirect effect was not significant (.195ns). The indirect effect for females was also not significant (.097ns). Thereby indicating that there is no difference between genders when examining the mediated relationship between ambiguity tolerance and learning via creativity. Thus, providing evidence that **H6a is not supported**.

Further, our results show that when creativity was added to the relationship of domain expertise and learning, it provided partial mediation for both genders. For example, the direct betas between domain expertise and learning for males (β =.615***, p < .001) and females (β =.733***, p = < .001) were both positive and significant. When we added creativity as a mediator, we saw the direct betas for males (β =.384***, p < .001) and females (β =.369*, p = .025) decrease but remain significant. It should be noted that the direct beta with mediator for males is substantially more significant than for

females. The indirect effects for males (.059as) and females (.080as) were both approaching significance, implying partial mediation and thereby indicating that there are only slight differences between genders. Although the differences are not substantial, **H6b is supported**.

Additionally, our results show that when creativity was added to the relationship of diagramming and learning, it provided partial mediation for males and no mediation for females. The direct betas between diagramming and learning for males (β =.279***, p < .001) and females (β =.210**, p = .033) were both positive and significant. When we added creativity as a mediator, we saw the direct beta for males decrease and remain significant (β =.249**, p = .003). The direct beta for females increased and remained significant (β =.263**, p = .013). However, the indirect effect for males (.075as) was approaching significance; while the indirect effect for females (.623ns) was not significant. These results indicate creativity partially mediates the relationship between diagramming and learning for males; while it provides no mediation for the relationship between diagramming and learning for females. Thus, **H6c is supported**.

Table 6: Regression Results on Mediated Relationships when Moderating for Gender (Males)

Hypotheses	Direct Beta w/o Med	Direct Beta w/ Med	Indirect	Mediation
H6a: AT --> CR --> LE	.023 (.725ns)	-.127 (.051as)	.195ns	No mediation
H6b: DE --> CR --> LE	.615 (***)	.384 (***)	.059as	Partial mediation
H6c: DG --> CR --> LE	.279 (***)	.249 (.003**)	.075as	Partial mediation
Notes: Standardized regression weights shown; *** p-value < 0.001; ** p-value < 0.01; * p-value < 0.05; as = approaching significance; ns=not significant; NH = not hypothesized				

Table 7: Regression Results on Mediated Relationships when Moderating for Gender (Females)

Hypotheses	Direct Beta w/o Med	Direct Beta w/ Med	Indirect	Mediation
H6a: AT --> CR --> LE	.058 (.357ns)	.008 (.901ns)	.097ns	No mediation
H6b: DE --> CR --> LE	.733 (***)	.369 (.025*)	.080as	Partial mediation
H6c: DG --> CR --> LE	.210 (.033**)	.263 (.013**)	.623ns	No mediation
Notes: Standardized regression weights shown; *** p-value < 0.001; ** p-value < 0.01; * p-value < 0.05; as = approaching significance; ns=not significant; NH = not hypothesized				

Hypothesis 7 proposed that attending hacker conventions would moderate the effect of the mediated relationships between ambiguity tolerance (H7a), domain expertise (H7b), and diagramming (H7c) with learning via creativity, such that the mediated relationships would be less significant for those that do not attend hacker conventions. Our results can be seen in Tables 8 and 9.

The results show that when creativity was added to the relationship of ambiguity tolerance and learning, it did not mediate the relationship for hacker convention attendees or hackers that do not attend conventions. For example, the direct betas between ambiguity tolerance and learning for convention attendees (β =-.072ns, p = .388) and those that did not attend conventions (β =-.039ns, p = .617) were both negative and not significant. When we added creativity as a mediator, we saw the direct betas for convention attendees (β =-.063ns, p = .394) and those that do not attend conventions (β =-.041ns, p = .593) remain negative and not significant. The indirect effects for convention attendees (.323ns) and those that do not attend (.140ns) were not significant; thereby indicated that there is no difference between those that attend conventions and

those that do not when examining the mediated relationship between ambiguity tolerance and learning via creativity. Thus, providing evidence that **H7a is not supported**.

Further, our results show that when creativity was added to the relationship of domain expertise and learning, it did not mediate for either group. For example, the direct betas between domain expertise and learning for convention attendees (β =.550***, p < .001) and those that do not attend conventions (β =.344***, p < .001) are both positive and significant. When we added creativity as a mediator, we saw the direct betas for convention attendees (β =.486***, p < .001) and those that do not attend conventions (β =.341***, p = .001) decreased slightly but remained significant. The indirect effects for convention attendees (.216ns) and those that do not attend conventions (.179ns) were not significant, implying that there is no mediation for either group. Thus, **H7b is not supported**.

Additionally, our results show that when creativity was added to the relationship of diagramming and learning, it provided no mediation for convention attendees or those that do not attend conventions. However, the direct betas between the groups were substantially different. In fact, the direct beta for convention attendees (β =.202ns, p = .093) not significant while the direct beta for those that do not attend conventions (β =.229**, p = .008) was positive and significant. When we added creativity as a mediator, we saw the direct beta for convention attendees (β =.178ns, p = .124) decrease and remain non-significant; while the direct beta for those that do not attend conventions (β =.216**, p = .010) also decreased and dropped slightly in significance. However, the indirect effect for neither group was significant (Attend Conventions: .193ns; Do Not Attend Conventions: .526ns). Thus, **H7c is not supported**.

Table 8: Regression Results on Mediated Relationships when Moderating for Hacking Conventions Attendance (Attend Conventions)

Hypotheses	Direct Beta w/o Med	Direct Beta w/ Med	Indirect	Mediation
H7a: AT --> CR --> LE	-.072 (.388ns)	-.063 (.394ns)	.323ns	No mediation
H7b: DE --> CR --> LE	.550 (***)	.486 (***)	.216ns	No mediation
H7c: DG --> CR --> LE	.202 (.093ns)	.178 (.124ns)	.193ns	No mediation
H8a: AT --> CU --> LE	-.072 (.388ns)	-.154 (.279ns)	.186ns	No mediation
H8b: DE --> CU --> LE	.550 (***)	.339 (.201ns)	.175ns	No mediation
H8c: DG --> CU --> LE	.202 (.093ns)	.078 (.672ns)	.176ns	No mediation
Notes: Standardized regression weights shown; *** p-value < 0.001; ** p-value < 0.01; * p-value < 0.05; as = approaching significance; ns=not significant; NH = not hypothesized				

Hypothesis 8 proposed attending hacker conventions would moderate the effect of the mediating relationships between ambiguity tolerance (H8a), domain expertise (H8b), and diagramming (H8c) with learning via curiosity, such that the mediated relationships will be weaker for those that do not attend hacker conventions. Our results can be seen in Tables 8 and 9.

The results show that when curiosity was added to the relationship between ambiguity tolerance and learning, it did not mediate the relationship for convention attendees; however, it did mediate the relationship for those that do not attend conventions. For example, the direct betas between ambiguity tolerance and learning for convention attendees (β =-.072ns, p = .388) and those that do not attend conventions (β =-.039ns, p = .617) were both negative and not significant. When we added curiosity as a mediator, we saw the direct betas for convention attendees (β =-.154ns, p = .279) and for those that do not attend conventions (β =-.095ns, p = .261) remain negative and non-significant. However, the indirect effects for the groups differed substantially. The indirect effect for those that attend conventions (.186ns) was not significant; while the indirect effect for those that do not attend conventions (.006**) was significant; thereby

there is a difference between groups when examining the mediated relationship between ambiguity tolerance and learning via curiosity. This is an interesting finding; however, it provides evidence that **H8a is not supported**.

Further, our results show that when curiosity was added to the relationship of domain expertise and learning, it provided no mediation for convention attendees and partial mediation for those that do not attend conventions. The direct betas between domain expertise and learning for convention attendees (β =.550***, p < .001) and those that do not attend conventions (β =.344***, p < .001) were both positive and significant. When we added curiosity as a mediator, we saw the direct beta for convention attendees (β =.339ns, p = .201) decrease and lose significance; while the direct beta for those that do not attend conventions (β =.247**, p = .008) decreased but remained significant. The indirect effect for convention attendees (.175ns) was not significant; however, the indirect effect for those that do not attend conventions (.008**) was significant. This indicates that curiosity partially mediates the relationship between domain expertise and learning via curiosity for those that do not attend conventions. This finding is interesting; however, it provides the evidence that **H8b is not supported**.

Additionally, our results show that when curiosity was added to the relationship of diagramming and learning, it provided no mediation for convention attendees and partial mediation for those that do not attend conventions. In fact, the direct beta for convention attendees (β =.202ns, p = .093) not significant while the direct beta for those that do not attend conventions (β =.229**, p = .008) was positive and significant. When we added curiosity as a mediator, we saw the direct beta for convention attendees (β =.078ns, p = .672) decrease and remain non-significant; while the direct beta for those

that do not attend conventions (β =.191**, p = .024) decreased but remained significant. The indirect effect for convention attendees (.176ns) was not significant while the indirect effect for those that do not attend conventions (.043as) was approaching significance. This provided evidence that curiosity partially mediates the relationship between diagramming and learning via curiosity for those that do not attend conventions. Thus, **H8c is not supported**.

Table 9: Regression Results on Mediated Relationships when Moderating for Hacker Convention Attendance (Do Not Attend Conventions)

Hypotheses	Direct Beta w/o Med	Direct Beta w/ Med	Indirect	Mediation
H7a: AT --> CR --> LE	-.039 (.617ns)	-.041 (.593ns)	.140ns	No mediation
H7b: DE --> CR --> LE	.344 (***)	.341 (.001***)	.179ns	No mediation
H7c: DG --> CR --> LE	.229 (.008**)	.216 (.010**)	.526ns	No mediation
H8a: AT --> CU --> LE	-.039 (.617ns)	-.095 (.261ns)	.006**	Full mediation
H8b: DE --> CU --> LE	.344 (***)	.247 (.008**)	.008**	Partial mediation
H8c: DG --> CU --> LE	.229 (.008**)	.191 (.024**)	.043as	Partial mediation
Notes: Standardized regression weights shown; *** p-value < 0.001; ** p-value < 0.01; * p-value < 0.05; as = approaching significance; ns=not significant				

Hypothesis 9 proposed that professional credentials would moderate the effect of the mediated relationships between ambiguity tolerance (H9a), domain expertise (H9b), and diagramming (H9c) with learning via creativity, such that the mediated relationships would be less significant for those that do not possess professional credentials. Our results can be seen in Tables 10 and 11.

The results show that when creativity was added to the relationship of ambiguity tolerance and learning, it did not mediate the relationship for either group. For example, the direct betas for those that possess professional credentials (β =-.056ns, p = .419) and

those that do not possess professional credentials (β =-.098ns, p = .303) were both negative and not significant. When we added creativity as a mediator, we saw the direct betas for those that possess professional credentials (β =-.056ns, p = .357) and those that do not possess professional credentials (β =-.092ns, p = .334) remain negative and not significant. The indirect effects for those that possess professional credentials (.136ns) and those that do not possess professional credentials (.454ns) were not significant; thereby indicating that there is no difference between the groups when examining the mediated relationship between ambiguity tolerance and learning via creativity. Thus, providing evidence that **H9a is not supported**.

Further, our results show that when creativity was added to the relationship between domain expertise and learning, it did mediate the relationship for those that possess professional credentials; however, it did not mediate the relationship for those that do not possess professional credentials. For example, the direct betas between domain expertise and learning for those that possess professional credentials (β =.573***, p < .001) and those that do not possess professional credentials (β =.344***, p < .001) were both positive and significant. When we added creativity as a mediator, we saw the direct beta for those that possess professional credentials (β =.434***, p < .001) decrease but remained significant; while the direct beta for those that do not possess professional credentials (β =.372**, p = .003) increased and remained significant. The indirect effect for those that possess professional credentials (.006**) was significant while the indirect effect for those without professional credentials (.787ns) was not significant. Our results show that creativity provides partial mediation when examining the mediated relationship between domain expertise and learning for those that possess professional credentials.

This implies that there is a significant difference between the two groups. Thus, **H9b is supported**.

Additionally, our results show that when creativity was added to the relationship of diagramming and learning, it mediate the relationship for those that possess professional credentials; however, it did not mediate the relationship for those that do not possess professional credentials. For example, the direct betas between diagramming and learning for those that possess professional credentials (β =.175as, p = .073) and those that do not possess professional credentials (β =.284**, p = .004) were both positive and significant. When we added creativity as a mediator, we saw the direct beta for those that possess professional credentials (β =.124ns, p = .163) decreased and dropped out of significance; while the direct beta for those that do not possess professional credentials (β =.271**, p = .005) decreased and remained significant. The indirect effect for those that possess professional credentials (.014**) was significant while the indirect effect for those without professional credentials (.782ns) was not significant. Our results show that creativity provides partial mediation when examining the mediated relationship between diagramming and learning for those that possess professional credentials. This implies that there is a significant difference between the two groups. Thus, **H9c is supported**.

Table 10: Regression Results on Mediated Relationships when Moderating for Possession of Professional Credentials (Possess Professional Credentials)

Hypotheses	Direct Beta w/o Med	Direct Beta w/ Med	Indirect	Mediation
H9a: AT --> CR --> LE	-.056 (.419ns)	-.056 (.357ns)	.136ns	No mediation
H9b: DE --> CR --> LE	.573 (***)	.434 (***)	.006**	Partial mediation
H9c: DG --> CR --> LE	.175 (.073as)	.124 (.163ns)	.014**	Partial mediation
Notes: Standardized regression weights shown; *** p-value < 0.001; ** p-value < 0.01; * p-value < 0.05; as = approaching significance; ns=not significant; NH = not hypothesized				

Table 11: Regression Results on Mediated Relationships when Moderating for Possession of Professional Credentials (Do Not Possess Professional Credentials)

Hypotheses	Direct Beta w/o Med	Direct Beta w/ Med	Indirect	Mediation
H9a: AT --> CR --> LE	-.098 (.303ns)	-.092 (.334ns)	.454ns	No mediation
H9b: DE --> CR --> LE	.344 (***)	.372 (.003**)	.787ns	No mediation
H9c: DG --> CR --> LE	.284 (.004**)	.271 (.005**)	.782ns	No mediation
Notes: Standardized regression weights shown; *** p-value < 0.001; ** p-value < 0.01; * p-value < 0.05; as = approaching significance; ns=not significant; NH = not hypothesized				

SUPPLEMENTARY ANALYSES

To date, most of the studies relating to this area of research have adopted a bivariate interaction analysis to evaluate the joint effects of two independent variables on a dependent variable. To shed more light on the complex relationships that exist between perception of environment, perceived skills, intrinsic individual characteristics, and learning and forward thinking, this study extends prior research by introducing the notion that there may be cognitive mechanisms that may be interdependent with each other, which would ultimately affect the outcome variables.

Curiosity Strengthens the Effect of Creativity

Throughout our attempts to understand the mind, we have made many assumptions about individual creativity and curiosity, but some would argue that we have yet to fully grasp these concepts (Amabile, 2001). Many people believe that creativity, at the individual level, is primarily dependent on talent; however, there is much research-based evidence that proposes that hard work and intrinsic motivation are instrumental to the process (Amabile, 2001). As stated by Kashdan and Fincham (2002), "the most successful scientists often are not the most talented, but the ones who are just impelled by curiosity" (p. 373). Other research (Nakamura & Csikszentmihalyi, 2002) supports this by positing that intense curiosity and enduring love of a topic is necessary to fuel long,

hard work. Kashdan and Fincham (2002) suggest that curiosity is a fundamental motive critical in facilitating creativity and innovation. Others reinforce this concept (Kashdan & Fincham, 2002; Martindale, 2001; Sternberg, 2001) by asserting that the act of pursuing success and creativity are not enough to motivate an individual to consistently put in the extensive 10–16 hour work days; intense curiosity must be present.

As previously discussed, hackers are individuals with a strong, intense sense of connection with technology which explains their ability to be *wired* for extended periods of time without concern of nourishment. The research suggests that they feel one with technology and that curiosity and creativity play an important part in their sensemaking process. As asserted by Deci and Ryan (2010), individuals with intrinsic interest in a specific domain feel that activities relevant to that domain are hugely satisfying and are relevant to their state of being and sense of self. Although it is creativity that enables us to formulate fresh solutions, curiosity is a prerequisite for exploring the environment and self, thus "leading to the attainment and integration of novel perspectives and experiences" (Kashdan et al., 2004).

The foregoing discussion suggests that the two intrinsic individual characteristics work interdependently and that in order to achieve better results in learning and forward thinking, there must be an appropriate fit between them. In other words, a hacker's effectiveness will be influenced by the interaction between the level of creativity and curiosity present. This suggests the following for testing: will there be an interactive effect on learning and forward thinking between the curiosity and creativity, in such a way that curiosity will strengthen the positive effect of creativity on the outcome variables. The analyses results can be found in Table 12.

Based on the analyses, we saw that the direct effects of creativity on learning (β =.169, p = .009) and forward thinking (β =.258, p < .001) were strong and significant; however, we saw that curiosity dampens the effect of creativity on forward thinking (β =.069, p = .022). Although, it the interaction effect is significant, it is substantially lower than the effect of creativity on forward thinking. The effect of the interaction on learning was not significant.

Table 12: Interaction Effects Results

			Estimate	P
Learn	<---	cuxcr	-.038	.230
ForThink	<---	cuxcr	.069	.022
Learn	<---	dexdg	.004	.921
ForThink	<---	dexdg	-.110	.008
Learn	<---	cu	.210	.001
ForThink	<---	cu	.074	.209
Learn	<---	cr	.169	.009
ForThink	<---	cr	.258	***
ForThink	<---	dg	.146	***
Learn	<---	dg	.124	.008
ForThink	<---	de	.171	.001
Learn	<---	de	.205	***

Diagramming Strengthens the Effect of Domain Expertise

Expertise within a domain is usually represented by the possession of substantial amounts of knowledge about that domain—to the point that it seems or feels like second nature. Many researchers (Dreyfus et al., 1987b; Dreyfus & Dreyfus, 1980) have conducted studies to understand how one builds their knowledge to the level of *expert*. However, in recent years, academics and educators have begun taking advantage of diagramming as a way to build critical and analytical skills and develop the ability to *see* relationships between concepts (Davies, 2011). As asserted by Eppler (2006), is a

"visualization technique that fosters learning or knowledge sharing in a constructive and systematic manner" that is used in "such diverse areas as psychology, computer science, requirements engineering, or business administration." Referred to by many different names: "concept mapping", "mind mapping", diagramming can come in many flavors such as "cognitive mapping, mind mapping, entity-relationship models, flow charts, Toulmin maps, IBIS argumentation maps, semantic networks, swim lane diagrams, clustering, UML diagrams, system dynamics, evocative knowledge maps, soft system modeling, or process event chains" (Eppler, 2006: 204). There has been much research conducted on representing complex information visually for advanced understanding (Horn, 1999; Nassi & Shneiderman, 1973; Tufte & Graves-Morris, 1983); however, with the assistance of advanced computing technology, enabling the visual construction of complex information has become more easily achieved (Eppler, 2006).

Domain expertise is presented by superior knowledge of that domain; however, diagramming is necessary to facilitate the deep, not surface, level of comprehension and understanding of problems abound with complexity. Diagramming enables the expert to "imagine and explore associations between concepts", "understand the relationships between concepts and hence understand those concepts themselves and the domain to which they belong", and "display inferential connections between propositions and contentions, and to evaluate them in forms of validity of argument structure and the soundness of argument premises" (Eppler, 2006: 204). Additionally, some researcher propose that diagramming enables efficient learning and integration with information stored in memory (Eppler, 2006; Van Gelder, 2007).

The foregoing discussion suggests that the two perceived skills, domain expertise and diagramming, work interdependently and that in order to achieve superior results in learning and forward thinking, there must be a strong relationship between them. In order words, a hacker's effectiveness will be influenced by the interaction between the level of domain expertise and diagramming; thus, we decided to test for the following: will there be an interactive effect on learning and forward thinking between diagramming and domain expertise, in such a way that diagramming will strengthen the positive effect of domain expertise on the outcome variables. The analyses results can be found in Table 12.

Based on the analyses, we saw that the direct effects of domain expertise on learning (β =.205, $p < .001$) and forward thinking (β =.171, $p = .001$) were strong and significant; however, we saw that diagramming dampens the effect of domain expertise on forward thinking (β =-.110, $p = .008$). The effect of the interaction on learning was not significant.

DISCUSSION

In this study, we examined an integrated moderated mediation model to address gaps in the literature on the nature of sociocultural facets of the hacker community and how those facets impact certain elements of hacker effectiveness. Findings of our study, which was based on survey data collected within the computer security and hacker communities, contribute to the existing in knowledge in three ways. First, we found support for our hypotheses that there are differences between the ways that the genders use visual representations to understand complex issues, especially when ambiguity is involved. However, when ambiguity is present, it wasn't creativity that mediated the

relationship, but curiosity. Our results indicate curiosity facilitates how males address ambiguity; however, it had no effect for females. This finding addresses perspectives represented in previous research (Spertus, 1991; Trahan & Quintana, 1990; Wilder et al., 1985) that females may be impacted by their lack of certainty or timidity with issues concerning complex technical issues. In addition, our finding extends the current literature on the topic of gender inequality that exist in the hacking community and perhaps even the larger field of information systems and technology. Second, our integrated moderated mediation analysis demonstrate general support for our hypotheses H1b and H2b, which suggested that there were differences between how hackers that participate in intellectual capital sharing environments use visual representations to learn and perform forward thinking, in comparison to those that do not participate in knowledge sharing environments. Third, our moderated mediation analysis demonstrates support for our hypotheses H3b and H4a, which suggested that there are differences between how hackers that have professional credentials address ambiguity. For example, we found that for those that possess professional credentials, creativity facilitates learning in environments abound with ambiguity; whereas, for those that do not possess professional credentials, it appears that curiosity is instrumental for learning in a similar environment.

In contrast, our results do not support moderated mediation of convention attendance on the link between ambiguity tolerance and learning or forward thinking via creativity. Instead, results show that curiosity mediated the effects of ambiguity tolerance on learning and forward thinking. This finding does suggest that ambiguity tolerance, which is strongly associated with leadership and confidence, could be the trait that is

highly susceptible to differences in creativity and curiosity when learning and forward thinking effectiveness is being predicted.

Table 13: Hypotheses and Support

Hypothesis	Supported?
H1: Attending hacker conventions moderates the effect between domain expertise (H1a) and diagramming (H1b) with learning, such that the relationship will be weaker for those that do not attend hacker conventions.	H1a: No Support H1b: Supported
H2: Attending hacker conventions moderates the effect between domain expertise (H2a) and diagramming (H2b) with forward thinking, such that the relationship will be weaker for those that do not attend hacker conventions.	H2a: No Support H2b: Supported
H3: Professional credentials moderates the effect between domain expertise (H3a) and diagramming (H3b) with learning, such that the relationship will be weaker for those that do not possess professional credentials.	H3a: No Support H3b: Supported
H4: Professional credentials moderates the effect between domain expertise (H4a) and diagramming (H4b) with forward thinking, such that the relationship will be weaker for those that do not attend hacker conventions.	H4a: Supported H4b: No Support
H5: Gender moderates the effect between diagramming with learning (H5a) and with forward thinking (H5b), such that the relationship will be weaker for females.	H5a: Supported H5b: Supported
H6: Gender moderates the effect of the mediated relationships between ambiguity tolerance (H6a), domain expertise (H6b), and diagramming (H6c) with learning via creativity, such that the mediated relationship will be weaker for females.	H6a: No Support H6b: Supported H6c: Supported
H7: Attending hacker conventions moderates the effect of the mediated relationships between ambiguity tolerance (H7a), domain expertise (H7b), and diagramming (H7c) with learning via creativity, such that the mediated relationship will be weaker for those that do not attend hacker conventions.	H7a: No Support H7b: No Support H7c: No Support
H8: Attending hacker conventions moderates the effect of the mediated relationships between ambiguity tolerance (H8a), domain expertise (H8b), and diagramming (H8c) with learning via curiosity, such that the mediated relationship will be weaker for those that do not attend hacker conventions.	H8a: No Support H8b: No Support H8c: No Support
H9: Professional credentials moderates the effect of the mediated relationships between ambiguity tolerance (H9a), domain expertise (H9b), and diagramming (H9c) with learning via creativity, such that the mediated relationship will be weaker for those that do not possess professional credentials.	H9a: No Support H9b: Supported H9c: Supported
H10: There will be an interactive effect on learning (H10a) and forward thinking (H10b) between the curiosity and creativity, in such a way that curiosity will strengthen the positive effect of creativity on the outcome variables.	H10a: No Support H10b: No Support
H11: There will be an interactive effect on learning (H11a) and forward thinking (H11b) between diagramming and domain expertise, in such a way that diagramming will strengthen the positive effect of domain expertise on the outcome variables.	H11a: No Support H11b: No Support

IMPLICATIONS

With the power of the Internet, organizations are more intelligent, efficient, and connected than ever. In this information-driven world, organizations need access to top cybersecurity talent, knowledge and technology resources to response to threats, and advanced training capabilities.

Identifying Capable Talent with Requisite Cognitive Skills

A recent study by the RAND Corporation (Libicki et al., 2014) argues that there is a substantial shortage of cybersecurity professionals within the United States and the rest of the world. They suggest that these shortages of sufficient talent will complicate public and private sector efforts to secure the IT infrastructure. The RAND study discloses that organizations are becoming increasingly aware of the personality characteristics that correlate with cybersecurity skills, particularly intense curiosity. It suggests that this evolved understanding of the hacker community has allowed organizations to improve the promotion and training of the appropriate individuals with or without waiting for those with specialized university degrees. This has led organizations to outsource to external sources of talent, particularly in newly found hacking organizations. These organizations pride themselves on hiring the best of the best hacking talents throughout the industry.

Academic Institutions in the Hacking Business

Many universities have decided to get into the business of training cybersecurity specialists. Over the past few years, programs of this type have grown at an exponential rate with the demand for cybersecurity experts being at an all-time high (Libicki et al., 2014). Although the universities claim to have qualified professors, most of them are

computer science and information technology professors. The effectiveness of this approach is debatable. The RAND study argues that the reason for using computer science professors is that demand for computer science and information technology professors is because there is considerable institutional spare capacity since the technology downturn circa 2000. In addition, many universities have found success with building cybersecurity programs around a specific focus, such as industrial control systems, application security, cloud security, and other subareas of the field.

Cognitive Training and Development

From the dawn of mankind, there has been a co-dependence of technology and the development of humanity. This symbiotic relationship started with the invention of stone tools and has continued into modern life through information technologies (IT), like the Internet. As humans have matured, society has developed a desire and fixation on superior technologies and information access. This desire has been instrumental in making IT an important component of modern human life.

It is no secret that technology is radically reshaping humanity. But hackers are radically changing technology. Although hackers have had a troubled past in the media, their "playful cleverness" is part of what drives their thriving intellectual culture, focusing on problem solving, self-directed learning, and the free exchange of information.

Anyone who has read about the history of hackers and hacking is aware that much of the culture and mindset is deeply rooted in the scholarly traditions of universities. The hacker ethic shares many similarities with academe. Most literature on hackers and hacking traces its history to the Massachusetts Institute of Technology in the 1960s. Winn

and Neary (2011) state that at the core of hacking is the academic practice of peer review, the opportunity for academics to closely examine, modify and use other people's work. Through open source, hackers have collaboratively built the foundational elements of the Internet, which not only represents one of the most substantial technological advances of our time, but a shift in the way we live and conduct business.

So, what is a hacker? According to Schneier (2006):

> "A hacker is someone who thinks outside of the box. It's someone who disregards conventional wisdom, and does something else instead. It's someone who looks at the edge and wonders what's beyond. It's someone who sees a set of rules and wonders what happens if you don't follow them. A hacker is someone who experiments with the limitations of systems for intellectual curiosity."

Hackers are, as Gabriella Coleman (2013) suggests, technologists with a love for figuring things out and a "hack" is a clever solution arrived through non-obvious means. In essence, many of the world's innovators, like Steve Jobs, Mark Zuckerberg, and Elon Musk, are hackers. Hacking is a cognitive activity that requires exceptional technical and reasoning abilities. To facilitate these abilities, hackers, like all humans, use mental models. Mental models are the medium of thought and allows the mind to construct concepts, conceive alternatives, and search out consequences of assumptions (Craik, 1967). The mental models of hackers are dependent on a set of intrinsic cognitive skills and motivational traits (Summers et al., 2013). These cognitive skills and traits contribute to a hacker's ability to innovate. By improving these cognitive functions, we can improve the way that a hacker solve problems and makes decisions.

In my experience, training in the cybersecurity community occurs through technical courses, certifications, and as of decade, degree granting institutions. However,

none of these channels makes use of cognitive development training. Some researchers (Hardy & Scanlon, 2013) suggest that with the right kind of stimulation, cognitive training can improve job performance. Therefore, as a practitioner-scholar in the fields of organizational management and cybersecurity propose that there may be an opportunity for the development of a cognitive development platform specific to innovative thinking and/or hacking. Initial research on the topic indicate that it could be a web and/or mobile-based platform having the following attributes:

- Apply research based on psychometric and neuroscience models to build modules that will be designed to improve performance across a variety of cognitive functions instrumental for skilled hacking;
- The platform will be designed and created by scientists working closely with game developers;
- Will feature activities that provide highly effective brain training and highly engaging games;
- Each game will target specific cognitive skills using unique experiences that challenge the brain to create new and more efficient neural connections;
- There will be activities that train speed of processing, memory, attention, problem solving, and the cognitive functions of skilled hackers (Summers et al., 2013).

At the core of the platform could be activities designed to improve performance across a variety of cognitive functions. A platform like this would need to be designed and created by researchers, sciences, and developers working closely to create activities that are both highly effective and engaging. Each activity would target a specific set of cognitive skills and traits using unique experiences that challenge the mind to create new and more efficient mental model linkages. The activities would be adaptive, becoming

increasingly more difficult as performance improves and becoming easier if performance declines.

A platform like this could provide to be effectively useful in the organization and education institutions. According to The Daily, a newsletter at Case Western Reserve University, students at Case Western and Cleveland State University will begin learning to hack computers for credit. Both universities are offering the first of three courses in a new curriculum in which engineering and computer science students will learn to break into and then protect hardware, software, and data. The goal is for the students to understand how they can protect their own, or their employer's computers from viruses, phishing attacks, and other cyber attacks. According to Swarup Bhunia, Associate Professor of Electrical Engineering and Computer Science, "we're doing a lot of computer security research, but we've failed in the need to educate and train students—the future users, developers, and controllers of these systems" (CWRU, n.d.). They believe that the courses will teach students how to analyze, validate and build secure computer hardware and systems. Perhaps there is room for the development of a platform like this one to aid in courses like those now being offered at Case Western Reserve University. If so, it would offer substantial benefits to the establishment of specific security functions and processes.

LIMITATIONS

Our study mediation model implies causal relationships between perception of environment, perceived skills, intrinsic individual characteristics, learning and forwards thinking. However, our current research does not allow us to conclude definitively that a hacker's perception of environment, perceived skills, and intrinsic individual

characteristics leads to higher effectiveness in learning and forward thinking. To further ascertain causality, future studies could seek the power of experiments that would better establish the direction of relationships posited in our model.

Our moderated mediation model could be expanded to examine other important hacker performance outcomes from multiple perspectives. In the current study, hacker effectiveness was assessed using self-reported information about the hacker's thoughts on their learning and forward thinking. Future research could assess hacker performance with superior's ratings on multiple technical tasks. Future research could also examine hacker effectiveness and performance by ratings from colleagues.

Finally, given that our study was conducted with data gathered from the general information security and hacking contexts, we caution against generalizing our findings to other settings. To ascertain generalizability of results obtained in our current study, future research should attempt to replicate our design in different vocational settings and different cultures (Ang et al., 2007; Gelfand, Erez, & Aycan, 2007).

Our results may assist in better understanding the hacker population; however, we recognize that they cannot explain all hacker cognition. While our sample size was adequate with more than 350 surveys completed, there are limits to the generalizability of the findings. We did not test for all factors that may contribute to how a person hacks. Similarly, to the best of our knowledge, the scales used in the study have never been used in combination, in our context, and there are no acceptable tests for scale validity. Some caution should be acknowledged with regard to some of our measures. Specifically, we had low levels of reliability for *flexibility*, which calls for future instrumentation and measurement development. We recognize that as a mediator and given its low reliability

this could increase type I and type II errors. It is our belief that the reason for this low reliability is that due to the nature of the construct itself. *Flexibility* can be seen from multiple viewpoints and refers to the individual's ability to shift focus from one concept to another which can be misinterpreted and complex to discern from other constructs used in this study. Finally, we could not assess response biases because we utilized third party collection.

CONCLUSION

Our study responds to previous calls (Summers et al., 2014) for a more systematic and careful study of mediating and moderating effects of sociocultural facets in the hacking community. Specifically, we developed and tested a model that simultaneously examines intrinsic individual characteristics as mediating mechanisms and gender, participation in intellectual capital sharing environments, and possession of professional credentials as moderating factors to the links between perception of environment, perceived skills, learning, and forward thinking. In doing so, we provided a rare examination of a moderated mediation model of the sociocultural facets of hackers that advances current understanding of hacker effectiveness in learning and forward thinking. Our study empirically validated sociocultural facets and intrinsic individual characteristics as the specific motivational mechanisms that account for relationships between perception of environment and perceived skills with particular aspects of hacker effectiveness. We encourage future research toward a more integrative approach of theorizing mediating and moderating effects, so as to offer a more sophisticated cognitive theory of the hacker mind.

REFERENCES

Adams, V., Murphy, M., & Clarke, A. E. 2009. Anticipation: Technoscience, life, affect, temporality. ***Subjectivity***, 28(1): 246-265.

Adelson, B. 1984. When novices surpass experts: The difficulty of a task may increase with expertise. ***Journal of Experimental Psychology: Learning, Memory, and Cognition***, 10(3): 483.

Adorno, T. W., Frenkel-Brunswik, E., Levinson, D. J., & Sanford, R. N. 1950. ***The authoritarian personality***. Oxford, England: Harpers.

Ainsworth, S., & Th Loizou, A. 2003. The effects of self-explaining when learning with text or diagrams. ***Cognitive Science***, 27(4): 669-681.

Ajzen, I. 1991. The theory of planned behavior. ***Organizational behavior and human decision processes***, 50(2): 179-211.

Amabile, T. M. 2001. Beyond talent: John Irving and the passionate craft of creativity. ***American Psychologist***, 56(4): 333.

Ang, S., Van Dyne, L., Koh, C., Ng, K. Y., Templer, K. J., Tay, C., & Chandrasekar, N. A. 2007. Cultural intelligence: Its measurement and effects on cultural judgment and decision making, cultural adaptation and task performance. ***Management and Organization Review***, 3(3): 335-371.

Anonymous. 2012. What is Cyberpunk?, Vol. 2014: Cyberpunkforums.com.

Argote, L., & Miron-Spektor, E. 2011. Organizational learning: From experience to knowledge. ***Organization Science***, 22(5): 1123–1137.

Argyris, C., & Schon, D. 1978. Organizational learning: A theory of action approach. ***Reading, MA: Addision Wesley***.

Ash, R. A., & Levine, E. L. 1985. Job applicant training and work experience evaluation: An empirical comparison of four methods. ***Journal of Applied Psychology***, 70(3): 572–576.

Ashford, S. J., & Black, J. S. 1996. Proactivity during organizational entry: The role of desire for control. ***Journal of Applied Psychology***, 81(2): 199.

Ausubel, D. P. 1961. Learning by discovery: Rationale and mystique. ***NASSP Bulletin***, 45(269): 18-58.

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

Baer, M., & Oldham, G. R. 2006. The curvilinear relation between experienced creative time pressure and creativity: moderating effects of openness to experience and support for creativity. ***Journal of Applied Psychology***, 91(4): 963–970.

Baldwin, T. T., & Ford, J. K. 1988. Transfer of training: A review and directions for future research. ***Personnel Psychology***, 41(1): 63–105.

Bandura, A. 1977. Self-efficacy: Toward a unifying theory of behavioral change. ***Psychological Review***, 84(2): 191.

Bandura, A. 1993. Perceived self-efficacy in cognitive development and functioning. ***Educational psychologist***, 28(2): 117-148.

Barab, S. A., Hay, K. E., & Duffy, T. M. 1998. Grounded constructions and how technology can help. ***TechTrends***, 43(2): 15-23.

Baron, R. M., & Kenny, D. A. 1986. The moderator–mediator variable distinction in social psychological research: Conceptual, strategic, and statistical considerations. ***Journal of Personality and Social Psychology***, 51(6): 1173.

Barron, F., & Harrington, D. M. 1981. Creativity, intelligence, and personality. ***Annual Review of Psychology***, 32(1): 439–476.

Bartlett, K. R. 2002. ***The perceived influence of industry-sponsored credentials in the information technology industry***. Columbus, OH: National Dissemination Center for Career and Technical Education.

Bartunek, J. M. 1984. Changing interpretive schemes and organizational restructuring: The example of a religious order. ***Administrative science quarterly***: 355-372.

Barwise, M. 2010. What is an internet worm?: BBC. Retrieved December 9, 2014 from http://www.bbc.co.uk/webwise/guides/internet-worms.

Beach, L. R. 1990. ***Image theory: Decision making in personal and organizational contexts***: Wiley Chichester.

Benner, P. 1982. From novice to expert. ***The American Journal of Nursing***, 82(3): 402–407.

Benner, P. 1983. Uncovering the knowledge embedded in clinical practice. ***Image: The Journal of Nursing Scholarship***, 15(2): 36-41.

Berlyne, D. 1950. Novelty and curiosity as determinants of exploratory behaviour. ***British Journal of Psychology. General Section***, 41(1-2): 68-80.

Berlyne, D. E. 1978. Curiosity and learning. ***Motivation and Emotion***, 2(2): 97–175.

Biggs, J. B. 1987. ***Student approaches to learning and studying. Research monograph***: ERIC.

Billo, C., & Chang, W. 2004. ***Cyber warfare: An analysis of the means and motivations of selected nation states***: Dartmouth College, Institute for Security Technology Studies.

Boehm, B. W. 1977. Software and its impact: a quantitative assessment. ***Datamation***, 19.

Boland, R., & Collopy, F. 2004. ***Managing as designing***: Stanford University Press.

Bolton, R. N. 1991. An exploratory investigation of questionnaire pretesting with verbal protocol analysis. ***Advances in Consumer Research***, 18(1): 558–565.

Bowles, M. 2012. The Business of Hacking and Birth of an Industry. ***Bell Labs Technical Journal***, 17(3): 5-16.

Bowman, R. F. 1982. A Pac-Man theory of motivation. Tactical implications for classroom instruction. ***Educational Technology***, 22(9): 14-17.

Bracey, G. W. 1992. The bright future of integrated learning systems. ***Educational Technology***, 32(9): 60-62.

Brandt, J., Guo, P. J., Lewenstein, J., Dontcheva, M., & Klemmer, S. R. 2009. ***Two studies of opportunistic programming: interleaving web foraging, learning, and writing code***. Paper presented at the Proceedings of the SIGCHI Conference on Human Factors in Computing Systems.

Brandt, J., Guo, P. J., Lewenstein, J., & Klemmer, S. R. 2008. ***Opportunistic programming: How rapid ideation and prototyping occur in practice***. Paper presented at the Proceedings of the 4th international workshop on End-user software engineering.

Bratus, S. 2007. What hackers learn that the rest of us don't: Notes on hacker curriculum. ***Security & Privacy, IEEE***, 5(4): 72–75.

Brooks, R. 1977. Towards a theory of the cognitive processes in computer programming. ***International Journal of Man-Machine Studies***, 9(6): 737-751.

Broos, A., & Roe, K. 2006. The digital divide in the playstation generation: Self-efficacy, locus of control and ICT adoption among adolescents. ***Poetics***, 34(4): 306-317.

Brown, K. W., & Ryan, R. M. 2003. The benefits of being present: mindfulness and its role in psychological well-being. ***Journal of Personality and Social Psychology***, 84(4): 822.

Brown, S. R. 1980. ***Political subjectivity: Applications of Q methodology in political science***: Yale University Press New Haven, CT.

Brown, S. R. 1986. Q technique and method: Principles and procedures. In W. D. Berry, & M. S. Lewis-Beck (Eds.), ***New tools for social scientists: Advances and applications in research methods***: 57–76. Beverly Hills, CA: Sage Publications.

Bruner, J. 1978. The role of dialogue in language acquisition. In A. Sinclair, R. J. Jarvella, & W. J. M. Levelt (Eds.), ***The child's conception of language***: 241-256: Springer-Verlag.

Bruner, J. S. 1996. ***The culture of education***: Harvard University Press.

Bryman, A. 2007. Barriers to integrating quantitative and qualitative research. ***Journal of mixed methods research***, 1(1): 8-22.

Bryman, A., Becker, S., & Sempik, J. 2008. Quality criteria for quantitative, qualitative and mixed methods research: A view from social policy. ***International Journal of Social Research Methodology***, 11(4): 261-276.

Buchanan, R. 1992. Wicked problems in design thinking. ***Design issues***: 5-21.

Budner, S. 1962. Intolerance of ambiguity as a personality variable. ***Journal of personality***.

Butler, D. 2000. Gender, girls, and computer technology: what's the status now? ***The Clearing House***, 73(4): 225-229.

Caltagirone, S. A Practical Ethical Assessment of Hacktivism.

Campbell, P. L. 2011. Peirce, pragmatism, and the right way of thinking. ***Sandia National Laboratories, Albuquerque***.

Campbell, R. L., Brown, N. R., & DiBello, L. A. 1992. The programmer's burden: developing expertise in programming. In R. R. Hoffman (Ed.), ***The psychology of expertise***: 269–294: Springer.

Campion, M. A., Cheraskin, L., & Stevens, M. J. 1994. Career-related antecedents and outcomes of job rotation. ***Academy of Management Journal***, 37(6): 1518–1542.

Cañas, J. J., Bajo, M. T., & Gonzalvo, P. 1994. Mental models and computer programming. ***International Journal of Human-Computer Studies***, 40(5): 795-811.

Cannon-Bowers, J. A., & Salas, E. 2001. Reflections on shared cognition. ***Journal of Organizational Behavior***, 22(2): 195-202.

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

Chandler, A. D. 1962. Strategy and structure: Chapters in the history of the american enterprise. ***Massachusetts Institute of Technology Cambridge***.

Charmaz, K. 2006. ***Constructing grounded theory: A practical guide through qualitative analysis***: Pine Forge Press.

Chiesa, R., Ducci, S., & Ciappi, S. 2008. ***Profiling hackers: The science of criminal profiling as applied to the world of hacking***: CRC Press.

Churchill Jr, G. A. 1979. A paradigm for developing better measures of marketing constructs. ***Journal of Marketing Research***, 16(1): 64-73.

Clarke, R. A., & Knake, R. K. 2011. ***Cyber war***: HarperCollins.

Clough, B., & Mungo, P. 1992. ***Approaching zero: Data crime and the computer underworld***: Faber & Faber.

Coleman, E. G. 2013. ***Coding freedom: The ethics and aesthetics of hacking***: Princeton University Press.

Coleman, E. G., & Golub, A. 2008. Hacker practice Moral genres and the cultural articulation of liberalism. ***Anthropological Theory***, 8(3): 255-277.

Collins, A., & Brown, J. S. 1988. ***The computer as a tool for learning through reflection***: Springer.

Collis, B. 1985. Psychosocial implications of sex differences in attitudes toward computers: Results of a survey. ***International Journal of Women's Studies***.

Compeau, D. R., & Higgins, C. A. 1995a. Application of social cognitive theory to training for computer skills. ***Information systems research***, 6(2): 118-143.

Compeau, D. R., & Higgins, C. A. 1995b. Computer self-efficacy: Development of a measure and initial test. ***MIS quarterly***: 189-211.

Compeau, D. R., & Higgins, C. A. 1995c. Computer self-efficacy: Development of a measure and initial test. ***MIS Quarterly***, 19(2): 189–211.

Constantin, L. 2012. NSA Chief Seeks Help From Hackers. ***Computerworld***, 46(14): 4-4.

Corbin, J., & Strauss, A. 2008. ***Basics of qualitative research: Techniques and procedures for developing grounded theory***: Sage.

Cornwall, H. 1987. ***DataTheft: computer fraud, industrial espionage and information crime***: Butterworth-Heinemann.

Corritore, C. L., & Wiedenbeck, S. 1991. What do novices learn during program comprehension? ***International Journal of Human-Computer Interaction***, 3(2): 199–222.

Costello, A., & Osborne, J. 2011. Best practices in exploratory factor analysis: four recommendations for getting the most from your analysis. Pract Assess Res Eval 2005; 10. ***pareonline. net/getvn. asp***, 10: 7.

Cowley, S. 2012. NSA wants to hire hackers. ***CNN Money***, 7: 27.

Cox, R. 1999. Representation construction, externalised cognition and individual differences. ***Learning and instruction***, 9(4): 343-363.

Craik, K. 1943a. The Nature of Explanation. ***Cambridge: Cambridge UP***.

Craik, K. J. W. 1943b. ***The nature of explanation***: Cambridge University Press.

Creswell, J. W., Klassen, A. C., Plano Clark, V. L., & Smith, K. C. 2011. Best practices for mixed methods research in the health sciences. ***Bethesda (Maryland): National Institutes of Health***.

Csiksczentmihalyi, M. 1991. ***Flow: The psychology of optimal experience***: Harper Perennial.

Csikszentmihalyi, M. 1991. ***Flow: The psychology of optimal experience***: HarperPerennial New York.

CWRU. n.d. Students to hack hardware, software and data to build security skills: Case Western Reserve University, School of Engineering. Available from http://engineering.case.edu/cyber-security-courses.

Cyert, R. M., & March, J. G. 1963. A behavioral theory of the firm. ***Englewood Cliffs, NJ***, 2.

Dambrot, F. H., Watkins-Malek, M. A., Silling, S. M., Marshall, R. S., & Garver, J. A. 1985. Correlates of sex differences in attitudes toward and involvement with computers. ***Journal of Vocational Behavior***, 27(1): 71-86.

Davies, M. 2011. Concept mapping, mind mapping and argument mapping: what are the differences and do they matter? ***Higher Education***, 62(3): 279-301.

Davis, E. A. 2000. Scaffolding students' knowledge integration: Prompts for reflection in KIE. ***International Journal of Science Education***, 22(8): 819-837.

Day, H. I. 1971. Intrinsic Motivation: A New Direction in Education.

De Bono, E. 1992. Serious creativity: using the power of lateral thinking to create new ideas. ***New York: HarperColins***.

de Bono, E. 1995. Serious creativity. ***Journal for Quality and Participation***, 18(5): 12-18.

De Kleer, J., & Brown, J. 1983. Assumptions and ambiguities in mechanistic mental models. In D. Gentner, & A. L. Stevens (Eds.), ***Mental models***: 155–190. Hillsdale, NJ: Lawrence Erlbaum Associates.

De Schutter, B. 2010. Never too old to play: The appeal of digital games to an older audience. ***Games and Culture***.

Deci, E. L., & Ryan, R. M. 2010. ***Self-Determination***: Wiley Online Library.

Denzau, A. T., & North, D. C. 1994. Shared mental models: ideologies and institutions. ***Kyklos***, 47(1): 3-31.

DeVellis, R. F. 1991. ***Scale development: Theory and applications*** (3rd ed.). Newbury Park, CA: Sage Publications.

Dewett, T., & Jones, G. R. 2001. The role of information technology in the organization: a review, model, and assessment. ***Journal of management***, 27(3): 313-346.

Dewey, J. 1997. ***How we think***: Courier Dover Publications.

Dewey, J. 2001. Democracy and education. ***The Pennsylvania State University: Hazleton***.

Dewey, J. 2004. ***Reconstruction in philosophy***: Courier Dover Publications.

Dewey, J. 2012. ***How we think***: Courier Dover Publications.

Dill, W. R. 1958. Environment as an influence on managerial autonomy. ***Administrative science quarterly***: 409-443.

Dillman, D. A. 2000. ***Mail and internet surveys: The tailored design method*** (2nd ed.). New York, NY: John Wiley & Sons.

Dixon, N. M. 1997. The hallways of learning. ***Organizational Dynamics***, 25(4): 23–34.

Dreyfus, H. L., & Dreyfus, S. E. 2005. Peripheral vision expertise in real world contexts. ***Organization Studies***, 26(5): 779–792.

Dreyfus, H. L., Dreyfus, S. E., & Athanasiou, T. 1987a. Mind over machine: The power of human intuition and expertise in the era of the computer. ***IEEE Expert***, 2(2): 110–111.

Dreyfus, H. L., Dreyfus, S. E., & Zadeh, L. A. 1987b. Mind over machine: The power of human intuition and expertise in the era of the computer. ***IEEE Expert***, 2(2): 110-111.

Dreyfus, S. E., & Dreyfus, H. L. 1980. A five-stage model of the mental activities involved in directed skill acquisition: DTIC Document.

Driskell, J. E., & Dwyer, D. J. 1984. Microcomputer Videogame Based Training. ***Educational Technology***, 24(2): 11-17.

Duncan, R. B. 1972. Characteristics of organizational environments and perceived environmental uncertainty. ***Administrative science quarterly***: 313-327.

Durcikova, A., & Gray, P. 2009. How knowledge validation processes affect knowledge contribution. ***Journal of Management Information Systems***, 25(4): 81-108.

Edelson, D. C., Gordin, D. N., & Pea, R. D. 1999. Addressing the challenges of inquiry-based learning through technology and curriculum design. ***Journal of the Learning Sciences***, 8(3-4): 391-450.

Eisenhardt, K. M., & Graebner, M. E. 2007. Theory building from cases: Opportunities and challenges. ***Academy of Management Journal***, 50(1): 25–32.

Entwistle, N. J. 1981a. ***Styles of learning and teaching: An integrated outline of educational psychology for students, teachers and lecturers***. Chichester: John Wiley.

Entwistle, N. J. 1981b. Styles of teaching and learning. ***Chistester: Wiley***.

Eppler, M. J. 2006. A comparison between concept maps, mind maps, conceptual diagrams, and visual metaphors as complementary tools for knowledge construction and sharing. ***Information Visualization***, 5(3): 202-210.

Eskildsen, J. K., Dahlgaard, J. J., & Norgaard, A. 1999. The impact of creativity and learning on business excellence. ***Total Quality Management***, 10(4-5): 523-530.

Evans, J. R., & Lindsay, W. M. 1996. ***The management and control of quality*** (3rd ed.). Minneapolis, MN: West Publishing Company.

Fann, K. T. 1970. ***Peirce's theory of abduction***: Martinus Nijhoff La Haya.

Filos, E. 2006. Smart organizations in the digital age. ***Integration of Information and Communication Technologies in Smart Organizations. Idea Group Publishing, Hershey***: 1-38.

Fiol, C. M., & Lyles, M. A. 1985. Organizational learning. ***Academy of management review***, 10(4): 803-813.

Fiske, S. T., & Taylor, S. E. 1991. Social cognition, 2nd. ***NY: McGraw-Hill***: 16-15.

Flowers, S. 2008. Harnessing the hackers: The emergence and exploitation of Outlaw Innovation. ***Research Policy***, 37(2): 177-193.

Ford, J. K., Quiñones, M. A., Sego, D. J., & Sorra, J. S. 1992. Factors affecting the opportunity to perform trained tasks on the job. ***Personnel Psychology***, 45(3): 511–527.

Fornell, C., & Larcker, D. F. 1981. Evaluating structural equation models with unobservable variables and measurement error. ***Journal of marketing research***, 18(1): 39-50.

Frederiksen, J. R., White, B. Y., & Gutwill, J. 1999. Dynamic mental models in learning science: The importance of constructing derivational linkages among models. ***Journal of Research in Science Teaching***, 36(7): 806-836.

Frese, M., & Fay, D. 2001. Personal initiative: An active performance concept for work in the 21st century. ***Research in organizational behavior***, 23: 133-187.

Gabelhouse, G. 2002. Certification, salaries & the IT market. ***Certification Magazine***, 4(12): 26-34.

Gee, J. P. 2003. What video games have to teach us about learning and literacy. ***Computers in Entertainment (CIE)***, 1(1): 20-20.

Gelfand, M. J., Erez, M., & Aycan, Z. 2007. Cross-cultural organizational behavior. ***Annual Review of Psychology***, 58: 479-514.

Gentner, D., & Stevens, A. L. 1983a. Mental models. ***LEA, Hillsdale, NJ***.

Gentner, D., & Stevens, A. L. 1983b. ***Mental models***. Hillsdale, NJ: LEA.

Gentner, D., & Stevens, A. L. 1983c. ***Mental models***: Psychology Press.

Glaser, B., & Strauss, A. 1967a. The discovery of grounded theory. 1967. ***Weidenfield & Nicolson, London***.

Glaser, B. G., & Strauss, A. 1967b. ***The discovery of grounded theory: Strategies for qualitative research***. Chicago: Aldine.

Gligor, D. M., Holcomb, M. C., & Stank, T. P. 2013. A multidisciplinary approach to supply chain agility: conceptualization and scale development. ***Journal of Business Logistics***, 34(2): 94-108.

Golann, S. E. 1963. Psychological study of creativity. ***Psychological Bulletin***, 60(6): 548.

Gomes, A., & Mendes, A. J. 2007. ***Learning to program-difficulties and solutions***. Paper presented at the International Conference on Engineering Education–ICEE.

Gordon, R., & Lovelock, J.-D. 2014. Global IT Spending on Pace to Grow 2.1 Percent in 2014, ***Forbes.com***, Vol. 2014: Gartner, Inc.

Gordon, S., & Ma, Q. 2003. Convergence of virus writers and hackers: Fact or fantasy?: Symantec Security Response, http://www.symantec.com. Accessed March 28, 2005.

Gorriz, C. M., & Medina, C. 2000. Engaging girls with computers through software games. ***Communications of the ACM***, 43(1): 42-49.

Graham, B. 2013. Innovation and Organisation: Towards an Art of Social System Design: Monash University.

Graham, P. 2008. ***Hackers & painters: big ideas from the computer age***: O'Reilly Media, Inc.

Grant, A. M., & Ashford, S. J. 2008. The dynamics of proactivity at work. ***Research in organizational behavior***, 28: 3-34.

Gray, P. H., & Meister, D. B. 2004. Knowledge sourcing effectiveness. ***Management Science***, 50(6): 821-834.

Greene, J. C., Caracelli, V. J., & Graham, W. F. 1989. Toward a conceptual framework for mixed-method evaluation designs. ***Educational evaluation and policy analysis***, 11(3): 255-274.

Greenglass, E., Schwarzer, R., Jakubiec, D., Fiksenbaum, L., & Taubert, S. 1999. ***The proactive coping inventory (PCI): A multidimensional research instrument***. Paper presented at the 20th International Conference of the Stress and Anxiety Research Society (STAR), Cracow, Poland.

Gressard, C. P., & Loyd, B. H. 1987. An investigation of the effects of math anxiety and sex on computer attitudes. ***School Science and Mathematics***, 87(2): 125-135.

Gros, B. 2007. Digital games in education: The design of games-based learning environments. ***Journal of Research on Technology in Education***, 40(1): 23-38.

Guía, E., Lozano, M. D., & Penichet, V. M. 2014. Educational games based on distributed and tangible user interfaces to stimulate cognitive abilities in children with ADHD. ***British Journal of Educational Technology***.

Gurteen, D. 1998. Knowledge, creativity and innovation. ***Journal of knowledge Management***, 2(1): 5-13.

Güven, M. 2008. Development of learning strategies scale: study of validation and reliability. ***World Applied Sciences Journal***, 4(1): 31-36.

Guzdial, M. 1994. Software-realized scaffolding to facilitate programming for science learning. ***Interactive Learning Environments***, 4(1): 001-044.

Hafner, K. 1998. ***Where wizards stay up late: The origins of the Internet***: Simon and Schuster.

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

Hair, J., Black, W., Babin, B., & Anderson, R. 2010a. Multivariate Data Analysis: New Jersey: Pearson Prentice Hall.

Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. 2010b. ***Multivariate data analyais*** (7th ed.). Upper Saddle River, NJ: Prentice Hall.

Halasz, F. G., & Moran, T. P. 1983. ***Mental models and problem solving in using a calculator***. Paper presented at the Proceedings of the SIGCHI conference on Human Factors in Computing Systems.

Hannemyr, G. 1997a. ***Hacking considered constructive***. Paper presented at the position paper for the 1997 Oksnoen Symposium on Pleasure and Technology, available at: http://home. sn. no/home/gisle/oks97. html.

Hannemyr, G. 1997b. ***Hacking considered constructive***. Paper presented at the Position paper for the 1997 Oksnoen Symposium on Pleasure and Technology, available at: http://home.sn.no/home/gisle/oks97.html.

Hartmann, B., Doorley, S., & Klemmer, S. R. 2008. Hacking, mashing, gluing: Understanding opportunistic design. ***Pervasive Computing, IEEE***, 7(3): 46-54.

Hay, K. 1999. ***The digital weather station: A study of learning with with 5D visualization***. Paper presented at the Annual meeting of the American Educational Research Association, Montreal, Canada.

Hayes, J. R. 1978. ***Cognitive psychology: Thinking and creating***: Dorsey.

Hebb, D. O. 1955. Drives and the CNS (conceptual nervous system). ***Psychological Review***, 62(4): 243.

Hedberg, B. 1981. How organizations learn and unlearn. In P. C. Nystrom, & W. H. Starbucks (Eds.), ***Handbook of organizational design***: 8 - 27. London: Oxford University Press.

Henderson, G. 1999. Learning with Diagrams. ***Australian Science Teachers' Journal***, 45(2): 17-25.

Hendrix, G. 1961. Learning by discovery. ***The Mathematics Teacher***: 290-299.

Hildreth, S. 2001. ***CRS Report to Congress: Cyberwarfare***. Washington, DC: Congressional Research Service

Hill, R. C., & Levenhagen, M. 1995. Metaphors and mental models: Sensemaking and sensegiving in innovative and entrepreneurial activities. ***Journal of Management***, 21(6): 1057–1074.

Holt, T., Soles, J., & Leslie, L. 2008. ***Characterizing malware writers and computer attackers in their own words***. Paper presented at the The 3rd International Conference on Information Warfare and Security: Peter Kiewit Institute, University of Nabraska, Omaha USA: 24-25 April 2008.

Holt, T. J., & Schell, B. H. 2010. ***Corporate Hacking and Technology-Driven Crime: Social Dynamics and Implications***: IGI Global.

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.

Holton, E. F. 1996. The flawed four-level evaluation model. ***Human Resource Development Quarterly***, 7(1): 5-21.

Horn, R. E. 1999. Information design: Emergence of a new profession. ***Information design***: 15-33.

Hu, L. t., & Bentler, P. M. 1999. Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives. ***Structural Equation Modeling: A Multidisciplinary Journal***, 6(1): 1-55.

Huang, H. M. 2002. Toward constructivism for adult learners in online learning environments. ***British Journal of Educational Technology***, 33(1): 27-37.

Hutchins, E. 1995. ***Cognition in the wild***. Cambridge, MA: MIT Press

Ibarra, H. 1999. Provisional selves: Experimenting with image and identity in professional adaptation. ***Administrative Science Quarterly***, 44(4): 764–791.

Jarvis, C. B., MacKenzie, S. B., & Podsakoff, P. M. 2003. A critical review of construct indicators and measurement model misspecification in marketing and consumer research. ***Journal of Consumer Research***, 30(2): 199–218.

Jeffries, R., Turner, A. A., Polson, P. G., & Atwood, M. E. 1981. The processes involved in designing software. ***Cognitive skills and their acquisition***, 255: 283.

Jelinek, M. 1979. ***Institutionalizing innovation: A study of organizational learning systems***: Praeger Publishers.

Jiang, Z., & Benbasat, I. 2004. Virtual product experience: Effects of visual and functional control of products on perceived diagnosticity and flow in electronic shopping. ***Journal of Management Information Systems***, 21(3): 111-147.

Jih, H. J., & Reeves, T. C. 1992. Mental models: A research focus for interactive learning systems. ***Educational Technology Research and Development***, 40(3): 39-53.

Johnson-Laird, P. N. 1983. ***Mental models: Towards a cognitive science of language, inference, and consciousness***: Harvard University Press.

Johnson-Laird, P. N. 1980. Mental models in cognitive science. ***Cognitive science***, 4(1): 71-115.

Jonassen, D. H. 1995. ***Operationalizing mental models: strategies for assessing mental models to support meaningful learning and design-supportive learning environments***. Paper presented at the The first international conference on Computer support for collaborative learning.

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

Jordan, T., & Taylor, P. A. 2004. ***Hacktivism and cyberwars: rebels with a cause?***: Psychology Press.

Karniol, R., & Ross, M. 1996. The motivational impact of temporal focus: Thinking about the future and the past. ***Annual review of psychology***, 47(1): 593-620.

Kashdan, T. B., & Fincham, F. D. 2002. " Facilitating creativity by regulating curiosity": Comment.

Kashdan, T. B., Rose, P., & Fincham, F. D. 2004. Curiosity and exploration: Facilitating positive subjective experiences and personal growth opportunities. ***Journal of personality assessment***, 82(3): 291-305.

Kastelein, R. 2014. Are ethical hackers the alchemists of our time...The masters of the binary evolution?

Kieras, D. E., & Bovair, S. 1984. The role of a mental model in learning to operate a device. ***Cognitive Science***, 8(3): 255-273.

Kim, D. H. 1998. The link between individual and organizational learning. In D. A. Klein (Ed.), ***The strategic management of intellectual capital***: 41-62: Butterworth-Heinemann.

Kim, T.-Y., Cable, D. M., & Kim, S.-P. 2005. Socialization tactics, employee proactivity, and person-organization fit. ***Journal of Applied Psychology***, 90(2): 232.

Kimbell, L. 2011. Rethinking design thinking: Part I. ***Design and Culture***, 3(3): 285-306.

Kipnis, D., & Schmidt, S. M. 1988. Upward-influence styles: Relationship with performance evaluations, salary, and stress. ***Administrative Science Quarterly***: 528-542.

Kirzner, I. M. 1985. ***Discovery and the capitalist process***: University of Chicago Press Chicago.

Kivinen, O., & Ristela, P. 2003. From constructivism to a pragmatist conception of learning. ***Oxford Review of Education***, 29(3): 363-375.

Klahr, D., & Kotovsky, K. (Eds.). 2013. ***Complex information processing: The impact of Herbert A. Simon***: Psychology Press.

Kluepfel, H. 1989. ***Foiling the wiley hacker: more than analysis and containment***. Paper presented at the Security Technology, 1989. Proceedings. 1989 International Carnahan Conference on.

Koedinger, K. R., & Anderson, J. R. 1993. Effective use of intelligent software in high school math classrooms.

Kofman, F., & Senge, P. M. 1993. Communities of commitment: The heart of learning organizations. ***Organizational Dynamics***, 22(2): 5-23.

Kosslyn, S. M. 1987. Seeing and imagining in the cerebral hemispheres: a computational approach. ***Psychological review***, 94(2): 148.

Kozlowski, S. W., & Bell, B. S. 2008. Team learning, development, and adaptation. ***Group learning***: 15-44.

Kozlowski, S. W., Gully, S. M., Brown, K. G., Salas, E., Smith, E. M., & Nason, E. R. 2001. Effects of training goals and goal orientation traits on multidimensional training outcomes and performance adaptability. ***Organizational Behavior and Human Decision Processes***, 85(1): 1–31.

Krueger, N., & Dickson, P. R. 1994. How believing in ourselves increases risk taking: Perceived self-efficacy and opportunity recognition. ***Decision Sciences***, 25(3): 385-400.

Lakhani, K. R., & Wolf, R. G. 2003. ***Why hackers do what they do: Understanding motivation and effort in free/open source software projects***: MIT Sloan School of Management.

Lakhani, K. R., & Wolf, R. G. 2005. Why hackers do what they do: Understanding motivation and effort in free/open source software projects. ***Perspectives on free and open source software***, 1: 3-22.

Lakoff, G., & Johnson, M. 2003. ***Metaphors we live by*** (2nd ed.). Chicago: University of Chicago Press.

Langer, E. J. 1989. Minding matters: The consequences of mindlessness–mindfulness. ***Advances in experimental social psychology***, 22: 137-173.

Lawrence, P. R., & Lorsch, J. W. 1967. Organization and Environment: Managing Differentiation and Integration. ***Homewood, IL: Irwin. LawrenceOrganization and Environment: Managing Differentiation and Integration1967***.

Leahey, T. H., & Harris, R. J. 1989a. ***Human learning***: Prentice Hall Englewood Cliffs, NJ.

Leahey, T. H., & Harris, R. J. 1989b. ***Learning and cognition*** (2nd ed.). Englewood Cligffs, NJ Prentice Hall.

Leiner, B. M., Cerf, V. G., Clark, D. D., Kahn, R. E., Kleinrock, L., Lynch, D. C., Postel, J., Roberts, L. G., & Wolff, S. 2009. A brief history of the Internet. ***ACM SIGCOMM Computer Communication Review***, 39(5): 22-31.

Lenhart, A., Kahne, J., Middaugh, E., Macgill, A. R., Evans, C., & Vitak, J. 2008. Teens, Video Games, and Civics: Teens' Gaming Experiences Are Diverse and Include Significant Social Interaction and Civic Engagement. ***Pew Internet & American Life Project***.

Levesque, L. L., Wilson, J. M., & Wholey, D. R. 2001. Cognitive divergence and shared mental models in software development project teams. ***Journal of Organizational Behavior***, 22(2): 135-144.

Levy, S. 1984. Hackers, New York: Anchor: Doubleday.

Levy, S. 2001. ***Hackers: Heroes of the computer revolution***. New York: Penguin Books.

Libicki, M. C., Senty, D., & Pollak, J. 2014. ***Hackers Wanted: An Examination of the Cybersecurity Labor Market***: Rand Corporation.

Lieberman, H., Paternò, F., Klann, M., & Wulf, V. 2006. ***End-user development: An emerging paradigm***: Springer.

Lim, D. H., & Johnson, S. D. 2002. Trainee perceptions of factors that influence learning transfer. ***International journal of training and development***, 6(1): 36-48.

Linn, M. C. 1985. Fostering equitable consequences from computer learning environments. ***Sex Roles***, 13(3-4): 229-240.

Litman, J. 2005. Curiosity and the pleasures of learning: Wanting and liking new information. ***Cognition & emotion***, 19(6): 793-814.

Little, B. R. 1983. Personal projects a rationale and method for investigation. ***Environment and behavior***, 15(3): 273-309.

Littman, D. C., Pinto, J., Letovsky, S., & Soloway, E. 1987. Mental models and software maintenance. ***Journal of Systems and Software***, 7(4): 341–355.

Lockheed, M. E. 1985. Women, girls, and computers: A first look at the evidence. ***Sex Roles***, 13(3-4): 115-122.

Loewenstein, G. 1994. The psychology of curiosity: A review and reinterpretation. ***Psychological Bulletin***, 116(1): 75.

Loyd, B. H., & Gressard, C. 1984. The effects of sex, age, and computer experience on computer attitudes. ***AEDS journal***, 18(2): 67-77.

Mac Donald Jr, A. 1970. Revised scale for ambiguity tolerance: Reliability and validity. ***Psychological reports***, 26(3): 791-798.

MacCallum, R. C., Widaman, K. F., Zhang, S., & Hong, S. 1999. Sample size in factor analysis. ***Psychological Methods***, 4(1): 84.

MacDonald, J., A Po, & Games, R. G. 1976. Some characteristics of those who hold positive and negative attitudes toward homosexuals. ***Journal of Homosexuality***, 1(1): 9-27.

MacDonald Jr, A. 1970. Revised scale for ambiguity tolerance: Reliability and validity. ***Psychological Reports***, 26(3): 791-798.

MacLean, A., Carter, K., Lövstrand, L., & Moran, T. 1990. ***User-tailorable systems: pressing the issues with buttons***. Paper presented at the Proceedings of the SIGCHI conference on Human factors in computing systems.

Madden, J. 2015. Leveraging Design: How the Design Process and a Design Framework Strengthen Nonprofit Management Pedagogy. ***Journal of Nonprofit Education and Leadership***, 5(1): 6-11.

Malone, T. W. 1980. ***What makes things fun to learn? Heuristics for designing instructional computer games***. Paper presented at the Proceedings of the 3rd ACM SIGSMALL symposium and the first SIGPC symposium on Small systems.

Marmon, W. 2011. Main cyber threats now coming from governments as "state actors", ***European Affairs***. Washington D.C.: The European Institute.

Marsh, H. W., Hau, K.-T., Balla, J. R., & Grayson, D. 1998. Is more ever too much? The number of indicators per factor in confirmatory factor analysis. ***Multivariate Behavioral Research***, 33(2): 181-220.

Martindale, C. 2001. Oscillations and analogies: Thomas Young, MD, FRS, genius. ***American Psychologist***, 56(4): 342.

Marton, F., & Säljö, R. 1976a. On qualitative differences in learning—ii Outcome as a function of the learner's conception of the task. ***British Journal of Educational Psychology***, 46(2): 115-127.

Marton, F., & Säljö, R. 1976b. On qualitative differences in learning: I—outcome and process. ***British Journal of Educational Psychology***, 46(1): 4-11.

Marton, F., & Säljö, R. 1976c. On Qualitative Differences in Learning: I—Outcome and process*. ***British journal of educational psychology***, 46(1): 4-11.

Massimini, F., Csikszentmihalyi, M., & Carli, M. 1987. The Monitoring of Optimal Experience A Tool for Psychiatric Rehabilitation. ***The Journal of Nervous and Mental Disease***, 175(9): 545-549.

Mathieu, J. E., Heffner, T. S., Goodwin, G. F., Salas, E., & Cannon-Bowers, J. A. 2000. The influence of shared mental models on team process and performance. ***Journal of applied psychology***, 85(2): 273.

Mathieu, J. E., & Taylor, S. R. 2006. Clarifying conditions and decision points for mediational type inferences in organizational behavior. ***Journal of Organizational Behavior***, 27(8): 1031-1056.

Mayer, R. E. 1981. The psychology of how novices learn computer programming. ***ACM Computing Surveys (CSUR)***, 13(1): 121–141.

Mccall, M. W., Lombardo, M. M., & Morrison, A. M. 1988. ***Lessons of experience: How successful executives develop on the job***: Simon and Schuster.

McDougall, W. 1926. Outline of abnormal psychology. ***American Journal of Physical Medicine & Rehabilitation***, 5(6): 473.

Miles, R. H., & Cameron, K. S. 1982. ***Coffin nails and corporate strategies***: Prentice Hall.

Miller, D., & Friesen, P. H. 1980. Momentum and revolution in organizational adaptation. ***Academy of management journal***, 23(4): 591-614.

Milliken, F. J. 1987. Three types of perceived uncertainty about the environment: State, effect, and response uncertainty. ***Academy of Management review***, 12(1): 133-143.

MIT, T. M. R. C. o. 2014. TMRC History, Vol. 2014.

Moneta, G. B., & Csikszentmihalyi, M. 1996. The effect of perceived challenges and skills on the quality of subjective experience. ***Journal of personality***, 64(2): 275-310.

Morecroft, J. D. 1984. Strategy support models. ***Strategic Management Journal***, 5(3): 215–229.

Murray, J. H. 1997. ***Hamlet on the holodeck: The future of narrative in cyberspace***: Simon and Schuster.

Mylopoulos, M., & Regehr, G. 2009. How student models of expertise and innovation impact the development of adaptive expertise in medicine. ***Medical Education***, 43(2): 127-132.

Nahm, A. Y., Rao, S. S., Solis-Galvan, L. E., & Ragu-Nathan, T. 2002. The Q-sort method: assessing reliability and construct validity of questionnaire items at a pre-testing stage. ***Journal of Modern Applied Statistical Methods***, 1(1): 15.

Nakamura, J., & Csikszentmihalyi, M. 2002. The concept of flow. ***Handbook of positive psychology***: 89-105.

Nanja, M., & Cook, C. R. 1987. An analysis of the on-line debugging process. In G. M. Olson, S. Sheppard, & E. Soloway (Eds.), ***Empirical studies of programmers: Second workshop***: 172–184. Washington, DC: Ablex Publishing Corp.

Nassi, I., & Shneiderman, B. 1973. Flowchart techniques for structured programming. ***ACM Sigplan Notices***, 8(8): 12-26.

Navon, D. 1977. Forest before trees: The precedence of global features in visual perception. ***Cognitive psychology***, 9(3): 353-383.

Nickell, G. S., & Pinto, J. N. 1986. The computer attitude scale. ***Computers in human behavior***, 2(4): 301-306.

Nikitina, S. 2012. Hackers as Tricksters of the Digital Age: Creativity in Hacker Culture. ***The Journal of Popular Culture***, 45(1): 133-152.

Noe, R. A., & Schmitt, N. 1986. The influence of trainee attitudes on training effectiveness: Test of a model. ***Personnel Psychology***, 39(3): 497-523.

Norman, D. A. 1983a. Some observations on mental models. ***Mental models***, 1.

Norman, D. A. 1983b. Some observations on mental models. ***Mental Models***, 7(112): 7–14.

Norman, D. A. 1986a. Cognitive engineering. In D. N. Norman, & S. W. Draper (Eds.), ***User centered system design***: 31–61. Hillsdale, NJ: Lawrence Erlbaum Associates.

Norman, D. A. 1986b. Cognitive engineering. ***User centered system design***: 31-61.

Norton, R. W. 1975. Measurement of ambiguity tolerance. ***Journal of Personality Assessment***, 39(6): 607-619.

Novak, J. D. 1990a. Concept mapping: A useful tool for science education. ***Journal of research in science teaching***, 27(10): 937-949.

Novak, J. D. 1990b. Concept maps and Vee diagrams: Two metacognitive tools to facilitate meaningful learning. ***Instructional Science***, 19(1): 29-52.

Novak, J. D., Bob Gowin, D., & Johansen, G. T. 1983. The use of concept mapping and knowledge vee mapping with junior high school science students. ***Science education***, 67(5): 625-645.

Novak, J. D., & Cañas, A. J. 2006a. The theory underlying concept maps and how to construct them: Technical Report IHMC Cmap Tools 2006-01. Retrieved 21/6/07, Florida Institute for Human and Machine Cognition, from http://cmap.ihmcus/Publications/ResearchPapers/TheoryUnderlyingConceptMaps.pdf.

Novak, J. D., & Cañas, A. J. 2006b. The theory underlying concept maps and how to construct them. ***Florida Institute for Human and Machine Cognition***, 1.

Nurmi, J.-E. 1991. How do adolescents see their future? A review of the development of future orientation and planning. ***Developmental review***, 11(1): 1-59.

Oblinger, D. 2006. Simulations, games, and learning. ***ELI White Paper***.

Ocker, R., Hiltz, S. R., Turoff, M., & Fjermestad, J. 1995a. The effects of distributed group support and process structuring on software requirements development teams: Results on creativity and quality. ***Journal of Management Information Systems***: 127-153.

Ocker, R., Hiltz, S. R., Turoff, M., & Fjermestad, J. 1995b. The effects of distributed group support and process structuring on software requirements development teams: Results on creativity and quality. ***Journal of Management Information Systems***, 12(3): 127-153.

Owen, W., & Sweeney, R. 2002a. Ambiguity tolerance, performance, learning, and satisfaction: A research direction. ***School of Computer and Information Sciences***.

Owen, W., & Sweeney, R. 2002b. Ambiguity tolerance, performance, learning, and satisfaction: A research direction. Mobile, AL: School of Computer and Information Sciences, University of South Alabama.

Parker, S. K., Williams, H. M., & Turner, N. 2006. Modeling the antecedents of proactive behavior at work. ***Journal of applied psychology***, 91(3): 636.

Pasquale, F. 2015. ***Black Box Society: The Secret Algorithms that Control Money and Information***: Harvard University Press.

Pea, R. D., & Kurland, D. M. 1984. On the cognitive effects of learning computer programming. ***New ideas in psychology***, 2(2): 137-168.

Peirce, C. S. 1974. ***Collected papers of charles sanders peirce***: Harvard University Press.

Peirce, C. S. 1997. ***Pragmatism as a principle and method of right thinking: The 1903 Harvard lectures on pragmatism***: SUNY Press.

Pennington, N. 1987. Comprehension strategies in programming. In G. M. Olson, S. Sheppard, & E. Soloway (Eds.), ***Empirical studies of programmers: Second workshop***: 100–113. Washington, DC: Ablex Publishing Corp.

Peretti, K. K. 2008. Data breaches: what the underground world of carding reveals. ***Santa Clara Computer & High Tech. LJ***, 25: 375.

Peterson, C., & Seligman, M. E. 2003. Character strengths before and after September 11. ***Psychological Science***, 14(4): 381-384.

Piaget, J. 1973. To understand is to invent: The future of education.

Podsakoff, P. M., MacKenzie, S. B., Lee, J.-Y., & Podsakoff, N. P. 2003. Common method biases in behavioral research: a critical review of the literature and recommended remedies. ***Journal of Applied Psychology***, 88(5): 879-903.

Poeter, D. 2012. DefCon: NSA Boss Asks Hackers to Join the Dark Side. ***PC Magazine***, 29.

Preacher, K. J., & Hayes, A. F. 2004. SPSS and SAS procedures for estimating indirect effects in simple mediation models. ***Behavior Research Methods, Instruments, & Computers***, 36(4): 717-731.

Preacher, K. J., & Hayes, A. F. 2008. Asymptotic and resampling strategies for assessing and comparing indirect effects in multiple mediator models. ***Behavior Research Methods***, 40(3): 879-891.

Provenzo Jr, E. F. 1991. ***Video kids: Making sense of Nintendo***: Harvard University Press.

Pylyshyn, Z. W. 1984. ***Computation and cognition***: Cambridge Univ Press.

Quiñones, M. A., Ford, J. K., & Teachout, M. S. 1995. The relationship between work experience and job performance: A conceptual and meta-analytic review. ***Personnel Psychology***, 48(4): 887–910.

Quintana, C., Eng, J., Carra, A., Wu, H.-K., & Soloway, E. 1999. ***Symphony: A case study in extending learner-centered design through process space analysis***. Paper presented at the Proceedings of the SIGCHI conference on Human Factors in Computing Systems.

Ramalingam, V., LaBelle, D., & Wiedenbeck, S. 2004. ***Self-efficacy and mental models in learning to program***. Paper presented at the ACM SIGCSE Bulletin.

Ramsden, P. 1992. ***Learning to teach in higher education***. London: Routledge.

Rasmussen, J. 1979a. On the structure of knowledge-a morphology of metal models in a man-machine system context: Riso National Laboratory, Denmark, RISO-M-2192.

Rasmussen, J. 1979b. ***On the structure of knowledge: a morphology of mental models in a man-machine system context***: Risø National Laboratory.

Rasmussen, J. 1983. Skills, rules, and knowledge; signals, signs, and symbols, and other distinctions in human performance models. ***Systems, Man and Cybernetics, IEEE Transactions on***(3): 257-266.

Raymond, E. S. 1999. A brief history of hackerdom. ***DiBona, Ockman y Stone, Open Sources, y www. tuxedo. org/~ esr/writings/cathedral-bazaar/hacker-history/(primera versión 1992)***.

Raymond, E. S. 2001. ***The Cathedral & the Bazaar: Musings on linux and open source by an accidental revolutionary***: " O'Reilly Media, Inc.".

Reber, B. H., Kaufman, S. E., & Cropp, F. 2000. Assessing Q-Assessor: A validation study of computer-based Q sorts versus paper sorts. ***Operant Subjectivity***, 23(4): 192-209.

Reid, A., & Petocz, P. 2004. Learning domains and the process of creativity. ***The Australian Educational Researcher***, 31(2): 45-62.

Reio, T. G., & Wiswell, A. 2000. Field investigation of the relationship among adult curiosity, workplace learning, and job performance. ***Human Resource Development Quarterly***, 11(1): 5-30.

Reiser, B. J. 2004. Scaffolding complex learning: The mechanisms of structuring and problematizing student work. ***The Journal of the Learning Sciences***, 13(3): 273-304.

Ricci, K. E., Salas, E., & Cannon-Bowers, J. A. 1996. Do computer-based games facilitate knowledge acquisition and retention? ***Military Psychology***, 8(4): 295.

Robillard, P. N. 1999. The role of knowledge in software development. ***Communications of the ACM***, 42(1): 87-92.

Robins, A., Rountree, J., & Rountree, N. 2003. Learning and teaching programming: A review and discussion. ***Computer Science Education***, 13(2): 137-172.

Rosenbaum, R. 1971. Secrets of the little blue box. ***Esquire Magazine***, 76: 117-125,222.

Rosenzweig, R. 1998. Wizards, bureaucrats, warriors, and hackers: Writing the history of the Internet. ***American Historical Review***: 1530-1552.

Rosoff, M. 2012. Mark Zuckerberg Explains 'The Hacker Way'To Facebook Investors. ***San Francisco Chronicle***.

Rouse, W. B., & Morris, N. M. 1986. On looking into the black box: Prospects and limits in the search for mental models. ***Psychological bulletin***, 100(3): 349.

Saks, A. M., & Ashforth, B. E. 1996. Proactive socialization and behavioral self-management. ***Journal of Vocational Behavior***, 48(3): 301-323.

Sarkar, K., Drescher, D., & Scanlon, M. 2007. Working memory improvement following web-based cognitive training. ***Bay Area Neuroscience Gathering, San Francisco. Retrieved from http://hcp. lumosity. com/research/completed***.

Scaife, M., & Rogers, Y. 1996. External cognition: how do graphical representations work? ***International journal of human-computer studies***, 45(2): 185-213.

Scanlon, M., Drescher, D., & Sarkar, K. 2007. Improvement of visual attention and working memory trough a web-based cognitive training program. ***A Lumos Labs White Paper***.

Schaeken, W., Johnson-Laird, P., & d'Ydewalle, G. 1996. Mental models and temporal reasoning. ***Cognition***, 60(3): 205-234.

Scheffler, I. 2013. ***Four pragmatists: A critical introduction to Peirce, James, Mead, and Dewey***: Routledge.

Schell, B. H., & Dodge, J. L. 2002. ***The hacking of America: Who's doing it, why, and how***: Greenwood Publishing Group Inc.

Schell, B. H., & Melnychuk, J. 2010a. Female and male hacker conferences attendees: Their autism-spectrum quotient (AQ) scores and self-reported adulthood experiences, ***Cyber crime: Concepts, methodologies, tools and applications***, Vol. 144: 1075–1099. Hershey, PA: Information Science Reference.

Schell, B. H., & Melnychuk, J. 2010b. Female and Male Hacker Conferences Attendees: Their Autism-Spectrum Quotient (AQ) Scores and Self-Reported Adulthood Experiences. ***Corporate hacking and technology driven crime: Social dynamics and implications***: 144-169.

Schifreen, R. 1994. What motivates a hacker? ***Network Security***, 1994(8): 17-19.

Schlesinger, J. 2010. ***Founding a Hackerspace***. Worcester Polytechnic Institute.

Schneider, B. 2006. What is a hacker?, ***Schneier on Security, https://www.schneier.com/blog/archives/2006/09/what_is_a_hacke.html***.

Schneider, W. 1985. Training high-performance skills: Fallacies and guidelines. ***Human Factors: The Journal of the Human Factors and Ergonomics Society***, 27(3): 285-300.

Schrader, S., Riggs, W. M., & Smith, R. P. 1993. Choice over uncertainty and ambiguity in technical problem solving. ***Journal of Engineering and Technology Management***, 10(1): 73-99.

Schubert, R., Brown, M., Gysler, M., & Brachinger, H. W. 1999. Financial decision-making: are women really more risk-averse? ***American Economic Review***: 381-385.

Schubert, R., Brown, M., Gysler, M., & Brachinger, H. W. 2000. ***Gender specific attitudes towards risk and ambiguity: an experimental investigation***: Institut für Wirtschaftsforschung, Eidgenössische Technische Hochschule.

Segaller, S. 1999. ***Nerds 2.0. 1: a brief history of the Internet***: TV Books, LLC.

Senge, P. M. 1990. The fifth discipline: The art and practice of the learning organization. New York: Currency: Doubleday.

Senge, P. M., & Sterman, J. D. 1992. Systems thinking and organizational learning: Acting locally and thinking globally in the organization of the future. ***European journal of operational research***, 59(1): 137-150.

Senge, P. M., & Suzuki, J. 1994. ***The fifth discipline: The art and practice of the learning organization***: Currency Doubleday New York.

Shimomura, T., & Markoff, J. 1995. ***Takedown: The Pursuit and Capture of Kevin Mitnick, America's Most Wanted Computer Outlaws-by the Man Who Did It***: Hyperion Press.

Simon, H. A. 1977. The structure of ill-structured problems, ***Models of discovery***: 304-325: Springer.

Soloway, E., & Ehrlich, K. 1984. Empirical studies of programming knowledge. ***IEEE Transactions on Software Engineering***(5): 595–609.

Sonnentag, S., Niessen, C., & Volmer, J. 2006. Expertise in software design.

Spertus, E. 1991. Why are there so few female computer scientists?

Squire, K. 2003. Video games in education. ***Int. J. Intell. Games & Simulation***, 2(1): 49-62.

Staddon, J. E. 1975. Learning as adaptation. ***Handbook of learning and cognitive processes***, 2: 37-98.

Staggers, N., & Norcio, A. F. 1993. Mental models: concepts for human-computer interaction research. ***International Journal of Man-machine studies***, 38(4): 587-605.

Sterling, B. 1992. ***The Hacker Crackdown, law and disorder on the electronic frontier***. New York: Bantam.

Sternberg, R. J. 2000. Images of mindfulness. ***Journal of Social Issues***, 56(1): 11-26.

Sternberg, R. J. 2001. What is the common thread of creativity? Its dialectical relation to intelligence and wisdom. ***American Psychologist***, 56(4): 360.

Sternberg, R. J., & Lubart, T. I. 1995. ***Defying the crowd: Cultivating creativity in a culture of conformity***: Free Press.

Stoycheva, K. 1998. Ambiguity tolerance: Adolescents' responses to uncertainty in life: Project Report. Education Resources Information Center.

Stoytcheva, K. 2003. Tolerance of ambiguity. ***Pleven: Lege Artis (en bulgare)***.

Strauss, A., & Corbin, J. 1990a. ***Basics of qualitative research: Grounded theory procedures and techniques***. Newbury Park, CA: Sage.

Strauss, A., & Corbin, J. M. 1990b. ***Basics of qualitative research: Grounded theory procedures and techniques***: Sage Publications, Inc.

Summers, T. C., Lyytinen, K. J., & Gaskin, J. 2014. How Hackers Think: Understanding the Mental Models and Cognitive Patterns of High-Tech Wizards: Case Western Reserve University.

Summers, T. C., Lyytinen, K. J., Lingham, T., & Pierce, E. A. 2013. How Hackers Think: A Study of Cybersecurity Experts and Their Mental Models, ***Third Annual International Conference on Engaged Management Scholarship***. Atlanta, Georgia.

Sussman, S. W., & Siegal, W. S. 2003. Informational influence in organizations: An integrated approach to knowledge adoption. ***Information Systems Research***, 14(1): 47–65.

Tashakkori, A., & Teddlie, C. 1998. ***Mixed methodology: Combining qualitative and quantitative approaches***: Sage.

Taylor, P. A. 1999. ***Hackers: crime in the digital sublime***: Psychology Press.

Taylor, S. E., Pham, L. B., Rivkin, I. D., & Armor, D. A. 1998. Harnessing the imagination: Mental simulation, self-regulation, and coping. ***American psychologist***, 53(4): 429.

Teddlie, C., & Tashakkori, A. 2009. ***Foundations of mixed methods research: Integrating quantitative and qualitative approaches in the social and behavioral sciences***: Sage Publications Inc.

Temple, L., & Lips, H. M. 1989. Gender differences and similarities in attitudes toward computers. ***Computers in Human Behavior***, 5(4): 215-226.

Thomas, D. 2002. ***Hacker culture***: U of Minnesota Press.

Thomas, D. M., & Watson, R. T. 2002. Q-sorting and MIS research: A primer. ***Communications of the Association for Information Systems***, 8(1): 9.

Thomas, J. 2001. Ethics of Hacktivism. ***Information Security Reading Room***, 12.

Thompson, B., & Daniel, L. G. 1996. Factor analytic evidence for the construct validity of scores: A historical overview and some guidelines. ***Educational and psychological measurement***, 56(2): 197-208.

Thompson, J. D. 1967. Organizations in action. . ***SHAFRITZ, Jay M.; OTT, J. Steven. Classics of organization theory***, 4.

Tittel, E. 2000. Charting the certification business. ***Certification Magazine***.

Tiwana, A., & Mclean, E. R. 2003. Expertise integration and creativity in information systems development. ***Journal of Management Information Systems***, 22(1): 13-43.

Trahan, D. E., & Quintana, J. W. 1990. Analysis of gender effects upon verbal and visual memory performance in adults. ***Archives of Clinical Neuropsychology***, 5(4): 325-334.

Trevino, L. K., & Webster, J. 1992. Flow in computer-mediated communication electronic mail and voice mail evaluation and impacts. ***Communication research***, 19(5): 539-573.

Tronco, T. R. 2010. A Brief History of the Internet, ***New Network Architectures***: 1-11: Springer.

Tufte, E. R., & Graves-Morris, P. 1983. ***The visual display of quantitative information***: Graphics press Cheshire, CT.

Turkle, S. 1984. ***The second self***: Simon and Schuster New York.

Turkle, S. 2005. ***The second self*** (Twentieth Anniversary Edition ed.). Cambridge, MA: The MIT Press.

Turkle, S., & Papert, S. 1990. Epistemological pluralism: Styles and voices within the computer culture. ***Signs***: 128-157.

Turner, D. W. 2010. Qualitative interview design: A practical guide for novice investigators. ***The Qualitative Report***, 15(3): 754–760.

Ullman, S. 1989. Aligning pictorial descriptions: An approach to object recognition. ***Cognition***, 32(3): 193-254.

Urban, K. 2003. Toward a componential model of creativity. In D. Ambrose, L. M. Cohen, & A. J. Tannenbaum (Eds.), ***Creative intelligence: Toward theoretic integration***. Cresskill, NJ: Hampton Press Inc.

Van Beveren, J. 2000. A conceptual model of hacker development and motivation. ***Journal of E-Business***, 1(2): 1-9.

Van de Ven, A. H. 2007. ***Engaged Scholarship: A Guide for Organizational and Social Research: A Guide for Organizational and Social Research***: Oxford University Press.

Van der Veer, G. C. 1989. Individual differences and the user interface. ***Ergonomics***, 32(11): 1431-1449.

Van Exel, J., & de Graaf, G. 2005. Q methodology: A sneak preview: Online document. http://www.qmethodology.net/PDF/Q-methodology.

Van Gelder, T. 2007. The rationale for Rationale™. ***Law, probability and risk***, 6(1-4): 23-42.

Vandenbosch, B., & Higgins, C. 1996. Information acquisition and mental models: An investigation into the relationship between behaviour and learning. ***Information Systems Research***, 7(2): 198–214.

Venkatesh, V., Morris, M. G., & Ackerman, P. L. 2000. A longitudinal field investigation of gender differences in individual technology adoption decision-making processes. ***Organizational behavior and human decision processes***, 83(1): 33-60.

Vernon, P. E. 1970. ***Creativity: Selected readings***. Middlesex: Penguin.

Voiskounsky, A. E., & Smyslova, O. V. 2003. Flow-based model of computer hackers' motivation. ***CyberPsychology & Behavior***, 6(2): 171–180.

von Krogh, G., & Von Hippel, E. 2003. Special issue on open source software development. ***Research Policy***, 32(7): 1149-1157.

Vosniadou, S., & Brewer, W. F. 1992. Mental models of the earth: A study of conceptual change in childhood. ***Cognitive Psychology***, 24(4): 535-585.

Vygotsky, L. S. 1978. Mind and society: The development of higher mental processes: Cambridge, MA: Harvard University Press.

Vygotsky, L. S. 1986. ***Thought and language (rev. ed.)***. Cambridge, MA: MIT Press.

Wall, D. 2007. ***Cybercrime: The transformation of crime in the information age***: Polity.

Wanberg, C. R., & Kammeyer-Mueller, J. D. 2000. Predictors and outcomes of proactivity in the socialization process. ***Journal of Applied Psychology***, 85(3): 373.

Wark, M. 2006. Hackers. ***Theory, Culture & Society***, 23(2-3): 320-322.

Weick, K. E. 1993. The collapse of sensemaking in organizations: The Mann Gulch disaster. ***Administrative Science Quarterly***, 38(4): 628-652.

Weick, K. E., & Roberts, K. H. 1993. Collective mind in organizations: Heedful interrelating on flight decks. ***Administrative science quarterly***: 357-381.

Weizenbaum, J. 1976. Computer power and human reason: From judgment to calculation.

Wiedenbeck, S., Ramalingam, V., Sarasamma, S., & Corritore, C. 1999. A comparison of the comprehension of object-oriented and procedural programs by novice programmers. ***Interacting with Computers***, 11(3): 255–282.

Wilder, G., Mackie, D., & Cooper, J. 1985. Gender and computers: Two surveys of computer-related attitudes. ***Sex Roles***, 13(3): 215-228.

Wiles, W. 2010. Insight: Design Hacks, Vol. 2015: ICON Magazine.

Williams, J. S. 1976. Proactivity and Reinforcement: The Contingency of Social Behavior. ***Small Group Behavior***, 7(3): 317-329.

Williams, M. D., Hollan, J. D., & Stevens, A. L. 1983a. In D. Gentner, & A. L. Stevens (Eds.), ***Mental models***: 131–153. Hillsdale, NJ: Erlbaum.

Williams, M. D., Hollan, J. D., & Stevens, A. L. 1983b. Human reasoning about a simple physical system. ***Mental models***: 131-154.

Winn, J., & Neary, M. 2011. Hackers are vital to the university culture of openness and innovation. ***The Guardian***: [Online] October 18, 2011.

Winn, W. 1993. A conceptual basis for educational applications of virtual reality. ***Technical Publication R-93-9, Human Interface Technology Laboratory of the Washington Technology Center, Seattle: University of Washington***.

Wolfberg, A. 2014. ***A theory of overload and equivocality effects on learning during knowledge transfer within policy making dyads*** Case Western Reserve University, Cleveland, OH.

Xu, Z., Hu, Q., & Zhang, C. 2013. Why computer talents become computer hackers. ***Communications of the ACM***, 56(4): 64-74.

Yoo, Y., Boland Jr, R. J., & Lyytinen, K. 2006. From organization design to organization designing. ***Organization Science***, 17(2): 215-229.

Young, R. M. 1981. The machine inside the machine: Users' models of pocket calculators. ***International Journal of Man-Machine Studies***, 15(1): 51-85.

Zenasni, F., Besançon, M., & Lubart, T. 2008. Creativity and tolerance of ambiguity: An empirical study. ***The Journal of Creative Behavior***, 42(1): 61-73.

Zhou, J. 2003. When the presence of creative coworkers is related to creativity: role of supervisor close monitoring, developmental feedback, and creative personality. ***Journal of Applied Psychology***, 88(3): 413–422.