Sim-Cyberpunk: Serious Play, Hackers and Capture the Flag Competitions

by

Alex Dean Cybulski

A thesis submitted in conformity with the requirements
for the degree of Doctorate in Philosophy

Faculty of Information
University of Toronto

Sim-Cyberpunk: Serious Play, Hackers and Capture the Flag Competitions

Alex Dean Cybulski

Doctorate of Information

Faculty of Information
University of Toronto

2023

Abstract

Capture the flag (CTF) is a style of game developed within the hacker community to simulate/emulate the practice of vulnerability research. In a CTF players identify security vulnerabilities in information systems and exploit these flaws to undermine their operations, which gives them access to a “flag” which they score for points used to win a competition. An exploratory study of this game, this dissertation uses ethnographic methods including observation of three CTF competitions and semi-structured interviews with 47 CTF players and designers. Analysis of this data considers the co-constitution of the game through the practices of its designers and players, concerning the values of the hacker community and its linkages to the information security industry whose membership constitutes the preponderance of CTF participants. Utilizing Sara Grimes and Andrew Feenberg’s (2009) theory of “games as sites of social rationalization” this paper argues that CTF has been instrumentalized as a tool of cultural reproduction. This function of CTF is used to discursively shape and sustain knowledge acquisition, identity formation and work in the cybersecurity industry through the affordances of play in alignment with hacker values, translating intellectual capital into social capital through playful game systems.

Acknowledgements

A dissertation has one author, but like a ship with one captain, many hands keep it afloat and tack towards its destination. I am deeply indebted to my committee, fellow academics, research participants, close friends and family that supported the research and writing process to make this dissertation a reality, particularly when that process of reification was messy, difficult, or contentious (and when I was too).

My express gratitude to the hacker communities, conferences, CTF teams, secretaries, media officers and research participants including players and organizers who allowed me to perform observation at three different fieldwork sites in both Canada and the United States. This dissertation was part of a lifelong dream to closely work with and study the fascinating technical practices of hackers that I have been obsessed with since boyhood. I have found researching and writing this project immensely satisfying and that is due in no small part to the unparalleled access I was given to the hacker community by generous individuals. In response to this unparalleled generosity, I am committing 100 hours of my time back to the hacker/security community as a volunteer at various conferences and events over the next 5 years as the best gesture of reciprocity I can offer.

There are many individuals to thank for the support I received in producing this project, chief amongst them is Dr. Sara Grimes. Sara is a visionary. I know that because she had the vision to understand this project from vague descriptions that I came up with in the earliest days of her supervision and who coaxed along my research, understanding it better than I did in many cases. The greatest gift Sara ever gave me was the language to write about games in a way that makes sense to my understanding of the world. I'm humbled to have been mentored by someone whose research is not only extremely applied and diverse, but also someone I consider to have a towering intellect in the field of Game Studies. Similarly, Dr. Leslie Reagan Shade has provided mentorship and encouragement since we met on an elevator in September of 2012 when I was a fresh Masters' student. Leslie's prolific and timely feedback was the fuel that kept me writing, but her wit and personable qualities always helped me feel like I was seen and understood by at least one other person in academia. Ultimately a dissertation on hackers and hacker culture wouldn't have been possible without Dr. Alessandro Delfanti who joined this project mid-stream and provided a tremendous amount of energy, direction and feedback which has shaped this

project and influenced my thinking. Alessandro created and supported opportunities for me to teach that were immensely valuable in allowing me to stay in this graduate program. Finally, special thanks to Dr. Alan Galey who supported me through the comprehensive exam and provided excellent guidance in the preliminary stages of this project.

I hold a lot of academics outside my committee in high esteem for their guidance, mentorship and camaraderie which sustained me over my PhD. Outstanding here is Dr Rhonda McEwen, an institution within the Faculty of Information and at the Communication, Culture and Information Technology department at UTM. There are many institutions in higher education, but none supported my professional development to the extent that Rhonda did or helped me keep my bills paid on time. Thank you to Dr. Jennifer Whitson and Dr. Paula Bialski who, at various (different) times, provided me with opportunities to present my work and answered many questions you'd have thought I would have figured out before even becoming a graduate student. Hacker studies as a discipline probably couldn't exist without the influence of Dr. Gabriella Coleman and she frequently gave me cool opportunities to study this field that were unfathomable to me when I started. Thanks to Dr. Molly Sauter who was influential to this project in helping me to become acquainted with ethnographic research, but also for persuading me to be audacious and do fieldwork at places I was originally too self-conscious to approach. Two other people I'd like to thank are Dr. Victoria Kannen and Dr. Aaron Langille for publishing some of my early work on this dissertation.

I am also lucky to have a ton of academic friends who provided guidance for this journey. The top conspirator here is Dr. Daniel Joseph who suggested this whole damn PhD enterprise to begin with and is the king of road trip companions. Dr. Ciara Bracken-Roche whose candour and wisdom helped me understand that the things I was going through in this doctoral program were pretty normal and yes, deeply annoying. Dr. Ian Kalman was a constant voice of reason and a great conversationalist, Dr. Jack Jamieson who never judged me for being a mess, and the great Dr. Fenwick McKelvey who was always willing to sound out my ideas and recommend resources. Also, thanks to my physician Dr. Joel Krivy for sorting me out.

This dissertation was written during the pandemic and I managed to face social isolation only because I had truly amazing, compassionate friends. Dave Vasquez-Abrams, whom I've known since high school was always around to listen and sound-off about teaching and working in higher-ed. Then there is Morgan Alan, whose film-festival programming and compelling conversations gave my life structure one week at a time. Friends like Luke Simcoe and Matt Evans were always around to listen to me grumble, commiserate about work and tolerate my garrulous online gaming sessions. Goodbye to my lifelong friend Wayne Laitila (2017), I miss you dearly.

There were a lot of people in the capture the flag community who donated their time and patience explaining this game to an outsider. To that end, I'd also like to thank Dr. Giovanni Vigna who provided early guidance and insight into CTF and deserves his reputation as the godfather of this game. Thanks also to Jordan Wiems and Zach Wade for sitting down with me and providing me with feedback and guidance on the project when I was especially clueless, misguided or confused. Similar thanks to Alexei Bulazel and Dave Aitel for feedback. A few hackers and security community members including z3r0fox, gh0s7, Ironfrog and the research participant Jonah were willing to answer difficult technical questions or issues I had deciphering the baroque language of information security and vulnerability research. Thanks to Don Mallory and Alex Taylor from the Toronto information security community for acting as lab rats for early drafts of my interview scripts, as well as Martin Loeffler, James Goodwin and Leah Honeywell and Sue McGlashan who created opportunities for me throughout this project and afterwards, colleagues I hold in the highest esteem.

Last but not least, I have an inner circle of people and creatures who were here for me every day. Thanks to my mom and dad, who never second-guessed my decision to pursue graduate education. My brother for sharing the same vile sense of humour. Thanks to my dog Hogan, an enormously good boy, who let me walk him when I needed to clear my head or sit on my lap when I needed company.

Finally thank you to my wife Jessica Dubeau who believed in me, believed in this project and believed in my future when I couldn't do it myself. You are my *torch* that lights up the dark places inside me and keep my vision clear as I made every step of this journey, I couldn't have done any of this without you. I love you.

Table of Contents

List of Appendices

Introduction

It's 8:30 AM on a Monday morning in August as I find myself standing at an intersection in Las Vegas about four city blocks off the strip, headed to an information security conference. To my right is an employee centre for a casino conglomerate which outfits and shuttles service workers to their daily jobs, directly ahead is an electrical substation routing power to the bright lights on Las Vegas Boulevard. Relatively speaking, I am firmly in the backstage area of Las Vegas, away from the neon lights and garish imitation architecture of Europe and ancient Egypt, on an industrial artery. I find myself at an appropriate intersection given that I am headed to an annual information security conference, WorkSec, targeted at the rank-and-file employees of the information security industry, workers whose job it is to maintain the seamless operation of technologies and to preserve the integrity of data for major technology companies. At WorkSec I observe a game organized and played by cybersecurity experts to train their peers in emergent skills and new technologies. While games and simulations aren't uncommon in many industries, it is the nature of this game which makes it idiosyncratic to the information security industry: playing in this game utilizes the techniques, software and procedures pioneered by hackers to subvert the security of information systems. The game is referred to as "capture the flag" or CTF and its origins can be traced back to the hacker underground of the 1980s and 1990s, when transgressive computer experts sought to demonstrate their mastery over these systems by undermining the secure operations of many technologies.

At least symbolically, CTF continues this tradition from the hacker underground allowing information security professionals to demonstrate their capability at hacking and enhance their knowledge by spending a weekend attacking the kinds of systems they are often entrusted to defend. In a CTF players perform practises related to the discovery of security vulnerabilities and the exploitation of these flaws, emulating the practise of vulnerability research: techniques pioneered by hackers in the last 40 years to undermine the security of information systems by identifying and engineering unanticipated functionality from these technologies which undermines their security. As an increasingly popular game, CTFs are emblematic of the diffusion, if not the outright ascension of hacker approaches to knowledge, production and sociality which have become mainstream in the technology industry. Vulnerability research is part of the larger field of security research used by hackers and security professionals alike to identify security flaws and gaps in a variety of sociotechnical systems. This transgressive application of this field of knowledge through vulnerability research is a distinct trait of hackers and their culture, who demonstrate their expertise in computer security by subverting it, not to mention the meritocratic culture of celebrating these acts of subversion as a demonstration of supremacy over their intended functionality. The fact that the event I am headed to is only one of the hundreds of CTF competitions that will be organized that year at security conferences, educational institutions or government agencies speaks to a transformation of the hacker: once marginalized by mainstream technology experts, academics and law enforcement for their transgressive practises, hackers and their practises are not just sanctioned, but sought-after, a recognition of their skill as workers vital to the secure operation of high-tech businesses and governments. As a result, understanding their practises, what they produce, the way they share knowledge and in particular, the way they play provides insights into the rapid valuation of hackers within both culture and industry.

A month after my trip to Vegas I’m interviewing Claudio, one of the 100 or so players I observed over the year I attended CTF events. After we review the interview procedure and I remind him of his rights as a research participant, he responds: “I like to talk with people! I'm talking about CTF! There's nothing like classified here, so it's like I'm totally chill!” Claudio’s ebullience and his stated intention to conduct our interview openly flies in the face of many stereotypes about socially awkward, secretive and taciturn hackers built up in our public imaginary. The response also speaks to the methods used in this study and its approach:

observing and interviewing hackers under the auspices of studying a game they participate in has given me unparalleled visibility into the social and professional lives of my research participants. This approach has provided me with access to their intimate personal experiences in the hacker community and patterns of production in their professional lives, the latter often precluded from sociologists studying workplaces and industries which are often secluded from academics, as well as the personal relationships which structure work in high tech industries. At the same time, Claudio's use of the word "classified", whether deliberate or incidentally, serves as a reminder that much of the world of the cybersecurity industry is highly secretive, often over matters of proprietary intellectual property and clandestine knowledge of undocumented vulnerabilities in technologies sold to brokerages and governments often for millions of dollars to enable cyberespionage and sometimes, cybercrimes. In his book, @war (2014) author Shane Harris describes the almost conspiratorial origins of the Military-Internet complex in the United States, the sprawling network of government intelligence agencies and their multi-billion-dollar collaborations with military-industrial contractors to redefine espionage in the 21st century through signals intelligence. The military institutions and private corporations Harris documents are lucrative employers for hackers, who are hired to work as spies, soldiers and alternatingly, as defenders of an increasingly militarized Internet.

By contrast to the proprietary cybersecurity industry and the secretive cyber-military-industrial complex, hacker culture, the fusion of practises and communities that coined offensive methodologies of software manipulation, social engineering and network penetration, is itself notoriously open. The hacker community happily shares tradecraft and technologies on platforms like GitHub and YouTube, they organize conferences and workshops to exchange knowledge and they publish the results of their research and coordinate the remediation of unpatched vulnerabilities with software vendors under the banner of "responsible disclosure" (Frei et al., 2008). Used constructively, this knowledge of vulnerabilities is iteratively applied to patch and defend vulnerable systems, documenting and fixing such flaws to prevent this knowledge from being used destructively by unscrupulous hackers, in pursuit of cybercrime and espionage. There is undoubtedly a paradoxical or perhaps Manichean quality to the relationship between cybersecurity and hacking, which vacillates between extreme secrecy and openness, between undermining and securing systems.

As observed, hacker culture is informed by numerous paradoxes necessary to understanding the vitality of hackers within the political economy of computing and technology industries: some hackers produce insecurity, others security and still others produce insecurity in pursuit of security, finding then fixing flaws. To this point, in a recent essay Héctor Beltrán (2022) describes hacking as “alternative practises and means of exchanging knowledge; modes of cultural and technical production that defy convention; counter-cultural ethics and politics; and most saliently, computing expertise.” Here Beltrán accentuates the alterity of hacking, how hackers and their practises often operate in contrast or outright opposition, a kind of computing heterodoxy to authoritative and traditional modes of knowledge and technology production. Many scholars have acknowledged that there are a multitude of hacker cultures oriented towards different practises, which are often defined by their alterity to heterodox approaches to technologies and their use ranging from 3D printing firearms to free and open-source software production, music piracy and cybernetic body modification under the auspices of biohacking.

The focal topic of this dissertation, CTF competitions, operate on a similar logic of alterity: the practises of the security research community, hackers whose expertise in cybersecurity allows them to undermine the controls protecting information systems, to better understand how to secure those systems. Historically, this behaviour has been understood as part of a male-dominated, transgressive and meritocratic hacker identity. It could be said that CTF, emerging out of the hacker underground of the 1980s and 1990s fits into this identity neatly, as a game which allows hackers to demonstrate their hacking capability in a competitive format, by undermining information systems. More recently, scholars have described hackers as exemplary “entrepreneurial subjects” (Irani, 2014) whose autonomous practises around learning to develop their careers. Again, it could be said that CTF fits neatly into this narrative too, that the game serves as yet another venue through which hackers develop their capabilities and expertise. Yet these understandings can’t satisfactorily explain the vast gift economy of hacker culture which circulates in online communities and in-person venues where CTF takes place, nor the votive mobilization and communal spirit which drives the organizers of these events to spend hundreds of hours doing unwaged development work.

In studying the laborious, work-like form of play that occurs in a CTF it is necessary to reconcile narratives about the hacker identity with their practices and in doing so grasp at the presence of cultural structures, forms of meaning and communities they have generated, particularly as these systems relate to the game itself. To support this objective, this dissertation uses Sara Grimes & Andrew Feenberg's (2009) theory of "social rationality", to unpack how games "become the basis for the production of a form of "institutional order"" which can be analyzed to understand how play and playfulness fit and relate into the "complex lifeworld" of their players, but also identify the influence of "social, cultural and political forces" and systems deployed through these games. Understanding the deployment of rationality through hacker games holds space for how such activities are "socioculturally meaningful" to the experiences of their participants while serving "technically rational" functions including commodification and professionalization of the play experience (p. 106). This dissertation will demonstrate that CTF is instrumentalized as a tool of enculturation, that the mode of design/play mobilized by these competitions promotes the circulation of intellectual capital in the hacker community through its commodification as cultural capital within the structure and outcomes facilitated by the game. In making this argument this study will demonstrate how CTF serves to engage players with systems of meaning and forms of knowledge within hacker culture[s] and sustain hacker practice, but also how it helps them to produce identities, new applications of knowledge and understanding as it relates to both security research and working in the information security industry.

These arguments are supported by ethnographic research conducted at three fieldwork sites in the United States and Canada, observation of nearly 100 players and semi-structured interviews with 47 CTF organizers/designers and players, as well as original historical and archival research into the history of the game. Towards developing my argument, this doctoral thesis is composed of six (6) chapters. The first chapter is a historiography of hacker studies. To this end, it examines the field of literature and academic studies of hackers with specific attention to how this identity, culture and community emerged from certain historically rooted and culturally situated understandings. Specifically, as a history of thought on hackers it considers how scholars and journalists have conceived of the production of knowledge and technology amongst hackers, their relationships to games and play and their ability to produce contingency in information systems. The second chapter is a theoretical framework which draws on labour theory, learning theories (constructionism) and post-ludic critiques of game studies to consider how cultures of computing have understood play and games in relation to education and sociality. The third chapter covers the methodology and ethnographic methods used in this study, which utilized original historical research, observation of CTF events and semi-structured interviews with both CTF players and designers. In the fourth chapter, I consider hacking as a potentially playful media practise and theorize the activity as the production of contingency in information systems by looking at security and the experience of CTF play. In the fifth chapter, I consider the role of CTF in the reproduction of hacker culture, specifically examining hacker practises around security research and the emergence of an empirically oriented form of hacking in the game, which is a shift away from the commodification of subversion and transgression within the hacker identity. For the sixth, and final, chapter I examine the relationship between hackers and the information security industry, considering the role the game plays as part of a public discourse within the security community and how it relates to the professional life of its participants.

Before going into depth on the research conducted it is important to provide a general and succinct description of CTF as a game, given that the technical practises of hackers are extremely complex, but also because competitions tend to be unique and idiosyncratic, making it hard to generalize from specific examples I directly encountered. In all CTF competitions players are given access to some kind of information system designed by the game's organizers/designers which features a known weakness. Using various methodologies and methods players must discover/identify this vulnerability in that system and then devise conditions under which that weakness can be exploited, usually by manipulating the execution of code or the operation of the system. Typically, this hacking involves undermining some kind of security control, consisting of a sort-of hacker puzzle; for example, getting access to a password-protected terminal or leaking information from a website's database that is protected from public access. Upon successfully identifying and exploiting the vulnerability the player will be presented with a flag, often an encoded string of text like "fl4g- 24aee2532e2e18ce5b3a6b6c023818c4a2fb30cd" which they submit to a scoring system, typically referred to as a "scoreboard" run by the game's organizers which redeems the flag for a certain number of points, usually based on the complexity of the hacking involved, with some flags being worth more, or less, than others. Generally, a CTF is run between 24-72 hours, usually the course of a weekend and the player and/or team that wins is the one with the most points at the end of a competition.

There are two major formats of CTF competitions: "Attack and Defend" and "Jeopardy-style." In the Attack and Defend format of CTF, teams of players are given control of information systems which are running vulnerable software known as “services” and must attack identical systems run by their opponents to retrieve flags, while attempting to prevent their enemies from doing the same. By comparison, in a Jeopardy-style competition players generally do not have to defend their systems, but are given access to a multitude of vulnerable systems known as “challenges” wherein they must discover and exploit vulnerabilities. The format is more like a scavenger hunt than a head-to-head competition. Jeopardy-style competitions are the most common format of these games because they are more tolerant of asynchronous play by a large number of teams or players with varying degrees of skill and knowledge involving hacking, which also makes this format more common for CTFs played online. By comparison, attack & defend CTFs utilize synchronous play to support back-and-forth forms of network penetration and defense, often requiring larger teams which can afford to segregate duties between offense and defense or specialized forms of hacking involved in attacking the services run by their opponents. Added to this, attack & defend CTFs are usually best played by teams of hackers with roughly commensurate skill levels to encourage a fair level of competition and challenge for the teams involved, making it difficult to get enough players in the same space at the same time. Consequently, attack & defend CTFs are less common than their Jeopardy counterparts. Capture the flag events are played both in-person and online, though for the purposes of my research, I chose to study competitions played in-person because of the richness of attending the event and the opportunity to observe player and organizer interactions, all of which were valuable sources of ethnographic data. As this dissertation explores this game, more distinctions around the play and organization of CTF will emerge and my analysis will situate these practises of CTF both as they relate to hacker culture and the cybersecurity industry at large.

Chapter 1

1 A Historiography of Hackers & Computer Insecurity

One of the biggest challenges in analyzing capture the flag competitions and their role as information security education and training exercises is that the practises and knowledge utilized in these competitions are typically those which are used to undermine the security of information systems; inherently, play in these games relies on knowledge of computer insecurity. Conspicuously, these practises do not historically originate in legitimized corporate or institutional discourses around computer security, but instead from hacker subculture which has often been characterized through its alterity as an illicit, deviant body of practises, knowledge, communities and actors which has historically been marginalized by mainstream corporate interests, the media, academia and law enforcement.

As is often the case today, as it was in 1996 when the first in-person capture the flag contest was launched, the term hacker is evocative of criminal connotations. Recent scholarship speaks to this tension: Leonie Tanczer's (2020) ethnographic research into German information security professionals would suggest that the stigma of the hacker as a criminal is still a fairly common perception amongst certain enclaves within that industry; while Joseph Menn (2019) noted in his recent book on the Cult of the Dead Cow, that much of the contemporary information security enterprise in America is now run by professionals who identify as hackers and are responsible for securing systems amongst its corporations and within the echelons of its national security apparatus. This research recognizes an understanding of a moment in which the identity of hackers remains stigmatized while the practises and knowledge work of hackers could never be more clearly valued. The mainstream popularity would suggest that something has occurred that has rehabilitated the hacker identity, or at least rehabilitated hacker practises/knowledge as a legitimate body of knowledge. A question persists: how do we account for this rehabilitation?

To explain the contentious discrepancy over what it means to hack and who might be considered a hacker it is helpful to understand historical contestations over the identity of hackers and the divergent definitions of this term. In a 2017 article Sebastian Kubitscko, in conversation with Annika Richterich and Karin Wens, argues that "there simply is no unified hacker movement and there might not even be clearly distinguishable hacker generations" and that “conceptualizing hacker cultures in the singular bears the risk of annulling both context and temporality” (p. 187). This argument is an effort to recognize the “plethora of motives, aims and means that fuel hacker cultures” and to study hacker cultures pluralistically while acknowledging that the “popularisation” of the term hack and the socially constructed identity of a hacker has often contributed to totalizing definitions which can limit empirical research into and understanding of hacker cultures (p. 187). This explanation provides a means of accounting not only for the manifold and variated definitions of hacking but also helps to explain the contentious debate around the definition over what it means to hack, as the terms are fluid, shifting around various cultures, periods of time and public imaginaries. If we approach the idea of hacking and hackers pluralistically, it is possible then to appreciate differences, distinct communities and disparate values within various hacker cultures. By arresting this difference, it also becomes possible to delineate specific practises and histories which have led to the marginalization of the hacker identity and distinctly different hacker cultures. A pluralistic approach to hacker cultures also makes it possible to then identify certain commonalities, shared values, activities and aesthetics, and possibly some sense of continuity which may shed light on attributes rather than explicitly shared histories between the manifold hacker identities.

Towards this pluralistic appreciation of hackers, this chapter examines the literature which has studied these figures and their culture for roughly the past 40 years, not only to understand how writers have defined hacker identity, practise and communities but also to evaluate how these understanding relate to the practise of security and the marginalization of the hacker identity. Early hacker studies by Sherry Turkle (1984) and Steven Levy (1984) in the 1980s make only sparse connections between hackers and criminality, but nearly a decade later in the 1990s almost every scholarly source written about hackers examines them through the lens of criminal activity, pathology or deviance. Later in the early 2000s writers including Yochai Benkler (2006) and Chris Kelty (2008) focused on the role of hackers in the free/open-source software community, while scholars like Matthew Goerzen & Gabriella Coleman (2022) and Leonie Tanczer (2020) return to analyzing the relationship between hackers and security, to account for a relationship between these figures and the information security industry. Given these manifold and sometimes antithetical or oppositional understandings of hackers, it is worth asking: are these bodies of literature studying the same subjects? Do there exist commonalities in the hacker identity, its practises, culture and communities in these texts which provide a useful understanding of hacker practises? Are there historical and/or intellectual continuities between the hackers at MIT in the 1960s and the "computer underground" of hackers in the 1990s, much less the way they are studied? This literature review argues that despite topical differences amongst scholarship the cardinal quality of hackers observed by writers over the past 40 years has been the capability of hackers to produce emergent behaviours from technologies and systems (both technical and social) that were assumed to be stable. Additionally, apprehending the accumulation of emergent behaviours allows us to understand the radical openness, intellectual rigour and subversive qualities of the hacker community interested in security research.

There are many suitable theoretical fields for studying capture the flag; as game/eSport through the lens of game studies or as technologically mediated expressions of hacker culture through the lens of communications studies. While all of these approaches are valid and will be utilized within the body of this dissertation, this literature review specifically approaches the body of literature on hackers written in the past 40 years from a historiographical lens to situate and explain the relationship between hackers and computer security as it has emerged historically within writings that discuss the subject. To this end, it considers the historical emergence of the term hack in the early 18th century, through early descriptions of hacker culture, criminality, production and the growing body of literature that explicitly situates hackers in relation to the industry of information security. This historiography does not claim to be exhaustive nor totalizing: it is not an attempt to summarize all literature written about hackers or come to a definitive conclusion about the true meaning of this identity or associated bodies of practise and knowledge. Instead, this chapter utilizes an explicative lens: identifying salient elements which can be used to support this dissertation's focus on the relationship between hacker practises (including games) and security knowledge. This approach is intended to draw out historical details, arguments and concepts which, through the dialectical process of history, become context and background, a body of invisible knowledge which informs a present moment, but which is often left unsaid, unexplained and obscures the origin point of significant historical changes: for example, the rehabilitation of hacker practise within the professionalized information security industry.

A Genealogy of the Term Hack at MIT

To situate the production of literature about hackers, it is useful to provide some historical context to situate and explain its emergence. Historically, the term "hack" originated at the Massachusetts Institute of Technology (MIT) at some point in the early 20th century, where the term was used to describe clever on-campus pranks. MIT has a long history of campus mischief and pranks, dating back to the 1800s, but also a cultural practise of recording such activities in campus letters, newspapers, yearbooks and other ephemera used to document student life at the university. This documentation describes campus traditions like the "Dorm Goblin" pranks, a title given to a fictional prankster who serves as metonymic agent for all student mischief during the 1920s (Peterson, 2011, p. 36). One of the best early documented pranks at MIT was the transportation of a cow onto the roof of the 1893 dormitory, an impressive feat of both engineering and mischievous whimsy. Modern examples include inflating a balloon at midfield during a rival school’s football game or installing the door to a port-a-potty at the base of the John Harvard statue in Harvard Yard to make the rectangular base of the monument look like an outhouse.

MIT, known for its academic programs and research in engineering and sciences, has used the symbol of the beaver throughout its history as a mascot for the university, both as a symbol of productivity and simultaneously as an icon of subversion and mischief. Given the Beaver's relationship to wood and production, it is also possible the term "hack" is connotative of the engineering or woodworking performed by beavers in the construction of a dam or shelter. The animal was selected on January 17th, 1914 (though some accounts suggest that this choice was made in 1889) as the mascot of the technology club at MIT at a dinner between technology club president Lester D. Gardner and University President Richard C. Maclaurin (M.I.T., n.d.). Supposedly Gardener is to have said that the Beaver was selected as the club mascot because "of all the animals in the world, the beaver is noted for his engineering and mechanical skill and habits of industry. His habits are nocturnal -- he does his best work in the dark" (Mihalik, 1999, p. 6). The language in this quote and the icon of the beaver are a sort of double entendre: the beaver is recognized for its productive and intellectual capacity, but the animal’s preference for performing this work at night shares obvious behavioural similarities with campus pranksters who undertake clandestine activities that demonstrate their technical capability, not to mention their audaciousness. Given MIT’s subversive student culture, it is also well within the realm of possibility that the term hack at MIT has no clear relationship to the beaver, and that its origin or genealogy is fabricated. MIT's student life has a longstanding culture of folklore regarding campus history and pranks which tends towards fabulism, or at least cheekily winking accounts of student life and pranks at the university. The explanation for the beaver's selection as MIT's mascot and the dinner between Gardner and McLaurin is one such dubious example of campus folklore: its explanation is conspicuously self-aware of its subversive qualities and the exact date of this justification by Gardner vary to when exactly the prankster's totem was selected: either 1889 or 1914. In this way, it is possible that the explanation of the beaver as a kind of subversive figure is a post-propter-hoc justification, an anachronistic myth used to enshrine a campus culture of pranks, so interrogating this yarn its factual accuracy is probably unhelpful. Instead, it is simply more practical to interpret the meaning offered by this mythology from a phenomenological standpoint: what is important about these elements of the early history of the term hack or even the tendency towards folklore at MIT is that the idea of a hack connotes a clandestine or subversive form of production, whether in the form of an elegant prank, or irreverent yarn. That this culture exists on MIT's campus and predates a modern-day understanding of hackers and even computers; it is significant insofar as it establishes a cultural understanding of the term rooted in transgression, mischief and subversion.

1.1 The 1980s: Hackers Enter the Popular Imagination

Given that origin of the term "hack" at MIT has nothing to do with computing or computer security it would be easy to argue that the term hack has no historical relevance to either concept. In point of fact, early accounts of computer security breaches do not use the word "hack", to describe early computer crimes nor the title "hacker" to describe the culprits. For example, a series of articles in *Newsweek* from the late 1970s describe some of the earliest computer security incidents documented in the media as "computer crime." Accounts of computer crime from this period tend to conceive of such behaviour as insider threats to corporations and businesses by their employees. One account in *Newsweek* documents a bank teller who was caught manipulating a computer system to cash bad cheques (Pauly & Greenberg, 1976, p. 58), while another describes the computer-assisted embezzlement performed by a corporate accountant (Hutton, 1983, p. 54). The nature of both accounts in *Newsweek* fixate on the technical capacity and knowledge of these criminals to use computers against the companies who employ such experts, as white-collar crime. In both cases, the stories are accompanied by editorial cartoons depicting a smug-looking businessman manipulating a computer, his face disguised by a domino mask, common to the archetypal cartoon burglar. What's interesting about the early accounts and iconography of computer crime, as opposed to those which will crop up in the next decade, is the degree to which computer crime is described as a white-collar crime, not much different from accounting fraud or embezzlement, performed by individuals with clerical expertise who manipulate computers using a highly technical skillset and their knowledge of financial systems. In this fashion, early computer crime reporting is relatively anodyne as compared to the breathless uncertainty and curiosity ascribed to the activities of those labelled hackers in the media after 1983.

These observations about the nature of computer criminals are reinforced by an early analysis of computer crime written by Donn Parker, a computer scientist and researcher, in a report for the Stanford Research Institute in 1975. In this survey, Parker notes that computer crime is predominantly committed by managers, accountants or highly experienced computer professionals in firms where computerized control of transactions can allow for fraud or embezzlement (p. 3). Another interesting statistic from this report is that only one of the 17 crimes described in the report was caused by a perpetrator from outside the organization affected, that a preponderance of computer crimes recorded during this time were caused by insiders (p. 4). Parker's research is some of the first to interview the perpetrators of computer crime, but interestingly he never uses the word "hack" to describe their activities or the term hacker to identify any subjects in the reports produced from his research in 1976, or in a follow-up published in 1980. In this way computer crime prior to the 1980s is largely defined by both expertise in understanding computerized financial transactions, but also proximity to the affected systems, underscoring the degree to which such crimes were conceived of as white-collar offenses.

In 1982 the term hacker appears for the first time in *Newsweek,* albeit inconspicuously, used offhand to solicit interest in the thriller novella *Silicon Valley*, "if you've never heard of a hacker, a Turning Test or a floppy you're in for some instruction and a lot of fun with Michael

Rogers's computer caper" (p. 94a). Wedged on 1/4 of the bottom of a page between a 3/4 black and white ad for Montreal tourism, the language of the book solicitation suggests that the word hacker is likely unfamiliar to readers of *Newsweek*, an arcane piece of technical jargon, and one not imparted with any clear provenance or meaning. It wasn't until a year later that the term hacker would feature prominently when *Newsweek* broke the story of the 414s, a teenaged group of cybercriminals who infiltrated computer networks throughout the United States and Canada. On the September 5th, 1983 cover of *Newsweek* the cover story reads "Computer Capers" "Trespassing in the Information-Age: Pranks or Sabotage?" accompanied by a picture of a skinny teenage boy wearing a red polo shirt, grinning as he sits in front of a Radio Shack TRS-80-II computer. On the bottom left corner, an inter-title identifies the smug-looking youth as "414 'Hacker' Neal Patrick." The cover's treatment of Patrick is indicative of the magazine's feature on the 414s and more broadly, the phenomena of teenaged hackers in the popular imagination circa 1983.

Feature coverage of the 414s in this issue of *Newsweek* is marked by contrast, clearly grappling with the weight of their crimes against their identity as teens. The 414s were responsible for breaching information systems belonging to the Los Alamos National Laboratory, the Sloan-Kettering Cancer Center and Security Pacific Bank. Despite the significance of their targets the 414s considered the successful breach their ultimate satisfaction and their intrusions had no evident collateral impact: the boys never stole funds or tampered with radioactive/radiological materials (Middleton, 2017, p. 11). *Newsweek*'s coverage of the 414's vacillates between the magnitude of the organizations they trespassed against and the juvenilia of the teens responsible: one of the first facts reported about the hackers notes that they met through their Milwaukee Boy Scout Troop (Marbach et al., p. 42). Contributing to the infantilization of hackers in this coverage is an accompanying profile of MIT student Burt Sloane who admits to having broken into computers belonging to federal agencies and MIT's own computer network. The profile also notes that Sloane was paid $10,000 by game publisher Broderbund to break the copy protection and reverse engineer the code for their game Choplifter! so that the company could recover the game's source code which had accidentally been deleted by employees (p. 44). In both these features on young hackers, the article identifies a certain degree of playfulness and/or a fascination with games as an impetus for their activities. The article also includes still images from the film WarGames which debuted four months prior in May of 1983, wherein Matthew Broderick portrays a teenager who breaks into a federal computer network incidentally while attempting to pirate games using his home computer, drawing an overt comparison between the story of the 414s and the events of the movie (p. 42). It should be noted that the 414's Neal Patrick's coifed brown hair and skinny build give also give him more than a passing resemblance to a young Broderick and beyond that, both are paradigmatic examples of white, middle-class teenaged boyhood.

The duality of this coverage, its attempt to convey the gravity of this trespassing and the newfound significance of computers and computer crime is marked for contrast in *Newsweek* to its perpetrators' age and the juvenile quality assigned to their transgressions. This coverage is emblematic of what Carly Kocurek describes as an emergent "technomasculine" identity, during the 1980s. It is characterized by an identity tightly bound to values around gender (namely boyhood) which imbued the hobbyist pursuit of technology among boys with a kind of virility, but also accepted their "willingness to disregard rules and standards," as a healthy behaviour amongst young men (Korcurek, 2014**,** p. 131). As Korcurek observes, these values were extensively portrayed in "mediated narratives" about boyhood and computing in films from the period including WarGames and Tron (p. 135); *Newsweek*'s coverage of the 414s shares a similar premise, a reading of these crimes that openly draws comparison between fictional boy-protagonist of the film as the counterpart to real-world teenaged hackers. What is important about this fluctuation in coverage of the 414s is how it configures the identity of hackers for a large public audience, conflating the term hacker with an identity of boys and particularly a sense of play, a youthful and gendered gamesmanship[1] in the subversion of computer security.

Newsweek's inclusion of WarGames is therefore conspicuous, and indicative of the degree to which the film's impact should be considered regarding the public imaginary of hackers and computer security. Like Donn Parker's writing on computer crime, WarGames, which was

[1] Though given the juvenile quality perhaps the correct term is "gamesboymanship."

released in the summer of 1983, just months prior to this *Newsweek* story, never uses the term hacker to describe a character nor the term hack to describe the intrusions performed by Matthew Broderick's character David Lightman in its script (Lasker, et al., 1982). Outside of coverage in *Newsweek* alongside the 414s Wargames' cultural influence is also enshrined in U.S. law and policy from the 1980s regarding computer crime. The film was referenced in a report on the proposed Counterfeit Access Device and Computer Fraud and Abuse Act of 1984 (H.R. 5616) before the U.S. House of Representatives. In testimony before the House's Committee on the Judiciary, William J. Hughes, then a Democratic member of the house representing New Jersey's Second Congressional District, cites the film. "For example, the motion picture "War Games" [sic] showed a realistic representation of the automatic dialing capabilities of the personal computer" (Hughes, 1984, p. 10). H.R. 5616, which Hughes' testimony was given in support of, would ultimately coalesce into the Computer Fraud and Abuse Act, America's first set of anti-hacking laws which drew heavily from the provisions first established in H.R. 5616 and its rationale.

While the CFAA is frequently and correctly criticized by digital rights activists like the EFF for being overly punitive and vague, it is also often ridiculed for having been inspired, even in some small part by a children's film like WarGames (Williams, 2016). What these critics often take for granted is that Hughes' reference to WarGames reflects a distinct understanding of the changing face of computing and telecommunications in the 1980s. In describing the relatively weak standards for computer security used in strategic and business applications, Hughes also acknowledges that new modes of computing threaten what was once a fairly innocuous problem: "Within the last two years this has changed with the advent of the personal computer. The personal computer allows its user to employ the power of a computer to break into other computer systems by systematically speeding up what would otherwise be a slow, hit or miss process" (Hughes, p. 10). This testimony is a reflection on the prolific commercialization of computers during this time, their penetration into homes via the consumer market, a distribution of not just computing resources outside of governments, universities and businesses but also the distribution of expertise outside these established channels. In this way, Hughes' testimony is prescient of the looming changes to the landscape of computing and the security of computers that will accelerate throughout the 1980s and 1990s as computer use spreads and computer networks grow vastly in size and significance to commercial and strategic enterprises. The idea that expertise, particularly that related to computer security would spread beyond a small group of technical experts, is key to understanding how access to information systems decentralized a threat once limited to the espionage activities of nation-states. Hughes's 1984 testimony is a significant reflection on a shift in the public availability of computing expertise, and also the public understanding of who might be considered the perpetrator of computer crime. Where once computer crime was the purview of well-educated insider threats described by *Newsweek* and Donn Parker in the 1970s, such opportunities were now open to transgressive teen hackers and groups like the 414s in the 1980s.

1.2 Opening the Field of Hacker Studies: Levy and Turkle

In this early phase of public fascination with hackers during the 1980s two key monographs are written about hacker culture and the identity of hackers: Sherry Turkle's *Second Self: Computers and the Human Spirit* and Stephen Levy's *Hackers: Heroes of the Computer Revolution.* Both works document the culture of software and technology production at MIT and consider how hackers are representative of an emergent relationship between technology, identity, culture and computing. While neither of these texts explicitly broach the topic of computer security or hacker-related computer intrusions, they both identify behaviours and values which are helpful in understanding early hacker cultures, their values and the marginalization of these figures within the public imagination.

One of the most widely read accounts of hackers, Steven Levy's text was also one of the first to be published.[2] In this book, Levy documents an oral history of hacker culture arising out of MIT in the late 1950s. The term "hack," as Levy (incorrectly) asserts, originates from the Tech Model Railway Club (TMRC), a club for model train enthusiasts at MIT, who defined a hack as a clever technical solution to a complex problem (Levy, 1984, p. 10). In the context

[2] Joseph Weizenbaum's Computer Power and Human Reason, first published in 1976 briefly discusses the identity of hackers prior to Levy or Turkle. In the book Weizenbaum describes the hacker as a "compulsive programmer" and "superb technician" (p. 119) but devotes less than two paragraphs diving into what the title might mean, mostly calling attention to the title's existence as a piece of jargon within the computing community.

of model railroads, the term hack is generally understood to be a clever way of managing the electrical signals used to power model railroads, an achievement that the TMRC's Signals & Power subcommittee believed was a demonstration of technical mastery. The relationship between model trains and computing might seem like a bit of an unusual fit, but both share a logical, systems-driven approach to electronic signalling which govern both technologies at a fundamental level. Levy's emphasis on the boyish pursuits of early hackers mirrors *Newsweek*'s coverage of the 414's through his description of the juvenile rationale for their interest in computing and technology. At many points throughout the book, Levy describes his subjects' early interest in technologies, often documenting disruptive or subversive incidents in their early childhoods: one hacker constructed a Tesla coil that caused a neighbourhood blackout (p. 9), while another melts dynamite in his parents' stove forcing a neighbourhood evacuation (p. 97). Whether these stories are true or fabrications, Levy threads a connection between his subjects' technical acumen and their childhoods, underscoring a mediation of a technomasculine narrative ascribed to hackers: that technical mastery arises out of exploratory and transgressive forms of play in boyhood.

Levy's book also famously describes the "hacker ethos" consisting of several tenets which ascribe certain values and behaviours, a unifying set of beliefs which Levy argues are common to all hackers. A chief concern of this ethic is "access to computers… should be unlimited and total" (p. 28) and "all information should be free" (p. 28) as well as a tendency to mistrust authorities or organizations that might interfere with these principles of access (p. 29). These aspects of this ethos are constitutive of a meritocratic belief system amongst Levy's hackers who feel that their expertise entitles them to access computing resources, technology and information that might otherwise be off-limits or governed through exclusive relationships (e.g.: research, employment, administrative authority). In particular, this sense of entitlement amongst hackers is expressed through the primacy of their "hands-on imperative," the accrual of experiential knowledge through access to computing resources (p. 9). This emphasis on experiential knowledge drives many of Levy's accounts of transgressive behaviour amongst TMRC hackers who frequently trespass into locked electrical closets and boiler rooms to study campus infrastructure up close (p. 3), steal keys (p. 96), tools (p. 98) and time on expensive research computers (p. 113). When depicting confrontations over these transgressions, Levy often suggests that his hackers are willfully aloof of behavioural norms around permission, or have a moral imperative via their ethos to transgress against norms and standards for authorization and access in pursuit of knowledge. As Levy writes: “evil, of course was a locked door. Even if no tools were behind lock doors, the locks symbolized the power of bureaucracy, a power that would be used to prevent full implementation of the Hacker Ethic” (p. 96). This passage is useful in understanding the way in which Levy depicts a typical hacker understanding of security as an impediment to knowledge and suggests that hackers have a pathological desire to remove or undermine obstacles to their system of values.

If the concept of security identifies a site of ideological struggle amongst Levy’s hackers, it also establishes the parameters necessary to understand contradictions and incongruities within the hacker ethos. As Levy notes systems which governed and authorized access to computers were widely despised amongst MIT’s hackers: “passwords were even more odious than a locked door” (p.113). Central to this observation is his documentation of hacker struggles over the Compatible Time Sharing System (CTSS) at MIT, a system designed to allocate scarce and expensive computer time on campus research computers using usernames and passwords. A consequence of the CTSS at MIT is that it deprived hackers of total access to a research computer’s resources as its power was distributed across terminals which did not have full access to the systems’ processing power and use of the system was now billed and tightly governed by central administrators, who tamped down on more leisurely applications of the campus’s computers. Quoting MIT Professor & early AI expert Marvin Minsky, Levy notes that hackers took great pride in interfering with CTSS’s functionality, eliding its authorization system or in some cases, sabotaging and/or interrupting other projects governed by CTSS which they felt were unworthy of the computer’s time (p.114). Such inference undermines the argument that hacker culture is purely meritocratic, based on respect for capability. Instead, this sabotage demonstrates an ideological incoherence of a supposedly meritocratic culture, that the hackers he describes embrace a style of computing, based on an entitlement to control and access determined by those *who deem themselves* the most capable.

While Chris Kelty (2008) would later describe similar behaviour as a deliberative aspect of hacker culture (p. 44), it is worth considering if this interference is demonstrative of contradiction in their ethos. While Levy’s hackers desire a negative liberty, for access to systems of computing without impediments, this incident emphasizes the degree to which the ethos is not a universal ethic: as Levy's hackers would deny the same freedom to others. These incidents over the CTSS are presented through the lens of boyish intransigence and an idealistic quality of the hacker ethos, a philosophical and aesthetic (material) desire for purity in computing. However, this conflict over security emphasizes an eremitic relationship to extrinsic social structures which, despite its idealism, hacker culture refuses to reconcile through solution, or compromise.[3] So, while the hacker ethos described by Levy is not explicitly against security, its determinism is irreconcilable with social considerations that might require such safeguards, protections for the integrity and availability of systems or considerations of confidentiality.

Levy's deployment of the hacker ethos also demonstrates a tendency in his writing to totalize the identity of hackers to fit within this framework. The fourth tenet of Levy's hacker ethos states that: "hackers should be judged by their hacking, not bogus criteria such as degrees, age, race, or position" (p. 31). Conspicuously absent from Levy's bogus criteria for hackers is gender. Nor is it clear if Levy's exclusion of gender is an intentional or a systemic failure on Levy's part given the portrayal of women in his book. For example, the all-male members of the TMRC who hung around the lab computers used by early computer scientists at MIT are branded by Levy as hackers for re-writing the PDP-1's assembler, the software used to translate human-readable code into machine-readable code, from the provided DECAL software to their own system, MIDAS. Levy describes this undocumented upgrade as typical hacker behaviour: the students perfected an assembler they felt was more robust and efficient, expanding the capabilities of the PDP-1, even if it was no longer interoperable with programs written for its predecessor, DECAL. By comparison, Margaret Hamilton, a female graduate student at MIT, is branded derisively as an "Officially Sanctioned User [capitalization his]" by Levy for writing her program using the PDP's original DECAL compiler, unaware of the modifications and frustrated with the S&P hackers when her program did not compile properly

[3] While Levy does not acknowledge this contradiction, nowhere it is evident than in the final chapter when hacker culture at the university bifurcates into multiple institutions unable to cooperate due to ideological and material disagreements over the LISP operating system, while research in computing at the University is subsumed by the U.S. government's strategic interests and an aggressively commercialized computing industry.

(p. 89). Hamilton, who is discursively branded through this story as someone who is bureaucratically entitled to use a computer, and decidedly 'not' a hacker, would later go on to write the on-board flight software for the Apollo 11 mission, a significant achievement in the history of software engineering, a term which Hamilton coined during her career (NASA, 2003, p. 13). Similarly, Roberta Williams, a pioneer of game design at Sierra Online is referred to by Levy as "Ken Williams' timid wife" in an appendix which identifies important figures in the book (p. xvi). This description not only fails to provide credit for many of Williams's bestselling games but understates her technical capacity as an early PC game designer. These depictions of Hamilton and Williams seemingly disregard much of their capability working with software, an insinuation that the essential quality of hackers isn't necessarily skill or capability. This exclusion within Levy describes the idea of hacking as a kind of leisurely technical culture, which values an *a priori* fixation with computers themselves and the ability to realize and express their capability, rather than their functional capacity: a user's ability to apply that knowledge to a pragmatic solution. What's significant about this value and the seemingly egalitarian ethos which Levy describe is that it is exclusive to those who can engage with computers at their leisure, a luxury which has historically been denied to women due to gendered social expectations around their domestic roles (Deem, 1982, p. 29). This approach is demonstrative of how the technomasculine framing of Levy's hackers is indicative of an expansion of existing heteronormative identities to encode technological mastery as a masculine quality; that the hacker identity is not a particularly radical reconfiguration of who might be considered a figure of expertise based on technical skill or knowledge, but an identity which more closely hews to existing, gendered identities of proficiency and leisure.

Considering the idiosyncrasies and limitations of the hacker identity by Levy it is important to contextualize the book and the impact it has had on the public imaginary around hacker culture. As Fred Turner has observed, shortly after the publication of *Hackers* in 1984, Stewart Brand, the founder of the *Whole Earth Catalogue*, organized The Hackers Conference with the explicit objective of bringing together many of the people he had read about in Levy (Turner, 2006, p.135). Invitation-only and attended by many prominent creators in the computing industry at the time, the conference was also the subject of a television documentary called *Hackers: Wizards of the Electronic Age* which includes interviews with members of the hacker community who enjoyed a newfound prominence. In lionizing these figures in Levy's book, Brand's conference not only established the status of certain people featured in the book but also reified a paradigm of hacker culture around their story, enshrining their history and behaviours as a definitive formulation of the hacker identity. Brand himself would go on to write a book about the MIT Media Lab, *Inventing the Future* (1988), picking up where Levy had left off in documenting technological culture on the campus. The shifting publishing rights of Levy's book is also evident of its cultural transformation from a work of non-fiction into something more prescriptive. First published in 1984 by Anchor Press/Doubleday, Levy's book was republished as recently as 2010 by O'Reilly Media, a publishing house largely responsible for producing technical manuals for software. While the republishing is indicative of the book's cultural significance, the shift by a publisher of technical manuals on subjects like SQL, Sendmail and PERL emphasizes the degree to which Levy's book might be interpreted as a literal proscription of who hackers are and what they do, rather than the description of a particular hacker culture delimited by time, geography, and practise. Ultimately, these observations are an attempt to describe how Levy's framing of hacker culture has proven durable and pervasive, a dominant portrayal of hackers through a cultural lens which needs to be accounted for when framing the discussion of hacker identity and practise.

Published a few months after Levy's *Hackers* in 1984, was Sherry Turkle's *Second Self,* which analyzes the culture of academics studying artificial intelligence as well as home computer enthusiasts, extending her analysis of hackers outside of the MIT community. Central to Turkle's book is her argument that computers are "evocative objects," an understanding of how computing shapes social and psychological development, the subjective experiences of its users through their experiences with this technology (p. 19). In that regard, hackers are key figures in Turkle's analysis, as she identifies them as a social group who "use their mastery over the machine to build a culture of prowess that defines itself in terms of winning over ever more complex systems" (p. 25). Like Levy, Turkle identifies hackers as a group whose relationship to computing is wrought through extracting greater capability out/from these devices. Turkle's anthropological approach fixates on the degree to which experiences with computing reshapes a user's subjective experience with the world, grasps more firmly at the root of hacker idealism than Levy by emphasizing the role which productive capacity and virtuosity with computers is votive within early hacker culture, part of an individual's effort to self-actualize their thoughts through computing (p. 18). The uniting feature of these groups, as Turkle argues, is an interpretive interest in computing: "I found that for them, the computer is not just what it does, but how it makes you feel" (p.25) that "the means-ends relationship is dropped. The fascination is with the machine itself… mastery became highly charged, emotional, colored by a desire for perfection, and focused on triumph over other things" (p.187). Similar to Levy's description of hackers at MIT, Turkle acknowledges an *a priori* fixation with the capability of computers but adds to that an expressive characteristic of this fascination, that for hackers evoking these capabilities represents an emotional desire for control and mastery. Turkle's ontology of who can be considered a hacker based on this quality is subsequently more inductive: for Turkle the term hacker can include members of the academic artificial intelligence community, but also the small community of home computer users, as both share an interest in expanding the capabilities of computers and an interest in how a relationship to computing shapes their lives (p. 24). Turkle's observations here also suggest that there is an expressive quality to hacking: that a user's skill in expanding the capabilities of computers is an expression of their capabilities and experiences, and that hacking serves as a means of self-realization through computing.

Unlike Levy, who centers/centres hacker culture at MIT, Turkle focuses on the gradual induction of computing into the workplace and later the home to emphasize the way in which hacker values are a product of tensions around technical cultures in education and the workplace throughout the 1970s and 80s. Turkle notes that many early adopters of personal computers saw the home computer as a way to engage with scientific and rational forms of labour in ways from which they had previously felt excluded (p. 158). As she describes, many early hackers saw the PC as a pragmatic tool for rendering a procedural and "transparent understanding of scientific processes and principles", which Turkle describes as the hacker "aesthetic" (p. 156), envisioned as a politics of personal computing. Concomitantly, Turkle observes that many early PC users were frustrated with working conditions where an industrial "assembly-line" model of production had, in many workplaces, increasingly de-skilled forms of intellectual labour (including, but not limited to programming), driving dissatisfaction with social conditions around technology work (p.165). In response, many early hackers saw the personal computer as an opportunity to reclaim their intellectual autonomy, allowing them to solve “whole problems” (p.160) and “facilitate a rich intellectual life” (p.162).

What Turkle is describing is how personal computing re-invigorated a dialectical conflict around the deskilling of labour in industrial workplaces, that personal computers were identified by labourers, both intellectual and otherwise, as an opportunity to “control their destinies” and take back a measure of autonomy that they have been deprived of in their working lives (p.162). While Turkle notes that this sentiment around the PC inspired some petit-bourgeoise interest in entrepreneurial business using the home computer, it also gave rise to a hacker “style”: an understanding of computing “characterized by transparency, simplicity and a sense of control” distinct from both the social conditions around work and politics which were marked by mechanization, opacity and the resulting loss of autonomy for individuals (p.162).

Based on this conflict it can also be understood Turkle is describing the parameters of a labour struggle between workers attempting to realize rational and intimate (p. 175) forms of labour through personal computing, specifically hacking, against an industrial model of computing marked by the mechanization and ultimately, a depersonalization of their work. Without inserting too much of a Marxist analysis into Turkle’s book, it is worth pointing out that the identity of hackers as she describes it emerged as an alternative mode of knowledge and technology production, distinct from a dominant mode of work at the time. In this way hacking could be understood as a reaction to distinct social conditions relating to technology and labour; that hacking emerged in the 1970s and 80s as a mode of production facilitated by emerging personal computing, intended to recapture intellectual autonomy through the expertise over these devices.

Similar to Levy, Turkle observes a cultural disdain amongst hackers towards systems of control over computers and data. Towards this worldview Turkle notes many hackers “are expert lock pickers and carry their “picks” around with them on their key chains… their pleasure is in “beating” the lock””, describing the game-like approach and pleasurable experience these individuals perceive in defeating technical systems of complexity. However, Turkle also indicates that defeating a lock represents a hacker's ability to overcome obstacles to a hacker's productive tendencies, noting that "if you can't tolerate a locked door on a computer system, you are going to be an enemy of what is usually called "system security… [which] comprises all of the feature of a computer system that protect the information within the system and the privacy of its authorized users" (p.213). In this consideration, Turkle emphasizes how hackers approached security as an impediment to their efficient work. Turkle recognizes that such behaviour is an expression of self-realization amongst a subculture of hackers, a game-like substrate of hacker behaviour, who relate "to the machine as a puzzle and who share their glorification of "the win"" (p.214). Ultimately, Turkle suggests that this behaviour is well understood within hacker culture as "hack the system, leave a trace, get a little famous and be recognized by the big guys has become part of the hacker myth" (p.214). In this way, defeating system security is both an intellectual challenge, but also partly a social indicator of computing prowess, that hackers ascribed an identity to their capability in defeating the complexities of system security created by their peers, and that such victories are deliberative acts which reify their status through their skills.

Turkle's writing about the relationship between subjectivity and computers is also marked by another conflict involving hackers, a negative perception of their intimacy with technology. As Turkle describes, hackers are marked by a kind of stigma due to the way computing often subsumes their relationship to the world: "as people whose involvement with computers has drawn them away from involvement with other people" (p. 181). Expanding on this, Turkle notes that "hackers' marginality stirs controversy…. public controversies about hackers are fueled by the fact that hackers externalize fears about the dangers of too intimate relationships with machines" (p. 190). What Turkle is describing here is a moral panic around hackers and their close, pervasive relationship with technology; while such anxieties might seem antiquated now in an era of ubiquitous computing, from a historical perspective these kinds of close relationships were unusual, construed as a potent anti-social stigma regarding a hacker's relationship to the material world. Turkle notes that hackers were often described as having "a computer addiction" that caused a "withdrawal from society" noting specifically that hackers were embodied as "undesirable", people who "prefer machines to sex, they don't care about being productive" (p.190). While these stereotypes parallel hacker interest in the capability of machines, rather than their functional productivity, they also emphasize a belief that the hacker identity is one which has withdrawn from the reproductive functions of a wider society, and that their isolation may threaten the conventions of a productive social order. Ultimately Turkle suggests that this may be a reaction to the penetration of interactive technologies into the home & workplace and the depth of relationships that began to emerge from an engagement with these formal systems amongst the public; hackers are stigmatized because they represent "a fear about oneself is projected onto the perceived excesses of another. Such processes proceed by stereotyping, by mythologizing" (p. 186), suggesting that these characterizations of hackers are "symptoms of a profound unease" (p.218). The idea that the hacker identity is subject to a kind of cultural mythology is meaningful in establishing these figures as part of a technological culture of alterity, an anxiety situated around intimacy and expertise with computers.

This consideration of hackers in both Levy and Turkle's early work has identified four salient attributes of hacker identity. First, that hackers share distinct values around computing, specifically a desire for unmitigated autonomy, which is enabled by computing's transparency and/or total access to information. Second, that hackers are interested in using this autonomy *as a means of expression*: to produce and exert control over systems of technical complexity, but also to demonstrate their ability to harness the rational and productive elements of computing to its fullest extent. Third, authors observe transgressive behaviour as being an expression of these values, and while this activity is not common to all hackers, breaking the security of physical or digital systems has been observed both within the culture and externally by those studying this culture. Finally, these elements of hacker identity are marked by a pathology, which in Turkle manifests itself through a stigma towards their intimacy with computing and in masculine, transgressive behaviours amongst Levy's hackers. This pathology is constituted by idealism regarding the rational and mechanistic systems embodied by computing and on the other a kind of alterity that poises the figure of the hacker as central to anxieties around computing, particularly in the popular imagination. Thus, while the term hacker is not observed to carry a particular criminal connotation, it is not hard to see how the mediated narrative around these figures and their culture lends itself to a conflation with otherness, and as a kind of antagonism or anti-sociality.

1.3 Pathologizing Hackers and Producing the Culture of Computer Insecurity

Moving into the late 1980s through early 2000s, the stigma of the hacker identity became the predominant focus of writing and research around hackers and their culture. During this period several non-fiction, true crime books are published on the subject of criminal hackers including Clifford Stoll's T*he Cuckoo's Egg* (1989), Katie Hafner and John Markoff's *Cyberpunk* (1991), Bruce Sterling's *The Hacker Crackdown* (1993), Michelle Slatalla & Joshua Quittner's *Masters of Deception* (1995) and Tsutomu Shimomura's *Takedown* (1996), as well as a surfeit of newspaper and online articles about the crimes of hackers signalling a shift in the public imagination of hackers from mischievous pranksters to a more nefarious, increasingly criminalized identity. As well, academic publications by Dorothy E. Denning (1990), Gordon R. Meyer (1989), Eugene Spafford (1992), Paul Taylor and Tim Jordan (1998) document the hacker identity and practise as one which connotes criminality or at least a perceived illegitimate expertise in computing. All of these works emphasize with greater prominence the relationship between hacker knowledge/practise and computer security, and the hacker's capability for discovering flaws and weaknesses in information systems which allow them to trespass, surveil and/or damage information systems, attempting to establish a linkage between criminality and the deconstruction of computer security.

In 1988 and 1989 two major computer security incidents would garner significant attention from journalists which signalled a shift in the public perception of hackers as it relates to computer security. The first was the Morris Worm in 1988, malicious software (a computer virus) designed by Cornell graduate student Robert Tappan Morris. This worm infected systems at MIT but also replicated across at least 2,000 computers on ARPANET in many other universities and institutions connected to the network (Markoff, 1988, D10), disabling those computers and grinding network traffic to a halt (Stoll, 1989, p. 322). The virus spread itself to other computers on the network using a vulnerability in the Sendmail program running on the popular Berkeley Software Distribution version of Unix (BSD Unix) widely used on terminals connected to ARPANET at the time (Stoll, p. 314). As reporter John Markoff noted, Morris conceived of the virus as a “clever hack”, after speaking to the student who theorized and implemented the virus’s self-replicating and infectious design “simply to prove that it could be done” (Markoff, D10). Morris’ justification here is indicative of the kind of hacker logic described by both Levy and Turkle: the Morris Worm’s design was motivated by an aesthetic, to demonstrate the capability of computers to replicate and transmit a malicious program, with limited functional concern for the impact that such a program might have on infected systems. Morris would be the first hacker tried under the Computer Fraud and Abuse Act (CFAA) and was sentenced to three years of probation, fined $10,050 and forced to perform 400 hours of community service (Kelty, n.d.).

The second incident was described in Clifford Stoll’s book *The Cuckoo’s Egg,* documenting the activities and his investigation into a hacker breaking into academic systems, leading to the arrest of Markus Hess, a KGB spy operating from West Germany who infiltrated computer networks throughout the United States and stole industrial secrets from its networks (Stoll, 1989). Stoll calls attention to the increasing geo-strategic concentration of strategic and industrial information now available on the early Internet and the relatively lax standards of computer security amongst this largely academic network.

Another noteworthy aspect of Stoll’s book is the consideration of the relationship between hackers, their legacy in technology and their relationship to security. In the epilogue to his book, Stoll acknowledges the transgressive behaviour of hackers, whom he describes as “fun-loving student[s]” who might break “into systems as a game (as I might once have done), and forgets that he’s invading other people’s privacy, endangering data that others have sweated over” and suggests that such behaviour is in tension with the nascent Internet designed by a competing hacker logic of openness and accessibility (p. 323). Stoll concludes that the eventuality of these transgressions could threaten to preclude the openness of the nascent Internet, its capability as a human network of collaboration; that ARPANET “could consume itself with mutual suspicion, tangle itself up in locks, security checkpoints and surveillance; wither away by becoming so inaccessible and bureaucratic that nobody would want it anymore” (p. 323).

Fundamentally, what Stoll is acknowledging is the aforementioned critique of the hacker ethos I identified in Levy: that a hacker community which has enshrined negative liberties around freedom from impediments and interference, would find itself in contradiction with the positive liberty it enshrines towards unmitigated access and is realized through a culture that is permissive of transgression into information systems.[4] That fundamentally, the hacker aesthetic, pertaining to transgression finds itself in a contradiction when operating at a larger scale. Noting his reputation for catching hackers in the case of Hess and identifying Morris, Stoll writes "I don't want to be a computer cop. I don't want our network to need cops" (p. 323). This quote is a meditation on a looming crisis, with hackers poised as both the architects and vandals of a massive new digital community/infrastructure whose values could be fundamentally undermined by securitization.

One element missing from these early accounts of hacker criminality is an explanation for the social rationale of hackers and the proliferation of system intrusions being observed. For a paper presented at the 13th National Computer Security Conference, Dorothy E. Denning of the Digital Equipment Corporation (DEC) presciently argues that hacking is part of a "discourse", "the invisible background of assumptions that transcends individuals and governs our way of thinking, speaking and acting" which exists in response to "larger conflicts that we are experiencing at every level of society and business" (Denning, 1990). In support of her observation about the discursive quality of hacker culture Denning contrasts the hacker identity of the 1990s, aligning software rights and the policy focus of the Free Software Foundation and figures like Richard Stallman, against "security-breaking hackers" more interested in understanding the vulnerabilities of communications networks and the computers that utilize these networks. In doing so, Denning acknowledges an emerging polysemic quality to the identity of hackers as it arises from these interest groups and notes that the categorical definition of hackers has begun to splinter. To this end, she identifies hackers both as "a person who enjoys learning the details of computer systems and how to stretch their capabilities", but also "a malicious or inquisitive meddler who tries to discover information by poking around ... possibly

[4] Stoll's self-incrimination, acknowledging his trespasses into the information systems of others is illustrative of how commonplace such an activity was considered within this culture.

by deceptive or illegal means", concluding that many hackers "are both learners and explorers who sometimes perform illegal actions" (1990) -- an argument which concurs with Clifford Stoll's self-incrimination.

In this passage, Denning recognizes that hackers, a term increasingly connotated to criminal activity, do not exist in discontinuity with the existing hacker culture, but are a distinct configuration of an existing cultural formation, sharing many of their ideals, but who perform a distinct cultural practise: "`a hacker is someone who experiments with systems... [Hacking] is playing with systems and making them do what they were never intended to do" (Denning, 1990). What Denning identifies here is that hacker approaches to security are a distinct permutation of existing practises, that hacking in this context is not about building out the capability of new software, but rather subverting the functionality of existing software and networks to find unintended capabilities, typically those that allow for, or which further transgressive acts of exploration. Moving forward, this understanding of hacker practise as undermining or trespassing against computer security as an expression of the exploratory trait of hacker culture is useful in understanding both its continuity within existing forms of hacker culture but also in how this approach is distinct from a previous generation of hacker practise.

The other element of this transgressive practise of hacking which deserves consideration is the community that supported this form of hacker culture through the 1980s and into the 1990s, often described using one of two synonymous terms: the 'computer underground' or 'digital underground' as it was coined by Bruce Sterling (1993). In a thesis, Gordon R. Meyer conceptualizes the computer underground as the "social network" of "mutual association" which organizes this subculture into a community, a network through which information is collected/disseminated and a technical infrastructure which sustains this practise which includes: "electronic bulletin board systems (BBS)", "voice mail boxes" and "e-mail", as well as phone bridges and loops, created by tampering with phone networks (a practice known as phreaking) to establish hacker party lines over telephony systems (Meyer, 1989, pp. 5-6). In Meyer's analysis, the computer underground also includes a number of prominent newsletters and hacker zines including the Youth International Party Line (YIPL), 2600 and the Phrack (p. 8), which are understood as channels through which information is shared amongst the computer underground, but also a place of discourse and discussion. Amongst this subculture, Meyer identifies a typology of three activities common to the computer underground including hacking (to gain unauthorized access to computer systems), phone phreaking (to manipulate telecommunications networks) and piracy (the bootlegging of software in contravention of copyright laws) (pp. 16-20). While he notes that there exists mutual mistrust between practitioners of these activities (hackers, phreaks and pirates), critically Meyer emphasizes that these “communities co-exist and share resources and methods” over their networks and publications even though in practise these groups tend to “function separately” in pursuit of distinct activities (p. 21). What’s important about Meyer’s observations is that the computing underground embodies not just a community of mutual association amongst actors who might be lumped together as hackers, but also that they share common practises, behaviours, social norms and critically, computing resources and information related to hacking itself (p. 38), a trait which bears more than a passing resemblance to the radical openness attitudes towards access to information of the hacker cultures described by Levy and Turkle. In consideration of Denning’s observations, this would suggest that the computer/digital underground operates in a kind of historical continuity, or at least acknowledgement and/or mimicry, of previous forms of computing culture.

Speaking to this continuity it’s worthwhile to examine how undermining security can be understood as a form of hacker practise as compared to earlier, less transgressive explorations of computing capability. In their article, The Moral Cracker?, Bruce Baird, Lindsay Baird and Roland Ranuaro (1987) discuss the potential for applying hacker expertise in pursuit of securing information systems, rather than undermining them. Baird et al., describe the “Friday Night Irregulars” a team of “crackers”, employed by their company responsible for assessing the security of their client’s systems, a practise which was novel amongst professional computer security consultancies in the 1980s given the stigma and mediated narrative around hackers. Referencing Turkle’s insights into hacker practises regarding security, the authors note, their crackers “share the same intense interest in computers exhibited by hackers” but “consider themselves to be elite hackers” who “trade information concerning… methods of defeating security devices and operating systems. They even trade information concerning how to make computers do “neat things”” (p. 472). Similarly, Eugene Spafford notes that hackers are highly skilled in the identification of the security flaws of computer systems, even if he argues that they are unfit to remediate these problems. Using the case of Robert Morris, Spafford considers how the virus designed by the graduate student was intended “to reveal security defects”, bugs in the design of systems which might allow for undesirable actions to be taken without the consent of administrators.[5] The practise of identifying unintended functionality as described in Baird et al., and Spafford as discovering the insecurity of technologies, reflects a permutation of hacker practise present in both Levy and Turkle: that hacker practise, as it pertains to computer security, is the process of extracting unanticipated capabilities from a computer system and manipulating these capabilities into unintended functionalities, often in spite of security controls which should prevent these actions. Both Spafford with Baird et al., denote a distinct expressive interest in this procedure tied up in the sociality of hacking, and that knowledge or the performance of such security breaches is intended to indicate a hacker’s capability.

Approaching Spafford and Baird et al., from an explicative reading, to identify what they are both describing, indicates that these authors present a way of understanding a deconstructive epistemology of hacker practise regarding security. The texts describe the way in which hackers produce knowledge regarding the insecurity of computer systems through the decomposition of their operations and design to perform unanticipated functions. This deconstructive epistemology of insecurity used by hackers resonates with the National Institute for Science and Technology (NIST) description of a vulnerability in a computer system as a “flaw that may be exploited by a threat, to cause a computer system or application to operate in a fashion different from its published specifications” (1976, p. A-2). In this way, the practise of hacking in security can be understood as the ability to derive unintended capabilities from a computer’s vulnerabilities; that insecurity in these information systems is created when flaws are correctly exploited by a hacker, producing inadvertent affordances in their functionality. In this way, hacker culture’s approach to exploring and producing knowledge about the capability of computing is complimentary to security, as such values towards an epistemology of technology favours experimental, deep understandings of these systems used to produce emergent (unanticipated and undocumented) functions which allow them to undermine the structure and/or operations of a computer.

[5] Though Spafford contends that not only are such actions clearly unethical, but the ignore established channels for the remediation and disclosure of these flaws amongst academics.

Given their capability in identifying security vulnerabilities Baird et al., and Spafford's articles also share another commonality around investigating the idea that hackers could contribute to the work of security in the computing industry, though both come to significantly different conclusions about their ethical and professional qualifications. As Baird et al., note, their hackers on staff comport themselves with the highest degree of moral integrity, and have used their deconstructive skills to identify problems that would have slipped past more formal tests (p. 472). By contrast, Spafford describes the hacker practise involving security as a kind of "break-in" and argues that as a technical practise such an approach is unsound for a variety of reasons. In particular, he notes that simply identifying vulnerabilities is a piecemeal solution with the final result that "we [systems administrators and software developers] would spend all of our time verifying our systems and never be able to trust the results fully" (p. 45). This critique identifies problems with the verifiability of the hacker method in that a deconstructive epistemology of security is incompatible with the traditional assurance-based approach to security where protections are formally modelled during design, implementation and auditing (Gollman, 2007, pp. 632-634). In this way, Spafford's critique speaks for the traditional, orthodox approach to computer security of the prior 30 years which utilizes design and assurance-based approaches to the verification of security controls through security architecture and mathematical theorems (Feiertag and Neumann, 1979), a way of securing systems which is fundamentally undermined by the emergent vulnerability of identification and exploitation performed by hackers.

In addition to grievances with their methodology, Spafford also contends that the unsolicited method in which hackers publicly expose insecurity, typically by intruding into affected systems, is ethically compromised, calling into question the tendency of hackers to trespass into computer systems during their hacks (p. 44). Spafford concludes that "even if the result is an improvement in security the activity itself is disruptive and immoral" and that "the results of the act should be considered separately from the act itself" (p.46). Spafford's concerns realize that responding to security vulnerabilities is subject to material limitations of labour and economic resources; that the scope of work necessary to remediate a vulnerability far outstrips the work required to discover them -- limitations which are also preponderant in the present-day landscape of information security. In a later newsletter for the Association of Computer Machinery (ACM)

(1990), Spafford took his critique one step further and urged "colleagues to refuse to do business with any firm that would employ a known hacker" (Steier, p.477). This critique of hacker ethics and their role in security work would ultimately inform the orthodox position towards hackers in the software industry and academia, stigmatizing the identity of hackers and their practises for the next decade and throughout much of the early 2000s.

Speaking to this marginalization of hackers by academia and the computer industry, Tim Jordan and Paul Taylor discuss hacker practise as it relates to culture reproduction in their article "A Sociology of Hackers" (1998). Similar to Meyer and Denning, they observe a distinct community amongst the computer underground, who sustain their practises through their dissemination of knowledge about computer insecurity and note that their transgressive practises and discourse poise hackers "on the wrong side" of "dominant social and cultural norms" regarding privacy and confidentiality on an increasingly commercialized Internet (p. 760). Speaking to their discursive interest in transgression, Jordan and Taylor observe that hacker identity is constructed through communal participation in its infrastructure, which not only serve as networks for the dissemination of information that sustains hacker practise but that these spaces like bulletin boards, websites and chat rooms serve as a site of cultural reproduction by enabling a discourse of identity within hacker culture: "these are resources hackers use to discuss their status as hackers with other hackers" (p. 769).

This pattern of producing social capital in the hacker community returns to the expressive elements of hacker culture previously observed in Turkle and meritocracy in Levy, that the hacker identity is both realized through explorations of technology and through comparison to their peers. These observations recognize that this sociality is part of the pattern of production within this community, which can be used to understand the continuous private discussion of misadventures amongst its members but also understood to motivate the production of freshly identified vulnerabilities and software to exploit these flaws. Jordan and Taylor also note that hacker social skills play a key role in their attacks on systems as well, highlighting how social engineering, methods of manipulating people through conversation or illicitly obtaining data through non-digital means like "dumpster diving" is a key practise used by the community to further their knowledge of systems or enable illicit intrusions (p. 759). This secondary style of attack is indicative of the way in which not all hacker practise is digitally mediated. Indeed, hackers interested in insecurity have also developed a deep understanding of how technologies are situated within human organizations and have devised strategies identifying sociotechnical vulnerabilities in institutional bureaucracies and business procedures.

In considering these writings on the computer underground and the production of insecurity within a distinct permutation of hacker culture, these texts emphasize a distinct set of salient traits which inform the practises, communities and culture of these hackers. First and foremost, what distinguishes this generation of hackers is predominantly based in practise: the hackers described engage in production by identifying and exploiting vulnerabilities (e.g., bugs, flaws) in technical and socio-technical (in the case of social engineering & dumpster diving) systems. While this practise shares some similar cultural traits observed by Levy and Turkle who both observed a hacker epistemology engaged in the realization of computing's capabilities, the explicit transgressive application of this knowledge against security positioned this community outside of the previous generation of hacker practise, as well as mainstream corporate and academic approaches to computing, a position described by Spafford. Secondly, as Denning and Baird observed, not all members of this hacker culture focused on computer insecurity are responsible for illicit intrusions or acts of criminality, but using Meyers, Jordan & Taylor's observations, it is clear that the marginalization of hacker practises and knowledge around insecurity generally drove interested parties into common, secretive communities -- the computing underground -- where such information was circulated and practises were discussed. Third, as Taylor & Jordan and Denning have identified, these communities were essential not only as infrastructure for disseminating information, which sustained the deconstructive epistemology of computing insecurity amongst these hackers but also drove discursive forms of identity construction based on skill and contribution to this community as meritocratic identifiers of status. In many of these analyses, hackers' values are often expressed through meritocratic identity construction, but also their approach to communities which share values around access and knowledge/software production. However, what looms large is the mediated identity of hackers, overshadowing previous generations: hackers are increasingly understood as secretive and transgressive, a countervailing force to civil and commercial interests in computing and the nascent Internet.

1.4 Hacker Production

In the 2000s the focus of scholars studying hackers underwent a fairly dramatic shift, away from a fixation with the computer underground and hacker pathology, toward the free and open-source software (F\OSS) movement and the practises related to its production. This re-orientation reflects two key factors, namely the prolific output of free labour in the design and development of F\OSS software and the rapid success as understood through the proliferation and adoption of F\OSS software throughout the technology industry in the late 1990s and early 2000s. Accordingly, the writing reflects the societal re-assessment of the valuation of hackers, their culture and practises during this period, a significant turning point in their study of these figures. At the same time, the re-organization of labour and copyright law performed by hackers in the F\OSS movement lead scholars to question whether hacker practises and values are a distinct break with traditional modes of production and intellectual property ownership in an attempt to subvert them or are simply a re-configuration of existing practises optimized to the needs of technologists. Both contingencies still reflect a degree of alterity in the hacker identity and the polysemic and subversive quality of the label of hacker remains a point of contention through this period.

In a 2002 history of free and open-source software David Bretthauer considers the recent and rapid F\OSS as a movement by reflecting on its 30-year history and the legacy that hacker values play in its constitution. As Bretthauer notes, the mode of F\OSS production is intimately tied to hacker culture and its values: “since hackers have largely sustained this movement” (p. 3) through free labour and common intellectual resources which they have protected by an open licensing agreement, what Yochai Benkler (2006) understood as the pillars of “commons-based peer production of free software” (p. 74). As well, Bretthauer emphasizes the distinct hacker aesthetic of this work: describing participants as “wanting to take control” of their software purely for “the joy of working at an operating system just for the sake of working at it” (p. 7). Speaking to some continuity between early hacker cultures and the F\OSS movement Bretthauer identifies the success of a variety of concomitant F\OSS projects started as early as the 1970s which had been transformational in configuring a loose set of hacker ideals into useful software. Primarily Bretthauer highlights the policy innovations of the Free Software Foundation in their

GNU General Public License, whose regulation of the appropriation and modification of its software not only protected free and open software from commercial enclosure but enshrined its collaborative and iterative production (p. 5). Bretthauer notes the widespread success of F/OSS through the adoption of popular projects including Berkeley Software Distribution's network protocols for Unix and the Linux operating system, software both developed and governed by free and open-source licenses that have overshadowed their commercial counterparts in network functionality and operating system stability respectively. As he argues, the success and advancements of these two projects were contingent on the ease of their distribution and the collaborative quality of their development (pp. 6-7), which overcame traditional commercial bottlenecks in the adoption of new technologies. In their totality, Bretthauer's observations about the history of free and open-source movement demonstrates that F\OSS projects created value for the technology industry despite their non-commercial production, an unconventional if not counter-narrative to the market-driven, commercialized logic of the software industry. It is understood that the success of these projects reflects the veracity of hacker values inherent to their mode of production and that such values are not solely altruistic, but that they also have material affordances and advantages regarding the efficient production of technology, as evident in the proliferation of F\OSS software during the late 1990s and early 2000s. What is implicit in this analysis is that the 30-year history of the F\OSS movement prior to its success in the late 90s reflects the time it took for a critical mass of participation and production of such projects to yield a noteworthy impact on production of software, but also the maturation of markets that would ascribe valuation to this hacker mode of production.

Focusing on the specific cultural practises of F\OSS software development Chris Kelty argues in his book *Two Bits* (2008) that hacker culture constitutes a distinct social formation, which he describes as a "recursive public", "vitally concerned with the material and practical maintenance and modification of the technical, legal, practical and conceptual" (p. 18). Key to understanding the recurrent nature of this public includes the sharing of source code, which sustains the open sharing of intellectual capital which has been historically observed within the hacker community (p. 29) and the "modifiability" of their code "using something without restrictions… to transform it for use in new contexts, to different ends, or in order to participate directly in its improvement" which is enabled through the alternative licensing and continuous iteration and improvement of free and open-source projects (p. 26). These qualities described by Kelty characterize the nature of Bretthauer’s observations about the collaborative and policy-driven aspects of the F\OSS movement, in that both are an extension of distinct vision of pragmatic software production which is not necessarily “anticommercial”, but “acts as a check” on the “moral order of markets” and “commons” to ensure/protect the necessary circulation of intellectual capital as source code and the distribution of software (p. 43). To this end, Kelty characterizes F\OSS as a way in which technologists utilize a specific logic to correct and reform intellectual property and software production to address inefficiencies and blockages arising from the traditional ownership and the firm-based production of software.

The recursive nature of hacker culture also informs Kelty’s most important observations about its deliberative qualities of this production both in software but also in discourse: "geeks use technology as a kind of argument, for a specific kind of order: they argue about technology, but they also argue through it. They express ideas, but they also build infrastructures through which ideas can be expressed (and circulated) in new ways” (p. 44). This observation describes the way in which the production of software and the reproduction of a discourse around the mode/order of production are intimately co-constituted in the modifiability, sustained concurrently through technical infrastructure used in circulation. In this way the production of F\OSS reflects the collaborative peer-production and deliberation evident in bulletin boards and listservs for its projects; such observations also parallel the discursive qualities of the computing underground, which shares similar circulatory practises which Jordan & Taylor observed for the exchange of knowledge accrual of social capital amongst hackers interested in security throughout the 1990s. What’s important about these observations is that hacker production is understood as greater than a singular practise, and is rather a constellation of practises and a style/mode of production, Further the F\OSS movement itself represents the crystallization of values into action, which I would argue is not limited to free and open-source projects, but can be identified as a substrate of other hacker cultures such as the computer underground whose mutual infrastructure performs many of the same functions.

As these analyses demonstrate, there is some ambiguity in situating hacker values through the production of free and open-source software, particularly how this practise fits into existing social paradigms of values and ethics around knowledge and productivity. In their 2008 article

"Hacker Practise" Gabriella Coleman and Alex Golub seek to situate hackers within "prevailing political and cultural processes" to articulate correlations between this identity and classical liberal values (p. 256). In a savvy appreciation of the variation amongst hacker practises and genres of hacking (F\OSS and security, for example), Coleman and Golub focus on the philosophical disposition of these practises to analyze the values common amongst hackers, rather than trying to account for the moral valence of hacking in a cumulative or totalizing sense. Key to their conceptualization of hacker values is the "cultural sensibility" of liberalism (p. 267), which similar to Turkle, Coleman and Golub emphasize the degree to which hackers share an interest in "expressions of selfhood" through technology (p. 267), that "ground their production of technology as a form of imaginative expression that ensures technical progress and should never be subject to limitations and barriers." (p. 270). In *Coding Freedom* (2013) Coleman concisely summarizes these liberal values through the idea of "productive freedom", the degree to which hackers seek to preserve their productive and intellectual autonomy through "the institutions, legal devices and moral codes that hackers have built in order to autonomously improve on their peers' work, refine their technical skills, and extend craftlike engineering traditions" (p. 3). Accordingly, the liberal essence of productive freedom in hacker culture should be understood as values related to maintaining the autonomy of work with technology, protected through the circulation of knowledge and technology, which safeguards the expressive potential of an individual's productivity and intellectual engagement.

Speaking to the autonomous nature of free and open-source projects George Dafermos & Johan Söderberg (2009) examine how F\OSS constitutes a re-organization of labour practises involving technology production. In examining this history of F\OSS they argue that the open, academic traditions of the hacker community (observed in Levy) "clashed" with the "establishment of a market in software" for home computers in the 1970s, leading to a politicization of the hacker community due to "attempts by capital to enclose computer programmes under intellectual property law" (p.59). As such, they see this conflict in "historical continuity between hackers and labour struggle" which arises out of a conflict between workers and capital over "alienated work practises" (p. 53), that are the result of attempts by capital to discipline and subsume the intellectual labour of programmers within the technology industry (p. 58). In response to increasing efforts in the workplace to discipline programmer labour and enclose intellectual property, Dafermos & Söderberg cite the creation of the GNU General Public License as an effort to use the structuring of intellectual property rights to expand, rather than restrict the rights of users, to create a “regime of common ownership” and open production to more autonomous models which create a common cause for producing useful software (p.59). Specifically, they cite the autonomous structure of the Linux project, which operates in a “distributed” fashion with “no deadlines,” “in the absence of a centrally planned division of labour” (p.60) through a “modular architecture” of programmers providing free labour by writing and reviewing code for recognition amongst their peers (p.61). Dafermos & Söderberg note that the power structure of F\OSS projects might be informed by its leaders but is ultimately determined by contributors who determine the “relevance” of a project through the flow of their voluntary labour through “parallel releases” or forks of a project which are used to shape its trajectory. They suggest that this model of production strengthens social relations amongst technologists, and has the potential to radicalize the hacker movement, by allowing them to draw on their collective and autonomous organization (p. 67).

However, Dafermos & Söderberg also consider the potential for the free labour provided by F\OSS to serve as a form of value extraction and how that capital shapes the autonomous flow of voluntary labour in such projects. As they argue, the free circulation of code has diminished the scarcity of expertise required for skilled software production: that the circulation of code provided through open-source development might serve to discipline the “living labour” of programmers by de-skilling their field (p.67). The authors also note the existence of corporations like RedHat, contracted and outsourced F\OSS development which customizes the code for corporate clients, work where “the input of waged labour is marginal in comparison to the vast amount of volunteer labour involved in writing the main body of code” (p. 65). In addition, Dafermos & Söderberg acknowledge the corporate contributions to the code base of open-source projects, the repository of source code for certain projects as an indication that market-based firms have begun to influence the direction of such projects which “raises the question of how work is distributed in the hacker community” (p.62). Consequently, Dafermos & Söderberg’s scepticism of F\OSS is useful in considering the totality of gains made by hackers in continuity with the economic system in which it operates: while hackers have restructured intellectual property and software production to ensure the circulation of information and tools that give them a degree of autonomy, such a system also has the potential to suppress their labour by optimizing the extraction of value, ultimately alienating intellectual labour of programmers by diminishing the labour of authorship.

In emphasizing corporate engagement with F\OSS projects, the authors correctly anticipate that while autonomy may be provided in the management of these projects they still function in continuity with the existing economic system, so while figures like Yochai Benkler suggested that such production would free "programmers" allowing them to "participate in free software projects without following the signals generated by market based, firm based or hybrid models" (p. 72), we can understand that such production, particularly at-scale, can be enclosed and subsumed by the market-based forces in which it operates. Accordingly, F\OSS production is understood not as a rejection of capital-oriented modes of producing intellectual labour, but as a radical shift in the style and organization of production.

Analyses of hacker production emerging out of the 2000s demonstrate a greater degree of complexity in their analysis of the hacker identity. Within these texts there is almost no mention of the game-like quality of hacking, or childhoods of hackers, the technomasculine narratives that were preponderant throughout writings in the 1980s and 1990s (though most scholars do directly observe that hacker culture is overwhelmingly male). In focusing on intellectual property and the organization of software development as labour in the F\OSS movement, these texts emphasize a distinctly more serious hacker identity, though consideration of how hackers subvert these systems remains a consistent feature of their analysis, emphasizing their alterity from mainstream traditions. As well, all these texts make observations about how F\OSS production reflects hacker values, and how technical infrastructure created by these figures is used to circulate both intellectual and social capital. One key contribution of this era of hacker studies is an identification of intellectual and productive autonomy as a key element of the hacker identity, which had been emphasized as early as Levy and Turkle but becomes a clearly identified trait within these texts on hacker production.

1.5 Hacking and Security

It is within the framing of hackers through particularly their valuation, their labour and their relationship to the organization of production that we can begin to appreciate the rehabilitation of the hacker identity and thus consider how hackers are understood to contribute to the production of computer security. To do this it's useful to proceed from the models and approach to security used by the computing industry in the 1970s and 1980s to understand how the emergence of hackers influenced the technology and discourse around this topic. This section of the historiography will thus shift to a model of examining events in a chronological order, rather than an analysis of their publication history.

In her 2016 chapter "Framing Computer Security and Privacy, 1967-1992", Rebecca Slayton analyzes the historical role of the Association of Computing Machinery (ACM), the professional/academic association of technologists, in shaping the discourse around the security of computing and hackers through its various journals, conferences and newsletters. As Slayton notes, a subdivision of the ACM, the Operating Systems special interest group (SIGOPS) had an early, influential role in research and the computing industry's approach to security as "protection," which promoted security models and heuristic functions "inscribed in operating system's hardware and software, and thereby controlled access in a mechanized, automated way" (p.298). These inscribed controls were understood as the best way to prevent a user or program from abusing the shared memory or processing power of centralized systems where a user and/or poorly/maliciously designed program could potentially abuse them.[6] Thus, SIGOPS promoted research and development which "sought to formally specify policies" which would prevent their abuse and "prove their correctness", using the process of "formal verification" where these controls are tested against mathematical models. Slayton notes that SIGOPS "demonstrated a consistent interest in formal verification" becoming something of a dominant paradigm in its research and amongst the computing industry for securing systems (p.298). However, she also observes that because SIGOPS was not predominantly security-focused, but more interested in

[6] For example, the abuse of the CTSS system at M.I.T. described by Marvin Minsky mentioned earlier in the chapter.

the functionality of operating systems, its prevailing interest in “system efficiency, adaptability and reliability” often framed security as a “tradeoff” against a “broader agenda about improving operating systems” (p. 298). Ultimately, the security and the marketability of operating systems were competing paradigms under SIGOPS, with the former being at the subaltern expense of the business functionality of the latter.

What’s important about this analysis is that it indicates that the dominant framing of early computer “protection” framed productivity, rather than security as its highest priority. In the 1980s Slayton documents the emergence of dedicated security research amongst the ACM which changed the tenor of its approach to the topic (p. 305), noting that members of the Security, Audit and Control SIG (SIGSAC) had, as early as the 1980s begun to question the veracity of the protection approach. In particular, Slayton notes that SIGSAC observed that many security vulnerabilities had been discovered in systems that had undergone SIGOPS’s preferred form of security assessment, formal verification. Consequently, SIGSAC advocated that formal verification was unreliable for ensuring system security (p. 304). This criticism of SIGOPS’ methods was also coupled with concern amongst ACM members who saw the increasing interconnectedness of computer systems and the relatively poor state of communications security, like encryption, as a source of further vulnerability (p.311) alongside governmental strategic concerns about such vulnerabilities (p. 308). Slayton’s description of the shift away from formal verification towards more critical and adversarial concerns regarding security indicates the way in which academic and industrial specialization in security shifted priorities and values in both the design and labour of computing.

In considering the emergence of security as a specialization within computing through the ACM’s publications, Slayton also identifies the role that hackers played within the discourse around computer security vulnerabilities and how they were understood by computing academics and professionals. As she notes the ACM engaged in fractious debate over hackers, particularly over who was responsible for their trespassing and the damage they caused as security incidents escalated in the 1980s. While many ACM members saw hackers as being solely responsible for their own misdeeds (p. 314), a significant amount of ACM contributors held that developers were *also* culpable for creating systems with lax security (p. 314) and refusing to fix software with known flaws (pp. 317-318), such that the president of the organization referred to prolific infections caused by the Morris worm, as a "hygiene lesson" for developers and sysadmins (p. 317). Specifically, Slayton cites publications by ACM members who noted that these vulnerabilities weren't the result of hackers creating the flaws used in security incidents, but that such problems were intrinsic, often deliberate gaps or known problems with the security of these systems which were less of a priority than their business functionality (p. 319). These observations are significant, as they indicate that while hackers were obviously a responsible party in security incidents, the root cause of such problems was understood by many professionals and academics as an unhealthy tolerance for risk in the computing industry. As Slayton notes, the rise of computer crime put enough pressure on the ACM to shift its often-conservative neutrality on social issues and openly lobby to shape legislation on computer crime (p. 320), while members like Dorothy Denning engaged with the EFF and the underground hacker community through the ACM sponsored Conference on Computers, Freedom and Privacy (CFP) in the 1990s (p. 321) to consider emergent policy interests regarding computing. These observations in the communications and activities of the ACM indicate that hackers were not necessarily the catalysts of change in the computing industry's approach to security, but that the practises of the computer underground and the profusion of security incidents in the 1980s was a turning point in the history of computer security, characterized by the acceleration of a trend towards understanding computer system security through its vulnerabilities, and a recognition that hackers played a key role in influencing technology and policy in this domain.

Examining legislative efforts to address security in his article "The Birth and Death of the Orange Book" Randy Lipner (2015) examines the failure of the Trusted Computer System Evaluation Criteria, referred to as the "Orange Book." Created by the U.S. Department of Defense (DoD) in 1983 and later refined by the National Computer Security Center (NCSC), in an attempt to establish security controls through formal verification for vendors selling computing products to the U.S. government, this policy framework was initially rooted in formal verification promoted by the computing industry but its assurance-based approach to security was quickly rendered obsolete by changes to the computing and security landscape. Specifically, Lipner cites the rapid commercialization of the personal computer (p. 27), competing international security policy frameworks by other governing bodies (p. 29) and "the emergence in the late 1990s of an industry of vulnerability finders who demonstrated security problems with commercial products made it evident that evaluated products fared no better under attack than any others" (p. 29), the kinds of contracting described by Baird et al., in 1987 where hackers were hired to find security vulnerabilities in systems and technologies. The problems noted by Lipner acknowledges the laborious pace of formal verification, but also industry recognition of the offensive security methods popularized by hackers, which called into question the veracity of assurance-based approaches when emergent, high-severity flaws could easily slip through such testing.

Speaking to the growing industry recognition, Joseph Menn (2019) has described the gradual legitimization of key figures within the computer underground throughout the 1990s and early 2000s. While Menn acknowledges that security-oriented hackers were often "blacklisted" and struggled against the stigma of criminalization, early in the 1990s many were sought out by corporate leadership to consult on security issues; figures like Scott Chasin of the prolific underground crew Legion of Doom, was one such hacker who went on to found numerous successful security start-ups (p. 26). Another, central figure of Menn's book, is Peter Zatko, aka Mudge of the hacker collective L0pht Heavy Industries, a group which famously testified before the U.S. Senate Committee on Governmental Affairs regarding the geo-strategic risks of insecure software (p. 53). As Menn notes L0pht's engagement with policy and governmental entities gave Mudge a degree of legitimacy, and he is believed to be the first hacker to brief a sitting U.S. president on information security issues (p. 75) and later served as an executive of the Defense Advanced Research Projects Agency (DARPA) (p. 109). Many other members of L0pht went on to found the security company @stake which enjoyed consulting contracts with major companies in Silicon Valley including Microsoft (p. 80), while Menn notes that members of the underground found their calling in the intelligence industry using offensive skills to hack into information systems and perform surveillance (p.101). Menn's coverage is indicative of an emergent entrepreneurial spirit amongst the hacker underground. Once marginalized, many sought to turn their knowledge of a computer's insecurities into a lucrative career in the burgeoning field of information security, often striking out for themselves on new ventures. It also indicates that while hackers have been central to many debates around surveillance and the role of government in undermining privacy, with the correct economic opportunities many hackers abandoned such positions for lucrative employment, which suggests that these were not universally held values.

While much of these histories consider how hackers were understood at a high level by scholars and leaders in the computing industry, it is worth considering how hackers and their practises were perceived and contrasted against the mainstream security industry of the 1990s and early 2000s which had marginalized hackers. In her ethnography of the antivirus software industry Technological Turf Wars (2009) Jessica R. Johnston notes that overwhelmingly, anti-virus software developers of the time tended to see hackers (virus writers) as “technically inadequate” (p.27) and little more than “thieves” who stole “bandwidth and [computing] resources”; compromising systems and “making them insecure” (p.28).[7] As she observes: “from this [anti-virus] researcher’s position breaking into a computer system does not demonstrate any competency of skills” (p.198), Johnston continues, “hiring a virus writer to work within the antivirus industry interferes with the industry’s boundary maintenance, which must continually demarcate the seemingly obvious differences between each of their knowledges” (p. 199). Johnston’s observation here is important for two reasons: first, it indicates the persistence of hacker stigma well through the early 2000s. Indeed, when Johnston was researching and writing the book, in continuity with the positions established by figures like Eugene Spafford, many rank-and-file professionals still saw hackers as outsiders, fundamentally antithetical to the work of securing systems. Secondly, hacker practise is suggested here to purely exist to undermine computer security and the labour of the industry itself, rather than to be considered in dialogue

[7] This is a slight problem with Johnston’s book. Due to the fact that that she focuses on the anti-virus industry specifically rather than the broader computer security industry, her understanding of computer security implicitly inherits anti-virus firms’ framing of security problems as an extrinsic fault introduced by hackers. While this is sometimes be the case with viruses which require a user to open or run a malicious program/backdoor into the computer (usually called a trojan), the most potent and prolific viruses, self-propagating worms tend to infect a much larger swathe of networked computers are usually the product of an intrinsic vulnerability/flaw which is exploited by the malicious software and require no user interaction. So, while vendor created patches to remediate vulnerabilities is a better solution to many of the worst viruses, the anti-virus industry benefits from this narrative in Johnston’s book because its products create value as a solution to police systems which are understood to always be vulnerable. With that being said, Johnston’s analysis of the anti-virus industry *itself* and the significance of computer security for global capital is excellent and the book is criminally under-cited as a major work in the sociotechnical study of computer security.

with it, something later scholars like Slayton and Lipner (as well as Coleman & Gozern later in this chapter) have demonstrated.

The rupture between hackers and security is not just symbolic, over the semantic identity of hackers, but also speaks to the values and mode of production of the anti-virus industry in the production of security expertise and technology. In her ethnographic narrative of its participants Johnston describes an industry in "conflict" between an elite academic "epistemological community" (p. 77) responsible for detecting and identifying treatments for viruses who were deeply suspicious of the "business systems" of software firms which commodified the knowledge in the form of anti-virus software (p. 10). The nature of this conflict led to a discourse in computer security at that time that as "an analytic space that is specialist, exclusive and proprietary" (p. 199): despite internal openness amongst peers, Johnston observes that academics working in this space were often worked to exclude industry organizations. In particular, she notes the dynamics around the Computer Antivirus Research Organization (CARO) which "formed a knowledge monopoly" in the field. As Johnston details, while CARO started out with an "altruistic" objective to "counterbalance industry marketing and profit motives" she indicates that through its exclusive membership which was often used as clout in the promotion of its members (p. 41), "CARO is reinterpreted as an instrument of corporate profit and unaccountable power" which "merely perpetuates a power relationship that serves its members economic agenda more than industry priorities" (p. 201). What Johnston describes is exactly the un-checked enclosure of technological and intellectual capital that the free and open-source movement sought to resist, though in the context of the restriction of security practises often bound tightly to a small group of trusted practitioners who exploited the asymmetries of their knowledge for profit, often at the expense of public interest in broader security gains. In contrast to the openness observed by Meyer, Taylor & Jordan in the underground hacker community, the early security industry is a space where security knowledge is extensively restricted and commodified.

In an ethnography of German cybersecurity experts, primarily managers, *50 Shades of Hacking* Leonie Tanczer describes the contemporary impact of hacking expertise in the information security industry, as well as lingering issues around the marginality of the hacker identity. Tanczer identifies the entry of hackers into the workforce by employers who "employ hackers", "employ "former" hackers" and "employ "good hackers" (p. 113), indicating through this ontology there remains a spectrum of opinions on the ethical valence of hacking as both an identity and methodology. As Tanczer observes, the managerial class of the cybersecurity industry highly values the hacker methodology which "allows for the identification of "weak spots" and stands in contrast to the testing of systems in "conventional ways" (p. 114). What Tanczer identifies is recognition amongst managers in the IT industry that the offensive methodology of hackers grew in mainstream recognition over the 30 years since Baird et al., described their practise of hiring hackers in 1987. In summarizing her findings Tanczer notes that "hackers would be legitimate as long as they operate alongside the field of professionals' interest […] and resist the possibility of working against" legitimate interests (p. 118). This depiction emphasizes that the identity of hackers and the practise of hacking retains an implication of a negative moral valence fairly common, at least within the German cybersecurity industry. One criticism that might be made of this article is that Tanczer attempts to situate and identify a model for the moral valence of hackers, to establish how their practises might be placed in continuity (p.122). Instead, it would be more useful if this model could establish how hackers are either *understood* in the public imagination and/or labour market, or to more clearly delineate hacker morality based on other ethical frameworks including laws or social values. The latter approach is more valuable here in disentangling the valuation of hacker practise and its increasing normativity, as evidenced in Tanczer's study, from the potential harms caused by the subversion of technologies.

One final text worth discussing is Matthew Goerzen and Gabriella Coleman's *Many Hats: The Rise of the Professional Security Hacker.* In the report, the scholars identify the popularization of the security research practise of openly disclosing security vulnerabilities to the public, a process known as "full disclosure" as a key development in the rehabilitation of the hacker identity geared towards professional work (p. 2). Towards the practise of full disclosure, Coleman & Gozern cite the creation of the BugTraq, an online mailing list where hackers would post security vulnerabilities they had discovered (p. 28). As they note, the mailing list ran contrary to the predominant logic of computer security at the time which was to hold such information amongst a small body of trusted parties, in particular the computer emergency response team (CERT), which was increasingly seen by hackers as an unresponsive bureaucracy and a black box (p. 13) and Microsoft who were similarly opaque and often intransigent in dealing with emergent security issues involving its software (p. 43). Posting vulnerabilities to BugTraq allowed hackers to openly identify the source of security vulnerabilities, but also served as a powerful tool of recognition for many security hackers who received recognition for their discovery. In many ways, the open disclosure of security vulnerabilities rendered hacker values into hacker practise, as the public disclosure meant that such flaws could easily be rendered "practical" or "unignorable" (p.46) to responsible parties like Microsoft and CERT who would be compelled to act in response. The other element of this rehabilitation that Goerzen & Coleman emphasize is the careful and often savvy rebranding of hacker knowledge and expertise during the 1990s; in particular, the way hackers like those affiliated with the L0pht challenged the false ontology of "white hat" (good) and "black hat" (criminal) hackers, through careful engagement with the media and public relations, citing the popularization of the term "grey hat" at the time. What this scholarship emphasizes is the way in which hackers sought to instantiate their practises outside of the underground, and the slow and careful navigation of the industry and media landscape that led to the growing legitimacy which is corroborated by other scholars.

Conclusion

Drawing to a close this historiographical analysis of hackers, their culture, history, identity and practises, it becomes possible to composite some common understandings of hackers as they have emerged in this literature.

First, one of the longest-standing elements of hacking and hacker identity is subversion, usually mediated through technical or sociotechnical systems. This trait goes back to the 1800s when the idea of a hack was simply an audacious prank organized by students at MIT. This subversive quality oscillates between different forms, depending on the hacker practises involved. As Turkle (1984) emphasized, often this subversion is an expression of mastery, sometimes indicating a game-like or playful approach to extracting unintended functionality from technical and sociotechnical systems. For example, in the Tech Model Railroad Club's handbook published in 1960, Peter Samson describes a hack as "1) an article or project without constructive end" (Samson, 1960) and within the confines of an academic institution this meant applying multi-million-dollar research computers for less-than-academic purposes often simply to explore and dabble with their capabilities. In the F\OSS movement, understood as one of the more serious and economically rationalized hacker cultures, a subversion of copyright policy and the model of production for intellectual property, efforts to safeguard productive autonomy and intellectual development of technologists. In the hacker underground, those hackers interested in security subversion take on three forms: historically, this emerges in the practises of hackers subverting the functionality of computers to undermine their security, the 'outlaw' status of hackers who have been stigmatized by law enforcement and mainstream computing cultures, and finally in sustaining knowledge of these marginalized practises through semi-secretive digital infrastructures. Drawing from these examples, the idea of a hack and of hacking is usually a subversive re-orientation of technical practises, applying them towards an outcome that was not anticipated based on their hegemonic application (particularly copyright) or historically understood function. Similar cultural observations of subversion are evident in the cryptography work of the cypherpunks, software pirates and many other hacker cultures. This subversive quality of the hacker identity is at the forefront of our cultural understanding of these figures, particularly the juvenilia of technomasculine narratives of the teenaged hackers in the 1980s, yet also persists in more scholarly analyses of economics and labour through Dafermos & Söderberg's (2009) consideration of the role of hackers in labour struggles. As such, the relationship between the idea of hacker and subversion is a key frame for understanding both the cultural dynamics of the hacker identity in the popular imagination, but also the application of their practises. Chapter 4 explores the idea of hacking as an alternative media practice, one which reorients the user's approach to media and explicates playful aspects of this mode of engagement.

The second salient trait that emerges from this historiography of studies of hacker culture is understood through the expression and efforts to preserve the productive and intellectual autonomy of technologists by hackers. Initially, this is described by Turkle as an attempt to reclaim autonomy due to the alienation of intellectual labour on computer labour, but over time as Kelty, Dafermos and Söderberg (2009) note, increasingly this reclamation turned into more of a struggle over the autonomy of intellectual labour with technology, an attempt to preserve their productive freedom, as described by Coleman (2013). While this is certainly evident in the F\OSS movement it is also evident in the computer underground described by Meyer (1989), Jordan & Taylor (1997) and Goerzen & Coleman (2022) where hackers performing security research and offensive methods of security assessment sought legitimization in the technology industry which had marginalized hacker practice. As chapters 5 and 6 detail, the capture the flag competition retains many of these characteristics of hacker labour, examining how the game serves as a form of expression for a kind of hacker imaginary and allows participants to maintain an intellectual output not subsumed by their work in the cybersecurity industry.

Ultimately, this historiography of hackers also identifies the role hackers played in the shaping of the discourse of computer security as it emerged historically and the gradual valuation of hacker practise within the computing industry. While traditionally hackers have been framed adversarially in the history of information security, it is worth considering how security emerged as a topic within this literature which reflected certain aspects of hacker culture: in Levy (1984) and Turkle (1984) security issues are fairly trivial often described through the lens of pranks and games, but moving into the 1990s hackers are increasingly framed as the perpetrators of computer crime, and yet it is worth pointing out that many scholars have emphasized how these figures influenced security practise (Baird et al., (1987) Gozern & Coleman (2022)), policy (Lipner, 2015), as well debates about privacy (Denning, 1990) and risk (Slayton, 2016) within the computing industry itself. Chapter 6 explores the relationship between CTF as a game originating in hacker culture, specifically the computer underground, that now configures industrial relationships and allows for the circulation of knowledge within the cybersecurity industry.

As this chapter has demonstrated, hackers and particularly their values around openness have provided a powerful counter-practise to the commodification of security knowledge and expertise that was a dominant paradigm of the computer security industry in the 1990s and 2000s as identified by Johnston (2009). Already much of this scholarship has indicated some continuities between the intellectual and cultural economy of hackers and the security and computing industries. This is a common thread throughout the entire dissertation, which seeks to identify the communal and votive sharing of knowledge amongst hackers, but specifically focuses on the values situated not just in sharing, but in providing labour and expertise to discursively sustain the hacker community, that hackers participate in a cultural economy in which knowledge, infrastructure and engagement are key factors the sustenance of this system.

Chapter 2

2 Theoretical Framework

As a genre of game, capture the flag is challenging to neatly theorize. It would be disingenuous to say that capture the flag is predominantly a learning exercise, as so many of its players have achieved an expert-level of domain knowledge prior to many of the events they compete in and take the game seriously as an expression of their capabilities -- an approach much more emblematic of professional sport, or in the case of digital games, eSports. At the same time, even at the highest levels, CTFs' focus on contemporaneous knowledge of information security topics clearly has a discursive element and over the last decade the game has seen increasing engagement from educators and their institutions as a resource to train students in the niche field of computer security. Additionally, this act of knowledge transmission is pragmatic, reflecting not only contemporaneous information about cybersecurity, but practises considered "occupationally relevant" (Saari et al., 2020, p. 2501) to the labour and the tradecraft of information security workers and professional hackers alike. While the last chapter sought to situate the relationship between hacker cultures and security, this chapter identifies theoretical approaches to hacker play and sociality which can account for and explain CTF activity as both a game and in continuity with the social structure and behaviour of the hacker community.

As such, this dissertation approaches CTF through the lens of serious play/constructionism and eSports. It attends to a critical approach to each subject through a critical lens using labour theory, media literacy and post-ludic critiques of games. The diversity of theoretical approaches is necessary for both a skeptical analysis of common frames around the educational value of games and play, but also to understand their laborious, competitive and social dynamics. Accordingly, this theoretical framework identifies CTF as an instrumentalized (post-ludic) eSport, one that fuses play and work-like structures, but cannot be totalized as a game or labour, but as a rationalized tool of enculturation which incentivizes civic engagement through competition and exploration of hacker culture.

In theorizing CTF as an instrumentalized eSport, whose organization and play are rationalized as a means of transmitting of knowledge and the reproducing of hacker culture, this chapter also looks at the body of literature examining leisure activities within the hacker community. In doing so, this portion of the theoretical framework seeks to ground hacker culture in transgression, but also emphasizes the importance that sociality plays within the hacker community though games, conferences and mutual expressions of hacker identity.

2.1 CTF as Serious Play, eSport and Labour

Approaching CTF as a form of "serious play" is sensible, given the way the game has been associated with an educational purpose within the information security industry, but may also serve a specific reproductive function within hacker culture. Matt Statler, Loizos Heracleous & Claus Jacobs (2011) provide a useful definition of serious play as: "when actors engage deliberately in a fun, intrinsically motivating activity as a means to achieve a serious, extrinsically motivated" objective or goal (p. 236). The utility of this definition comes from the fact that it is agnostic of digital games and explicitly a game or game-like structure; the definition recognizes that the essential serious quality of the activity is that play itself is extrinsically motivated. Yasmin Kafai and Quinn Burke (2015) argue that contemporary scholarly interest in serious play has largely been re-ignited by James Paul Gee's (2003) article "What video games have to teach us about learning and literacy" (p. 313). However, the relationship between games and play as educational tools has been a long-persistent part of their appeal in the learning theories of Jean Piaget (1951), in pedagogy of wargames (Brewer & Shubik, 1979) and hybrid educational-entertainment, or "edutainment" software (Buckleitner, 1999, Wood, 2001). Consequently, it is apt to say that the present-day scholarly study of serious play in the field of Game Studies was kicked off by Gee in 2003, but scholarly interest in games and play as a source of edification has persisted before current game studies. Debate over the educational value and merit of serious play sustained nearly two decades in the field of game studies ranging from optimism (Charsky, 2010, Wouters, van Nimwegen, von Oostendorp & van der Spek, 2013) to ambivalence (Girard, Ecalle & Magant, 2012, Romero, Usart, & Ott, 2015), to skepticism and outright dismissal (Bogost, 2011, Young et al., 2012). These studies emphasize that evidence on the educational value of serious play is mixed and contingent upon other factors including the learning environment in which this activity is performed and the politics of their deployment, and whether they are used to replace or augment traditional pedagogical practises. As such, it is important to identify critiques and critical approaches which not only offer to ground serious play as a form of knowledge transmission but provide an approach which also considers the way play and games may serve corollary cultural functions closely tied to edification, sociality and cultural reproduction.

Games scholars have identified a range of serious play experiences which distinguish their function from their approach to play, as well as the way they interface with extrinsic objectives. To this end, games scholars have isolated the appropriation of games "for productive purposes" (Brandstätter & Sommerer, 2016, p.260) including human-based computation games (ibid) and games with a purpose (Alahanaki et al., 2014) to describe serious games that utilize play as a tool to perform a task extrinsic from play using computation like scientific discovery, or player interaction as a tool to realize a productive end. Towards an understanding of these productive and generative activities around play and games, Sonia Fizek and Anne Dippel (2019) theorize "laborious playgrounds" as games in which play "enters the non-game domain" and changes it into a "playful entity" (p. 511). However, the authors are careful to argue that the non-game activity is not entirely captured by play, as "play itself undergoes a transformation" (p.515) in this interaction. Thus, what we might call 'laborious play,' is understood as "oscillating between qualities associated previously with leisure or pastime and with productive or useful time" (p. 511). This conceptualization of laborious play, in particular, is useful to both understand how the information-intensive and rigorous activity of security research (security-oriented hacking) can be transformed into a game, and how the game serves an extrinsic motive not only to teach, but to circulate "occupationally relevant" (Saari et al., 2019) knowledge and reproduce cultural structures (meritocracy) as well as ways of knowing and understanding (epistemic structures) technologies common to hackers.

Similar approaches to situating play and sociality around the development of knowledge structures have been identified in the learning theories of constructionism. Kafai and Burke (2015) note that constructionism has generally been neglected in discourses around serious play as a theoretical approach which shares a similar interest in educational impact of immersing learners in an embodied and meaningful learning experience. Construction*ism*, an adaptation of Jean Piaget's cognitive learning theories of construct*ivism,* was popularized by Seymour Papert (1991), who argued that learning was "reconstruction rather" than the "transmission of knowledge" and closely associated this theory with computation and computers as technologies as the medium for learners to (p. i). Constructionism theorizes that effective learning is highly embodied and immediate, wherein the learner is able to establish meaningful linkages between knowledge structures through a pragmatic application within a suitable social environment (p. 5). While hacker culture or CTF does not overtly engage with the terminology of theory of constructivism,[8] Papert's theorization references Sherry Turkle's (p. 16) observations of hacker cultures; indeed, she frequently collaborated and consulted on the latter's constructionist projects (p. 27). It would therefore be apt to suggest that ideas like Turkle's affective and personal aesthetics of computing demonstrate a naturalized appreciation of qualities which can be associated with constructivism which is intuitively understood within hacker culture. Similarly, Morgan Ames (2019) observes a "strong alignment between constructionism and the 'hacker ethic'" (p. 14). At the same time Ames is critical of Papert's approach to this theory due to its tendency to homogenize the motivations of learners and its failure to attend to the support of teachers and the scaffolding of educational environments and cultures which empirical analyses of constructivism have emphasized as critical to socializing learners. (pp. 5-6). A similar fixation is present in Statler, Heracleous & Jacobs' definition of serious play which emphasizes "extrinsic motivation" but implicitly, not an extrinsic *intent* either to teach, or to identify the rationally understood purpose of ideas communicated through a playful experience. In this way, it is important to recognize in critically approaching serious play and by extension, CTF, that the embodied nature of the exercise is also closely intertwined with the objectives of its designers, players and the larger cultural scaffolding of the hacker community and its culture which players encounter through the act of playing in these games.

Understanding the role of cultural scaffolding in the organization, design and play of CTFs is of critical importance to this dissertation's desire to understand the game's purpose within the hacker community and its relationship to the security industry. To describe the relationship between games and larger cultural formations, Sara Grimes and Andrew Feenberg theorize that games are systems of "ludification" whose play is instrumentalized, appropriated and

[8] Nor serious play for that matter. What is interesting about CTF is the fact that serious play and constructivism are both latent within the structures of this genre of game, but whose origins make no explicit reference to discourses around either. In the case of serious play CTF's earliest formations predate

transformed from unstructured into uninform experiences, a process shaped by the "social, political and cultural conditions" in which it is situated (pp. 106-107). By that, they mean that games structure the experience of play through rules and forms of technical mediation in which games become "institutionalized" and the act of play is "rationalized" (p. 116) into systems congruent with larger cultural formations. Grimes and Feenberg describe this process as a product of "social rationality" which aligns both the play of games and their socially understood function with dominant paradigms and attendant narratives regarding the meaning of play within a capitalist society. This analysis draws on critical theory/social theories derived from Marx's (2011) critique of society under capitalism and Weber's (2012, 2019) analysis of the structuring effect rationality has on social formations. Of particular concern to the pair of scholars is the way in which games are instrumentalized towards commodification and professionalization, as the act of play takes on meaning amongst its players, becoming associated with their status and social capital (p. 116). This theory is particularly fluid and useful, because it does not attempt to establish a hierarchy between the players and designers of games, arguing instead that meaning (rationalization) is co-constituted and always in a state of contestation between these parties who are attempting to accumulate capital through the formalization of systems and emergent behaviours and systems produced through their use (p. 111). This theorization is relevant to the study of hackers, particularly in that it recognizes that technical practices are constantly being re-negotiated towards productive ends by both those who make technologies and those who use them.

Similarly, Grimes and Feenberg's theories does not attempt to distinguish play from work, as they contend that a meaningful distinction has already collapsed and that games and their players are already subject to rationalization which structures their "lifeworld as a whole" (p. 116). This approach is relevant to studying hacking, particularly security research, given that so much of the scholarship and history often denotes simultaneously playful, non-serious attitudes and behaviours towards the quotidian technical artifacts of computing. Ultimately, Grimes and Feenberg's theories of ludification and social rationality are appropriate for studying CTF as a game associated with contested technical practices, but whose meaning is also similarly subject to constant re-negotiation, both as a way of accumulating social capital in the hacker community (commodification) and for its utility in teaching precepts of cybersecurity (professionalization).

An emphasis on the pure utility of games as learning tools can be found in recent scholarship on CTF and more broadly "vulnerability discovery" games by Votipika et al., (2020) who argued that many gamified learning platforms related to computer security do not abide by educational best practises for teaching computer skills (p. 1268). Votipika et al.'s study is valuable for understanding the ad-hoc quality of CTF design as a learning environment and the nascent state of these games in their development as educational venues. However, the pedagogical framework utilized by Votipika et al., derived from Ada Kim and Amy Ko's (2017) study of coding tutorials uses a highly traditional, orthodox pedagogical communications model. In Kim & Ko's model isolated users engage with a single learning platform which is assessed for the degree to which it a self-contained educational resource across 24 criteria (p. 322). An interesting idiosyncrasy of Kim and Ko's criterion is that it is not inclusive of, nor does it weigh the significance of the paratextual learning-by-Googling problem-solving procedure commonly observed and analyzed by scholars like Jaanus Pöial, (2021) amongst beginner coders hacker hackers which connects them to websites like StackOverflow, W3Schools and the many coding subreddits. Such communal resources connect users to knowledge resources, but also immerse them in environments which are discursive, subject to their own form of sociality and rationalizations for how learners interact and contribute to these participatory knowledge structures.

Understanding the deficiencies of CTF from a pedagogical lens is common amongst the game's practitioners. Chris Eagle (2013) an academic, as well as a prolific CTF player and organizer, argues that hacker games in this tradition are not necessarily ideal learning environments for the maturation of skills or knowledge: "[CTF] organizers seldom offer to prepare competitors for the event… it's incumbent upon them [players] to acquire the skills necessary to compete well" (p. 69). To this point Eagle, an instructor at the U.S. Navy Post-Graduate school, proposes a pedagogical intervention more common to military exercises wherein drills "of increasing strategic complexity" and "intermediate evaluation" are used to provide timely support for the development of knowledge and skills amongst learners, a critique which re-centers the importance of scaffolding within this activity (p. 69). Additionally, the deliberate heuristic quality of CTF was acknowledged by designers of the 2018 PicoCTF targeted at high-school students, which deploys learning guides to centralize some knowledge, but expects students to “continue researching” outside the provided materials “to have success with more challenging problems” (Owens et al., p. 4). Given these considerations and the autodidactic traditions of hacker culture (Turkle, 1984), such considerations would indicate that the heuristic properties of CTFs are, as this dissertation argues, features approportionated to enculturate and socialize hackers, while serving a culturally reproductive function, driving learners to circulate and engage in the knowledge economy that sustains these socio-technical practises. Pointing out such deficiencies does not undermine the potential educational value of CTF competitions, or Votipika et al.’s study of hacker learning platforms, but proportionally it recognizes the discursive and heuristic qualities of such games, as access points to “cultural infrastructures” (Turner, 2008, p. 75), the way these games drive individual discovery and use of hacker communities, knowledge and tools stored on the Internet. This element of CTF is emblematic of the environmental learning considerations of constructivism and interest in the immediate application of such knowledge.

Applying constructivist approaches to serious play supports arguments that engaging in participatory culture with peers can lead to corollary skills which build linkages to knowledge structures. Kafai and Burke argue that the production of paratextual materials reflects skill and knowledge development which "is not limited to play itself" (p. 314) but can be understood in the production of paratextual materials including strategy & cheat sites (Kafai & Fields, 2013) and participation in online discussion forums (Steinkuehler & Duncan, 2008). Such resources, what Gee (2004) refers to as “affinity spaces” (p. 70), provide “informal mentorship” for the games themselves, but their access and evaluation by players also reflects Henry Jenkins’s observation that "participatory culture" online is a distinct application of digital literacy skills and knowledge work (Jenkins et al., p. 13). I would add here that a player’s efforts to *seek and identify* information represents a similar form of knowledge appropriation as players must search, analyze and evaluate relevant sources of information to inform play.

Similarly, Mia Consalvo (2009) argues that such paratexts deeply inform both the way games are played, but also a player’s recognition of their own expertise and the construction of an expert identity through knowledge appropriation (pp. 410-411). As this critique of serious play pertains to the study of CTF, it indicates that analysis of the game should not be limited purely to the knowledge application performed by players (their expression of pre-existing knowledge and skills) or educational outcomes (what knowledge or skills are developed during the competition), but to the experiences of players interacting with cultural formations subsumed by and encountered during play. Accordingly, study of CTF will be inclusive of how play and knowledge structures are shaped and augmented by engagement with paratextual sources of knowledge as well as the networks they are transmitted through.

Returning to the concept of access points, this study considers how such games draw attention and help players navigate the preponderance of security-relevant technologies and knowledge in the hacker community, as well as the subsequent production of paratextual materials by players, acts which represent a deepening literacy and forms of cultural reproduction amongst players. Thus, understanding how players perceive, navigate and develop their literacy of the vast gift economy of hacker and security communities online is understood as a key function of the enculturation function of CTF as a game.

Attending to the sociality arising out of serious play identified by constructivist approaches is helpful in calling attention to the camaraderie of CTF teams and the competitive dynamics of these hacker games as an eSport. CTFs are distinctly social, as both a team activity and in their use of points, scoring and ranking to motivate play through the quantification of skill and knowledge. The visibility of such scores and ranks have historically been common to digital games to motivate players (Cybulski, 2014) and reflect meritocratic tendencies observed in hacker culture. In fact, one of the most publicly visible hubs for CTF is ctftime.org a website which tracks past and upcoming competitions, noting the ranking of participating teams in these events and providing a global ranking of CTF teams based on their performance across all the tracked events (ctftime.org). Speaking to the way play and its outcomes are mobilized by competition, but to constrain the negative impact that global comparison might have on the motive of learners, the designers of the PicoCTF implemented a “classroom” feature that allowed teachers to locally rank and support groups of their students, driving independent micro-level competitions between local players. Activity within these classrooms correlated with a greater complexity and number of problems solved by classrooms of students, indicating that sociality and competition drove greater engagement with more challenging knowledge structures (Owens et al., p. 5).

This understanding of CTF resonates with Michael G. Wagner's definition of eSports as an area of sport activities in which people develop and train mental or physical abilities in the use of information and communication technologies" (p. 3). Speaking to the impact sociality has on skill development, eSports studies have emphasized how consistent competitive play contributes to the development of successful in-game habits (Huang et al., 2017) and that pro-social play involving teams and friendships correlate with a higher level of skill amongst both individual players and teams (Mason & Clauset, 2012). While such observations reinforce a certain didactic utility from competition, they also emphasize how expertise and skill is closely tied to social structures and interaction between players. There are many other excellent analyses of eSports available, but for purpose of this dissertation these theories are the most useful for understanding how sport instrumentalizes player skills and development as part of culturally understood rational purposes for play.

While the ranking of learning may be considered gauche or regressive pedagogy, constructivist approaches to learning emphasize the role that "personal relationships" and the cultural environment in which knowledge is encountered become a key dimension to the acquisition of knowledge structures and skills (Papert, 1991, p. 14). As such, they cannot be discounted from the extrinsic motivations that inform serious play, particularly when they are integrated into the game-like structures and cultural institutions, such as CTF which use them. In constructivist discourses Michael Resnick has emphasized social spaces analogous to CTFs and hacker conferences as a "third space" outside of formal institutions like the school or workplace and the personal spaces of the home, social spaces like a coffee shop or academic conference. In particular, he argued that the expressive and homophilus nature of social spaces played a significant role in identity formation and knowledge exchange (1996, p. 232) something which Gabriella Coleman (2010) has also noted in her analysis of hacker conferences (pp. 59-60). Ostensibly, these social spaces might include competitive and/or performative spaces like a bowling alley, gym or CTF, which could be considered part of that third space where knowledge is transferred and identities both personal and communal are formed.

To reflect this understanding, this study of CTF considers the role of competition and camaraderie, but also how institutions within the culture of the game, including specific competitions and conferences, shape and render durable these practises and cultural characteristics within the hacker community. Critically, approaching the competitive and homophilic qualities of hacker culture not only aligns it with observations regarding its ideological commitment to meritocracy, but subsequently can also offer space for considering how the cultural reproduction of the hacker community can lead to exclusion and homogeneity observed by scholars like Christina Dunbar-Hester (2019). For example, one of the emergent characteristics of my interviews that will be discussed in chapter 6 is the phenomena of "survival bias" in the hacker community, described by interview participants wherein they identified and attested to struggling with arbitrary demarcations in both skill and identity as to who gets to be a hacker and who is unable to access this identity via CTFs and hacker conferences. In chapter 4 attending to competition also offers value in understanding the hacker community and its idealization of the technomasculine and transgressive characteristics at the expense of exclusion.

Considering the implicit characteristics and function of CTF and its play, it is also vital to examine how it reproduces the knowledge-structures and logic of labour within the cybersecurity industry, particularly as an objective of the game frequently identified by both designers and players. Labour theorists including Michael Crozier (1964) and Michael Burawoy (1982) have long compared the way workers and employers transformed labour into "something resembling a game structure" wherein strategies, worker self-interest and rules co-ordinate production in the workplace (Crozier, 2020, p. xvi). Through observation and autoethnographic experience Burawoy argued that such workplace game-like structures are important for coordinating production and the self-discipline of workers (p. 40). More recently Alessandro Delfanti (2021) described similar working conditions in the Amazon supply chain and its warehouses where "a culture of staged fun and participation" is designed to coordinate and maximize productivity (p. 57). While information security labourers and students are not factory workers, precariously toiling for minimal wages in a physically hazardous occupation, this scholarship emphasizes the value in considering how games which resemble work, influence conditions of production in the industry whose work its play mirrors; how its playfulness is rooted in managerialism. As Burawoy argued, games intricately linked to labour are important for shaping worker identities, sociality and hierarchies in the workplace (p. 42); game-like structures not only inform production but structure the politics of work and industries. To this end, this dissertation considers CTFs through what Lily Irani describes as an "emblematic site of social practise" (p.

799) which is figurative of a mode of production used by the hacker community and security industry, ascribing symbolic value in a player's capability based on their game outcomes common to many meritocratic forms. An identity at least partially rooted in the aesthetics of technological subversion and/or the transgression of security controls. Moreover, understanding the competitive and meritocratic nature of these games also provides insight into how they may construct a durable and stable identity for successful players and organizers for the purposes of economic mobility and their valuation as employees.

Certainly, CTFs with their autodidactic and meritocratic social rationalizations are also emblematic of Irani's conceptualization of "entrepreneurial citizenship" (p. 799). Yet at the same such an approach mediated primarily through an atomistic, self-interested lens is unhelpful in explaining the gift economy and labour under which most CTF competitions are organized largely as voluntary commitment from members of the hacker and security community. Certainly, these games are entrepreneurial but also represent an engagement with communal knowledge and meaning making through their heuristic qualities, that playing involves a level of engagement uncharacteristic of atomistic & isolated individuals. Ames argues that while the individualist logic of the hacker ethic predominates discourses around the hacker community, this makes it "difficult to envision alternative for computer-supported collaboration" and there is a need to account for "modes of social reciprocity" and "pro-social behaviour" in scholarly accounts of computing (p. 14). Similarly, Adrian Johns (2009) has observed a distinctly "convivial" culture of knowledge exchange and support that undergirds many early and proto-hacker communities (pp. 477 - 479). Appreciating the reciprocal, convivial and social elements which may motivate CTF organization and play also challenges the idea that these events can be totalized as a gamified activity, rather as a social and communal mode of care and camaraderie. To account for this sociality which transcends both play and work, this dissertation approaches CTF through what Fizek and Dipple describe as a "post-ludic" activity, one whose play may be informed by modes of production and work but is figurative of larger relationships between players and designers, such as those identified by Grimes and Feenberg in regard to social rationality. Similar observations have been made by Fred Turner (2009) in describing a "cultural infrastructure" of votive creative work, play and sociality which undergirds social relationships in the tech industry (p. 75). This appreciation is crucial to this study, as it recognizes that over the past two decades CTF could not be sustained by self-interested and isolated actors but requires coordination and deeply rooted structures of support & engagement. In this way, the vital gift economy of the hacker community which CTF is understood as part of, needs to be explored as a communal politics of care & conviviality.

Because of these critical approaches to meaning of play, competition and learning, this theoretical framework for this study approaches CTF as a game, but also as socially situated phenomena within hacker culture that considers both culturally reproductive and generative activity through its relationship to labour and industry of information security. Epistemically, attending to the social qualities of CTF recognizes a plurality of actors, cultures, motivations and resources which inform the design, play and the social world of hacker games. Such a framework resists the tendency to totalize the utility of serious play, by acknowledging that the social contexts and framing of the CTF is inextricable and indeed, informative for analyzing why and how members of the hacker community might engage with a game which is so intellectually demanding as a leisure activity. In analyzing CTF the theory used in this dissertation also provides insight into its relationship to labour and the ideological lens through which security knowledge work is conducted. As such, this analysis of CTF conceptualizes it as a post-ludic eSport, a competitive digital game whose central activity is tied to play and knowledge work, but whose organization and production signifies a reciprocal and convivial logic of the hacker community.

2.2 Hacking and Preponderance: Leisure, Games & Sociality

In explicating the sociality inherent to the hacker community and its ties to playfulness and work, it is worthwhile to identify some historical and theoretical observations which have previously identified similar behaviours. This discussion is more focused on theories and concepts that are useful in articulating the relationship between hackers, play and production as part of a theoretical framework, rather than the literature review in Chapter 1 which fixates on developing the cultural context of hackers. This section uses historical accounts of hackers to theorize a relationship between leisure, sociality and expertise amongst hackers. It thus foregrounds relationships between the material conditions of computing which have birthed hacker culture and the resulting playful and/or social practises and communities associated with their identity. In doing so, this analysis holds space for CTF as a game which can be understood as an extension of previously observed patterns of play and sociality tied to the subversion of technologies amongst communities of technologists.

An element of institutional culture that deserves consideration is how early computing at MIT was shaped by access to surplus technologies and computing, insulated from scarcity which allowed for leisure and the production of intellectual and social capital amongst train and electronics hobbyists at the university. The TMRC hackers' approach to computing was shaped by material conditions which allowed for non-serious behaviour, informing the kinds of computing they performed. Throughout the 1950s and 60s computers were largely the provenance of large academic, industrial or military institutions. These were places where unauthorized journeymen and curious teens were typically barred from access due to the serious nature of the work that occurs in such spaces, the astronomical cost of the computers and by extension, the economic value of each moment of operation in which a computer is performing a serious task. In Levy's account, the hackers at the TMRC discovered the EAM room which housed MIT's IBM-704 by playfully trespassing around campus. While Levy never identifies it as such, this behaviour is part of a longstanding tradition at MIT known as "roof-and-tunnel hacking" (Eichberg, 2019, p. 146), curious and transgressive explorations on campus, sometimes to learn and understand campus infrastructure and at other times an expression of social capital, a cunning performance of knowledge and audaciousness expressed by accessing off-limits areas of the university. In this way, MIT's culture of playful roof-and-tunnel hacking, curious and transgressive campus exploration and nerdy campus activities like its model train club played a direct role in informing how these early hackers approached computers, not out of economic, intellectual, or strategic necessity like many professionals or academics hired to work with or on the devices, but out of interests born from leisure, literal exploration and play.

The conditions for this leisure and play of TMRC members are necessary to understand how it is distinct from the milieux of computing and labour happening concurrently outside of MIT. The TMRC and the computer labs at MIT were heavily subsidized by private industry and the military. The TMRC's clubhouse and the vast amount of space needed for its model train layouts were housed in Building 20, a wooden structure built during the Second World War by the U.S.

military to house research into microwaves and radar, dubbed the "Radlab" (Hapgood, p. 89).[9] The reputation of Building 20 is such that it is often referred to as "the magical incubator" for hosting a variety of cutting-edge research in the sciences and technology throughout the latter half of the 20th century (Wright, 1998). Like the building space, the electronic relays and switches that conducted power throughout the TMRC's train layouts were provided by Western Electric's College Gift Plan program (Levy, p. 8), appropriated by the club's faculty advisor, Dr. Carlton E. Tucker, who received donations of surplus telephony equipment from his industry contacts (Hapgood, p.100).[10] Later the computers to which the TMRC's hackers got access were donated by Lincoln Labs and the Digital Equipment Corporation, in the latter's case explicitly to have MIT's hackers develop software that would eventually be distributed with the DEC's PDP-1 and without remuneration to the designers of these utilities (Hapgood, p. 105). While Levy's book gets tremendous mileage out of the argument that the TMRC's hackers were outsiders and misanthropes, the degree to which early hackers had been identified as a productive force by companies providing technology indicates otherwise: these students were part of a burgeoning post-war intellectual and technocratic elite.

Accordingly, both Western Electric and DEC donations to MIT were premised on the exploitation of intellectual capital at MIT, providing entrepreneurial training or producing software in reciprocity for these donations. In fact, Alan Kotok, one of the central TMRC members in Levy's early history of MIT hackers, had a summer job working for Western Electric as an engineer (Levy, p.40) and later would be one of the earliest employees at DEC. In this way, MIT served as a kind of 'circuit' of labour contrary to the "credentialism" of traditional higher education that leads to employment (Shade & Jacobson, 2015, p. 197), as even hackers who flunked out of the program rapidly found gainful employment in the technology industry or supporting computing at MIT. The reciprocal character of technology access at MIT has

[9] The website hosted by the TMRC also notes that an affordance of Building 20 was that as "temporary building" there was limited oversight into unsolicited modifications of the building's wiring or walls, giving club members a free hand in altering in modifying the space to fit their needs or curiosity. http://tmrc.mit.edu/history/

[10] The conspicuous surplus of this donation program was such that when Fred Hapgood wrote about the TMRC in 1993 he claimed that the club still had electromechanical switches and relays from the 1950s stacked neatly under the club's train layout, many of which were still new in box (Hapgood, p.100).

significant material implications: MIT and its benefactors created a space for the early hackers which was not subject to the economic rationale that historically governed access to technology and computing outside of the institution during the 1950s, 60s and 70s where million-dollar research computers were typically not accessible to curious teens and nerdy undergraduates, initiating even failed students into a technological elite. Similar to Johan Huzinga's (1944) concept of the magic circle, a space distinct from the real world which affords play, the "magical incubator" that housed the TMRC's hackers was not subject to the same rules as the one outside it, affording a leisurely, non-serious approach to computing. One hacker at MIT interviewed by Sherry Turkle references a similar idea explicitly: "for me, MIT isn't the real world" and described a struggle as a student to find time for "a world of things" at the school "and a world of people" he would encounter outside the school (pp. 184-185). In that sense, Turkle's subject recognizes that his engagement with technology at the school is provisional and not bound to the same relations that he needs to consider in a social life external to the campus.

The generally unfettered access TMRC's membership had to computers in the late 1950s and early 1960s also defines the early style and aesthetic of hacking. Playful, frivolous and later competitive behaviours amongst hackers can be identified in the activities of the Tech Model Railroad Club user of computers at MIT. For example, the Texas Instrument's TX-0, one of the first computers the TMRC had access to was equipped with a speaker that produced tones intended to be used diagnostically by the programmer as the device ran a program to help the user identify potential bugs or flaws in the software as it was processed by the device. While the speaker was only intended with this diagnostic function in mind, a TMRC member named Peter Samson figured out how to control the 14th bit in the computer's memory, the place in memory that controller's the TX-0's audio output. By writing a set of byzantine instructions, Samson's program could play classical compositions, altering the pitch and tone of the speaker. While making a computer play music was in itself a great hack, according to Levy what made the program particularly worthy of the term was that the code was inscrutable to anyone attempting to understand how it worked: unless the person reading the code was aware of how the 14th bit could be manipulated, control of the speaker and the composition it played was completely obfuscated by the instructions (Levy, p.21). In particular, the steganographic capacity of the music program for manipulating the computer in a non-obvious way is wryly subversive, a clever hack indeed. Samson, who drafted a document called the TMRC Dictionary in the early 1960s to explain the club's jargon, defined the term hack in this text as "1) an article or project without constructive end" (Samson, 1960). By his own definition, the music program was a reification of this frivolous definition of a hack: designed and built at Lincoln Labs the TX-0 which ran Samson's program was the successor to a computer named "Whirlwind", the brains of the U.S. government's Semi-Automatic Ground Environment (SAGE) air-defense system. In this way, Samson's use of the TX-0 as a synthesizer was subversive to both the purpose and function of this particular computer in this particular context. This isn't to imply that Samson or the hacker culture at MIT was some sort of anti-war radical movement sticking flowers in rifle barrels, but that the proximity of his leisure to the military surplus and the geostrategic excess of the Cold War allowed for frivolity and experimentation.

The TMRC also fostered conditions for sociality through technical leisure activities with computers and trains. As Fred Hapgood notes, the TMRC gave away "smiles" and "frowns" in recognition of members who had distinguished themselves through certain achievements on their train layout and those who had attained a level of infamy for poor behaviour in the clubhouse (Hapgood, p. 91). Hapgood argues that this system of recognition was part of the club's role as a social refuge for a group of young engineers, giving them a parallel social structure to other campus cultures (p. 93). Hacks and hacking itself wasn't performed in a vacuum solely for the hacker's enjoyment, but was socially significant, an expression of technical mastery and style which signalled to a shared set of values around technical work within the TMRC. Similarly, Levy describes a competitive culture among young programmers who challenged each other to write complex programs using the least amount of code on MIT's IBM-704, IBM-709 and TX-0 the computers available to TMRC members, largely undergraduates unaffiliated with any research project. The patron of hackers at MIT, Professor John McCarthy, described the activity of his students as "programming bumming" likening the behaviour to ski bums who jockey to shave seconds from their best times on ski hills (Levy, p.13). Virtuoso program bums at MIT in the early hacker community were often recognized by their peers for their ability to take a complex and lengthy set of instructions and reduce it to an increasingly minimalist and abstractly coded, but still functional program (Levy, p. 32). The obsession with minimalism, elegance and mastery shares the leisurely quality of other hacks insofar as it prioritizes form over function, the aesthetic of computing produced through both the rational capacity of their programmers.

A practise similar to program bumming emerged in European and smaller North American software piracy cultures of the 1980s. Called the "demoscene," it was characterized by a culture of writing minimalist programs with impressive procedurally generated audiovisual capabilities. Usually, programs from the "scene" were defined by the limited amount of code they are written in, particularly the extremely limited size the program occupies in a computer's memory. The demoscene originated largely out of Europe's pirate software and computer underground communities of the 1980s and 1990s. During this time young hackers would subvert or "crack", the copy protection on a game by altering its executable. Ritually, these hackers would alter the game's introduction to identify their work to the user and other pirates (Wasiak, p. 263). In these altered versions of the game pirates distributed, they would alter the game's introduction to include a title screen that would run before or after the game's developer or publisher's logo during the game's start-up procedure, what is referred to as a "cracktro." These screens usually included the pirate's pseudonym, the name of their pirate crew, a slogan,[11] shout-outs/insults to other pirates, phone numbers to their BBS board, as well as art, often elaborate graphical effects and perhaps music (Reunanen, Wasiak & Botz, 2015, p. 801). Adding a cracktro to their pirated games served as a calling card for their illicit accomplishments, like breaking a game's copy protection scheme or compressing a multi-disk game onto a single floppy (Oberhaus, 2019). The production of cracktros as part of the subculture of software pirates is emblematic of what Coleman and Golub (2008) describe as "transgression as a method of self-assertion" (Coleman & Golub, p. 269), an assertion of authorship and accomplishment. As Wasiak argues, such an assertion of authorship predates the recognition of programmer skill and ingenuity in a way that presages the contemporary free and open-source software movement (p. 263). What's interesting about these practises is that they demonstrate the way in which the production of technical artefacts through unanticipated and transgressive acts with a computer has consistently been used as a means of identity production and recognition amongst hacker subcultures.

[11] Famous pirate group Fairlight used the slogan "when dreams come true", or "… the home of the real crackers" but other common slogans might include "$authorname is back to kick ass again!" or "the legend is back!"

It is also worth considering how this leisure activity is also representative of a form of intellectual labour on the part of hackers. The piracy scene was largely borne out of the blanket implementation of copy protection and proprietary media formatting of digital games in the 1980s, which attempted to render games a static commodity by making their media immutable. As Graeme Kirkpatrick (2017) argues, this development was a significant break from the earlier iterations of that culture, in which videogaming magazines of the 1980s encouraged "dabbling and experimentation" providing readers with instructions for programming games and writing music in BASIC, facilitating readers with the code to games that they could write into their terminals and then play (p.21). As Kirkpatrick observes, concomitant with the shift towards copy protection and fixed media for games, enthusiast press coverage of digital games shifted from more consumer-oriented content that identities "vidkids," "gamesters," and ultimately "gamers" -- concepts that would configure videogame audiences as more passive consumers who were increasingly interested in the quality of games rather than self-production and coding (Kirkpatrick, p.24). As Wasiak notes, the piracy scene was largely borne by a game audience, reacting to the enclosure of games media and rendering audiences more passive (p. 260). Gavin Mueller (2016) argued that this reaction in the pirate community is representative of an effort to preserve their autonomy over their habits of both "production and consumption (p. 343) an explanation which historically resonates with Turkle's similar assertion that early home computer subcultures identified as hackers sought to preserve their intellectual autonomy in the face of de-skilled and depersonalized computing in the workplace (p. 161). Thus, the early PC game piracy scene can be understood to be suborn as a means of resistance to the enclosure of leisure and play by the economy of the digital games industry of the 1980s. Within the framework of this dissertation this understanding of computers is indicative of the ways in which use and access have not always been enclosed and provides the historical groundwork for a computing culture which accesses computerized media in ways which are constructed and informed by total access and control, as well as subversion.

Given the material limitations of home computers in the 1980s, including limited memory and storage, software pirates were often working under tremendous computing constraints; pirated games and the added cracktros had to consume as little storage memory as possible to ensure these modifications did not prevent the programs from being distributed on floppy disks or interfere with the game's operation, necessitating minimalist code. Like the program bumming of the TMRC described by Levy, in learning and exploiting software to defeat copy protection schemes, or in designing cracktros these pirates would utilize novel, sometimes unprecedented techniques for procedurally generating/rendering graphics or playing music that the pirates had discovered to keep the size of pirated software to a minimum. Piracy, as James Brown Jr. has argued, should be considered as a different kind of cultural production distinct from the initial commodity. As Brown suggests, pirated cultural texts are "different kinds of commodities" reconfigured by the act of piracy through the immaterial labour of pirates (Brown, p.396). While Brown takes the position that piracy is necessary for inspiring new works, the production of pirated games and cracktros could instead be read as a more iterative approach in that piracy opens spaces for play and innovation more rooted in the production of technology and knowledge about technology. Similar practices were observed amongst urban media cultures in India by Ravi Sundaram in their book *Pirate Modernity* (2009) where "low-cost technologies of mechanical and digital reproduction often blurred the distinction between producers and consumers of media" (p. 3.) and describes how this process caused these informal networks to take "on a life of their own" (p. 4). Building from Kirkpatrick's observation of the enclosure of the nascent hobbyist culture of computing, Sundaram's concept of "pirate modernity" explains how the "expansion" and "accumulation" (p. 12) of technology within communities are closely linked to piracy as a "contagion" (p.15) and a "creative corruption" (p. 12) which reappropriates technologies, blurring the boundaries between hegemonic markets with a vital cultural world that both resists the control imposed by, and reproductive affordances of these technologies. Faced with enclosure, hobbyists morphed into hackers embracing the technologies of play, while at the same time undermining the software market.

As Martin Paul Eve (2022) notes, the development of cracktro production branched off into its own genre known as "demo" programs[12], a programming subculture which developed concomitantly with the piracy communities of the 1980s, with crews of hackers "sometimes split between legitimate demo divisions" along with an "illegal" pirate division (p. 161). Such an

[12] Not to be confused with an adjacent concept of shareware "demos", semi-functional or restricted programs designed to serve as a trial before a user purchased the software.

explanation resonates with Gordon Meyer's (1989) observation of networks of "mutual association" between hackers, phreaks and pirates on electronic bulletin boards and other communities of the computing underground (p. 5). While pirate outfits remain well regarded in the hacker community for the quality and ingenuity of their work, over time the practise of creating these minimalist audiovisual endeavours emerged independently from software piracy. Hackers responsible for producing demos organized events and competitions called demoparties that allowed programmers to demonstrate their skill in producing dazzling, but minimalist programs as part of a larger culture referred to as the "demoscene." The demoscene constitutes its own hybridization of eSport and art jam: at contemporary demoparties, hackers attempt to create spectacles of coding often while working under strict technical or logistical limitations. At a demoparty demos are judged on their capacity to produce novel and technically and artistically impressive feats of code under a variety of constraints: in some cases, these limitations are imposed by the organizers to drive creativity or replicate the material limitations of earlier generations of computing. For example, at the demoparty Synchrony, participants must write their demo in the length of time it takes to travel via train between New York and Montreal (Oberhaus, 2019). The demoscene is a good example of how subcultures associated with hacking and activities like piracy have produced playful and intensely social cultures around activities once construed as illegitimate and illegal. These ideas and observations from Eve, Brown and Sundaram provide a conceptual space to understand games like CTF, where opportunities for play are wrought out of marginal contexts like software design and security, where hackers not only discover and manipulate novel technical faults but use their capabilities as the basis for socializing, connecting and accumulating cultural capital through their subversions of technology

Ultimately, this analysis of certain playful and game-adjacent practises within the hacker community underscores a theoretical linkage between digital labour, leisure and identity which has been a consistent undercurrent within hacker culture. As a history, it is indicative of the material relationship: how the accumulation of computing resources and expertise in western countries gave rise to a hacker identity and connotations of authorship. For the purposes of this study, appreciating CTF as a practise which utilizes offensive hacking techniques and a preponderance of expertise and computing technologies is useful in understanding both why the game might be considered a compelling component of identity formation, but also hints at how the game has been sustained through access to expertise and computing resources. Fundamentally, this analysis of identity and leisure emphasizes that hackers aren’t alien to the social, but rather that the hacker identity has deep intrinsic ties to sociality, mediated through technology, transgression and authorship. As such, acknowledging the hacker community as distinctly social puts CTF, as a social game, into direct continuity with existing hacker practises, rather than as an exception to the rule.

Chapter 3

3 Methodology and Methods

This study builds on scholarly literature studying hacker practises pertaining to play and information security, explicitly examining their fusion in capture the flag competitions. In a CTF competition, players emulate the experience of hacking software through the discovery and exploitation of real and bespoke software used in personal and business information systems. The simulation of these systems utilizes the same, everyday information technologies common to large, institutional environments, while their infiltration mobilizes many of the same techniques used by malicious hackers to attack such systems in the real world. The organization and play of CTFs relies extensively on a shared corpus of information security knowledge and skills shared by the information security community. For many competitors and organizers, the knowledge and skill required to play in a CTF directly parallels the work that they do in their careers as information security and information technology professionals. This dissertation considers how participation in these competitions transforms the act of play “into psychological, social and material resources for … post-industrial information work" (Turner, 2009, p.86) as well as its meaning within the hacker community. To do so this study seeks to explore the understanding of CTF from the perspective of its players and organizers and to explicate their rationale and the experience of participating in a gamified hacker competition using a phenomenological framework to apply interpretive ethnographic methods.

This chapter is structured into three sections. The first covers the methodology used in the study, describing the epistemological concerns of interpretive ethnographic research using a phenomenological framework. The second section covers the ethnographic research protocol and methods used, while the final section documents emergent elements of this research which led to iteration in my research design, notably issues around representation that speaks to its responsiveness in reaction to feedback from research participants.

3.1 Research Questions

This dissertation seeks to identify and understand linkages between the cultural formations of games and play within hacker culture with the laborious processes and structure of the information security industry. To structure this inquiry the following research questions were identified:

Research Questions:

1. **What can the longstanding, organic emergence of a serious play activity within the hacker community tell us about the history of hacker culture?**
    a. What are the historical, legal, political and cultural conditions that popularized capture the flag events at hacker gatherings?
    b. How might the history of capture the flag competitions inform a discourse which is critical of the concept of 'serious play'?
2. **Does the design and play of challenges in capture the flag competitions reproduce hacker culture as a mode of production? If so, how?**
    a. What kinds of information seeking and skill development occur during the performance of capture the flag competitions?
    b. What is the relationship between CTFs and hacker culture, from the perspective of participants? Do the participants perceive themselves or other participants as "hackers" or as part of hacker culture?
    c. How does participation in capture the flag competitions shape a participant's cultural perceptions of their own identity as hackers?
3. **Does participation in capture the flag competitions prepare or train participants for careers in information security?**
    a. Can capture the flag competitions be understood as a pedagogical exercise? If so, how?
    b. Do participants feel that participation in capture the flag competitions benefits them? In what ways? To what extent?

3.2 Methodology

In thinking about how to answer these questions, it is important to identify a methodology for producing knowledge which analyzes the rationale and experiences of CTF players and designers. In particular, the research questions seek to explore the role that games within the hacker community shape the identity formation and professional development of their participants. The methodology used in this study is grounded in a phenomenological framework for interpretive ethnographic research. As a project, this research is ethnographic insofar as it is "concerned with the study and representation of culture", specifically around a game within the hacker community, through the process of "subjecting one's self to at least part of the life situation of others" (Van Maanen, 2011, p. 219) to represent their "social reality" through analysis (Steinmetz, 2015, p. 128). As such, this study draws on an interpretive ethnographic approach which assumes that through analyzing the lives of research participants it is possible to access knowledge through their experiences to document reality (Denzin, 1997, p. 30). As Norman Denzin has argued, in documenting the experience and statements of research participants the researcher can begin to analyze and "understand how power and ideology operate through systems of discourse" which shape the "emergent political conditions" (p. 35) that inform the lives of research participants. Here, I am interested in how technical practise and practises of knowledge regarding technology specific to hackers are understood both in a game and also to reflect working experiences in the cybersecurity industry.

A phenomenological methodology is complementary to ethnographic research due to its interest in understanding the experiences of individuals. Scholars of phenomenological methodology have emphasized its ability to produce individual accounts of experience as well as "intersubjective" understandings constituted amongst groups, specifically to destabilize "those unexamined assumptions" and "engagements with reality" which undergird superficial (non-immersed) encounters with social structures (Desjarlais & Throop, 2011, p. 88). Considering the contentious identity of hackers and the shifting valuation of their work described in the history and theorizations of this community in the last two chapters, phenomenological epistemology offers a useful way to explore this culture directly through the experiences of its participants but also offers a way to examine prevailing conditions and mundane patterns of activity with simultaneously fresh and familiar eyes.

From the outset, it is worthwhile to examine the tension between the philosophy of phenomenology, as a study of individual and mutual experiences, in trying to understand wider structures like cultures, the predominant function of ethnographic research. Identifying this tension and addressing how it has been understood and compensated for by ethnographic scholars will also establish the utility of phenomenology within this research. Traditional phenomenology is emblematic of existential philosophical traditions derived from Edmund

Husserl (1963) and Martin Heidegger (1982), in which existence precedes essence, an epistemology wherein objective reality is superseded by the individual's experience. Critical approaches to phenomenology amongst ethnographic researchers have increasingly rejected the centricity of the subjective "ego" as the primary source of knowledge within this epistemology (Aho, 1998, p. 3), specifically because such an understanding takes for granted "symbolic images, conventional usages, habitual expressions, or the inherited past" (Jackson, 1996, p. 11). The epistemology drawn from traditional phenomenology is characterized succinctly by Leitiza Caronia (2018) as disconnected from obvious and observable structures, and as a result, key elements of experience: "from a phenomenological point of view there is no such thing as a deterministic impact of the socio-material context on the individual, no cause-effect relation between stimulus and response" (p. 2). Consequently, traditional phenomenology has been the subject of critique for being insular and isolated from other structures of knowledge and fields of scholarship and for its tendency to configure the experiences of others through the lens of the researcher's own experiences and knowledge structures.

In response to this disconnection between phenomenological epistemology and the study of culture scholars interested in understanding the lived experiences of individuals in relation to structures which influence experience have theorized approaches which rectify or remediate this gap. As Robert Desjarlais and Jason Throop (2011) note, social, radical and post-phenomenological approaches are indicative of the way "anthropologists and other scholars have drawn on phenomenological perspectives to consider the ways in which political, social, economic, and discursive formations intersect with the operations and felt immediacies of bodies in several sociocultural settings (Cohen 1998; Csordas 1994a, 1999a,b; Desjarlais 2003; French 1994; Lock 1993; Pinto 2008; Scheper-Hughes 1993; Throop 2010c)" (p. 90). As a result, there is a scholarly trend towards the analysis of larger formations while remaining inclusive of personal and intersubjective experience, a productive and cumulative fusion of two once disparate epistemologies of social phenomena. The epistemic implications for the phenomenological shift in ethnographic research are explained by Michael Jackson (1998) as a kind of co-constitution: "culture, therefore cannot be set over or against the person. It is, rather, the field of a dialectic in which the sedimented and anonymous meanings of the past are taken up as means of making a future" (p. 11). This understanding, referred to as the 'phenomenological turn' acknowledges this shift not just as a trend in the scholarship, but for its obvious pragmatism, in the ability to incorporate 'formations' including sociality, systems, identities and symbols into the epistemology of methods focused on the experience of individuals. As such, this turn in phenomenological epistemology offers to make the experiences collected from individuals whole, by considering the wider social reality in which they are experienced.

These shifts in phenomenological epistemology have been reflected in approaches which seek to recognize the co-constitution of experience with social, cultural and economic formations. As James Aho (1998) has argued, socially-oriented phenomenology is well-suited to the study of culture because of its interest in personal "quotidian", "everyday things" (p. 3) as well as the "logic and parameters", which *could* pattern experience, including its "social-historical circumstances" (p. 5) as well as the way these things change in their 'passage through time' (p. 3). In considering the relationship between experience and social structures Jackson (1998) has argued that phenomenological epistemology understands that "human experience vacillates between a sense of ourselves as subjects *and* as objects, making us feel sometimes that we are world-makers, sometimes that we are merely made by the world." (p. 21) This quality of phenomenology recognizes that experiences documented in the course of research are co-constituted; influenced by the immediacy of subjectivity and human agency, but also that such embodied experiences may be anticipated by structural forces or operate within systems and that moment-to-moment there is often a give-and-take between the immediate/personal and the structural. This co-constitution is most evident in the way phenomenological theorists foreground the importance of the "embodiment" which grounds "their theorizing, description, and analysis in close examinations of concrete bodily experiences, forms of knowledge, and practise" (Desjarlais and Jason Throop, 2011, p. 90). As a concept, embodiment emphasizes that structures are not simply extant to experience, but ones that are subsumed in and interact with a subjective experience of reality.

While this study itself takes an exploratory approach to its topic, phenomenological approaches to ethnographic research are a well-trod methodology amongst academics. Scholars including Gabriella Coleman (2010) and Kevin Steinmetz (2015) have both utilized ethnographic approaches with phenomenological elements in studying hackers, to analyze social rituals, production and identity formation within their communities. Key to Coleman's analysis in her book *Coding Freedom* (2009) as well as the subsequent article “The Hacker Conference” (2010) is the phenomenological concept of a “lifeworld” (2010, p. 50) which she derives from Jackson’s definition as “that domain of everyday, immediate social existence and practical activities with all of it habituality” which also extends to “its crises, its vernacular and idiomatic character, its biographical particularities, its decisive events, and indecisive strategies” (Jackson, pp. 7-8), a term which is itself derived from Edmund Husserl’s (1963) phenomenological theories how experience is structured.

The concept of the lifeworld is helpful syntactically in its immediacy, conveying an interest in the holistic experiences of others, while semantically within the domain of phenomenology it recognizes that there is often a relationship between the mundane and the exceptional parts of experience which are inextricable; that the relationship between social reality and experience can be understood to convey certain dynamics which need to be understood in the course of analysis, a kind of metaphysical exchange of energies and/or meaning between the subjectivity of individuals and larger formations they are experiencing. As such, the concept of a lifeworld has become central to phenomenological and ethnographic methodology as “a generative site in which the cultural and historical patterning of these various modalities of experience is currently being explored” (Robert Desjarlais and Jason Throop, 2011, p. 91). What’s important to recognize about this theorization of the lifeworld then, is that larger formations may mediate experience, but that they also provide an access point into the subjective realities of an individual and may speak to idiosyncratic, local and unique elements of their lives. To put it more concretely into the context of this study: while it is worth considering how CTF influences the experience of its participants as a game, learning tool and community it is also worth considering *why* this experience fits into a participant’s life and what is unique to *their* understanding of this experience and how *they* have arrived at *these* moments with *this* game. Recognition of this two-way street between formations and experience preserves the phenomenological core of the study’s methodology through an appreciation of the important knowledge to be gained from how a participant comes to access experiences which are the subject of the study.

The epistemic implications of the phenomenological turn accounts for the fact that experience may be structured by external forces, but that people are also guiding, shaping and building moments contingently (the interaction of subjectivity and agency), that ultimately the two coalesce dialectically into new experiences and structures. Such an approach has ethnographic implications, but historic ones as well by recognizing that identities, communities and their histories are not deterministic, instead they are concomitantly produced through both human subjectivity/agency and structure. Thus, good phenomenological scholarship is prepared to recognize 1) when contingent moments are incongruous with existing understood structures, and/or 2) when structure is being imposed or is understood to influence experience, but primarily it should 3) seek to navigate a negotiation between subjectivity and structure, where the boundary between contingency produced by human experience and objects (identities, cultures, technologies, systems) are messy and demarcation is not absolute. This understanding resonates with Desjarlais and Throop's (2011) argument that "phenomenological perspectives" allow scholars to "consider the ways in which political, social, economic, and discursive formations intersect with the operations and felt immediacies of bodies in a number of sociocultural settings" (p. 90). Epistemically, such an approach is well suited to exploratory research on knowledge-driven and highly social games like CTF because it can account for how the subjective experience of participating in such games is likely to create encounters with structures but is resistant to this experience being entirely determined by existing formations. In qualitative research scholarship often emphasizes the importance of unexpected or incongruous experiences in exploratory data collection as part of an emergent and iterative framework (Saldaña, 2013, p. 45, Woolf and Silver, 2017, p. 14**)**; a recognition that subjectivity and human agency may push back against anticipated or stable understandings. Such an approach aligns with Piaget's (1971) theorization that individuals do not possess "hereditary" knowledge of structures but that these structures are learned and understanding is often incomplete in the course of their application (p. 9). Social phenomenology recognizes that knowledge may be incomplete, but experience reflects an enacted or attempted understanding which describes a relationship between subjectivity and larger structures; to quote science fiction author Caitlyn R. Kiernan (2017) "I don't know what half of it means, and I don't pretend that I do. I can understand without perfect understanding" (p. 14). This appreciation of experience reflects Jackson's "radical" approach to phenomenology, which makes it possible to center moments when data is incongruous with existing formations (theory & structures) (p. 25) but can prioritize and explore emergent moments of incongruity to document development, but also novelty, alterity and variety in the experiences of research participants, specifically in their engagement with communities, identities and their interaction with technologies.

3.3 Methods & Research Design

To address and answer these research questions the study, in alignment with my methodology, utilizes a multi-method qualitative research design consisting of three methods:

1) Observation of three different CTF teams during three different competitions,
2) Semi-structured interviews with capture the flag organizers & competitors and;
3) Original historical and archival research into the history of CTF competitions.

This research design utilized an inductive, qualitative approach due to the exploratory nature of the subject matter and the methodology focused on the experience of play, but also the social structures and phenomena which help to contextualize the game. As such, the methods utilized for this project are intended to elicit an explanation of both 'what' a CTF is, who and why players engage with the game but also considered socio-historical procedures and context that shape the game.

3.3.1 Locating Fieldwork Sites and Participant Recruitment

Preliminary research into CTF indicated that it is a diverse practise representing distinct forms (game types), objectives (both learning and competition) and communities (specific hacking practises, geographic and cultural concentrations of expertise) who might play the game and at the same time the game's diffusion represents a shared logic and an accumulation of technical practises and technologies. As such, it made sense to utilize what George Marcus calls a "multi-site" ethnographic approach to "examine the circulation of cultural meanings, objects and identities" (p. 98) amongst the diffusion of CTF competitions to account for both diversity and commonality in how the game is orchestrated.

Based on the approach of performing a multi-site ethnographic study, a key objective of the research was to perform observation and recruit participants from the various competitions observed. To this end, I sought to represent both those who orchestrated and those who played in the competition as research participants to speak to the distinct and local character of CTF play, but in accumulation, this variety of participants should also draw similarities between the sites. As such, participants were broken up into two designated groups: “organizers” and “players.” The first group identified as organizers were individuals responsible for running CTF competitions I attended, including planning these events, designing various challenges as well as building and maintaining the computer infrastructure and networks the game operates on. In some cases these individuals might have multiple roles, both as an event organizer, producing the event itself and as a challenge designer, creating the technical challenges which are the central unit of play within a CTF. The second participant group “players” were individuals who were competing in the events that I studied. While the experience of both groups of participants are central to understanding the phenomena of CTF and both were identified as useful interview subjects, I prioritized the observation of players as their experiences during the CTF were more likely to be emergent and informed by forms of serious and laborious play within the competition itself. Comparatively, much of the organizer’s work would be done prior to the event in private and therefore, would be a more suitable source of data which to be collected in an interview.

In the course of this research, I set out to attend three CTF events, where I would observe a CTF team and recruit 3-4 of its players and 3-4 of its organizers for interviews from each event. To this end, I identified several CTF competitions organized during 2019 and selected those events which were scheduled late enough in the year for me to obtain advanced consent prior to the event. As CTF is a global eSport with players representing a diverse array of nationalities, cultures, languages, and dialects, events where the game would be predominantly in the language of the study, English, or at least partially conducted in English where I would be most likely to encounter English-speaking teams were prioritized. Ultimately, I settled on three events which were organized from May through November of 2019 in Canada and the United States. I contacted event organizers over e-mail using publicly available contact information. CTF organizers were identified as important gatekeepers to my fieldwork since they would be providing assent for me to attend the event and thus provide some level of access to players. My initial e-mail to the organizers used a template describing the study and identifying my personal contact information (including phone number) as well as my supervisors’ contact information to ensure the study operated with the highest degree of transparency and integrity. Being transparent with the nature of the study and openly sharing my contact information was a deliberate strategy to signal the authenticity of the research since many information security professionals whom I would likely be in contact with are charged with combatting phishing e-mails and other digital forms of fraud and abuse. As a result, being transparent as possible to secure the trust of and access to research participants was designated as a high priority in my initial communications.

Once I made contact with the CTF organizer, usually designated as a “captain” or “lead,” I requested: 1) assent to attend the event, 2) for the distribution of a recruitment flyer to players & other organizers and 3) an interview with the captain/lead organizer. Since scholarly research has emphasized interest amongst hackers in privacy, digital and civil rights, (Denning, 1990, Jordan & Taylor, 1996) I included my informed consent forms as part of a follow-up communication once I heard back from the organizer to indicate the rigour of the study and the rights of research participants. I deliberately did not include file attachments in any initial communications for two reasons: one, attaching a file would increase the likelihood that the communication would be intercepted by a spam filter and two, information security professionals are often wary of file attachments from strangers, as they can often contain malicious software. So informed consent documents were sent in subsequent communications so that I could build rapport and trust with a prospective participant and someone identified as an important gatekeeper to my research. I also made an informed consent document available from an un-indexed URL on my academic website so, if need be, prospective research participants could access the document using the maximum amount of discretion they saw fit to protect themselves from the document being malicious.

The recruitment flyer I requested for distribution by the organizers described the study and linked to my informed consent documentation. The protocol also accounted for the possibility that the organizers would be unwilling or uncomfortable in distributing a recruitment flyer on my behalf. In those cases, my protocol allowed me to request permission from the organizing committee to recruit a team of players myself either prior to, or at the event. Ultimately, only one event chose to distribute my flyer and the rest asked that I perform player recruitment myself. In those cases, I was extremely lucky in that the first two teams I approached (involved in separate events) assented to observation.

As part of the interviews I conducted with participants designated as CTF organizers, I also utilized snowball sampling. Having CTF organizers refer me to others through the process of snowball sampling was a logical part of the recruitment procedure, since my point of contact with CTF events tended to be with usually a captain or lead organizer and these individuals often had useful insights into which of their peers would be amenable to interviews. Added to this, publicly available contact information for other members of the organizing team was often not available, so I was reliant on a central point of contact to connect me to other participants. Snowball recruitment was extremely fruitful in that I was able to speak to many highly experienced CTF organizers and challenge designers and with some serendipity, a procession of former CTF organizers, who described playing in CTFs as early as 1998 and organizing them as early as 2001. These snowball research participants provided a great degree of historical insight into the maturation of CTF play and organization over the past three decades.

3.3.2 Informed Consent Procedures

Research participants were provided with a three-page informed consent document upon my initial contact with them, either in person or via e-mail. The informed consent document was written in accessible language which avoided specialized academic/legalistic terms or clearly defined the use of such language. The legibility of the informed consent documentation was identified as a high priority to create a level of transparency in the study and build trust and rapport with research participants. The informed consent documentation described their rights as a research participant and my responsibilities to their data and confidentiality. Informed consent documentation allowed players to assent to being observed by signing the document but included subsequent options regarding interviews and data transcription. One subsequent option on the form allowed participants to opt-in to being interviewed at a later date. I chose to make interviews optional to make participation in the study less demanding and to improve the feasibility of initial participant recruitment. I also provided an option on the informed consent document for participants to opt-out of having their interviews transcribed by a third party. In considering the historic propriety of hackers over their personal information and identities the informed consent document could be signed or, as an alternative participants could provide an alternate form of verbally recorded assent for those who chose to exercise that right. For this alternate procedure, I carried a dedicated digital voice recorder with me during fieldwork to record verbal assent to the documentation.

3.3.3 CTF Observation

CTFs can occur both in-person and online, depending on the nature of the competition, and is often contingent upon its affiliation with an established in-person information security conference. Since many CTF competitions are undertaken by teams at conventions, it made sense to study this cluster of participants in a unit as they compete in the context of the convention. To this end, I observed 3 CTF competitor groups of 8, 10 and 40 competitors as they participated at an in-person CTF competition, which occurred concurrently or overlapped with the program of an affiliated hacker conference. While interview-oriented data collection could account for the experiences of CTF players in these events, the study's ethnographic and phenomenological approach necessitated that I too should have direct contact with the experience of participating in an in-person event to understand the context and structure of such competitions. Establishing this context and structure of CTF play during fieldwork is important as scholars of ethnography have increasingly argued that "interviews are unlikely to be productive by themselves", and that "multiple methods should be used in any investigation" where ethnographic research is performed (Walford, p.118, 2009). Attending the events in person was also valuable insofar as I was lucky enough to develop a rapport with some research participants which was reflected in interviews where some indicated trust or appreciated a mutual understanding of my presence during their experiences. In some cases, those participants were able to reflect on shared and common moments of observation or indicated they were comfortable in describing some personal aspect of the game they might otherwise not communicate with a total stranger. I am deeply grateful for the level of access I was afforded through my observational fieldwork.

The CTF events I observed ran for roughly two to three days. Attending in-person rather than virtual competitions was valuable insofar as it took advantage of the co-presence of players at the event and availability for observation, giving me the flexibility to observe multiple members and their interactions simultaneously, but also to alternate between close observation of different participants. On a full day, I spent roughly 16 hours performing observation, logging 7 full days of observation and an additional 24 hours across partial days. In addition, I spent 3 days, approximately 48 hours at associated information security conferences, observing the proceedings when CTF competitions were not running. In total, I logged approximately 208 hours total of observation. Being situated with participants for long periods of time at the events was important, as ethnographers have argued that "continuous presence at the scene of action allows direct insights into the participants' different forms of knowledge" (Kalthoff, 2013, p. 271). For example, greater collaboration tended to occur near the end of competitions when the players were tired and a division of labour made certain tedious tasks easier to accomplish. All of the events accounted for in this study included a break at night for players to rest and return in the morning, and during that time the game services were taken offline and participants were not able to access challenges or submit flags. While there were likely times that participants worked on challenges after-hours with downloaded code or discussed strategies or plans while I was not present during evening breaks, taking this time was intended to provide research participants with a degree of personal privacy and space from observation, as well as allowing me to rest, collect my thoughts, notes and observations. Staying in my own accommodations, going to sleep late and waking up early to trudge over to the CTF was considered commensurately symmetrical to the experiences of my research participants who likely were doing the same during these competitions. Added to this, CTFs are competitive spaces, and the mood of players and organizers was commensurately tense, so holding personal space for research participants was a key objective in maintaining trust and safeguarding my access.

To document my interactions with competitors during a CTF, l made use of ethnographic field notes including both observations and reflections on what occurred during fieldwork (Bogdan & Bilken, 2007 p. 38). Observations were recorded in 9 notebooks and transcribed after the event into a digital document for later coding and analysis. Epistemically, these notes reflected my phenomenological approach, considering not only what is said or what occurs, but also the context and relationship to a procedure in which these observations occur. To this extent, my observations utilized "thick description", an interpretive framework to focus on the events themselves, but also bring to light "intentions and meanings that organized the experience" and establish this experience as part of a larger process (Holliday, p.75, 2007). As a specific method of recording notes during fieldwork, thick description popularized by the anthropologist Clifford

Geertz (1973) is well suited to a phenomenological and ethnographic research project in that it considers both the “phenomenalistic” (p. 6) aspects of an individual experience and activity with the “object of ethnography: a stratified hierarchy of meaningful structures” which are “produced, perceived and interpreted” by the researcher (p. 7). Thick description is as much a way of doing what John Van Maanen describes as “headwork” insofar as it conceptualizes an understanding of what data is valuable to the “representational practises” (p. 22), from what he distinguishes as “fieldwork”, the techniques for “gathering research materials” to “see, hear feel and come to understand the kinds of responses others display (and withhold) in particular social situations” (p.219). As such, notes taken during observations underwent multiple passes to identify linkages between observed experiences and larger events, formations and structures which were more obvious upon reflection as a method consistent with the approach used by other ethnographic scholars (Walford, p.125, 2009). My approach to thick description also served as an informal procedure during observation: 1) observe, 2) think and identify linkages between observations, as well as unique experiences 3) link and analyze events which share obvious procedural connections or share more symbolic connections, isolate unique experiences for further analysis.

The study’s application of thick description as an analytic framework was also useful in taking into account the function of CTF within certain fieldwork sites. Wynn and Williams (2012) have argued that thick description can allow a researcher to “take into account the breadth of information technology, social, organizational, and environmental factors” (p. 787) that come into play during fieldwork. Given that most prominent capture the flag competitions occur at hacker/information security conferences, it made sense to attend the event to situate the competition within the convention where possible. Understanding the conferences and their focus on specific practises and communities shed light on nuances and specific functions of the CTF within a local setting. This approach to close observation and thick description was useful in identifying local and specific experiences with the information security community and hacker culture, which informed the content of the interviews and my thinking as it pertained to specific events. In many interviews with organizers and participants, I used my field notes to inform the semi-structured interviews to identify relationships and linkages between specific moments or relationships I observed and the research participant’s own understanding of those moments.

3.3.4 Semi-Structured Interviews with Organizers and Players

Over a period of 12 months, I interviewed 20 members of the CTF organizer/design community. Predominantly, these were the individuals responsible for orchestrating the events I attended or designing challenges at the events but also included past organizers of one CTF and one well-respected organizer (whose event I did not attend) I was referred to through snowball recruitment. During the same period of time, I also interviewed 27 CTF competitors who were present for my observation at a competition I attended. All interviews were performed over various videoconferencing (voice over IP) applications, mostly Zoom due to its ability to record a local copy of the interview which could later be transcribed, but I also used a few other platforms based on the operational security and open-source ideological concerns of some participants which necessitated recording the conversations with an external audio recording device. To best focus my participants on description, I tried to ensure interviews took place in a short period after a competition, while their recall remained fresh. However, due to the fact that the ending of many competitions coincides with the end of a conference and are usually followed by a celebratory CTF after-party or travel home, I settled for interviews between one week and two a month later in most cases.

The interview questions I prepared for organizers focused on their personal history with CTFs, their knowledge of CTF history, their approach to communicating security knowledge through their challenges and any work they performed in the information security industry (see Appendix F: Interview Questions for CTF Designers). In almost every case, organizers were also highly experienced CTF players, so many of our discussions reflected on their rationale and design of CTF through their experience as players. These interviews lasted one to two hours, to speak to the breadth of an organizer's experience and to compensate for the fact that I had not observed their work at the CTF directly. By comparison, the questions I had for players focused on their experience at the CTF, prior experience with information security topics covered in the CTF and any relevant work or studies they perform related to information security (see Appendix G: Interview Questions for CTF Players). The number of questions for CTF players meant that the interviews lasted about one hour, but in three instances I recorded two-hour interviews with highly experienced CTF players who had a surfeit of experience and/or had also designed their own competitions.

Considering the study's primary objective was to engage with research participants about the relationship between playful and professional work, a majority of the questions were focused towards technical practise and personal experience. As Brinkmann has observed, ethnographic interview questions are the most effective when "their goal is to acquire concrete descriptions" from participants, "rather than thoughts about why they have certain experiences" (Brinkmann, p.1003, 2018). To this end, my questions tended to focus on challenges the players worked on, what resources including software, documentation and any acts of collaboration that occurred between players as well as relationships between the kinds of hacking performed at a CTF and the kind of security work they performed in their work/studies. These questions were intended to identify the laborious practises that constitute play, but also to tease out the participant's experiences and literacy of hacker culture. As it pertains to my methodology, I sought to use interviews as a "speech event for the mediation of the media experience", "leaving ample room for informants to express" and identify "their lifeworld-derived meanings and attitudes in their own discursive terms" (Schrøder, p.51). The nature of semi-structured interviews also allowed me to utilize activities and events I witnessed during the CTF to add context, provide prompts or clarify descriptions that occurred during the interviews to document "logic in use, the procedural knowledge used when people take action" (Knight, p. 115, 2002). Using observation to inform the semi-structured interviews were useful in helping participants ground their responses or to recall specific events, allowing me to map out coherent processes wherein a participant attempted a challenge, when they used intrinsic knowledge or accessed extrinsic information or software to assist in their play. For example, one term I consider having been co-developed with research participants was the idea of "advancing" a CTF challenge, a term which describes how a player might contribute to the solution of a complex challenge within a team context to identify their procedural contributions while relieving them of language that suggests their work was the sole solution to the problem.

3.3.5 Original Historical & Archival Research

In conjunction with observation and interview, this study seeks to ground its analysis of CTF in the history of hacker culture and its communities to explain its emergence and identify linkages to the professionalization of hackers in the information security industry. Ethnographers including Denzin (1978), Berg (1998), and Rowlinson (2005) have established the utility of using historical research to supplement ethnographic fieldwork, emphasizing its immediate value in assisting a researcher's understanding of a culture by identifying historic relationships and context (Rowlinson, p. 296) by synthesizing it with for the lived experiences of research participants (pp. 298-299). This approach is consistent with historian Geoff Eley's (2008) observation of general trends in historiography (the discipline of history) particularly since the 1990s which have shifted from broad social histories to "microhistories" which favour "particular communities, categories of workers and events", a fixation with "the specificity of the local account" that is capable of "generalizing its relationship to larger social processes via exemplification" (Eley, p. 184). Drawing on both the arguments of historians and ethnographers, it's clear that historical research has utility not only in helping to situate data collected through ethnographic methods but also shares a common interest in analyzing specific communities and practises in pursuit of understanding larger socio-historic trends.

To structure this effort of this effort, I conducted an extensive historiographical literature review found in Chapter 2, which contextualizes the scholarly study of hackers over the past 40 years. That chapter identifies a shift in literature on hackers, their practises and communities which initially focuses on concepts of alterity, deviance and criminality centred on the computing underground which gradually shifts towards an engagement with distinct political values around personal freedoms and the emergence of the free and open-source software movement. The historiographical shift in this literature on hackers emphasizes an understanding of the emergent valuation of hacker labour in the technology industry. Specifically, that chapter also identifies how hacker practises towards information security have been understood and have re-emerged as a focal point of scholarship in the last 10 years. In accordance, this study of how a hacker game relates to the production of information security practise and knowledge is understood to be presented in continuity with existing research. In Chapter 4 I contrast the information security practises of the computing industry and academia in the 1970s and 1980s to those of hackers to distinguish between their radically different epistemologies and practises, to establish why hacker approaches to security represented a fairly significant break from the dominant paradigms of the time, an approach which also contributes to an appreciation of why hackers were marginalized despite their obvious expertise. This historical analysis provides me with an entry point to discuss the practises used in CTF and how they are representative of certain forms of knowledge and technology production/practise within the hacker community.

In sourcing my historical research for this project, I made extensive use of the Defcon Media Archive, a repository of primary accounts of the conference where CTF originated and early secondary reporting on the conference, specifically examining instances of CTF and games related to technical labour. Documentation retrieved from the Defcon Media archive included past conference programmes, photographs, textfiles (blog-style journals usually shared on electronic bulletin board systems) and press releases and press clippings (scanned magazine articles and text ripped from now-defunct websites) that had been preserved in by Defcon's organizers. Also, I made use of secondary sources written from 1995 through 2005 in technical reporting and academic publications that referenced early CTF history, key figures and events. This research was supplemented with archival documentation preserved through the Internet Archive's Wayback Machine, which I utilized to access dead links referenced in primary and secondary materials I found to various hacker websites and communities. I typically used the information from these to corroborate data collected during fieldwork or in some cases, to supplement interview questions. Verifying ideas found in this documentation in interviews does provide a level of "external" or "negative criticism" of their veracity (Rowlinson, p. 298), but this is beside the point; rather my objective here in using historical documentation is to "concentrate on meaning and the forms of perception people make and display" in the communities, I am studying using this data (Eley, pp. 185). In that sense, my use of historical documentation and how it was used in interviews was to establish context and sentiment with my participants. Ultimately, in mobilizing historical data in this project I'm interested in documenting change over time in perceptions, practises and understandings of games, competitions, technologies and the social context of CTF within the hacker community, particularly as it pertains to labour and the form/value of hacking.

3.3.6 Data Analysis & Production

In considering information produced through observations, interviews and historical research, this dissertation must also consider how such information was organized in preparation for analysis. The course of research indicated that CTF was a diverse practise accounting for games, play and competitions which ranged from education to professional and competitive engagements with hacking. Accordingly, my line of inquiry with research participants in this project is oriented towards describing a variety of technical practises, communities and working conditions around hacking and the technology industry to represent a diffusion of experiences, rather than a totalizing or single voice representing a unitary experience. The methods employed in this research produced four distinct forms of data including notebook transcripts, interview transcripts, found media and archival research.

Transcribing 9 notebooks and 47 interviews consisting of 81 hours of recorded conversation produced a surfeit of complex textual data which required careful organization. To do so, I adopted a coding system to assign a "word or short phrase" to identify a "summative, salient, essence-capturing, and/or evocative attribute for a portion of language-based" data (Saldaña, p. 26). To manage the coding of text data produced from interviews and observation I utilized the computer-assisted qualitative data analysis software Nvivo for its ability to coherently organize both the coding and analysis process. Three methods of sub-coding were used to produce high-level "nodes" in Nvivo which distinguished between coded data based on the type of information the text contained and "codes" which referenced shared/similar concepts, processes and ideas. The first node was "descriptive" text, which housed codes for the description of a specific person, place, thing or event. For example, a participant's description of a CTF challenge would be tagged as "desc-challenge" but could be sub-coded to "desc-web challenge" if the challenge was oriented towards hacking a website or web-based application. The second node "process" identified a passage of text which described an experience procedurally. For example, if a participant described similarities or parallels between their job and a CTF challenge, that passage was tagged "proc-relationship to labour." Finally, the last node was "values" which was used when participants identified a belief or referenced a belief they associated with a specific community or form of politics. For example, "valu-openness" was applied to passages of a transcript where a participant described how and why open access to software, code or knowledge about a technology was meaningful to their experiences. This node hierarchy allowed my analysis to focus on objects and processes and was effective in the analysis process in that I was quickly able to identify and access similar passages to develop ideas coherently about certain experiences but was deferential to my phenomenological approach since it only attempted to isolate certain common textual artefacts within the corpus of the data, rather than reduce the data I had collected to simple themes.

3.4 Data Summary and Analysis

In the interests of transparency, the following is a summary of the data collected in this study.

Data collected in the course of this study included:

- I performed observation at three (3) fieldwork sites
- 9 fieldwork notebooks were produced from approximately 208 hours of observation[13]
- 83 signed informed consent documents were collected from research participants
- 61 were from participants identified as players
- 22 were from participants identified as organizers
- 17 of the CTF organizers were recruited through a snowball recruitment procedure
- 50 participants opted-in to be interviewed via their informed consent documentation
- 47 attended an online interview which was scheduled at their convenience
- None (0) of the research participants who contributed data to this study opted to use the alternate procedure of providing oral assent
- 16 did not consent to having their interview recordings transcribed by a third party and I manually transcribed their interview
- 1 manually transcribed interview was transcribed twice after my computer mysteriously destroyed the excellent transcript, I spent five hours producing
- 81 hours of semi-structured interviews were recorded from 21 interviews with organizers and 25 players

Finally, two (2) players who were present during one observation verbally assented to my presence but did not assent to being a research participant due to a shared conflict of interest on their part, which I cannot specify out of respect for their privacy. These players brought

[13] 160 hours at CTF competitions themselves and 48 from information security conferences I attended as part of the study, usually on days when the capture the flag contest was not running.

this to my attention at the outset of my observation and no data was collected on their activities or interactions with others during observation.

3.5 Emergent Characteristics and Limitations of the Research

3.5.1 Representation

I did not formally collect demographic data about my research participants as part of the research design. With that being said, I will disclose that research participants representing a spectrum of gender identities are underrepresented, but not absent in this study, as are people of colour. Three factors contributed to the diminished representation and recruitment of non-white, non-male participants in this research.

1) Priority & Limitations

Due to the exploratory nature of this study and the limited time and resources of the researcher, no particular priority was given to the recruitment of any particular demographic groups amongst participants. Concerns over the feasibility of participant recruitment were given priority over representation amongst participants to ensure the largest amount of data could be collected as possible during a 12-month period.

2) Recruitment & Research Design

The research design and participant recruitment were intended to be extremely deferential to the organizing committee in participant recruitment and did not express interest in participation from any particular group to ensure the highest likelihood and feasibility of being situated with participants.

3) The Provisional Nature of CTF Play and Teams

During preliminary research into the topic, I observed that CTF teams, particularly in smaller events, tend to be provisional and informal with no formal point of contact that could be secured prior to a competition. Considering these conditions, it would have been unfeasible to recruit more representative teams prior to the event as I would not have had access to these groups prior to a competition. Given that the fieldwork for this study required 4-8 hours of travel to sites, lodging and other provisions which the researcher paid for out of pocket, identifying participants prior to the event was given the highest priority to ensure the success of the study.

Through reflection on critical scholarship at the intersection of race and gender and the position of the researcher (Dunbar-Hester, 2019, pp. 26-27) and my own efforts at self-awareness I opted to be cautious during participant interactions and recruitment. I realize that as a six-foot tall, 220-pound white man in his 30s, I represent a potential source of physical/sexual violence as a stranger amongst my research participants. As such, I tried to be cautious in my participant recruitment and management to avoid imposing or leveraging my identity or work as a researcher to subtly manipulative or coercive ends. I had a personal protocol that accounted for difference in my participants when recruiting them for observation and interviews. To this end, I never conducted in-person observation alone, outside of a public space and I would only make a single request to teams for observation or to a player for a follow-up interview. If an individual was unresponsive, I would not make a follow-up request. In some cases, this meant not following up with individuals amongst groups who are underrepresented in this study.

Over the course of my research, I identified alternate venues, teams and recruitment strategies that may have yielded greater representation in future research. Studying events like the Diana Initiative CTF and potentially partnering with groups focused on the inclusion and education of women and people of colour in information security would be likely to yield more diverse players and organizers to understand and articulate the experiences of groups which are excluded or understudied in the technology community and as well as in my current program of research.

3.5.2 Failing Early and Failing Often: Documenting Iterations in Research

Qualitative research is often understood to be inductive and iterative (Woolf and Silver, 2017, p. 14) and the research protocol in this study required no small number of revisions which changed both the way I recruited and interacted with participants, but also informed how I understood the game and culture central to this research. I am documenting elements of the initial protocol and the rationale here because they not only reflect the protocol and methods employed in the study, but they also describe the very human side of my research program and the interaction I had with participants. Such personal and contextual negotiations were so frequent and developed on a case-by-case basis that their description as part of a procedure earlier in the chapter would have been too difficult. Additionally, many of these changes to the protocol required systemic alterations, where one change to the protocol necessitated a cascade of alterations which had to be negotiated in my documentation of the research as well as with my university's research ethics board. As a result of this complexity, I have documented the history and acknowledgement of iterations in my research protocol separately from the final research design described above, as these changes introduced a great deal of complexity into the texture of my work. I chose to document these changes to indicate the journey of my program of research and how its protocol was responsive in encountering research participants, their needs, requirements and idiosyncrasies which add texture and meaning to the study.

Originally, I had intended to study 4 players at each event and 4 organizers (16 of both), recruiting roughly 32 interview participants at most. In the end, I recruited 25 interview participants and observed 42 more players at a CTF event. The inflation of my initial estimates was necessitated by early interviews, when I realized in interviews that the diversity of experiences players and organizers had in a CTF were often highly incongruous and specialized. Further, after attending all three CTF sites in this study, I also realized that the competitions themselves were often quite different, not just in terms of the style of game being played, but also their audiences and the rationale behind their organization. Consequently, I attempted to interview as many participants as were willing to account for a range of experiences and to see as much of the 'bigger picture' in the CTF as I could account for. In truth, I could have collected half, or even a third as much data and completed this study in much less time, but curiosity (and ambition) got the better of me.

To recruit participants, I had initially planned to reach out to competitions through publicly available contact information, or through the administrators of the conferences the competitions were affiliated with. Initially, I identified four potential fieldwork sites. In two cases, I had direct contact with the organizers and in two others, I worked through a press liaison in the organization to connect with the CTF organizers over e-mail. In the latter two cases, the liaison was careful not to disclose contact information until a member of the organizing committee expressed interest. In one of those cases, the press officer noted that the CTF organizers never replied to their requests regarding my inquiry. By that time, I had already interviewed 40 CTF players and organizers and still had at least 17 scheduled interviews, so having exceeded the number of participants I had estimated and being oversaturated with data already the final event was determined unnecessary, and I thanked the liaison for their efforts and eliminated that event from my study.

While I was ultimately successful in recruiting a sufficient number of participants for my study, my initial approach to participant recruitment required significant iteration reflecting the variability of CTF teams and the competitions I studied. Originally, I had believed that CTF organizers would prefer to operate hierarchically and might distribute a recruitment flyer to players on my behalf over e-mail and any interested parties who saw the flyer would get in touch with me. Since players tend to pre-register or have to participate in a qualifying activity, I had assumed this approach would be deferential to the organizers who might prefer that a third party not use external channels to track down interested players and could retain some level of visibility and control over my recruitment.

This centralized, hierarchical approach to participant recruitment in my protocol was also intended to address the variability in CTF team composition. In preparation for this study, I looked at a number of online sources about CTF teams and informally surveyed the social media of CTF teams. My preliminary work indicated to me that while there are a number of well-established competitive CTF teams, they tend not to play in smaller, more regional competitions or those explicitly targeted at learners. Many of the better-established teams are composed of students from a university’s computer science department or are part of a computer security/hacking club, or funded lab, within these institutions which sustains their organization. By contrast, a vast majority of the teams that play in a CTF are informally organized, particularly for smaller competitions, where networks of friends, peers and co-workers self-organize into provisional, ad-hoc groupings often geographically situated clusters of expertise. Since such players represent the majority of CTF participants, recruiting and studying teams formed in this way was a priority in understanding the texture and lifeworld of an irregular and/or casual CTF player, to understand their social networks, motivations and engagement with the event they were playing in. Amongst both informal and more institutionalized teams, some members play regularly while others drop in and out based on interest and availability; while other teams may coalesce around a single event and dissolve entirely afterwards. For example, at one event I studied the players all worked at the same company and their employer-sponsored admission and travel to the CTF; the team's composition of players was ad-hoc based-on interest amongst employees, but many of the players had experience working with one-another prior to the contest. At another CTF event, the organizers had captains draft players anonymously from a list of de-personalized profiles based on their work experience (Chapter 6 will document the former and latter teams in greater detail). The last team I studied was well-established and well-known; playing at the highest level of CTF competitions was largely composed of students, academics and their extended social network of security experts/hackers. As a result of these variables in team composition observed in my preliminary research, it made sense to approach the organizers to centralize recruitment and I had assumed this approach was suitably deferential to the privacy of players and the integrity of these events.

This hierarchical recruitment approach was met with mixed success. One of the first organizers to reply to my initial request to study immediately rebuffed this approach to team recruitment but assented to my presence at the competition and agreed to participate in an interview. While this initially flustered my recruitment effort for his event it was an interesting data point and Pawel was happy to explain his rationale during our interview:

> I mean, that the basic idea is that [our event] is viewed as the world championship of hacking, and as such, we are pretty careful to maintain its integrity. So, it's, it's very easy to profit, not just financially, but you know, in all sorts of ways from a position organizing the world championship, right? […] It's very important to maintain a set of guidelines that you operate under. And so, my guidelines include, for example, that I don't, you know, as the captain of the organizing team, I don't use that position, and none of our people use that position to compel participation in in whatever: interviews, events, etc. And this extends well beyond the interview. So, I mean, I'm sure that if I had reached out as the [lead organizer] with a, with a request […] that someone participate in this interview, they would they would have a higher chance of doing it, but that would look pretty bad, right? *What are the implications of not doing it*? [Emphasis mine].

As he explained it, Pawel's event was extremely competitive and his body of organizers were commensurately careful to maintain a policy which ensured the organizers were understood as impartial by the players. Requesting to situate a researcher with a team, as Pawel explains, might have been considered an overreach of the organizing body's authority which would jeopardize their objectivity and integrity. Pawel did offer to send my request to a few close personal contacts who played in his CTF, but to maintain the integrity of his organizing committee he noted that I would have to reach out to recruit a team myself prior to the competition. While this demand created a new challenge for participant recruitment, it was an extremely rich encounter that added data to the study, helping me to comprehend issues of fairness, integrity and the intensity of the competition Pawel was responsible for administering. Understanding these efforts to preserve the integrity and competitive spirit of CTF was extremely significant to my understanding of the seriousness of these competitions and the consequent need to maintain the integrity of their operations. Ultimately, engaging Pawel and many other organizers about issues of competition and fairness proved to be a valuable source of data which is described in Chapter 6.

Adapting my research protocol from Pawel's feedback also helped me negotiate a more grounded recruitment method, wherein I could recruit teams directly. The early revision proved to be useful at another CTF where the organizers had been offered to situate me with a team but had become uncomfortable about doing so as the event launched because of a technical issue that caused a service outage in the game.[14] Due to the game interruption, the organizers asked that I stand by and spend the first six hours observing the game without a team. When I returned in the morning, the organizers were still reticent with the idea of situating me with a team themselves, so I requested permission to approach a team myself using my amended protocol. From my previous time spent observing, I identified a team that seemed to be mostly communicating in English and presented diversity in terms of gender, ethnicity and age that would be suitably representative for the study, and when I approached them, the 8 players unanimously provided

[14] Every CTF I attended launched late due to technical issues or with some kind of immediate service outage, so this was not conspicuous. I document this more in chapter 4 in discussing the complexity of the technical infrastructure of CTF.

their assent to be observed and signed the informed consent documentation in short-order (thank God!). Ultimately, at only one of the events did the organizers agree to situate me with a team and did so prior to the competition. While this outlier reduced the friction required to study the event, it was conspicuous after so many other efforts were rebuffed. Investigating the process of how I was situated with a team in interviews, emphasized that the organizing committee exercised a much more centralized control of player teams and the operation of the CTF. Team organization was conducted by a captain that acted on the organizing committee's behalf. Understanding this also reflected the degree to which the event was overtly designed to train and enhance the educational outcomes of this event (described in Chapter 5), with captains working to scaffold player experiences. As such, making efforts to develop a more responsive recruitment protocol deepened my knowledge of values and structures which coordinate CTF play.

Another issue with this study was that I had originally intended to do as much research prior to the event or 'in the field' as possible, interviewing organizers during the competition and performing action interviews with participants while they played. I had planned that this approach would be convenient for participants and would minimize my demands on a participant's time, as I would not need to be in contact, or could spend less time with them later. However, attending my first event demonstrated that such an approach was unfeasible for several reasons: the CTF environment is too hectic, competitive and demanding for all parties to privilege interviews. Organizers were often under immense pressure to maintain the stability of the technical infrastructure of servers, networks and services that their games run on to discuss any or their work in-depth. Not to mention in many cases, the CTF was a social culmination of many private hours of technical development: it was clear that doing interviews might interfere with privileged moments of camaraderie. These considerations, combined with the fact that prior to or during an event, organizers were extremely invested in the impartiality and confidentiality of the game and were often concerned that I might deliberately or inadvertently disclose confidential information about the game to the players I was observing. This meant that CTF designers were not forthcoming regarding details or their thinking in the contest I'd be attending at a later date. As a result, I only interviewed three organizers prior to the CTF I attended and realized it would be preferential to perform follow-up interviews after the competition, when the organizers were under less pressure and when they would generally be more forthcoming with information that provided no competitive advantage. As such, after-the-event interviews were considered more useful for providing relevant data between their experiences and what I observed, which could thicken the descriptions I produced during observation.

Similarly, I had planned to interview players during the event during certain tasks using “action interviews” and I had imagined there would be some downturns in a 48 to 72-hour competition suitable for an interview. While I collected some data from talking to players during observation, I found that players often jumped from challenge to challenge with minimal discussion and often required a great deal of concentration during play. It became obvious during observation that answering batteries of questions was extremely disruptive to the concentration of players[15] if I was not contributing to the solution of a problem and downtime was necessary for players given the cognitive strain they were subjecting themselves to by playing a laborious game. As Van Maanen writes, good fieldwork ultimately means coming “to terms with the situational dictates and pressures presumably felt by those studied” (p. 220) and as a result, I tried to be respectful of the competitive reality in which I was engaged. In an ethnographic study of baseball, the researcher would likely observe the game from the dugout or the stands, but almost assuredly not standing on the field beside the second baseman. Observing downtime was also interesting because players would network, discuss work and/or topics of mutual interest which helped me understand how non-play elements of CTF influenced their lifeworld and experiences. In a few cases during their downtime players wanted to chat with me, often because I was a stranger or because they were interested in the study, which I happily obliged given my imposition on their leisure. Being conscious of my demands on players during observation, I opted to ‘shoulder-surf’ certain players for as long as it was feasible, requesting their permission on approach. This form of observation of the team was extremely fruitful and informed the semi-structured nature of my interviews, allowing me to situate questions about observed experiences of players or use it as a prompt to jog a player’s memory. However, because many CTFs are held in extremely cramped quarters, and I am large enough to disrupt the seating arrangement of other

[15] As described in chapter 5, through observation I quickly realized players often acknowledged difficulty in sharing information and coordinating their efforts amongst their teammates without disrupting efficient play. In many cases where players coordinated their efforts or shared information, it was often acknowledged that a special effort had to be placed on such exchanged.

teams I had to be careful about situating myself. Ultimately, I think a better strategy for observation would have been to obtain a portable, battery-powered monitor and sporadic consent from a player to “mirror” their laptop screen, shoulder surfing from a less conspicuous vantage while being able to closely scrutinize what a player was doing with a console or application.[16]

These changes to the research protocol demonstrate the importance of negotiating the relationship between the researcher, participants and the context of what is being studied. While my initial protocol was too conservative and rigid in how it approached participant recruitment and data collection, being in conversation with my participants and iterating on the design was extremely productive in situating data collection, but also served as a valuable and generative source of data in itself, for understanding the culture and activity that was the subject of my study.

3.6 Conclusion: Situating theory, methodology and methods

The phenomenological and ethnographic methodology and methods described in this chapter are well-aligned with the theoretical framework which has established that many hackers are not only self-taught but learn and develop technology, practises and communities through various unstructured points of access. Put simply, outside of signals intelligence agencies and militaries who train their recruits there are few recognized ‘schools for hackers’ so to speak and thus accounting for the individual enculturation of hackers and the decentralized way in which information security practises and identity are reproduced is a focal point of production in this research. Weaving individual experiences into the larger fabric of hacker culture and communities can help to explain the proliferation of a culture and industry by individuals who utilize its practises and understandings while acknowledging the limited institutions and centralization which might otherwise sustain such a body of practise. As such, I think of CTF not as a totalizing force of access and enculturation amongst hackers, but one amongst many, with its own idiosyncratic and unique characteristics which represent larger cultural and industrial

[16] Such an approach presents its own challenges as it would require the security-conscious participants I am working with to connect a foreign device presented by a stranger to a USB or HDMI port, not to mention a device which had been connected to the computers of other talented hackers and could have been potentially compromised.

structures. Approaching CTF as such an access point and identifying how its play, organization and logic maps into individual experiences, while representing larger cultural structures of play, learning and patterns of labour and employment is therefore productive in situating the game's function.

Chapter 4

4 Hacking as Play: The Aesthetics of Subversion

Capture the flag (CTF) events combine the productive, subversive and expressive elements of hacking, specifically security research/vulnerability research, into a gamified competition. To apprehend hacking as both an activity and a skill, in this chapter I draw on participant interviews and my observations to theorize security hacking as a practise which represents the deconstructive imaginary of security research, an ontology of reverse engineering in computing to identify vulnerabilities. This deconstructive ontology of vulnerability research allows hackers to produce unanticipated or contingent behaviour in information systems, programs and other technologies which undermine their security. Applying this theorization of hacking to CTF, I argue that these games represent intellectual exercises designed to playfully demonstrate the deconstructive imaginary of hackers, how they identify relationships within computer systems and then decompose them to undermine their security. Within CTF this deconstructive imaginary is represented playfully through the emulation of security research activities including code analysis, reverse engineering and exploitation. The activities performed in a CTF are intended to demonstrate both the player's skill in decomposing the functionalities of technologies (a decompositional ontology), but also the challenge designer's security research acumen in identifying/diagnosing a security vulnerability that prompts. CTF demonstrates the capability of a hacker by creating a space where contingent behaviour in technologies can be produced and that this process is highly bound up in community and identity formation, tied to those who are understood as the most capable of forming unanticipated relationships within information systems.

4.1 Theorizing the Relationship Between Security and Hacking

To illustrate how hackers transgress against the security of information systems, and particularly how this activity can be turned into a game, it is useful to have a high-level appreciation of what the relationship is between security information systems and how the subversion of security is conceptually understood.

The concept of information security covers a broad remit of functions, policies and designs in computer systems and the programs they run. As scholars like Randy Lipner (2015) have noted, the U.S. government realized in the 1960s the significance of computers to its strategic interests and commissioned many of its branches to produce both research and policy on the security of information systems. Organizations like the U.S. National Bureau of Standards (NBS)[17] extensively researched the topic, but also consulted broadly with stakeholder groups from the early computing industry to develop a shared conceptualization of information security and develop policy and standards (NBS, 1978). The NBS and later the National Institute of Standard's (NIST) conceptualization of the subject remains influential. One of the earliest[18] codifications of high-level security goals are noted by Susan K. Reed (1977) in her report *Automated Data Processing Risk Assessment.* She writes **"**it would be difficult to list all the undesirable events which could have a deleterious effect on data processing", so instead of identifying all the possible vectors of interference she argued that "risk analysis should focus on the potential results of these undesirable events, i.e., on the harm which they could cause." To this end, Reed identifies three categories of harm "1. those which cause a loss of data integrity 2. those which cause loss of data confidentiality 3. Those which cause loss or delay in automatic data processing" (p.9).

In a subsequent report from the NBS on the proceedings of its invitational workshop, *Audit and Evaluation of Computer Security II* (1978), the categories of harms were later refined into three "security control objectives": understood as integrity, confidentiality and availability of information systems and the applications which operate on them (p.xxi). Confidentiality, integrity and availability are often referred to as the 'CIA triad' model for security goals and while some professionals have tried to augment or refine this criterion (Parker, 2005) they have generally served as industry standards (NBS, 1980, Guttman, 1995) and are taught as a

[17] The predecessor to the National Institute of Standards (NIST)

[18] Both Reed's report and the subsequent Audit and Evaluation of Computer Security II (1978) reference draft standards composed in 1976 that were ultimately published in the report Guidelines for Security of Computer Applications (1980) by NIST which identifies confidentiality, integrity and availability as "security objectives" "common to many diverse computer applications" (p.8) (thank you to James Foti & Patrick D. O'Riley from NIST's archives for helping me to find this document).

foundational element of many certifications in the field of information security (Conrad, Misenar & Feldman, 2016, Peter, 2021, p. 110). Given the widespread recognition of these categories, they are useful for conceptualizing functional controls in information systems and establishing a criterion for how security is undermined on a conceptual level.

In 1988 Don Parker wrote that for a computer to be secure it "must perform exactly to its specifications and, equally important, perform in no unspecified ways" (p.291). By framing security as the assurance of intended functionality, his explanation of security resonates with the NBS's (1978) definition of a vulnerability as "a design, implementation, or operational flaw" which causes a "computer system or application to operate in a fashion different" from its understood specifications (p. A-2). What's useful about this definition of a vulnerability is that it recognizes that a flaw in an information system can lead to emergent functionality, but also that a flaw isn't necessarily a purely technical fault like a bug in a program's code, but could represent structural insecurity, a contingency in its design or function that enables certain actions. This way, we might consider vulnerabilities as a kind of affordance or contingency, an unanticipated property of an information system that enables novel behaviour which undermines the security objectives of the system.

Here it's useful to explain how the unanticipated, emergent functionality of an information system could undermine its security goals. For the purposes of this example, I'll use the 1988 Morris Worm described in the previous chapter because the functionality of the virus has been well documented. While the virus is quite old, the vulnerability it uses was relevant for 30 years after the incident, and the premise of an "overflow" or "overrun" attack which it uses remains relevant to many present-day hacker methods and security research, including those described in this dissertation. The Morris Worm, a virus, infected computers by attacking a vulnerability in the network service *fingerd* used by BSD Unix to undermine the integrity of targeted systems.[19]

[19] The Morris Worm used three different vectors to attack and a system: a vulnerability in SendMail, fingerd or .rhosts. This vector the virus used to infect a system was contingent on which attack the system might have been vulnerable to (Page, 1988). I selected fingerd as the exemplar for this section because its functionality was the easiest to explain in relation to the security goals of the system and the buffer overflow attack against the memory architecture of a computer demonstrates a deep understanding of low-level computer operations.

Fingerd is a network service known as a daemon that responds to instructions from external users on the Internet requesting information about a system including its status, operators and other details. The virus uses an attack known as a “buffer overrun” or buffer overflow, which works by sending a carefully crafted command to fingerd that we might describe as a “payload” which contains machine code and instructions which can be readily interpreted by the system’s processor. The payload of the Morris Worm performs a buffer overrun by sending fingerd a command larger than the size of the program it is designed to receive (Vu, 2019). Due to the memory architecture of many computer systems, which store data and instructions for different applications across “addresses”, the excess elements of the payload are then written to adjacent memory addresses than those used by fingerd. Given that computer operations are designed to be rational and repeatable, if a payload is written carefully enough the buffer overrun can emulate the low-level instructions regularly used by the computer’s processor stored across memory addresses and trick the system into arbitrarily running the attack’s code by placing them in the memory location where the computer expects to find routine instructions.[20] This is the crux of the vulnerability in fingerd: the program was never intended to allow a user to write information to other parts of memory from these commands, only to return information about the system. Ultimately, the Morris Worm’s buffer overflow exploits the vulnerability in fingerd to write an instruction[21] to the computer’s memory which granted the virus remote access to the command prompt of the system, where it could arbitrarily run its own commands without authorization from the system’s administrators. In so doing, the Morris Worm undermines the system’s integrity by allowing the virus, an unauthorized program, to run commands at the level of an authorized user against the system.

[20] There is some contention amongst security professionals as to whether the ability to write to memory arbitrarily after exceeding the buffer of a vulnerable program constitutes a separate vulnerability. There are those who contend that the flaw in fingerd is the sole vulnerability which enables abuse and the memory architecture is operating normally, albeit with bad instructions. However, there are those who cite the existence of several possible security controls used in the memory architecture of present-day systems to prevent a buffer overrun/overflow as evidence that allowing a program to write to low-level memory is a separate vulnerability.

[21] Referred to as “shellcode” because it prompts a computer to provide access to its administrative console or “shell.”

In many cases a single vulnerability, or hack used against a security control, may not be enough to undermine the security protecting a system. An attacker may have to use a variety of known vulnerabilities or ones they discover, pivoting across vulnerable systems or programs to undermine the system in the way they intend. In many cases, an attacker does not directly attempt to override the security control protecting a system, but instead they work around it using their ontological understanding of the system's security, an approach wherein they reveal information or perform functions which were not properly isolated from their level of access. Ultimately an attack might be able to wrest enough information to bypass a security control or wrest enough control to mitigate the control entirely. This procedure of exploiting a series of vulnerabilities is popularly referred to as "cyber kill chain" or "killchain". However, the term is a registered trademark of Lockheed Martin and a few of the hackers I spoke to during this study preferred the term "attack procedure" or "attack taxonomy" as they were weary of the company's propriety over the phrase and/or the military-industrial complex.[22]

As an example of attack procedures, one CTF I observed had players simulate a process used by cybercriminals to break into a corporate computer network. To start, players had to correctly identify a corporate user from a list of 150 potential accounts to gain access to an employee's e-mail address at a fake company, attacking the confidentiality of the e-mail system. With access to the company's e-mail system players then used confidential engineering documentation found in the inbox to remotely connect to the company's computer networks. Connecting to a Windows terminal from a compromised account, players slowly gained control over the machine by using vulnerabilities in the operating system's password management system from an administrative console to reveal more confidential information that would allow them to gradually perform tasks that would have been prevented by security controls, a process which would culminate in accessing data stored in another user's account on the Windows terminal. The challenge reflected the procedural nature of hacking complex information systems, bypassing security controls by

[22] I will use the term "attack procedures" when applicable in this dissertation since is explains the sequential and procedural qualities of hacking. Procedure is a more open-ended term, where by comparison the term killchain is distracting, as it implies cessation, the 'killing' of an activity. While some attack procedures might culminate in disabling or destroying a computer, attacking its availability, many others are used to attack the confidentiality or integrity of the system.

extracting fragments of information and/or control and using this leverage to eventually wrest full control of the machine and undermine its security operations.

What's remarkable about these attack procedures, or the Morris Worm, is the degree to which these attacks leverage the relational elements of an information system in their totality (contingently) to undermine the security of the system. These attacks utilize a deconstructive understanding of a system's ontology, decomposing relationships between its components to identify vulnerabilities and reconstituting their functions to produce novel, unanticipated behaviour within the system. Eugene Spafford (1992) and Bruce Baird et al. (1987) recognized this is the expertise which hackers apply to information systems: through a deep meditation on the relationship between the design and functionality of a program, or system, hackers produce a new understanding of the system's functionality, one which differs from the implied purposes, an insight that comes from understanding how these operations can be repurposed. In the present, this kind of analysis and the identification of security weaknesses is called "vulnerability research", when a hacker 'gathers information' that identifies a vulnerability (Ryan Russell, 2002, p. 100) which allows them to undermine a security objective of the system. By harnessing the components of a system hackers effectively reverse engineer[23] contingent functionality, which can be said to be unanticipated by the system's original designers. A CTF player and security researcher Hollis provided this succinct definition of reverse engineering as a process: "you have to understand the way things exist - in order to understand how they could exist when you're trying to engineer things." This explanation of reverse engineering struck me as profound, as it is indicative of the ontological framing through which hackers apprehend the capability of computers. A framing which informs their ability to imagine alternate functions, rather than accepting a more proscriptive understanding of their utility. By analyzing the code, functionality and affordances of information systems, and applying a *decompositional ontology*, hackers are able to imagine and implement not only new operations, but ones that can be used to undermine the security of such systems, despite controls designed to prevent such behaviour in the system.

[23] I use this term in the broadest sense as reverse engineering has a well-understood meaning in vulnerability research and specifically in CTF where a participant decompiles the binary (the executable portion of a program) and attempts to reconstitute the machine code produced through this process back to machine readable code, usually C.

Applying this decompositional ontology to the Morris Worm illustrates the complexity required for the virus's conceptualization through the process we can understand as vulnerability research. Robert Morris used his knowledge of fingerd to identify a vector to communicate with a targeted machine, an affordance of networked computers, more so than an explicit vulnerability, to remotely access a system. Morris also understood that the program for this communication, fingerd, contained a flaw which could allow his virus the ability to communicate with the memory architecture of the system he was communicating with, beyond the standard input it was expecting. Then, using his understanding of the memory architecture of computers, Morris designed a payload to be used against fingerd which would trick a computer into arbitrarily running instructions that would allow his virus to gain a level of administrative access over the system. The attack procedure used by the virus demonstrates a mediation of how various functions of the system performed by its applications and operating system interact, and how those relationships can be harnessed to cause a system to perform functions unanticipated by its designers or users. This is the essential utility of hacking as it pertains to security via the process of security research: decomposing the design, analyzing the relationships amongst the functions and affordances of a system enables a hacker to produce contingent functionality that undermines its high-level security goals.

4.2 Play as Contingency

Considering the way hacking is framed as a decompositional activity provides insights into the playful and experimental qualities of hacking. It makes sense that many of the hackers Sherry Turkle (1984) interviewed would describe their experiences subverting the security of computers as being game-like or as a puzzle: the play involved in many games and specifically puzzles as a key objective usually requires players to reorganize information or game components to resolve an in-game objective(s) by identifying potential relationships between components. If these objectives are understood as undermining a system's security, then the play involved in this subversion is the reconstitution of information, functionality and affordances which allows a hacker to bypass the security, to "beat the lock" as one of her hackers explained. In Grimes and Feenberg's "ludification theory" (2009) the pair describe how play appropriates and transforms non-play activities, developing it rational system of games, which can be used to account for much of the behaviour Turkle describes as a playful, but unstructured as an “identifiable activity” which “does not have a definite locus” but fits “within the lifeworld” of early hackers through “undifferentiated moments of playfulness occur alongside of and parasitic on the communicative practices of everyday life, including of course “serious” activities” (p. 110), like the security of a computer. To this point, Grimes and Feenberg note that Bo Walther (2005) specifically uses the term “transgression” which he describes as the “initial stroke of distinction” to enclose “non-play” within the “region of play,” for a distinction to take place “elements have to be transformed into players or play elements to be fully operational, a tree is not a tree; it is a point of reference to an adventurous area with monsters and fairies.” In Turkle, a computer’s protection on confidentiality or integrity is not security, but an adversary to be beaten. The production of contingency here is twofold, the lock can be ‘beaten’ and a play can be wrought from transgressing from the mundane.

A similar decompositional ontology to the one used by hackers in their play is also evident in competitive games and eSports where player analysis of in-game actions like sprite animations and/or game processes can give rise to emergent actions that provide knowledgeable players with certain advantages. For example, in the game DOTA understanding how a character’s avatar is animated, the sprite, and how certain in-game actions can supersede others allows for “last hitting” where a player interrupts an in-game animation process to perform a precisely timed attack (Egilston, 2019, p. 994). Another example is “frame advantage” wherein a player can identify the steps and timing of animation cycles within the game to outpace an opponent, putting them at a disadvantage, getting free hits or allowing a player to time a counterattack. As Ben Egilston argues, being able to access this hidden layer of control is a performance of “contingency”, an expert understanding of the metaphysics of in-game systems and rules that is demonstrative of an “embodied competency” amongst eSports players (p. 996). In both hacking and eSports, expertise is often expressed through an alignment with this embodied competency, a total understanding of the contingency of systems that the player/hacker interacts with, specifically to the extent that this expression exceeds the anticipated functionality. This form of expertise is realized by transcending the proscriptive use and rules which govern a system and accessing a hidden layer of utility. The fact that competitive play in digital games is often heavily shaped by such contingency speaks to Grimes and Feenberg’s observation that “emergent and subversive play practices” are not an exception to, but in “continuum” with their design and whose “absorption required for the playing of specific games” (p.109). What’s important to appreciate then is that contingencies are formative in understanding a game, or games generally: contingencies describe not only the way a game is to be played and understood by its players but is indicative and descriptive of a culture(s) around a game.

4.3 Hacker Challenges and Proscriptive Regimes

As described, hacker culture has many playful and sometimes competitive forms of expression related to hacking. One of the earliest, formalized game-like activities involving hacking and security are so-called “hacker challenges” or “hacker competitions” -- events promoted by software vendors, wherein members of the public are invited to attack commercial software, and if successful would be awarded a prize, sometimes company-branded merchandise, but usually cash. Emerging in the late 1980s and early 1990s these challenges predate CTF competitions and appear to approach security in a way familiar to hackers, as participation would utilize an offensive methodology in attacking the software’s protections. Analyzing these games through the lens of hacker practises’ decompositional ontology is illustrative that, while these games may appear to use similar methods and share an overlapping interest in the subversion of security, their engagement with hacker practise and in particular, their contingent expertise with information systems is poorly realized. As such, hacker challenges serve as a useful place of introduction, examining aspects of hacker play to understand how a game might fail in attempting to enculturate hacker practises in a playful context, making these contests a useful counterpoint to the way this activity is handled in CTF.

Few early hacker challenges were well documented: what remains are mostly hacker textfiles and ephemera including press releases that have survived to sparsely document these events. Early documentation of hacker challenges identifies them being run as early as the 1980s; so, whether the absence of documentation, such as clear rules and procedures is circumstantial because such contests were simply intended to be ephemeral parts of a software’s marketing and are lost to time, or intentional because establishing a clear set of rules would formalize the developer’s obligations to a successful hacker, is unclear. To examine the phenomena around these games I will consider a contest run by Telegram and one organized at the hacker conference Defcon which will consider their limitations as games and as emblematic of hacker practices around security research.

One of the better-documented examples of such a contest and their failings is the recent challenge held in 2014 by the instant messenger service Telegram. The company/platform offered $200,000 USD in Bitcoin to anyone who could crack the company's MTProto encryption system used by its software. The challenge provided participants with two fake user accounts which players would intercept traffic from and attempt to decode their messages, the source code to Telegram's software and a description of Telegram's encryption system. The challenge instructions direct participants to "find ways of decrypting Telegram traffic" as it passes between the users, to perform vulnerability research that would demonstrate a weakness in the confidentiality of the messenger application's encryption system. The terms of this contest also establish that only the first participant to prove they had decrypted the messages between the two users would be given the purse of Bitcoin, that the prize for the contest is rivalrous, regardless of how many successful participants there are (Telegram, Winter Contest FAQ, 2014). Starting in January, the contest ran for two-and-a-half months and when it closed on March 4th, 2014, Telegram jubilantly announced that no participants had been successful in deciphering its encryption system (Telegram, Winter Contest Ends, 2014). Outside of this, the company provided no statistics about the competition: how many hackers participated, how many messages were intercepted, if any attacks were submitted to the organizers or other quantifiable metrics which might describe the contest's participation, scope or conclusions about player methodology. The structure and organization of this contest is archetypal of many hacker challenges: 1) participants are given access to a target and have some information about its functionality, 2) the rules describe a procedure that stipulates what the organizers consider to be a valid attack against their software, usually an extremely narrow definition, 3) the reward for participation is limited by scarcity, awarded only to a single participant who successfully hacks the product and 4) the contest itself and its conclusion are widely advertised, however at the outcome of the contest very little information or data is released about participation or knowledge gained in the contest.

Semantically, the negative results of Telegram's contest may have reassured the company's investors, existing users of the software's security or potentially attracted prospective users looking for a secure messaging platform. However, security researcher Jon Paterson at the mobile security firm Zimperium saw Telegram's announcement of a negative result as a questionable assertion that its application's confidentiality was beyond reproach. In a blog post to his company's website, Paterson refutes Telegram's findings through the contest by performing his own vulnerability research against the software. Paterson uses a number of well-documented vulnerabilities in mobile operating systems in 2014[24] to make short work of Telegram's security, accessing messages sent and received by the application which are stored in an unencrypted state within the phone's memory. While Paterson himself argues in the post that "I am not going to break the encryption process simply by avoiding it", he extracts the messages from the phone's memory which is stored at rest in an unencrypted state. Given the wording of Telegram's challenge, wherein the company stipulates that the data must be "in-transit" within their rules, it seems fairly obvious that Paterson's demonstration found the data at rest and thus he did not follow the instructions set forth by the company. In this way, Paterson does effectively ignore the rules of the contest, but in breaking these rules he calls into question the veracity of the contest as a game, but also as a form of vulnerability research in its conclusions: that Telegram cannot be said to provide sufficient confidentiality.

The pragmatism of Paterson's technique for subverting Telegram's confidentiality was borne out by history. A threat intelligence report from the security firm Checkpoint released in 2020, indicated that an Iranian intelligence agency had been utilizing this vulnerability in Telegram's unencrypted data storage to perform targeted surveillance against certain users. Since 2014 Iranian intelligence officials used this vulnerability to collect intelligence on government opposition groups and ethnic minorities who used the application, which is popular in Iran and amongst the Iranian diaspora (Checkpoint, 2020). While Paterson's findings can now be read as foreboding, they are also illustrative of how these contests approach security and vulnerability research in an unrepresentative fashion, alien to the decompositional ontology used by hackers,

[24] Temporal factors are of great significance to the exploitation of information security vulnerabilities. Known software and systemic vulnerabilities in information systems are generally routinely patched during a technology's lifecycle. A known vulnerability from 2014 is less likely to be meaningful to a hacker in 2015 if it has been patched.

signals intelligence agencies and security professionals alike in assessing the security of technologies from a contingent perspective.

Speaking to the game-like aspect of hacker challenges, Paterson's solution to Telegram's contest and the questionable veracity of the contest's rules is figurative of the larger problems with these vendor-organized hacker challenges. Towards understanding the faults with such a competition, we might consider Paterson's solution comparable to Rainforest Scully-Blaker's argument that speedrunners who abuse glitches in the design of games to expediate their traversal of a level/world, shouldn't be considered cheaters, but expert navigators. While speedrunners players use methods unknown or not imagined by the designers which figure into the game's "implicit" rules and structures, how these authors understood traversal within their game, a speedrunner's shortcuts function "according to the game's", and those proscribed to its play by the game's code (Scully-Blaker, 2014). Establishing a framework for this argument Blaker uses Michel de Certeau's (1984) distinction between "places", maps and representation of a location and the arbitrary demarcations which shape assumptions about their navigation from "spaces" the way in which "active navigation" constructs knowledge performed as "spatial practise" to efficiently navigate a place (Blaker, 2014).

Such a spatial distinction can also be understood in Paterson's rebuttal to Telegram: the researcher doesn't need to engage in interception or cryptanalysis of messages, actively navigating the architecture of mobile devices through well-established knowledge about these spaces produced by hackers in his community. Like the speedrunners described by Scully-Blaker, Paterson sidesteps the implicit central protections/structures, the static controls (places) that Telegram's post-contest communications imply are impregnable through an understanding of the environment (the space) in which they are deployed. In this way, Paterson's security research is a spatial practice, emblematic of the deconstructive ontology of security research, by demonstrating that the sum of security is in fact a relationship between various functions and spaces, which are larger than a single control. Paterson's attack and later, the similar attacks performed by hackers working for the government of Iran are demonstrative of the problems with hacker challenges, that their proscriptions in their rules conceive of an extremely narrow demarcation of valid play and thus the remit of valid vulnerability research that can be applied against them As their failings demonstrate, this challenges lacked a pragmatic approach to a realistic attack scenario by not accounting for the contingency of the environment in which Telegram software operates. Because Telegram's challenge limited the methodological remit of participation to attacking the application's encryption it could be considered an ineffective form of vulnerability research regarding the program's confidentiality, because it does not account for the expression of hacker skill in identifying such contingencies. As such, Telegram's challenge is unrepresentative of the kind of work that might be performed against it by knowledgeable practitioners, those who understand the practiced way in which the hackers navigate the spaces within a technology.

Similar hacker challenges appeared sporadically at hacker community events and venues throughout the 1980s and 1990s. The venerable hacker conference Defcon was not immune to hacker contests and challenges. From 1995 to 2001 the Secure Computing Corporation (SCC) ran a contest as part of Defcon's programming where attendees were challenged to attack a website defended by the company's Sidewinder 2.0 firewall, predating Defcon's CTF by one year. In 1995 the only prize offered was "bragging rights and an MA-1 flight jacket", but in later years SCC offered a $10,000 and ultimately a 100,000 dollar prize in 2001 to anyone who successfully penetrated its firewall (Landweher, 2007, p. 3.). Many of the problems with hacker challenges were evident at Defcon's Sidewinder contest as well. In a textfile from 1995 stored in the Defcon Media archive one of the conference's organizers Steve Kirk, also known as Lockheed, who passed away in 2019, describes the Sidewinder firewall as being "well patched with no exploitable bugs" and "locked down tight", protected against typical vectors for an attack against a firewall. Kirk also notes that the challenge was unusual insofar as the firewall "didn't actually appear to actually be firewalling anything. It was just sitting there on the net. Usually, we'd wanna get AROUND a firewall to get into the machine(s) in question – not necessarily into the firewall its elf [sic] […] regardless we found a straight-on attack pointless."

Similar to Paterson, Lockheed's analysis of the challenge indicates the absence realistic degree of spatiality/context that would be encountered in routine vulnerability research; in the challenge, the Sidewinder firewall wasn't defending a host (server) communicating over the Internet, but in real life, a firewall would be defending a website or server and its efficacy would be determined by how well it prevented against unauthorized ingress and egress against this service, while simultaneously allowing for routine traffic to flow between the server and its users. Lockheed also notes, that under normal circumstances an attacker would be trying to attack the server the firewall is protecting, rather than the firewall, which is typically ancillary to a hacker's objectives in compromising the confidentiality of information stored on the server or altering the functionality (attacking the integrity) of the system being protected. As a consequence, SCC's challenge is determined by Lockheed to be orthogonal to pragmatic vulnerability research, real hacker practice, as it provides none of the typical contingencies through which a hacker can engage with the technology. The way SCC's hacker challenge is considered counter-intuitive by Lockheed is indicative of its breach with meaningful hacker practices, to the ways in which a hacker might decompose its functionality; because the firewall sits in front of an empty or non-functional server, the firewall has virtually no utility.

At a superficial level, these accounts refute the argument that such contests demonstrate the security of these technologies by demonstrating that their application is atypical. More specifically, Lockheed and Paterson's experience with these contests would indicate that the eponym used by "hacker" challenges is ill-suited to their supposed audience, due to their rupture with valid hacker practices. As a test of security, these challenges are demonstrably incongruous with pragmatic methods of vulnerability research which focus on context and relationships between systems within a technology, relationships utilized and manipulated to undermine their security, a precept of hacker practices.

In order to understand the validity of these critiques and the incongruity of these games with their audience of players it is worthwhile to consider Thi Nguyen's (2019) argument that games require shared "social practises", to establish a "proscriptive ontology" which informs valid player engagement with the "material substrate of a game," practises which inform a common understanding of how a game is to be played. However, as Nguyen contends, players are not bound to the "ludic imperative"; the approach the media substrate set forth by designers and audiences may develop alternative "proscriptive regimes" that provide alternate approaches to play that vary in the way players engage with the media substrate of a game (Nguyen, 2019). In a hacker challenge the ludic imperative is shaped by the context in which the software subject to the challenge operates and the rules, which as discussed proscribe a very narrow interaction with the material substrate of this technology.

If we consider the experiences of Lockheed and Paterson and their complaints about hacker challenges, it's clear that these attempts to gamify hacking diverge in the proscriptive regime of the organizer and audience's approach to the material substrate of the technologies subject to these contests. While security research does not own the term hack in any authorial sense, the proximity of Paterson and Lockheed to the community of hackers and their practice does justify the validity of their critique that these corporately-sponsored contests are unfit "hacker" challenges, given how wildly their rules and objectives diverge from hacker modes of technology engagement and thus a hacker-oriented understanding of security. Effectively, how designers of the game and their audience define the task of hacking, the socio-technical practise of the contest which constitutes play, is incompatible. While both vendors and hackers understand hacking as an effort to undermine the security of the technology, vendors running hacker challenges limit their definition of security to a single system (an encryption system, a firewall), whereas hackers understand that security through a holistic sense of contingency, driven by the context and relationships (the ontologies) govern the use of a technology. Given that these contests are designed to enrol security professionals and hackers for their expert technical practises, the limitations imposed on the game's audience constitute an incompatible proscriptive regime. That embedded in their in the rules and design of hacker contests is either a bad faith effort to engage with their players, an effort to construct an unwinnable game, or it is a proscriptive regime based on a diminished understanding of hacker practise.

4.4 Producing Contingency

On a summer afternoon in August, over 40 members of Team Alpha are assembled in a three-room hotel suite preparing to play in a CTF. Shortly before the event begins, Daniel, a respected senior member of the team calls everyone to attention. After coaching the team on a few logistical matters, he closes the briefing with this statement: "remember, every CTF challenge is designed to be solved." The truism serves to remind players not to engage in fatalistic thinking that might impede their ability to solve a challenge, particularly one as sophisticated and challenging as those found at the world-class competition they are playing in this weekend. The reminder also identifies the characteristic that distinguishes CTFs from the hacker challenges that predated them: these challenges found at CTF competitions purely exist to be resolved. Unlike hacker challenges, the scrutable quality of CTF is a product of their authorship: a capture the flag competition is designed by-and-for hackers to demonstrate their skill in vulnerability research and the exploitation of security flaws. To illustrate how CTF is played and how the hacker practises are represented within the game, this section will provide a close reading of one CTF player I observed and interviewed, Morgan, and his experiences playing and solving a CTF challenge at a competition.

By design, CTF challenges are constructed to avoid providing players with clear guidance to solve a challenge. The solving process is entirely heuristic: play is self-directed and players are generally not given clues or tools to solve a challenge.[25] Instead, they must determine the solution from contextual details in the systems/software to be hacked. Morgan describes encountering a web challenge: “you’re first presented with - there’s an [web] application you need to get into […] when you visit the site like you’re only presented with a login screen and nothing else.” Here, Morgan describes his first encounter with the media substrate of the challenge, as a website through his browser, which presents him with a login form, but no clear way to interact with this interface since he does not have a username or password. This early stage of the process of solving a challenge is often referred to as “reconnaissance” wherein a player will attempt to identify an appropriate methodology, method, tools and potential vectors for discovering and exploiting a vulnerability. As Cameron, another CTF player explained, this involves some degree of forensic analysis of the software to “narrow down” the potential ways to analyze and investigate the challenge, using contextual information and knowledge of the field to identify a potential weakness: “and so, you're like […] what were, the popular exploits that existed [for this technology/software]?” This reconnaissance process described identifies a discursive element of CTF play: the game relies on a player’s contemporaneous understanding of their field, including security issues, but may also include knowledge of tools and documentation of procedures used to analyze or exploit the issue at stake in the challenge.

[25] Occasionally in complex binary analysis challenges organizers will demarcate a specific set of functions for players to investigate, to ensure that players don’t waste time examining superfluous code, but even within such demarcations there is often a burdensome amount of information to examine.

Web challenges, like the one Morgan encountered, often conceal a great deal of information that doesn't appear in our web browsers, hidden code loaded onto the page and in the back-end, the server running a site or application. An experienced web application security expert, Morgan knows this and uses software to access a hidden layer of information:

> I used a common tool called Burp, which is a web proxy, Burpsuite, and so looking at like their response size, it was quite large, compared to like what's actually on the page, so obviously there is going to be something hidden there, so looking at that you find a hidden form, and you can submit the form and create a user account, so that was pretty simple, straightforward.

A web proxy filters the code, assets and data exchanged between a site and a visitor's browser, decomposing this information, and can often perform the analysis in stages using "breakpoints" to halt and resume the flow of traffic for granular analysis of how the site communicates with the client. Burpsuite, the tool used in this case, is popular amongst security professionals and professional hackers alike to analyze websites and applications, unearthing hidden data, functions and relationships built into their code. Using Burp, Morgan is able to identify hidden functionality in the page and how to issue HTTP parameters and commands embedded in basic website traffic, which alter the functionality of a page/web application. Using his control of HTTP parameters Morgan is able to submit a command to create an account without accessing an actual interface (such as a form field) that would normally allow for account creation.

The web challenge Morgan encountered utilizes a track-style format, so after he logs in using his newly created account, he is presented with a flag to be scored, however, other flags remain in this challenge which requires an escalation in the sophistication of the attack procedures used thus far. Having obtained access to the application running on the server, Morgan is presented with more information and greater access to its functionality and begins to intuit a plan of attack:

> It's kind of implied that you need to get into the administrator's account, and I say that because the application has a number of sections that […] say things like 'things aren't set up for your account' or there are dead links for menus, and so they seem to imply that you need a higher privileged account, and so, for that, that was kind of like the exercise of, I don't wanna say frustration, but it's kind of like walking through all the different

> approaches that you could take to take over somebody's account so, like, testing parameter pollution, like can I add in 'I am an admin' on certain requests, or try to add a role to myself or log in as somebody else's account.

Here we can appreciate the way in which Morgan is attempting to decompose relationships within the web application he's accessing, however, the "frustration" that Morgan describes here is shared by many CTF players I interviewed who pointed out web challenges can involve a lot of guesswork due to the asymmetrical host/client relationship of web traffic. The operation of websites and web applications are often described as a "black box", where players/hackers can only examine the code running on the front-end of a site or application. Exemplary of this black box paradigm, Morgan describes using an empirical, laborious process of experimenting with the functionality of the site using Burpsuite to perform "parameter pollution," probing attempts to send the page a series of malicious instructions that would allow him to identify potentially exploitable vectors or elements of contingency. Here the decompositional ontology of hacker practise is in full swing, as Morgan is using data and functions revealed by Burpsuite to attempt to apprehend potentially vulnerable aspects in the web application and utilize their interaction with the security of the site to undermine protections of its confidentiality and integrity.

It is nearly 1 AM when Morgan utters "oh fuck, that was it?" to his team: after probing the application he identified a component significant to its confidentiality.

> I came to a functionality that was to change your password and so that stood out, because if I could change somebody else's password that would be really great. Looking at that request, sure enough, there is a user ID on that, and so trying to tamper with the USERID doesn't work, [when] trying to add roles to myself, [so] that maybe I could be that [privileged] user doesn't work. So [I] still spent some time banging my head against the wall, on that one. And then it finally occurred to me: I could change the user ID and maybe I remove the password confirmation the application wouldn't check to see if I submitted that. Sure enough, doing that I am able to change the administrator's password and so that was the second flag.

Here Morgan describes identifying a function of the web application, the password change function, that potentially offers a high degree of contingency, as it is central to the security controls used by this service. Knowing this and having analyzed how different functions of the website performed under experimentation he is able to formulate a second exploit to break through another layer of the website's security. Using this exploit Morgan is able to seize another flag by disabling the prompt that requires the user to know an account's existing password before changing it, allowing him to arbitrarily set the administrator's password to one chosen by the hacker and assert further control of the application.

During our interview, Morgan indicated that much of his skill and knowledge as a CTF player comes from the fact that he routinely read reports produced by bug bounty programs to provide "insight" into emergent security issues, documentation which also kept him abreast of new and novel exploitation techniques used by his peers to attack web services like the one encountered. Morgan's expertise in solving this challenge reflects the discursive quality of CTFs, how the game harnesses a player's knowledge of contemporaneous security issues and their awareness of information resources factors heavily into their success in these games. At the same time, Morgan was working on this challenge, his teammate Jonah is extensively consulting documentation for the GraphQL database language to identify potential ways to manipulate a different web challenge. The variation in their approaches does not necessarily indicate a difference in skill, as both are experienced with web security. The difference here is based in epistemic approaches to the decomposition of the technology: during our interview, Morgan noted that he prefers to analyze the media substrate of the challenge for potential contingencies, while Jonah recognizes a knowledge deficit with his understanding of GraphQL and is examining paratextual materials to identify potential ways of engaging with the media substrate. Morgan has greater confidence in his ability to identify contingency with this problem, whereas Jonah is approaching a fairly new language and technology that he is only partly familiar with. Such a straightforward approach has its drawbacks; by his own admission, Morgan indicated in our interview that he spent far too much time attempting to identify the vulnerability in the second stage of the challenge and he believed there was a third flag that was beyond the remit of his skills to retrieve. Rather than spend time trying to analyze documentation for the web technologies he encountered in the challenge, he backs off and focuses on lower-hanging fruit to score more points for his team.

4.5 Realism, Representation and Emulation in CTF

The example I've drawn on from Morgan's experience playing in a CTF identified many real-world tools, procedures and resources used by hackers and security professionals alike. However, unlike its antecedents, hacker challenges, which had hackers engage with real-world security technologies (albeit fruitlessly), the vulnerabilities discovered in a CTF are intentional and are designed to be found. However, it might be asked: can an intentional vulnerability said to be an actual form of contingency? Another question worth anticipating is whether hacking that happens in a CTF is realistic? To answer these questions, it's worth examining how CTFs represent the act of hacking as this understanding informs how these games are designed and played.

Given that play involves real-world tools used by hackers and realistic procedures used to discover and exploit vulnerabilities, it might be argued that the hacking that happens inside a CTF is realistic. On the other hand, the fact that such vulnerabilities are deliberate, rather than incidental suggests that CTF challenges rely on an inherent fiction in their design. During interviews, I asked CTF designers if realism factored into the way they went about designing challenges. However, this language proved to be contentious and many CTF designers bristled towards the premise of the question. During a competition, Daniel patiently explained to me that CTFs rarely use existing real-world vulnerabilities and that designers prefer to construct their own. As he explained, using software with real-world vulnerabilities was unfeasible because the attack procedures used to exploit existing vulnerabilities are not only well-understood but are often the subject of automated software and scripts used by certain sectors of the security and hacking communities. Daniel cited the open-source project Metasploit as an example. Metasploit is a framework popular amongst professional penetration testers and security analysts who rely on software to quickly survey, diagnose and sometimes attack systems with unpatched vulnerabilities or other security flaws and exposures. Tools like Metasploit which automate the exploitation of vulnerabilities are routinely updated to reflect emerging and documented security issues, thus these utilities would likely make short work of a hypothetical "realistic" CTF which used real-world vulnerabilities as the basis for its challenges, simultaneously, such a CTF design would require a minimum of effort from the player.

To Daniel’s point, another hacker I interviewed, Pearson, explained how his team used a similar technique to win an early CTF in the 1990s. Pearson’s team knew that the CTF would rely on challenges drawn from existing security vulnerabilities, so his team “brought the entire Packet Storm archive of exploits. So, we just had scriptkiddie tools for everything that was script kiddie-able on day one, and we just dominated the contest because of it!” Pearson, who acknowledges that utilizing such tools is a kind of “cheating”, uses the term “scriptkiddie tools” to refer to software written by one hacker to automate the exploitation of a vulnerability, programs or scripts often used by less experienced hackers (referred to as script-kiddies) who don’t understand the underlying vulnerability or are incapable of reliably exploiting the flaw themselves. This is not to say that using such a tool requires no technical knowledge, but in hacker culture, the term script-kiddie indicates that the authenticity, authorship and skill of a hack are diminished when the user is incapable of performing the fundamental intellectual work of vulnerability research involved in the hack themselves.[26]

Daniel and Pearson‘s commentaries on automation in hacking suggest that pre-existing solutions diminish the authenticity of a hack and that being a good hacker, particularly within a CTF, is an expression of skill and intellectual capacity as a security researcher. This observation also resonates with the fact that in a majority of CTFs challenges are bespoke, used only for that event and then retired, an approach which prevents players from gaining an advantage from immediate prior experiences.[27] In this way, if the solution to a CTF challenge is already a solved problem, particularly if the challenge directly reproduces a real-world vulnerability, then there are material and intellectual reasons it would be unsuitable for a CTF. There is also mutual recognition that if diminished technical practices were allowed to persist within the game, then

[26] The definition of the term “script-kiddie” (often abbreviated to “skiddie”) is contentious in the hacker community. Other hackers I spoke to like Vince, described a script kiddie as “people who will download Kali [a Linux distribution which includes many automated hacking tools] and they're gonna run Metasploit against their bank, not knowing how dangerous it is and how to law can come after them.” This definition of script-kiddie reflects a kind of technical inferiority as well as morally irresponsibility and ignorance of both procedure and laws around hacking. Both connotations retain the same effort to distinguish hackers by skill and intellectual capacity.

[27] There is one exception to this, some CTF designers might share the challenge outside the CTF on websites like Ringzero and Hackthebox, giving other hackers the opportunity to experience their challenges outside of the time and geographic limitations imposed by many competitions.

success could no longer be rationalized as an expression of intellectual capital (that the winner was a skilled hacker) and thus play and winning would be unrepresentative of valid social capital.

Given the rationale of how realism might undermine the play of a CTF, it is also worth analyzing how designers approach the concept. One organizer, Dylan explained: “like I don’t want them [players] to have to Nmap a network to find out what hosts and what ports are open […] it’s kind of the drudgework of a pentest.” Here Dylan argues that he doesn’t want his CTF to be directly comparable to tedious forms of labour in the information security industry, where a security professional comprehensively audits the information systems of an organization in a methodical to identify vulnerabilities that might lead to some form of security gap. By arguing that the work-like and more mundane elements of hacking might be considered “drudgework” in the context of a game, Dylan is making the argument that there is some distance between the way a CTF is designed, and the way hacking happens in the real world. Another organizer, Conroy remarked that realism was connotative of “boring stuff”,

> Like, network security is something that I don't really care about. I mean, honestly, the real world is sometimes really bad in terms of security. It’s so bad it’s not worth putting a challenge that reflects that, […] I think it would be a mistake to like, have a CTF that's trying to emulate the real world.

Conroy and Dylan’s remarks indicate that there is a shared understanding that much of the context under which hacking takes place would be undesirable to include a game about the activity and that some realistic elements would spoil play by making it onerous. One designer, Mikhail, expanded on this rationale: “CTF is just the fun parts [of vulnerability research/hacking] distilled into a competition format […] it doesn’t really reflect the overall life in the cybersecurity industry […] it reflects the specific hard to acquire technical skills.” This explanation alongside Conroy’s and Dylan’s connotes the degree to which CTF is an abstraction of the activity of hacking, which reduces certain technical externalities of the activity to derive greater emphasis from certain forms of intellectual engagement. Specifically, Mikhail notes that CTF is intended to engage with certain “technical skills” which might be considered an essential element of the vulnerability research he wants players to perform within his competition.

What these responses indicated to me was that the idea of realism was fraught in the CTF community. I became frustrated with my inability to articulate prompts or questions in a way which would allow a participant to speak to evident similarities between CTF play and real-world activities performed by hackers. While the parallels seemed obvious, providing a question/prompt which could allow organizers to articulate realistic aspects was challenging. For example, Mikhail's attack & defend CTF used the idea of "service levels" (short for service level agreement, abbreviated as SLA) to score teams, a term derived from the metrics used to evaluate corporate IT on the uptime of technology that supports business functions. When I asked him about this specific language, he pointed out that "SLA definitely is a king in the real world" but noted that his CTF was more oriented towards "vulnerability researchers and exploit writers" as opposed to operational information security staff who might be expected to attend to such a key performance indicator in their duties as a professional. Consequently, SLAs were not relevant to the class of hackers/workers (who are typically not responsible for business systems) Mikhail understood as the players/audience for his CTF. This explanation is significant because Mikhail establishes that the audience for CTF competitions is not homogenous. In many cases, I encountered very different skill sets amongst research participants that spoke to the nature of their specific competition. This conscious reflection on audiences is therefore a tacit acknowledgement that the way hacking is constituted at the competition might vary depending on whom it is designed for.

In many contexts within CTFs IT management and business concepts had their symbolic value recycled into game structures that were divorced from their original meaning. Returning to SLAs, Bruce emphasized the relevance of this real-world concept to the game:

> Service levels are critical, because a perfect defense [in a CTF] obviously, is to not run any services at all to reduce your attack surface to zero. But if you allow every team to do that, then there's no game at all. Everybody's got a perfect defense, but there's also nothing left to attack.

In this explanation, Bruce emphasizes that the concept of an SLA in CTF is not necessarily a consideration of real-world IT operations, but that the underlying metaphor which ensures the flow of information and thus the flow of the game. To maintain a state of play many attack-and-defend style CTFs used SLA as a coefficient, multiplying the percentage of uptime against the flags scored by a team,[28] while other competitions prevented teams from scoring any flags if their own service wasn't available. As the responses and deployment of this real-world concept indicate, the idea of an SLA is a useful symbol to facilitate the dynamics of the game, rather than an attempt to make it realistic. As a researcher, this insight was useful, as it identified the extent to which CTFs operated parallel to real-world issues and subsequently, a means of understanding how play and design was representational and might be approached as such.

Changing my question slightly in accordance with a reflective research design and semi-structured interviews I began asking if *verisimilitude or* realism factored into challenge design, hoping that the former term would allow participants to explore the aspects of their challenge that reflected commonly understood practises and problems. Dylan responded to this altered prompt by articulating the nuances he considers part of good CTF challenge design:

> **Alex:** Is verisimilitude or realism important to you when you're creating a challenge?
>
> **Dylan:** [sighs] Yes and no! It's important – I think it's more important in terms of the vulnerabilities – right? Like I think the best CTF challenges are inspired by real vulnerabilities. I'd say honestly some of the worst CTF challenges are actual CVEs [a labelling system used in the cybersecurity industry to identify a known vulnerability] where someone just takes Chrome, reverts it to a known vulnerable one, where maybe a public exploit isn't available and like that's the challenge – mainly because it requires no effort in thinking on the creator's part. But something inspired by a real-world CVE in a new or slightly different context or different take! That's what I think is most important! Like discovering maybe some new heap exploitation technique on the latest glibc that is supposed to fix a bunch of issues, right? Like finding a new bypass or something that's I think amazing! And the scaffolding around it doesn't have to be that complicated if that's your goal to get them to do that.

[28] For example, if a team scores 100 points, but has an uptime of 50%, they are only awarded 50 points.

In this response, Dylan navigates a distinction between realism and abstraction that occurs through the design and play of a CTF. This response seems to indicate, for him at least, that designing a CTF challenge has an expressive component. For him, a well-designed challenge demonstrates a kind of hacker imaginary, a discursive understanding of existing problems which allows the designer to imagine alternate and interesting variations on real-world security problems that might require novel forms of vulnerability research to solve. That same imaginary is harnessed by players, evident in Morgan and Jonah's experiences at a CTF, where they utilized their understanding of existing problems, software and procedures to solve the challenges provided by designers. Dylan uses the term "scaffolding" here to signify that many realistic concepts are abstracted away within the game to create a suitable environment for play. In abstracting away such impedances, this explanation connotes that there is an essential form of hacking, vulnerability research, which he wants to subject his players to within this challenge. Fundamentally, vulnerability research is connoted as the essential intellectual activity of CTFs in his argument. Subsequently, Dylan's challenges are designed to provoke novel and original expressions of hacker skill media through this practice. Coupled with concerns other organizers identified about the simplicity of realistic challenges and "scriptkiddie" solutions, Dylan's response emphasizes that representations of hacking encountered in a CTF can be intellectually demanding and technically rigorous, if not more so due to their novelty/originality, than types of hacking that might be grounded in a more realistic approach. What's significant about these observations is that they demonstrate the way security and vulnerability research is constructed through a social consensus within the parameters of a CTF competition. That CTF reflects very specific intellectual practices involved in hacking.

In considering how CTF approaches the practise of hacking it's interesting to return to language used by Conroy and Pawel who used the terms "emulate" and "reflect" respectively, to describe CTF. These terms are connotative of the idea that CTFs are symbolic, emblematic exercises, that they reflect the activity of hacking in a specific way. As Jesper Juul (2005) has argued, games are reliant on abstraction, that assuming "the quality of a game hinged on its degree of realism" "would be a serious detriment to the experience". To this end he argues that games are "half-real" activities which involve "adaptations of elements of the real world." In particular Juul observes that videogames rely on "low-fidelity simulations", for example "when the player enters a car in Grand Theft Auto III" "simply being near the car and pressing △ makes the protagonist run to the nearest car door, open the door, remove any persons in the car, get in and close the door." As Juul notes games deploy "stylized simulations" to facilitate play and expression: "game fictions and rules are not perfect and complete simulations of the real world; they are flickering and provisional by nature. But stylization is an expressive device that games can use" (p.172). This understanding of how games utilize "low fidelity simulations" is concordant with Dylan and Pawel's acknowledgements about the abstraction involved in CTF, which is intended to reduce the game to an intellectually engaging form of hacking that remains technically rigorous. By delimiting the kinds of hacking involved in a contest, their competitions can hone-in on a specific practise of vulnerability research and a set of relationships in the technology whose contingencies are considered interesting to the designers.

While some elements of CTFs can be explained by Juul's approach to stylization and representation, there are some elements of these digital games that are incongruous with his explanation. As Juul notes videogames employ "substitution" to replace "arbitrary real-world tasks" (p. 173). Unlike the substituted transgressions in Grand Theft Auto III, the activity within a CTF is far less abstract: players encounter real code, they consult real documentation and they use real-world software and procedures to transgress information systems as a hacker might outside the game. So, unlike many of the videogames Juul describes, CTFs do not substitute or simulate tasks or actions, rather they emulate. Here I deploy the word emulate as a counterpoint to simulation or substitution when describing CTF as a form of imitation, an activity which is more grounded in the reproduction of certain acts. While the stylized simulations described by Juul attempt to adapt an activity for a videogame through simplification, CTF uses the same technologies and procedures with a high degree of fidelity to how they are used in real-life, such that the activity is nearly indistinguishable from that which is represented through this task. In this way, the emulation that occurs within a CTF is a kind of bottom-up realism: the lowest levels of CTF play contain the highest degrees of intellectual and technical verisimilitude to hacker practise. Concomitantly, the higher-level elements of CTF competition abstract and simplify away onerous, mundane elements and context which are considered to distract from an essential activity. In abstracting away the banal, but retaining the meaningful activity of hacking through emulation, capture the flag isolates its own "prescriptive regime" a shared understanding of the essential intellectual exercise which constitutes hacking: the production of contingency through a decompositional ontology.

This understanding of how CTFs represent the act of hacking through stylized simulation and emulation is important for understanding the intentionality of vulnerabilities deployed in challenges. As previously acknowledged, vulnerabilities are typically considered unanticipated functions of a program, which raises the issue that intentional flaws might be considered inauthentic. As one organizer, Fraser, explained his challenges are "gonna have functionality that is realistic that could have been used in some sense in this setting." This comment highlights the fact that there is an effort by Fraser to ensure that the challenge he designed has some dimensions of authenticity, that it is not unmoored from a pragmatic purpose like many of the hacker challenges previously discussed, in which a hackers' engagement with the material substrate of the contest was confined to a specious form of access. Fraser contends that while the vulnerability at the heart of this challenge might be considered "not as realistic" due to its invention for the competition, he contends that the vulnerability he designed "definitely highlight a problem that *can happen* realistically [emphasis mine]." This explanation complements Dylan's rationalization of how CTF navigates the space between realism and abstraction within a CTF, emphasizing that the vulnerability is derived from a grounded imaginary of information security problems. In explaining what distinguishes games from the real-world Juul argues that "the space of the game is *part* of the world in which it is player, but the space of a fiction is *outside* the world from which it is created." From this observation about the representational quality of games, we can appreciate that the way vulnerabilities are constructed within a CTF follows the same pattern of emulation as their play, abstracting away tedious elements to access a playful form of hacking. Thus, the hacking that happens within a CTF isn't fictional or inauthentic; the hacking that happens at a CTF is grounded in realistic elements but is configured in a way distinct from the world outside of the game.

Juul's analysis of games is useful in that it can help to account for the representational activity of games and play, but it also helps to explain how CTF is a space apart from the real world, one that might provisionally appropriate certain elements while removing others. As Juul observes, in many games:

> The magic circle is inverted, and the space in which the game is played becomes larger than the space of the world in which it is played. The entire game becomes a superset of world space, and a series of fictional world spaces with magic circles inside are created and deleted during the course of a game. (p. 167).

In considering how real-world objects and practises are used, Fraser explained there are material reasons why abstraction within the CTF is useful as well "especially with web security challenges. One of the big challenges is actually not [to have to] create a website with 150 pages! Right? [Pages] that have different content and different functionality. Right? It's not feasible in the timeframe that I have!" Here it's clear that stylization is also informed by necessity, a reflection of temporal and laborious considerations of the feasible effort put into facilitating interesting forms of hacking. What this explanation demonstrates is that the abstraction and representation used in CTFs also construct a state of exception around the game: some provisions involving information systems and hacking are suspended to allow for timely design and play.

A good example of the exceptional element of a CTF's design is the way it sidesteps laws against hacking and allows play to unfold in a way which does not expose players and organizers to criminal prosecution or copyright infringement. Most laws against hacking, including the Computer Fraud and Abuse Act (CFAA) in the United States, prohibits unauthorized access to computer systems, bypassing or disabling security controls to gain access and accessing/altering files on those systems. To protect players from committing a crime, a CTF explicitly authorizes players to access the network of computers used for the competition, with one small exception: to gain access the player must disable the security controls which prohibit their use of the system. Through this nuance, hackers who are playing in a CTF are not transgressing against authorization (and the law), as they have socially explicit permission for access, but must overcome the technical controls preventing their legitimate access for the purposes of the game. Similarly, provisions in the Digital Millennium Copyright Act (DMCA) forbid tampering with copyrighted programs as they run in the memory of a system. However, protections or "carve-outs" stipulated in the DMCA now protect "security research" as a legitimate exception for some of these provisions and arguably the didactic quality of CTF falls under the remit of such rules. Consideration of the transgressive proclivities of hacker attendees was part of the initial rationale for organizing the first CTF at Defcon in 1996. As Myles, the organizer of the first explained at a panel for Defcon 25, the CTF offered an opportunity for hackers to demonstrate their skills "and not practise out on the live Internet where the con would get shut down." This explanation resonates with the argument that CTFs are spaces of exception, in this case sheltering players by creating a legally protected space for exhibitions of hacking.

By constituting the CTF as a space of exception, the origins of the Defcon CTF are congruent with Grimes and Feenberg's theorization of the second stage of ludification. Within the "lifeworld" of Defcon attendees "undifferentiated communicative action," in this case hacking, transitions into a "play-mode" outside "normal semantic space", laws and their enforcement, where "serious activities" such as computer intrusions are "positioned in relation to playfulness" (p. 110). In this case, playfulness was already approaching some degree of rationalization amongst jocular hackers at Defcon who wanted to distinguish themselves in front of their peers by hacking at the convention, to transform intellectual capital into social capital through forms of unstructured competition. At the same time, play is also subject to rationalization by Defcon's organizers who hosted the contest as a safety valve to channel the energies of their attendees into an event, which, in its organizer's own words, was intended to safeguard the event from legal repercussions. This attitude towards play is consistent with Grimes and Feenberg's argument that the constitution of games is reflexive, expanding an imagined place for playfulness while contracting the original space of play: "once inside the realm of play, all activities that fall outside that universe are reconceptualized as "non-play."" While unsanctioned computer intrusions performed by Defcon attendees have still likely taken place during the conference, the CTF and the conference that hosts it now appropriates those energies and by extension, produces its own form of social legitimacy and social capital by hosting the event.

One element of CTF that is emblematic of how the game is a space of exception is how the game approaches hacks that might disrupt the fabric of the game itself. The only consistent rule across the CTFs I studied and many others that I encountered in my research was against disrupting the availability of the game or other teams' ability to access the game, using techniques like denial of service (DoS) attacks. Simply put, a DoS occurs when the resources demanded of a system outstrip its capacity, causing it to slow its responses or crash altogether. DoS can be weaponized by deliberately automating excessive requests or overloading a system with inbound data. As Qais explained, DoS attacks have the potential to "destroy" a CTF, reducing it to a zero-sum state where play is impossible, particularly in games that use SLA: “once you destroy the uptime with other teams, they don’t get points.” As Elliot explained, such attacks can be catastrophic for a CTF regardless of which party is targeted: “if you were trying to DoS another team it would look exactly like if you trying to DoS our infrastructure”, effectively shuttering all play. While many CTF competitions allow a certain degree of subterfuge between teams of players to occur, DoS attacks have a systemic effect on the entire game which makes them unpalatable to players and organizers alike. Bruce explained that the rationale for a prohibition against “denial of service” attacks in a CTF was the result of the fact hacks are “trivial” and as a result “shouldn't be allowed.” In describing DoS attacks as trivial Bruce is arguing that such attacks lack a degree of technical sophistication. While DoS attacks do legitimately undermine the security objective of availability in information systems, it could be argued that they are unsophisticated because the vulnerabilities they exploit are the well-understood finite resources of a computational system. DoS attacks are trivially easy to execute within a CTF where infrastructure is limited to systems the organizers can afford to field, which are less robust than real-world public or enterprise systems designed for heavy traffic. Added to this DoS attacks have limited utility as they involve little interaction with the complexities of the system or its software. Consequently, disabling a system or service is far less impressive than obtaining confidential information or undermining its integrity to take control.

While the imaginary around hackers conceives of them as transgressive, anarchic figures, the presence of rules, structures and norms within their games establish the basis for a shared understanding of the values around security research as a form of hacking. Another very simplistic DoS attack was described by an organizer, Green: “we literally had somebody like sneak under another huge table and like cut their wire, like three Ethernet wires. And I was like: ‘come on, man. Like that's not in the spirit of the game.’ And like, we just straight ejected them.” Green’s comment, in particular, his observation that unsophisticated forms of disruption are against “the spirit of the game” is demonstrative of certain values as expressed through rules and priorities in CTF. Both Bruce and Green’s comments regarding attacks against availability and the consistency with which CTF organizers forbade DoS attacks to illustrate the degree to which attacking availability is widely understood as diminished technical practise. This shared understanding of DoS attacks is indicative of the fact that while hackers have many transgressive practises, there is, at least generally, a socially congruent proscriptive regime which undergirds how hackers approach the media substrate (hacker practise) within the confines of a CTF and what constitutes a valid expression of skill within such a game. Such an understanding emphasizes the presence of specific values around play. The presence of these values would suggest that CTF is generally understood as an intellectual exercise which demands some consistency in the values around play and that players approach the material substrate of the game in alignment with methods that demonstrate their intellectual capacity, rather than their brute capability as a hacker.

While I did not witness any DoS attacks while observing CTF competitions, the effect of a large group of players attempting to connect to a networked infrastructure often caused unanticipated availability issues, a problem with the same outcome as a DoS attack. The infrastructure for a CTF is remarkably complex, a layered network where high-level components like operating systems are virtualized and a single server might often be emulating multiple information systems or applications. Infrastructure fails often in CTFs and every event I attended started late and/or faced at least one mid-game disruption due to infrastructure issues. In an interview, Hollis explained a particularly fraught challenge: "the fun tapped out and it started becoming very seriously not fun when […] we realized that there was effectively a resource starvation problem that was happening on the technical level inside the game" which "basically turned from an infosec problem to an IT problem", that forced her team to carefully time attacks when computing resources became available. Hollis's observation here, particularly her last comment, is illuminating to understand the kind of hacking that is considered desirable in a CTF. As Hollis notes, the resource starvation issue she encountered took the emphasis off undermining security in the competition and forced her team to address a corollary skillset considered mundane and uninteresting. At another event, Flynn encountered extremely slow infrastructure. I recall watching over her shoulder as she logged into a networked Windows terminal, which took nearly 10 minutes to load after she provided the proper credentials. When I brought this up in our interview she admitted intense frustration, bordering on anger, as her diminished access denied her a sense of feedback from controls she had tried to implement to prevent the system from being hacked and thus a sense of enjoyment. DoS attacks are common in the real world, and many participants I spoke to had resolved them in their work lives, however within the remit of the CTF such remediations are left to the organizers who strictly govern the infrastructure and are limited by its capacity. These limitations within a CTF allude to the fact that while the game utilizes many realistic elements, play/hacking remains provisional within these competitions, reflecting the arbitrary limitations of game structures.

4.6 Conclusions

This chapter is intended to perform much of the conceptual 'heavy lifting' regarding the ludification of hacking into the game of CTF. It began by conceptualizing security, then shifted to hacking and the representation of this activity within the structure of a game both in how it is played and how it is designed. In doing so, this chapter has articulated hacking as it pertains to security research as the production of contingency used to undermine security objectives in information systems. Contrasting hacker contests to capture the flag competitions, it becomes clear that there are certain shared values around how this production of contingency is understood through security research's distinct approach to the material substrate of technologies which impacts how they navigate these experiences. To this end, corporately-sponsored hacker contests using real-world products were roundly criticized for their disjuncture with hacker practices around approaches to the material substrate. Comparatively, CTF competitions created by-and-for hackers which shares their engagement with the materiality and contextuality of technologies are afforded levels of simulation, abstraction and constraint based on a community-driven understanding of hacker practices. As such, the hacker practices allowed in a CTF illustrate certain shared values around what playful and meaningful hacking looks like. In identifying the presence of these values, it is possible to apprehend the expressive characteristic of CTF competitions which are in line with other forms of hacker culture observed by Turkle (1984), specifically their interest in self-expression through computing. Using Grimes and Feenberg's theory of games as sites of social rationalization, we can appreciate CTF as a tool for engaging with and producing communal understandings of practices and thus, meaning-making. Having identified the presence of these expressive qualities and human values in CTF, the following chapter will expand this analysis by exploring how research participants characterized play, fun (pleasure) and the intellectual qualities of CTF, as well as the motivations and purpose for participating in these competitions.

Chapter 5

5 CTF as Cultural Reproduction Amongst Hackers

5.1 The Pleasure of Binary Exploitation

One of the most challenging forms of hacking I encountered in studying CTF, both to understand and perform, was binary exploitation. Binary exploitation challenges are sometimes referred to as ‘binary analysis’ or, often abbreviated ‘pwnable’ or ‘binary’ challenges (not to be confused with the machine language of the same name composed of 0s and 1s). This activity involves a hacker analyzing the executable part of a program (the binary) by evaluating its source code to identify a vulnerability and then crafting a form of exploitation that will break a security control when executed under the right conditions. In many cases, analysis and exploitation will involve a manipulation of not only the program, but the computing architecture of the device running it. In this chapter, I contend that binary analysis is an emblematic practice of the security research community and its prominence within CTF rationalizes it as an aspirational practice within the hacker community. This chapter considers the prominence of binary analysis to describe how discourses and values around hacking as play have shifted from a more Western and male-dominated transgressive identity towards a more global culture of play, one rooted in the scientific imagination of hackers and the pleasures of empiricism in computing. Studying the prominence of binary analysis within the security research and CTF community is also demonstrative of certain cultural changes within the hacker community which have taken root in the last decade and continue to drive incremental shifts in the values and constitution of these groups and their practices.

Binary analysis is significant practice because when a hacker is performing this task, they are not only manipulating the software, but the computational environment running on the device being hacked. For example, in the last chapter, I described the Morris Worm which used expert knowledge of how computers store data in memory (outside of the program) to corrupt the instructions run by the operating system, using what is known as a buffer overflow attack. The use of buffer overflows became a popular method for abusing the architecture of computers in the 1990s and early 2000s. Executing a buffer overflow is an attack popularly referred to as "smashing the stack" which involves corrupting the procedure of instructions, the stack, executed by the computer's processor as it runs a program to make it execute code provided by the attacker (AlephOne, 1996). In 2019 contemporary runtime environments, the architecture of computers which operate the programs, has secured the stack using a variety of methods. Thus, a buffer overflow attack is less relevant and as a result, CTF challenges have begun to focus on other forms of exploitation that attack other elements of the runtime environment.

Given the depreciation of buffer overflows due to new security techniques built into the architecture of computers, new forms of attack have increasing prominence derived from other approaches to binary analysis and exploitation. A more recent exploitation technique is a "heap overflow", an attack which operates on a similar principle to buffer overflows. Heap overflows attack the dynamic memory allocation system used by a computer (the heap) whose structure is harder to anticipate and thus harder to secure than the stack. The challenge of anticipating how to exploit a heap also means that the attacks are more challenging to execute and security controls, which have been introduced to protect the heap add a dizzying amount of complexity to this form of binary analysis and exploitation. A heap overflow occurs when a hacker attacks the instructions used by one program to manipulate instructions or variables stored in the heap (Li, 2019). In both a buffer and heap overflow the attacker manipulates (exploits) an insecure set of instructions used in the code of the binary, which in turn allows them to interact with the memory architecture of the device and thus, inject their own code to be run in the program, or manipulate other functions.

Due to the challenge and the commensurate skill required for this kind of hacking binary analysis is a practise which is often understood as an ultimate expression of a hacker's ability. As Guy explained, for many CTF players and designers, as well as hackers: "binary is kind of the holy grail of, of sort of cybersecurity, right? It's hard. There's not enough people working in that area. It's complicated to grasp, you know?" Guy's explanation is indicative of the reverence many hackers have for binary exploitation, how it is understood as not only a challenging form of hacking but also a culturally significant practise that many hackers aspire to be capable of. Analyzing the practise and the cultural significance of binary exploitation amongst CTF players, designers and hackers illuminates the social dynamics through which prestige is associated with this form of technical labour and by association, those capable of performing it. Examining this process in the context of CTF also sheds light on the way that hacking can be considered a fun or enjoyable experience, but also a discursive one, speaking to its role in a gamified hacking competition and as a mode of the knowledge transfer emblematic to these competitions.

Throughout the study, many hackers described binary exploitation as a kind of sublime experience. Tony, a high-level CTF player who studies computer science and information security at a graduate level described the practise in this way: “I think binary exploitation just has this, like mysticism of being a little bit like black magic. […] For that kind of stuff, it's always it just has this mysticism of like, ‘Oh! I can do something cool! And it just kind of seems like I shouldn't be able to!’” Here Tony emphasizes the way in which binary exploitation produces a potent but also intellectually compelling form of manipulation. Conroy, a skilled CTF player and designer, described this form of hacking using similar language:

> **Conroy:** Being able to exploit something is very, very interesting.
>
> **Alex:** Could you elaborate on why you think that's interesting?
>
> **Conroy:** I mean, it's not that it should [sic] be possible. That's like the main thing, it shouldn't be possible to have a web browser execute some arbitrary code. That's not what this thing is designed to do. And you just misuse it completely to achieve that. And especially memory corruption is pretty magical in that in what it allows you to do. But I mean, the main part is, it's hard and it's magical in a sense.

Here Conroy explicitly describes the accomplishment of binary exploitation; that it allows the hacker to arbitrarily execute their own code as part of the program’s functionality. In this regard, Conroy specifically emphasizes the difficulty and skill required to perform something that “shouldn’t be possible.” One interesting trait of both Conroy and Tony’s explanation is that both describe binary exploitation as a kind of ‘magic’ which allows them to transgress the explicit function or purpose of a program, to bend it to their will. Their use of the term magic is interesting as it connotes a dual meaning both supernatural and performative. In the former connotation, it identifies a kind of supernatural, ineffable effect that a hacker has on a program causing it to act in a way which it otherwise shouldn’t. This understanding of magic conveys a kind of production of contingency which is altogether a source of fascination, something to behold and enjoy. In this arcane sense, the description of hacking as magic provides some insight into how hacking is a kind of ritual, that hackers find a kind of fun not just in producing contingent behaviour in the program but describes a kind of intellectual enchantment with this form of manipulation in and of itself.

The other potential connotation of the term magic used by Conroy and Tony speaks to hacking as a form of carefully rehearsed manipulation and substitution which serves as a performance of such skills, like a trained magician. Author Jon Erickson described hacking in his book *The Art of Exploitation* (2008) using this understanding of the term magic: "most hacker exploits are a lot like magic tricks – they seem amazing and magical, unless you know about sleight of hand and misdirection. In both magic and hacking, if you were to look in just the right spot, the trick would be obvious" (p.27). Erickson's explanation grounds hacking as a discreet form of subterfuge, which appears to be supernatural, but is inherently scrutable, operating mechanistically through careful acts of concealment and manipulation.

This mechanistic understanding of hacking speaks to its empirical foundations, the science of computing. In discussing the discursive objectives of his CTF which focused heavily on binary exploitation, Dorsett, a CTF designer, emphasized that his objective was to communicate this empirical quality of binary exploitation, to make it accessible to his players.

> **Alex:** You pointed out with binary analysis, a very limited population of people who could do that at the time [2013]. Did your team feel like when they were designing this CTF focused on binary analysis that they were sort of, in a lot of ways, sort of pushing the conversation forwards about getting people interested in doing that work and having people do that kind of work?
>
> **Dorsett:** Yeah, absolutely. And that was, like, that's something that even and part of it was like, we felt there are a lot of games we weren't working on that would do web challenges better than we ever could by focusing on binaries. Yeah, it was, you know, a thing that most people on our team were, you know, had their most expertise in. But, you still get a lot of people in other you know, in other fields of security that think that a binary is this immutable blob and that it's impossible to know what it does. *And, you know, they behave in predictable ways* [emphasis mine].

Here Dorsett identifies that one of his team's objectives was to introduce skilled hackers to a novel understanding of binaries as a mutable, mechanistic objects which could be subject to rational forms of analysis, understanding and manipulation. In part, he emphasizes the empirical and mutable qualities of binaries which he felt were poorly understood by other hackers focused on other areas of security at the time. This empirical quality of binaries is supported by Erickson who writes: "every aspect of a program's execution can be *deterministically examined* [emphasis mine], paused, stepped through, and repeated as often as needed" (p. 27). These explanations identify the scientific, empirical elements of binary exploitation that with the use of correct instrumentation, allows for a precise form of analysis required to identify alternative functionality.

To enable this kind of scientific analysis of binaries hackers need specialized tools/instruments. Debugging utilities and command line tools like Linux's GDB (the GNU Debugger) and object dump (objdump), originally designed for software development have long been used by hackers to reverse engineer and deconstruct a binary. Such software is often part of free and open-source distributions of Linux and Unix-based operating systems. However, one CTF player, Dave, emphasized that the rigorous nature of binary analysis also requires more refined and specialized tools for nuanced analysis. Disassemblers and reverse engineering software like Interactive Disassembler (IDA Pro) and Binary Ninja are some of the few commercial applications used by hackers who often pay eye-wateringly high fees for access to these tools. Of these applications, IDA Pro was cited by study participants as far and away the most popular due to the quality of its decompiler, Hex-Rays, which assists in the reverse engineering of already compiled programs written in the language C, one of the most popular and commonly used for complex programs. The decompiler takes the executable code (compiled) in the binary and translates it from a series of "assembly instructions", codes used by the processor into "pseudocode" which resembles the language C, which is considered easier to read and interpret (Andriesse, 2018, p. 138). This act of reverse engineering provides the conditions under which the functionality and instructions of a binary can be subject to analysis.

The IDA Pro Book (2011), a guide and manual for the application published by No Starch Press, was in fact written by prolific CTF player and organizer Chris Eagle. In this book, Eagle frequently uses snippets of code written for Defcon CTF binary challenges to explain certain functions of IDA Pro and to use as test cases (pp. 278, 496 & 500). Eagle's book walks a user through practises of static analysis: "attempts to understand the behaviour of a program simply by reading through the program [source] code", as well as dynamic analysis which allows a program "to execute in a carefully controlled environment (sandbox) while recording every observable aspect of its behaviour using any number of system instrumentation utilities" (p. 6). As well, Eagle coaches readers on the theory and practise of disassembling programs in IDA, which includes specific considerations of tasks like how to distinguish code from data, for example (p.7). Using this understanding of these applications, disassemblers like IDA Pro provide a sort of laboratory environment where a user can analyze and deconstruct a program using various tools and modes of analysis, disentangling various functions and information, examining the functionality of its components and any issues with how the program was compiled (Erickson, p. 21). Hackers do this to "discover a potentially exploitable condition in a program" and "once a problem has been discovered, further analysis is often required to determine whether the problem is exploitable at all and, if so, under what conditions" (Eagle, p. 6). Based on Eagle and Erickson's explanations we can appreciate that the science of binary exploitation requires a myriad of deconstructive capabilities which allow a hacker to ontologically map the functionality of a program, to understand the relationships it constructs to alter them, or as Hollis put it: "to understand the way things exist in order to understand how they could exist." We might understand this process as a kind of reverse engineering[29] used to identify the functions of a program and experiment in the production of alternative functionalities which undermine their security.

Vulnerabilities discovered with these tools are not pulled from the ether or generated purely through guesswork; hackers have a variety of well-established methodologies to discover a flaw in a program. As Ryan Russel (2002) explains, one of the primary tactics many hackers use to identify a vulnerability is to search out "error prone functions" (p. 101) in the source code of a program, common instructions executed in the code of a program which are known by hackers (and CTF players) to be a potential source of a vulnerability. Russel identifies the functions

[29] Though in CTF that term has a specific connotation around challenges focused on the decomplication of binaries without the source, an adjacent or sometimes overlapping field with binary exploitation.

strcpy() and sprintf as examples of instructions in code which do not perform “bounds checking” to check the size of input data and as a result, are vulnerable to a buffer overflow attack where they can be abused to write large malicious payloads that corrupt the instructions in the stack (pp. 107-108). Similarly, as Qais explained during the reconnaissance phase, wherein a CTF player examines a challenge to identify a likely vulnerability, encountering functions like memcpy or gets in the code may serve as markers that a certain type of exploitation, for example, a heap overflow, may be possible.

For example, in a 2016 paper by Tianyi Xie, [30] Yuan Zhang, Juanru Li, Hui Liu and Dawn Gu, the researchers perform a heap overflow by exploiting a memory allocation system known as ptmalloc, using the function memcpy, rewriting data already stored in the program’s memory. Normally it should not be possible to re-write existing pieces of memory allocated by ptmalloc, which allocates information in “chunks” of memory stored at a specific address, like chunk A stored at address 1, rendering these storage units static. However, the logic of ptmalloc has a weakness which creates an exploitable error: using the function memcpy the attacker can overwrite the instructions found in chunk A by triggering an “off by one error” to create chunk B, a very large chunk of data which it tells the computer to store at the address [2-1] (p. 5). This logical error causes the computer to think chunk A has been overwritten because logically chunk B should not overlap with A. As a result, chunk A at 1 is now considered empty, or “free” by this computational logic and can be written to by another instruction. Because chunk A is now considered free, the attacker can write their own arbitrary instructions and store them where the originals were found. These new instructions stored at chunk A get executed when the program calls them from memory (p. 3). To borrow a Bruno Latour-esque description of this attack, the effect is sort of like if a stranger, a belligerent friend-of-a-friend, shows up at a party you’re hosting and over time more of this stranger’s friends show up in your home and upset your invited guests with their own belligerent behaviour. Annoyed and disgusted, your guests leave and even more belligerent strangers displace your guests. Having displaced all the invited guests, the strangers then ransack your house, reading your mail and stealing the pizzas you ordered.

[30] It is worth mentioning that the lead author in this paper is the founder of the prolific China-based CTF team A*0*E.

Returning to CTF challenges, familiarity with Xie et al's., research, specifically the ability to abuse the function memcpy using an off by one error, would likely aid a player in identifying an error-prone function in a challenge using ptmalloc, which correlates with a vulnerability described, or conditions for exploitation. Thus correct play in a potential ptmalloc challenge relies on a discursive level of awareness in contemporary security research, specifically binary analysis.

However, as Bruce, a research participant and CTF challenge designer explained, there are limitations on the kinds of vulnerabilities a CTF designer can expect players to find and exploit in a CTF as it pertains to the labour of vulnerability research. During our interview, Bruce described a challenge his team designed which required players to perform heap exploitation against the memory allocation system jemalloc when no publicly disclosed vulnerability had been documented. As he acknowledged, players lacked a basis for comparison to known vulnerabilities and struggled to identify a flaw that could be successfully exploited during Bruce's weekend-long competition. As a result, the challenge was effectively unsolvable when Bruce's team used it in their CTF because the designer who created the challenge may have been one of the few hackers in the world to know that jemalloc was vulnerable and under what conditions it could be exploited. As Bruce conceded, this challenge was a sort-of failure:

> It is difficult to expect a competitor to come up with a technique in a compressed timeframe like a CTF, right? If within 48 hours if you haven't contemplated how to do this then that may not be [a] sufficient [amount of time] to allow for recognition of what's going on in development of an exploit.

To Bruce's point, hackers huku and argp who published their own research into vulnerabilities with jemalloc in *Phrack Magazine* noted they "spent about a month of continuous late nights in front of ugly terminals, eating junk and taking breaks only to piss and shit (funny times)" (2012). The experience involved in vulnerability research described by huku and argp's supports Bruce's observation that vulnerability research is time-consuming and laborious such that it is largely incongruous with the artificial restrictions introduced by game mechanisms within a CTF. To this end, Bruce's comments identify a temporal constraint required of laborious CTF play:

players cannot be expected to perform original vulnerability research within the game given that this process can be extremely time-consuming.

This temporal limitation identified by Bruce alludes to the fact that there must be some basis for the design of CTF challenges using pre-existing knowledge shared throughout the hacker and security community. As Mikhail explained:

> You definitely see CTF challenges change to keep up with trends and security. And there's no way to get around that and stay good at CTF. And as part of that, you know, to understand those trends, you have to keep up with what's happening in the security field, both in the academic and the industry part of it.

Here Mikhail foregrounds the discursive elements of CTF play as a fundamental requirement of competitive engagement with these games. To his point, Dave, a CTF player, explained that “there are new exploits that come out, you know, every couple months and you'll see it in the next CTF that you play”, as a result, players “need to be up to date enough to recognize something” consulting recent research papers and blogs posts to “read up how somebody did this in the wild, and then figure out what the hell is going on.” Both Mikhail and Dave touch on the discursive element of CTF and more broadly security issues within the hacker community: these games function, at least partially, as a kind of assessment of a player’s ability to engage with the intellectual capital of other hackers and vulnerability researchers.

Relevancy and novelty were also often identified by designers as a key objectives of their challenges, which accentuated their discursive qualities. As Kurt observed, in his CTF “everybody in our group and even groups before and after us are always looking for things that are pushing the envelope” of technical practices required of their CTF challenges. To this extent, Kurt describes how over time the “table stakes,” the basic vulnerability research skills required of the average CTF player have gradually become more demanding. As he notes, technical skills that were “cutting edge” five or ten years ago are now a necessity to “solve the easiest challenges” at his CTF. Along these lines, Bruce noted a best practise “you may not be able to have bleeding edge challenges, [but] let's say but you do want to stay up at the forefront” adding, “it's useful to think about when these types of transitions [between the bleeding edge and forefront] occur” when knowledge about a vulnerability or exploitation technique has begun to diffuse throughout the security community and to design challenges that speak to emergent security issues and problems. For example, in a more applied, penetration testing & web security-oriented CTF in 2019 players were asked to find an exploitation technique to use against a Java Struts app, the same kind of issue that led to the Equifax breach in 2017 (Bals, 2018), while in more research-oriented events players attempted to exploit a machine learning system attacking an emergent technology using techniques (Python pickle exploitation) that had only recently percolated into security research papers in academia. As a result of these discursive tendencies, CTFs inherently rely on an open, continuous circulation of knowledge and practise within the hacker community to disclose new and novel security vulnerabilities, exploitation techniques as well as software. In this way, the openness of the hacker community, specifically in vulnerability research is a generative resource for CTF. The differences in these CTF also allude to different audiences within the CTF community that dictates the kind of hacking and security knowledge involved. What's important about these explanations is that they identify temporality as a key element of hacking methodology; understanding a vulnerability and exploitable functions requires time for these ideas to disperse throughout the hacker community and into certain practises; there is a distinct metaphysics to the reliable dispersion of knowledge within the hacker community which CTF organizers and designers must leverage to create compelling challenges.

These discursive and temporal qualities of CTF are also evident in the way designers and players have adapted to changes in the security landscape and often software and techniques used by players. A good example of this is the history of "discovery through difference" the comparative analysis of two different versions of the same software or code to identify a recently patched security vulnerability (Russel, p. 102). Sometimes referred to as 'diff-ing', the significance of this kind of security research has changed over the history of CTF. As Kurt explained this kind of analysis became commonplace in the early 2000s when software vendors like Microsoft standardized the release of software updates on the 2nd Tuesday of every month, referred to as "patch Tuesday" and as a result hackers started:

> Exploit Wednesday or like, reverse engineer Wednesday where you go and you like, find out all of the safety that was added on Tuesday. And then you assert that nobody's

> applied those patches yet. So now you have like a lot of good offense capability out of what was publicly disclosed.

What Kurt describes here is an emergent capability of hackers to identify vulnerabilities in commonly used software and operating systems through comparative analysis of past versions. While such vulnerabilities are secured in an updated version of the software, they are still valid methods for attacking unpatched systems, which are not uncommon as some sysadmins are wary of patches that may disrupt the stability of business systems or are simply behind the curve when it comes to IT administration. As Green observed, "our predecessors had either like taken an old vulnerable software and put it on the network, or they had taken existing software and added vulns, which meant that if you could diff things out." In this quote, Green acknowledges that this methodology had some relevance in 2003, but noted his team moved to develop their challenges from custom-built software with no basis for comparison. The reason behind this change as Kurt noted, is because "a while back [a company] called Zynamics who did BinDiff, it's an IDA Pro plug-in that like facilitates the sort of thing," describing software that made comparative analysis "a lower bar" for play in his CTF. This process of re-trenching the skills required to play in a CTF reflects both the temporal and discursive qualities of hacker practise as it pertains to security: knowledge and practise go through cycles of relevance and deprecation as hackers adapt to and then secure against known flaws which make yesterday's techniques less relevant tomorrow. In a game so thoroughly focused on the contemporaneous discourse of computer security, the design of CTF challenges often serve as a barometer of what issues are considered novel and which have been relegated to an afterthought.

As a result of this fixation on novelty and temporality, CTF designers are highly sensitive to the way in which some tools and applications de-skill hacker practise. While openness was important to many CTF designers in the diffusion of knowledge amongst the security community (as described above), when I spoke to CTF designers first-to-mind to many of those interviewed about challenge design was a kind of arms race between their CTF challenges and tools which could automate their solution, similar to the script-kiddie tools Pearson described in the last chapter. Many of the CTF organizers I interviewed emphasized that this wariness was an effort to prevent hacking from becoming de-skilled in favour of automation. Bruce provided a rationale as to why resistance to automation was important to his competition: "I never wanted to have a

CTF that was all about the quality of your tools necessarily, we always want it to be about the quality of the human behind the tools. And having them find and solve the challenge." Similarly, Mikhail observes:

> There are CTFs that are, you know, in my opinion, that are less exciting, where you concentrate on, "okay, let's, you know, give everyone network access to a machine. And then they have to, you know, how well can you use Nmap to evade something, how well can you use Metasploit and so forth." There's entire CTFs like that. They're not the CTF that I'm interested in running. I'm more interested in people's underlying security skills.

In this quote, Mikhail references the Metasploit Framework, which can be used for both the development of exploits, but also contains many automated, pre-baked tools for exploitation. In this sense, what he describes as "underlying security skills" and what Bruce identifies as "the quality of the human behind the tools" is a player's ability to perform vulnerability research, to grasp the fundamental computing issues that lead to computer insecurity. As a result, CTF designers would often design challenges that were too novel for/oblique to automated analysis and exploitation tools or had been explicitly designed to counter their functionalities. Success at a CTF is intended as a check on the authenticity of players' skill and their ability to leverage sufficient and relevant intellectual capital against the problem.

It makes a certain amount of sense that an activity subject to such intense social rationalization of an otherwise laborious activity is constantly being contested by automated tools/play practices on the one hand and designers on the other. Many research participants I spoke to designed tools which automated vulnerability research in their day jobs or graduate research (for example, the symbolic analysis tool I describe later in this chapter) to make it easier/faster for professionals to identify flaws in software. Such tools are badly needed to address the preponderance of security issues in both existing and emerging technologies. However, if CTF is to serve as a demonstration of a player's contemporary and deep intellectual capital regarding vulnerability research, the core narrative of CTF play at a competitive level, then automated tooling risks collapsing that narrative by commodifying the software rather than the hacker. This is consistent with Grimes and Feenberg's argument that "no matter how highly rationalized the game, its players remain in a struggle to appropriate and make sense of play in their everyday lives" (p. 108), in this case attempting to wrest between an efficient mode of hacking and an expression of their intellectual capability.

This struggle was evident in interviews when I asked players and organizers what tools they used to assist them in "solving" a CTF challenge. With great frequency, they said "none" but later would refer to various applications, utilities and frameworks to help them analyze a challenge. Unlike automated tools, it's important to emphasize that applications like disassemblers (IDA Pro, for example) function more like instruments which provide hackers with analytic capabilities that assist in identifying vulnerabilities and understanding the conditions under which those flaws can be exploited, they are not programs which automate or "solve" the process of hacking, no more than how a microscope automates scientific discovery by extending the researcher's gaze: making sense of what they are seeing is still up to the scientist, or in this case, hacker. Certainly, microscopes and IDA Pro are not neutral in their political valence, but these commodities are understood to be necessary for accurate analysis. In a few cases, designers and players described tools that emerged in the hacker/vulnerability research communities which have all but solved certain classes of security issues and as such, were unsuitable for inclusion CTF where they could be trivially resolved. In many cases, creating a tool which did this was a mark of honour outside the CTF space, but inside the game, such tools were understood as passe. Players were not bitter or irresolute about the exclusion of such challenges, as they have bought into the social rationalization that the game of CTF is about their intellectual skills, rather than their ability to point software at a problem.

The quality of a practitioner's skills is particularly evident in the vulnerability discovery methodologies which require the "line-by-line" analysis of code. Using this technique, a hacker will identify "execution sequences" and "hypothetical execution sequences" of code, wherein they map out the functions of programs and how they respond to inputs to understand its behaviour and identify potential vulnerabilities or the conditions suitable to exploit the vulnerability (Russel, p.102). Effectively, the study of execution sequences is an attempt to discover how and under what conditions a program will produce a contingent state, and often requires imaging a vast and branching tree of outcomes the program is capable of realizing.

As a result of this complexity in studying execution sequences the analysis, visualization and automation of execution sequences was a popular topic amongst many of the academics I spoke to who participate in CTF competitions. As part of their own research and as assistants on projects, many worked to develop tools to help in analyzing this data and/or testing execution sequences rapidly, a technique known as 'fuzzing.' Prior to joining Team Alpha Franco was designing his own tool for visualizing the memory structure of the heap (to assist in heap exploitation) and as a graduate student he worked with Hollis, Hyun and Leon to develop a tool which automates parts of binary analysis process using machine learning using a technique known as "symbolic analysis." As Dorsett explained, this was a process wherein the tool turns the "program into almost like an algebraic equation and, you know, solves the answer [identifies the vulnerability or exploitation conditions] based on those constraints." Dorsett used the example of these tools which perform symbolic analysis as an example of how computer programs could be deterministically analyzed:

> The predictability and execution, like how [the] binary gets executed is at the heart of all these [tools]. Which makes it hard to fuzz certain programs that they're depending on, you know, [unpredictable] inputs from the outside to make decisions. And it makes symbolic execution is hard if you can't rely on you know, the same function evaluating to the same value every time. So, they're [(binaries)] predictable, but they are hard to predict.

Here Dorsett explains that there are challenges to the methodology at the heart of these tools, but that their design represents a significant intellectual achievement in rendering such processes intelligible. In understanding the production of these powerful tools and the methodology they utilize we can appreciate an aspirational quality to binary analysis. Not only do many hackers seek to personally understand and predict the empirical behaviour of binaries, but also produce tools to manage the complexities involved in analysis and to further the empirical study of these objects.

Line-by-line analysis of code and the ability to predict the behaviour of programs are particularly important in a binary exploitation challenge where participants have full access to the source code of the program they are charged with subverting. As a result of operating under full information, many players often remarked that binary exploitation was considered the true and fair test of a hacker's skill as all players operate with total information about the program. As Tony explains: "there's nothing you can't know. The only question is, do you figure it out? […] In most challenges, it's very much How well do you understand how to play with this program? How good are you at manipulating it?" Tony's explanation here is illuminating as it provides a clear understanding of how hacking functions as play, that in attempting to and in performing forms of manipulation a hacker experiments with different attempts at producing contingency and that successful play is attained when an intended, and novel form of contingency is produced by subverting the security controls in the program. Tony also spoke to the compelling competitive and meritocratic qualities of binary exploitation as a form of hacking: that what distinguishes players is their ability to understand the binary and to provoke these novel behaviours. This observation was shared by Conroy:

> If you have something that's open source, what might be hard about it is that 20 other people have already looked at it and haven't found bugs, or they have found easy-to-find bugs. And now, you're left with like, the hard ones to find. So, yeah, you have to understand a lot of things about probably, a pretty complex, piece of software. And then you have to be better than others that haven't really looked at it.

In this way, both Conroy and Tony both speak to the inherently competitive aspects of binary exploitation amongst CTF players as a source of distinction, if not outright prestige in out-analyzing their competitors. Binary exploitation serves as an expression of hacker expertise, being able to identify functionality (in particular, through understanding execution sequences) which were not recognized or were overlooked when operating under total information. Success in binary analysis is often understood by CTF players as connotative/demonstrative of differences in knowledge and skill, a distinguished signifier of intellectual capital.

As one might imagine, issues of fairness were a common theme in many of my interviews with hackers, who are often understood as transgressive figures. In its earliest days CTFs were free-for-all events where players not only attempted to hack their opponents' systems but as research participants described, would do things like hire a squad of call girls to distract opposing teams in the CTF space or steal media and passwords by knocking them off a table in the CTF space and picking them up with tape attached to a player's shoe. As Kurt noted, over the last 10-15 years the design of CTF competitions, in particular attack-and-defense competitions, have transitioned away from this sort of free-for-all model towards a more governed game structure which he described as the "brokered game." The brokered game places greater emphasis on technical practise over other behaviours commonly associated with hackers, for example, social engineering. Dorsett described how this transition was brought about by a wider international audience of CTF players and teams.

> So, whenever we first started in 2013, some of the things we discovered after the game, after talking to teams that were playing it. For a lot of CTF teams where, you know, English language proficiency is not a priority. You know because, they may be from countries where people, most people don't speak English, that kind of thing. And making it a free-for-all means that you know, teams from different cultural and language backgrounds are going to have very, very different ways of perceiving what the challenge is. And they may have like responses to it that prevent them from competing on the same level that like, you know, an American or a German team might be able to. And we kind of made a decision around 2014: that the challenges we worked were ones that were [going to be] about reverse engineering binaries, and anything that required teams to have like cultural knowledge or, you know, to do something that wasn't binary reverse engineering [was less essential to playing in the CTF]. […] And it was kind of a vindication you know, for making things, you know, very brokered very locked down.

Here Dorsett describes an effort to culturally de-centre the hacker practises at his CTF from Western-aligned understandings of hacking that required specific linguistic and behavioural knowledge of hacking towards a more empirical foundation for the game focused on binary analysis. Within the technical artifice of the game, the conduits for transforming intellectual and social capital were being re-written with values that prioritized empirical approaches to technologies, rather than those which embraced a more subversive aesthetic.

The brokered state of the game refers to the fact that the players themselves no longer host the challenges on a local computer network, but rather a cloud-computing-based instance or emulator which prevents players from radically altering the functionality of the systems they must defend. As a result, certain tactics involving “chump defenses” where players ‘hollow out’ a CTF challenge they must defend by simplifying its code to such a degree that the program so it only functions symbolically, but is devoid of any real functionality or vulnerability. The brokered game structure can also be used to prevent players from using network-based surveillance and forensic techniques to steal another team’s exploits, as teams no longer have visibility into the network their systems run on. Such a control prevents a technique known as “replay attacks” where teams of hackers reverse engineer the vulnerability and exploitation technique from analyzing packet captures, the raw data stream entering their network, effectively allowing them to copy the vulnerability and exploitation research used by other teams. As Dorsett pointed out this transition to the brokered game focuses attention on aspects of hacking that are deemed essential to the challenge and prevented other practises which diminished the core vulnerability discovery and exploitation work. The corollary of this change towards the brokered environment of the game is that more of the challenges resemble internet-based applications and cloud services, which are of increasing relevance as businesses and institutions transition from on-premise computing towards these solutions, ensuring that the game maintains its discursive parallels with the information security landscape.

By and large most of the CTF players I spoke to had no complaints about the brokered state of the game. Though one veteran player argued that this shift to cloud-based services in the game detracted from the importance of network security which he felt was still an essential technical practise amongst security researchers. On the one hand, it might be argued that CTF designers are constantly moving the goalposts, that by making their challenges harder and resistant to automation they are making the game exclusionary or elitist, gatekeeping some hackers out of what is ostensibly a hacking competition. On the other hand, the stated aim of the designers to retrench essential skills and in making these competitions less transgressive suggests that for a hacking competition to be rationalized as a worthwhile endeavour, it must commensurately reflect technical skill, rather than sheer audacity in the artifice of its game structure. This is supported by the fact that few players I spoke to expressed resentment towards the brokered structure, suggesting that there is alignment between designers and players with regard to the brokered game and the type of hacking it requires. Such iteration orchestrated by CTF challenge designers and emblematized in the brokered game reflects Christina Dunbar-Hester’s (2020) argument that “technical communities and their activities are co-constitutive. In other words, changing who there is may also chance practise, and *vice versa*.” (p. 32). In this case, an international audience has changed technical practise in CTF, shifting the game away from a transgressive hacker identity which is understood to be socially situated in Western values around hacker practise, to one more rooted in scientific practises related to the science of vulnerability research. As interview data suggests, this shift resembles a changing consensus around what the essential characteristics of hacker practise are towards hacking that resembles vulnerability research, but also a conscious effort to codify and standardize CTF play more as an intellectual competition or sport, than as the performance of a culturally situated hacker identity. As a result, we can appreciate that CTF competitions are a site of struggle, not only involving the discursive and ever-shifting temporal relationship hackers have to knowledge and practise involving the subversion of technologies, but that the competitive and meritocratic qualities of the game itself have refined what it means to hack and who might be considered a capable hacker.

5.2 The Function and Rationale of CTF Participation

Considering the challenges involved in playing or designing a CTF I’ve described so far in this chapter, it might be asked what participants get out of playing in these competitions. How is it worthwhile? The vast majority of the CTF players I interviewed in this study could identify no clear financial or economic motive for playing in a competition. Most players are not paid to be part of a team and the rare competitions that do provide prize money to the winners are few and far between, while the purse for such events is often negligible. Competition organization and challenge design is also unwaged. Financially some CTF teams and competitions are subsidized largely through corporate sponsorships and associated conference fees and rarely, an associated entry fee. Only one CTF I attended had a cost associated with attendance and it provided free food, drink, alcohol and live entertainment to participants throughout the nearly 72-hour event. Fees for the paid CTF also allowed the organizers to run an extensive infrastructure that supported roughly 600 players in person. Given the large amount of skill and effort involved, the non-existent remuneration, and the largely voluntaristic or votive quality of CTF participation in both the design and play, it makes sense to seek to understand the motivations of players and designers. While many players and designers identify an educational motivation behind their participation in CTF, it’s important to interrogate the educational outcomes tied to this form of serious play: to understand what kind of lessons are taught through these games and what purpose they serve, as well as other more prosaic motivations for participating in contest grounded in the practises of vulnerability research, like the accumulation of social and cultural capital within the hacker community.

Frequently, the CTF challenge designers I interviewed do not work in vulnerability research or an academic field involving security. Rather, they often had roles in application security, penetration testing and software engineering where they were responsible for fixing existing issues and preventing breaches. Fred, who works as a pentester (shorthand for penetration tester, someone who audits information systems using offensive methods to penetrate an institutional network), explained his rationale for developing CTF challenges:

> Very often the vulnerabilities that we find through the year, we can't really publish them because it very often involves vulnerabilities in software that's used by really large corporations. So, most of the vulnerabilities and things we find, actually we can’t freely publish it. But we can make challenges that are based on these ideas and things that we found in those products. So, it's sort of a way now, to like educate people on new things that we find through the pentests that we do. And yeah, and it's a way to indirectly talk about things that were that we usually can't publicly talk about. […] Very often, some of the vulnerabilities that we find have really interesting exploitation path so and we think it's like something useful for people to be able to find on their own and also figure out the exploitation path.

Here Fred identifies some parameters of confidentiality around his job in information security that make it prohibitively hard to disclose security issues which affect his clients. Traditionally, someone in his position might give a talk at an information security conference to improve their standing / social capital within the community about the kind of vulnerabilities or exploitation techniques he discovers during a pentest. Instead, Fred uses the affordances of CTF, namely its abstraction of technical issues through their playful representation as a way of bringing attention to vulnerabilities he encounters in a more oblique format. Certainly, not all the CTF designers I spoke to had the same restriction as Fred, but his experience and that of many others speak to how CTF serves as an outlet for informal security research with some utility that designers encounter routinely in their work. Similarly, Jean noted, “my next set of challenges for next year I think are going to be more inspired by my work that I'm doing.” While the hacker community has many conference venues to discuss new vulnerabilities, as many major cities, states, and provinces throughout the United States and Canada have a local security conference and many play host to international events, not every hacker I spoke to wanted to give a talk or write a paper. Like Fred, some saw utility in giving players hands-on, tactile experience with their vulnerability. In *Second Self* (1984) Turkle describes the way many of her hackers sought to recapture their intellectual autonomy through personal computing. In Fred and Jean’s responses, we can appreciate a similar effort to capture and express their work as hackers in the face of prohibitive confidentiality clauses, by creating CTF challenges that allow them to document their intellectual labour and promote the openness and circulation of security issues within the hacker community.

Speaking to the discursive objective of CTF, designers often use challenges as a way of exposing members of their community to novel problems. The reconnaissance/searching process within CTF play, wherein players begin analyzing a challenge to understand potential vulnerabilities, is well understood by CTF designers, who often create challenges to funnel players towards specific knowledge and ways of understanding insecure technologies. For example, one designer I interviewed, Jean, made a challenge using the GraphQL database query language created by Facebook which is increasingly popular for use in mobile applications. As Jean noted, GraphQL was a “new web technology” whose

> documentation is really not that good. There's not really good content about GraphQL security, I think. So, it [the challenge] was really about learning the technology, how it works, how a query works, and work from there basically and then get to like the SQL [structured query language] injection that is more widely documented.

In this quote, Jean is explaining that he expects players to discover what kind of database they are accessing, read the documentation for the language and begin to piece together how it could be attacked. In that passage Jean refers to “SQL injections” a very old web security problem in which a malicious user can send instructions to a vulnerable database running a query language through things like fillable forms on websites, often to steal the confidential information of other users like their passwords or other sensitive information. Jean was inspired to create this challenge having discovered the same vulnerabilities in GraphQL during his work as an application security engineer, realizing that due to its newness "developers will jump into it without really grasping all of the aspects of it." In this way, Jean's challenge is designed as an intervention: it explains that just because a technology is new does not mean it is secure, or that it can't be made insecure through improper implementation.

Jean's approach to designing a challenge illustrates how expert hackers use CTF to communicate ideas about computer security and new security problems they are thinking about. This approach was a common sentiment shared amongst many information security professionals involved in CTF that I spoke to. Conroy, for example, specializes in "browser exploitation", creating websites and web applications that can be used to steal data or run malicious code on a user's computer through their web browser. Working with a few other CTF designers he explained: "we have started putting browser exploits in CTFs. And I feel like that's quite an impact on the community where people would actually get into this field that wasn't very approachable before." Conroy's comments here describe the way his CTF challenge drew attention to a computer security issue he thinks is important by training players in how to think about the problem. He also described how his approach had a knock-on effect: "and now you had CTF style write-ups where people would explain their approaches to these things." Write-ups serve multiple purposes: they provide informal mentorship often teaching other hackers how a problem was solved or how similar problems might be solved. As Conroy notes, these documents can address shortcomings and gaps in security knowledge. Instead of giving a conference talk or writing a blog post or journal article about a vulnerability or a new form of exploitation, CTF designers leverage the expressive capabilities of games to transfer their knowledge to their peers, giving them the experience of undermining the technology for themselves. It also has a networked effect of increasing attention to certain issues through their inclusion in a CTF. In this way, many CTF challenges are designed to produce a new communal appreciation of insecurity in a specific technology.

Likewise, Fraser, who works in a more traditional educational role at a post-secondary institution explained: "I see CTF as a way for me to communicate to the security community what I'm interested in, but also see what they are interested in, right?" Fraser added that while many vulnerability researchers are comfortable publishing their findings, CTF provided a provocative and immediate sense of issues for audiences of like-minded hackers: "it's about how they approach security as people and as non-academics in some sense." Here Fraser, who is a tenured professor of computer security, acknowledges that not all CTF players, and by extension members of the hacker community, come from an academic background. As such, we can appreciate that Fraser is specifically considering various audiences through which to present his research and that CTF serves as an alternate and pragmatic venue for security knowledge. In this way, we can appreciate the design of CTF challenges both as a form of expression, but also as unfolding in dialogue with audiences and communities of hackers and security professionals who see value in CTF as an alternate venue for the diffusion and circulation of security knowledge. Given the temporal qualities of vulnerability research within the hacker community, the use of bespoke and contemporaneous CTF challenges functions to invigorate both dialogue and practise within the hacker community, generating energy and information which sustains the information security industry and its practitioners through this act of circulation.

Speaking to the educational function of CTF it is important to delineate the kind of education and knowledge transfer that occurs in the serious play of these games. Earlier in this chapter I described Kurt's use of the term "table stakes" to describe the basic capacities of CTF play which are often quite advanced, as well as Mikhail and Bruce's emphasis on building challenges which focus on emergent security issues. What this interview data emphasizes is that the educational outcomes of CTF we might not consider to be a traditional audience for a playful pedagogy: children or a casual audience of previously unengaged learners, groups typically targeted by gamified lessons. Rather, CTFs are oriented toward subject matter experts whose existing knowledge is extensive and who already demonstrate a high level of engagement. In every interview with players, I asked: "was there a time in the CTF where you encountered a CTF challenge you didn't know how to solve? What steps did you take to solve it?" In most cases, players responded along the lines of "that's not my speciality by any means, so I didn't think about that," implying they avoided challenges that did not speak to their expertise in security. Often they described unfamiliar challenges as potential time sinks that would not contribute to their team's success. One player noted: "when you're on a team, there's a desire, to want to contribute. So if you're not finding things [(flags)] it's almost like, I don't know, I can start to feel anxious." In many instances, players described how the basic skill/knowledge requirements of a challenge and/or the time-limited nature of CTF competitions disincentivised learning new skills. So, while CTFs are discursive and may have educational objectives it's important to consider that they are often incompatible with the acquisition of new knowledge. Their game-like format might therefore be considered disruptive and/or incongruous with certain pedagogical objectives.

To this end, many players spoke about the way in which knowledge and practises acquired in a CTF often made it difficult to disentangle what their objectives were in participating in a CTF from the outcomes they experienced. While many players indicated a desire to learn at a CTF event when I asked them what they learned they often struggled to identify a clear learning outcome directly related to their participation. When I interviewed Tony, who is a graduate student and plays regularly in CTFs (about twice a month), his explanation of the educational value of the game challenged traditional notions about the educational dimensions of play.

> Fundamentally, you're wasting your time when you could be reading papers [laughs hard]. And that's a that's a fine way of approaching it too. But I think it's certainly a different take than it you get different ideas than you would if you were to read academic literature in order to come up with new ideas. Because you end up doing a lot of stuff [in a CTF]. You'll find that even if there's a problem that some paper decides is already solved, or like there's this cool new tool someone made for a publication, and then you try it out in a CTF and it doesn't work at all. Like nothing works, everything is broken. And then you realize that the problems that you try to solve in research are very, very constrained. And CTFs are very good at breaking solutions to them [laughs]. And so, for that, it's certainly helpful. So, you get different ideas, I think, then you would from reviewing the literature.

Here Tony provides a critique of the common assumption that CTF players are motivated to play in these competitions for educational purposes. As he highlights, there are more productive ways of acquiring knowledge, through traditional modes of learning like reading an academic paper. At the same time, Tony provides a critique of academic vulnerability research: as he himself puts it, such work is produced under highly controlled conditions which are not necessarily analogous to real-world vulnerability discovery/exploitation or may even be incongruous with practical application, like in a CTF. To this end, one of the benefits he suggests from playing in CTF is that "you get better at problem-solving", in performing forms of analysis and exploitation which are more robust and resilient than they are in academic research. Holden, Tony's teammate, made a similar observation: "for the most part, [what I get out of playing in a CTF] it's just learning, getting better, getting better at all those exploitation [and] reversing tasks. It's fun. It's like, fun to learn that fun to get better and better at that. Yeah." Looking at the language Tony and Holden use to describe what they get out of playing in CTFs emphasizes improvement and refinement, rather than the acquisition of wholly new skills or knowledge. When I asked Jonah what he learned at the CTF related to his work in application security he responded that the vulnerabilities he encountered were often not very relevant, that for him at least, CTF was less about learning and more about developing an instrumental "style of thinking" where "the tools and skills you use to solve the problem tend to be the same ones that you would use to solve a real-world problem." When considered alongside Tony's response, both participants questioned the utility of CTFs for the acquisition of new knowledge. Instead, Jonah, Holden and Tony's responses reframe the educational value of CTF as a means of refining existing knowledge, skills and practises.

To develop this idea a bit further, some of the players I interviewed described the mode in which CTF provided them with training and insight into their field. As Morgan, an application security engineer suggested: "the utility is just kind of keeping things on the radar, right? Like I said, it's easy just to forget about certain vulnerability types." Morgan described how the discursive and circulatory mode of knowledge transfer involved in CTF allowed him to stay on top of security issues he might encounter in the code his company produces. Another interesting explanation of the utility of CTF came from Dave who observed: it's "like staring at smaller bones", and "you can actually get to a point where you can recognize [vulnerabilities]." He added,

> If you think about it, right: these exploits [we use in a CTF] that come out are just kind of compilations of like, 'Oh, it's this new way that you can exploit memory' or 'it's this new way that like, this thing handles something.'

This forensic capability Dave described allowed him to develop a kind of security imaginary, a way of interpreting possible vulnerabilities or modes of exploitation: “so you know, ‘hey, I can get into this region of stuff’, or ‘these are the things I can mess with over here’ and let me start looking, like ‘okay, is there anything that this interacts with that I do?’" Dave’s experience with CTF is complimentary to the methodologies described in the first half of this chapter which rely on an understanding of various known issues or the ability to extrapolate the various branching response structures of a program responding to input. If we are to consider competitive CTF games from the perspective of pedagogical theory, the players’ observations would suggest that these events serve best as a kind of training or practise for vulnerability identification and research, rather than a way to help players acquire unfamiliar knowledge or skills.

Outside of practise and training, it is worth examining some of the corollary motivations of CTF play. In my interviews with players and organizers, they often identified a social rationale for playing in CTF, that the game allowed them to engage in or with communities of like-minded hackers. For example, Guy founded a weekly meet-up where hackers come together to study and practise CTF challenges, often inviting CTF designers located elsewhere to attend virtually and give a workshop on a challenge they fielded at a competition in the past. Guy described it as being “kind of a practise, you know, like hockey.” Explicitly he ties this group activity to social factors that motivate learning:

> If it's not a group, if it's just me, it won't happen. Or you know, it won't be as fun, so I won't talk to people. So, this is why it's organized in a way that it's three hours of training and then we go to a bar, and we chat. And so, this is the kind of the, the gist or the idea behind why to do that group.

In this explanation, we can appreciate a strong parallel to constructivist practises, where learning is closely tied to sociality and in particular, a communal mode of engagement with knowledge, but also fellowship and booze. Similarly, as Dave observed, playing in CTF allowed him to engage with a “different social circle and because I guess a lot of like the people that I hang out with don't have this like super technical knowledge but all these other people [CTF players] do. So, we can talk about this stuff all day.” Like Guy, Dave’s comment here closely ties his interest in CTF to a certain sociality around technology enabled by the game, that it allows him to interact with a group of people based on his interests, rather than other social bonds. Flynn, one of the few women interviewed for this study, also remarked on how it let her network with the minority of women in her field: “it was really good to just sit there and talk to the couple people, I was very fortunate, there was actually several females on the team so I was really excited, but there was a couple, 2 or 3 that were actually around my age so it was nice to see and kind of also probably not the best thing for me to do, but slightly compare myself to and kind of see where I'm at.” To this end, participation in the CTF model facilitates the kind of constructivist learning Michael Resnick characterized as a “third space” (1996, p.232) which allows players to access a social milieux of other security research-oriented hackers. As I will explore in the next chapter, this kind of interaction creates opportunities for mentorship and career mobility, not to mention homophilous fraternization. Some hackers make friends in the CTF communities or find new career opportunities. Two young hackers I met even became romantically involved over the course of a competition I observed and are now engaged to be married.

Given that many of the players participating in highly competitive CTF events were graduate students studying information security, the social bonds formed through playing in these competitions often spoke to the importance of social networks in navigating academia. Mallory, a player on an academic team, gave this justification for participating in CTF as such:

> I mean, the basic reason is that, you know, the lab as a group plays a lot of CTFs. And it was something I was sort of curious about before I got here, and then I came here, and it was, you know, shoved in my face. So, I'm like, ‘Yes! Of course!’

Mallory’s comments identified CTF as essential to entering into the social fabric of his graduate program. Throughout my observation of his team, I often noticed Mallory approaching other graduate students to discuss their research or ongoing research projects he was working on, often encouraging others to come to his institution to do post-doc or doctoral studies. Similarly, Tim noted that one of his academic advisors, Daniel, routinely plays in CTF competitions, as he explained “I think Daniel’s stance is more than CTF is really good to get you to learn about problems that need solving,” he added, “I think Daniel is convinced that we've had this conversation.” In Tim’s case, he specifically indicates that his supervisor has well-known opinions about the value of CTF competitions and that there is an expectation he’d participate in them to develop his discursive understanding of emergent and important security issues which might influence his doctoral research. As both Mallory and Tim’s experiences suggest, playing in CTF was a way of aligning themselves with certain flows and formations of social capital, which gave them access to intellectual resources through graduate school and access to specific professors.

This approach also extended to the development of academic mentorships and partnerships in information security. As Xingzhe explained, through CTF he developed a strong working relationship with his teammate: “Pawel was my mentor. While I was at [university], throughout all my years at [name of university] he was my first research partner, while I interned in Summer 2012. It was his project. And then we've been collaborating on all our future papers. So, we've been collaborating on all our papers. And, you know, we did [application name] together. We have plans to like, you know, creative start-ups in the near future.” A similar kind of informal mentorship was described by Hyun as well with one of his peers: “I was shy before I knew him, but after we started playing CTF together so it became, we became good friends. He’s an expert in exploitation. Like every aspect exploitation and then he helped me a lot during my learning process.” In this regard, while CTF itself might not be explicitly useful for teaching new skills, playing in these competitions often allowed players to build and foster academic relationships through a personal and playful connection to their peers.

Reputational benefits were often not identified by research participants themselves as a reason for playing in a CTF, but they were often explicit in the way players and designers regarded one another. One experience which identified the prestige associated with CTF was the degree to which several players on Team Alpha spoke to me in admiration of their teammate Hyun. During observation, at least three members remarked to me that Hyun had placed highly on a scoreboard for a well-known binary exploitation wargame, which functions like a one-person CTF with no time limit and a persistent ranking system. When I asked Hyun about it his explanation describes a meritocratic culture on the site: “it’s where you can show off and learn from others. So, it’s like you have to solve challenges. After you solve a challenge you can see others’ solution, so of course you can learn new techniques or new how do you say, new thinking for ‘how to do exploitation […] how to develop an exploitation’. Yeah, I learned a lot from that website.” As Hyun describes it, the website serves as a sort of hub, an in-club for elite binary exploitation where hackers go to compare their skills, but only when they've proven themselves are they allowed to see a "write-up," documentation of how other practitioners solved the same problem and deepen their understanding of the methods used for this kind of hacking. Within the homophilic discourse of this binary analysis community success was closely correlated to identity and reputation formation.

In the CTF community write-ups are more commonly used to document the solution of CTF challenges publicly after a competition has concluded. In a majority of cases, write-ups are shared openly, hosted by hackers on publicly available platforms like blogs or code repositories repurposed as journals. During our interview, Leon explained how write-ups help him reflect on his methodology in vulnerability research.

> **Alex:** Do you ever look at write-ups for CTFs, for challenges that you've tried or anything else like that?
>
> **Leon**: Yeah, yeah, every time after CTF I read all day, write-ups of all the challenges [in a CTF], even the ones that I didn't work on.
>
> **Alex:** And do you ever write your own write-ups?
>
> **Leon:** Not yet, but I was thinking maybe I should start? It was [pauses] it's one of the projects that I have ongoing now.
>
> **Alex:** Okay, what, what motivates you to want to write the write-ups CTFs?
>
> **Leon:** But first of all, because I think doing a write-up after the challenge helps you to understand more or the logic passage that you did during the challenge because during the competition everything is [so] messy. So, if you do a write-up after I think you can learn more from what you did. Even if you didn't completely solve the challenge, I think this is really useful. And also, I don't know how to train myself to write more or that kind of stuff, mostly to schematize what I did during the challenge.

What can be appreciated in Leon's responses is an effort to use write-ups as a sensemaking document, that reflecting on his solution allows him to assess his methodology. For challenge authors, sometimes documenting a security issue in a CTF challenge often had a sort of network effect on exposing certain issues as players might document addressing providing a write-up of the challenge.

> I've had some bad experiences reporting to open-source projects. And sometimes I find bugs that are not like, crazy exploitable or, wormable RCE [remote code execution] and stuff like that. [I] just put it in challenge and put it out there for people to dig around and like, learn about it themselves. And after that, if they write a write-up, there you go, like there's documentation about it, and you don't have to do anything else.

Here we can appreciate a deliberative strategy with CTF challenge design. Like providing oxygen to a fire, documenting a security issue can have corollary effects on exposing certain security issues widely in the community to diffuse awareness and knowledge about the issue.

5.3 Conclusion

The utility and/or function of CTF as described in this chapter is multi-faceted. One key element of CTF is that it resists traditional norms around gamified education which is usually targeted at beginning learners who are acquiring new skills. Quite the opposite is the case with CTF, which focuses on developing and refining the skills of experienced practitioners. To this end, it also makes sense that CTF was often identified as an expressive or communicative medium for information security experts to not only share their knowledge but to communicate certain priorities and issues they have encountered in their intellectual work. In many ways we might think of CTF as a circulatory activity which is used to diffuse emergent knowledge throughout the information security and hacker community, that the game is part of a sort of security public, blending existing hacker cultural formations with contemporary security research and present-day security practises and tooling. To this end, CTF is described in the ritual of design and play as a site of struggle within hacker culture, as the game’s community increasingly essentialized practises related to the empirical security research while reducing the relevancy of a largely Western hacker identity based around transgressive manipulation of sociotechnical systems. To a certain extent, these developments coincide with the emergence of a professional class of vulnerability researchers, but also the developing international audience of the game which aligns hacking with explicitly empirical rather than social practises which do not readily translate between cultural and linguistic contexts and which prioritize intellectual achievement over the aesthetics of subversion.

Closely related to locating CTF as a site of struggle, the other key observation from this chapter is that CTF is a key site for communication and identity formation. Aspiring hackers, security researchers and professionals use the space of CTF competitions to explore issues relevant to the community, in a tactile way. These expressions sustain the discursive parameters of the hacker community and its vast gift economy of knowledge. That participation also allows CTF players to engage in identity production, situating themselves in relation to the cultural economy of the hacker community, through the act of competition and production. As the next chapter will explore, this identity formation often signals a participant's aptitude, but also their suitability for prestigious work in the technology industry.

Chapter 6

6 CTF and Work: Ludic Infrastructure for the Cybersecurity Industry

The same week I attend the Boss Battle CTF, news is breaking that two security researchers, Adi Ashkenazy and Shahar Zini, have discovered a vulnerability in the next-generation artificial intelligence-powered antivirus software created by the company Cylance, which at the time, had been recently acquired by the Canadian company, Blackberry, as part of their push away from phones to enterprise services utilized by largely corporate users. The vulnerability discovered by Ashkenazy and Zini works by manipulating the algorithm used to detect malicious software (malware), by appending 60 kilobytes of benign data from the videogame Rocket League to a malicious program. The game had been placed on an 'allow list' by Cylance's developers which permitted it to operate on protected systems. The data taken from Rocket League, used in the vulnerability, allows a malicious attacker to impersonate the game's program, permitting the malware in it to perform illicit functionality without detection. The researchers tested this vulnerability using 384 different samples of known malware against Cylance's anti-virus program, resulting in a 90% success rate in uploading malware to a protected system without detection (Ashkenazy & Zini, 2019).

The disclosure of this vulnerability is significant for two reasons: first, it demonstrates that more sophisticated security technologies do not deter hackers and in point of fact, creates the potential for security researchers to apply their deconstructive ontology to produce more sophisticated vulnerabilities, in this case, a glaringly severe, high-impact fault. Secondly, the vulnerability in Cylance's AI-powered anti-virus software demonstrates that while there is tremendous interest in using artificial intelligence to shore up staffing shortfalls in the information security industry, these technologies are not mature enough to operate without human intervention and oversight. Even in the era of AI encroachment on white-collar work, the Cylance hack identifies the way in which hackers continue to pierce the veil of advanced technologies with their usual playfulness and bravado, presenting their work in public at a security conference for their peers and press. The Cylance hack is also indicative of the ways in which information security labour remains in high demand and may be somewhat resistant to trends toward automation due to the capabilities of hackers to subvert these increasingly complex systems.

The week the Cylance vulnerability is announced, I am at WorkSec, the conference that hosts the Boss Battle CTF (BBCTF). WorkSec is a testament to the demand for information security labour in North America, with a distinct focus on training and career mobility for the cybersecurity industry. Accordingly, the BBCTF has an avowed focus on helping early-career and transitioning IT professionals by partnering their teams with a professional captain who leads the team and develops their understanding of how to effectively plan and strategize the securing of information systems, using a highly realistic simulation of a business environment. However, the BBCTF wasn't the only CTF I encountered in this study which had professional implications for its participants.

In his 2008 paper "Burning Man at Google" Fred Turner describes how participation in the annual festival serves as a "sociotechnical-commons" (p. 73) in which members of the technology industry engage in playful projects which afford "visibility" (p.76) to participants, describing their preparation for the event serves as a "cultural infrastructure" (p. 75) that structures the social conditions of labour in the technology industry. While Turner's Silicon Valley employees ride around on rivethead parade floats in the desert wearing loincloths, taking psilocybin mushrooms (Kane, 2018) and performing new-age spiritual rituals at Burning Man, the hackers in this study have a slightly less oblique connection to their cultural infrastructure. In this chapter, I argue that capture the flag functions as a ludic infrastructure, and that the procedures and knowledge work involved in the game transforms intellectual capital into social capital through playful activities, which configure relationships in their professional and social lives. To this end, I contend that CTF is a social ritual of the security public, which structures play into an act of circulation with intellectual capital, realized through knowledge and performance of hacking in these competitions. Through this chapter, I examine how CTF acts as a proxy for the social conditions of labour in the security industry, both in terms of the work that is done, but also in structuring relationships between workers in the security industry. To explore this relationship the chapter is broken into four sections. The first covers the historical tensions around hacker labour, its ludification and contestation in hacker contests. The second considers the reformation of playful practices in hacker conferences and the way in which these games mobilize social interaction and play to shape the social conditions of the information security industry. The third examines how CTF functions within the workplace, creating opportunities for identity formation and visibility through play. The final section examines ongoing frustrations, exclusions and challenges perceived amongst CTF players and designers in building their careers in relation to games, play and the hacker community.

6.1 Hacker Conferences, Labour and Contests

The upward mobility of security professionals, much less hackers and the valuation of both groups' labour was far less assured in the 1990s when annual hacker conferences began to spring up across the United States than it is today. Analyzing the cultural milieux in which capture the flag emerged is indicative of tensions over labour, professionalization and recognition of hacker expertise in the nascent cybersecurity industry. Hacker challenges, the gamified hacking contests, are precursors to the ludification of hacking found in CTF competitions that attempted to capitalize on the expertise of hackers as a source of free labour at these early conferences and in the community. Analyzing these contests and the discourse around them reveals many of the tensions over work in the hacker community in the 1990s and helps to situate the emergence of CTF as a game at a site of struggle, that speaks to its dual role as a site of identity formation in the hacker community, but also its function as an entrepreneurial exposition of talent.

In consideration of the economic context of the 1990s, hacker challenges and contests were controversial even at the time, because on the one hand, they recognized the utility of hacker labour in assessing the security of technologies, while on the other they were characterized for their exploitative nature and their potential to harm the market for security professionals. Well-respected industry pundits and subject matter experts like Bruce Schneier and Eugene Spafford had critiqued such contests not only for their invalidity as a test of a product's security but also lambasted the exploitative nature of such contests. In his commentary on a contest run by the company Comvista in 1996 Spafford argues that the advertised $10,000 reward for successfully hacking the company's firewall was insubstantial compared to the wages paid to a security professional: "seldom do the really good experts, on either side of the fence, participate in such [an] exercise. Thus, anything done is usually done by amateurs. The 'honor' of having won the challenge is not sufficient to lure the good ones into the fray. Good consultants command fees of several thousand $$ per day in some cases – why should they donate their time and names for what amounts to free consulting"? Here Spafford considers how these challenges have the potential to suppress the wages and opportunities of such professionals (1996).

Similarly, Schneier notes in his analysis of a challenge involving the FEAL encryption system that a capable cryptanalyst is paid about $200 dollars an hour for their highly specialized work. However, in a contest which so unevenly favours the company organizing the event, a payout was unlikely; even if a competitor were to win a contest, the reward would likely not be fair compensation for the work they would have been paid in hourly wages to a commercial contractor. Schneier and Spafford, both respected in their field at the time, share critiques which indicate that such challenges diminish the value of security work and conceivably, have the potential to rob security professionals of potential wages. In this way, Spafford and Schneier effectively offer critiques of the economy of hacker challenges in the technology industry, characterizing them as an effort to de-professionalize security work through casual labour and standardizing the suppression of wages. In this sense, hacker challenges like Comvista, FEAL and SCC's (described in the fourth chapter) were premised on a keenly exploitative discourse within the computer security industry of the time: in the 1990s, hackers were considered disreputable, but at the same time there was growing recognition of their expert labour in the field of computer security.

The SCC running the Sidewinder contest at Defcon in 1995 had, from day one, incorporated its contest into the marketing of its software. Copy from SCC's 1995 post-Defcon press release described the contest as "the ultimate beta test" which pitted "hackers around the world" against the company's firewall and "despite hundreds of attempts, they all failed Secure Computing's challenge." These blurbs perfectly encapsulate not only the way the contest was designed to extract free labour from Defcon's attendees but also how such contests served as free marketing for software vendors eager to prove their technology was hack-proof. What's interesting about this kind of tradeshow-oriented publication is that rather than associate the attendees of Defcon as potential clients, it positions them in an adversarial role. Comparatively, it's hard to imagine trade advertisements positioning doctors, insurance adjusters or any number of mundane professional groups as practitioners who would be disrupted by the technology in question. Such a discursive quality in SCC's marketing speaks to the poor reputation, but also the limited economic valuation of hackers for the information security industry in 1995.

One other interesting quote from SCC's 1995 press release is from Jeff Moss, the founder and lead organizer of Defcon. In SCC's press release, Moss notes that the "Secure Computing Corporation is the first large security company to realize the value of coming to a hacker conference". While the comment is conspicuous given the derisive tone of the document elsewhere, Moss has made similar comments, usually in the face of controversial decisions about Defcon's programming. Moss frequently cites the fact that Gail Thackeray, former U.S. District Attorney for Arizona, spoke at many early Defcon events. Thackeray is one of the federal prosecutors involved in some of the earliest organized law enforcement efforts in U.S. history to arrest and prosecute hackers, a campaign known as "Operation Sundevil" that was described by Bruce Sterling (1993) as "the hacker crackdown" (p. 13), a pivotal law enforcement campaign against hackers in the 1990s. Moss also provided similar remarks in a prologue to then director of the NSA Keith Alexander's keynote at Defcon 20 (Defcon, 2013). In the talk, General Alexander gave a fairly straightforward recruitment pitch to the conference's hackers, encouraging them to consider the symmetries between the skills of hackers and work at the signals intelligence agency (Defcon, 2012). In Moss's statements, like the preamble to Alexander's keynote, the founder of Defcon often positions the decision to invite law enforcement, vendors and spies to conferences as proof that the hacker community has nothing to hide from authorities, to show them that hackers are valuable members of the workforce and civil society. This is not to suggest that Moss's efforts are a violation of a communal ethos of the oft-anti-authoritarian politics of hackers, but rather that his inclusion of corporations and authorities at Defcon is representative of a long-standing strategy to reconcile the identity of hackers with major gatekeepers to their political and vocational legitimacy.

If Moss's longstanding approach to the inclusion of signals intelligence, law enforcement and corporate cybersecurity is representative of anything it is an early realization of the material need for hackers to find legitimate employment and make a living using their skills. Rhetorically, the inclusion of Thackeray, Alexander and companies like Secure Computing provided an air of professional legitimacy to Defcon and its attendees, who like many tradeshow conferences goers share economic concerns about employment and potential careers. Stigma against employing hackers was widely known within the hacking community, with positions circulated in many textfiles and zines including Phrack Magazine (Denning, 1990). A preoccupation with professional legitimacy is also reflected in Defcon 3's programming, which coincided with SCC's first Sidewinder demo: Stephen Cobb of the National Computing Security Agency and Carolyn Meinel both gave separate talks regarding job prospects for hackers. Cobb's talk was entitled "101 Things to Do with an Ex-Hacker" while Meinel's talk promised to discuss "the oppressive potential of employers" indicating that both speakers were considering anxieties and externalities around employment and the stigma against hackers throughout the technology industry.

One of the CTF organizers in this study, Green, spoke to anxieties about employment in the early hacker community as it matured during this period: "so, people were having kids and growing up and infosec […] it wasn't just something that like admins and programmers did on nights and weekends for intellectual curiosity, or it wasn't just for criminals." The quote reflects some of the growing material concerns of security researchers from the computer underground as they began to age and have greater economic concerns about their welfare and the material considerations of family life. Green's quote also denotes the fairly limited scope of security work available at the time, which outside a few specialized firms and the U.S. government (Lipner, 2015), was a fairly niche concern in the wider technology industry and whose valuation and necessity was becoming clear to practitioners, public institutions and the technology industry, alike. Matt Goerzen and Gabriella Coleman have described the rehabilitation performed by hackers through "a range of linguistic, rhetorical and mediatic labour" (p. 8) including the use of terms like "grey-hat" (p.50) to carve out an identity for hackers performing security research in pursuit of legitimate careers. At the same time, Defcon's programming alludes to how the technology industry and hackers were understood as heterogenous and still adversarial entities through this period who were beginning to reconcile through acts of labour and community reflection.

6.2 Hacker Conferences & Entrepreneurialism

In 2004, Riley Eller, one of the leaders of the Ghettohackers, Defcon's second group of CTF organizers, declared in a talk at the hacker conference Black Hat that it was his objective to use the event's/conference's prestigious CTF to rank information security professionals. To do this he proposed assigning players a score similar to the ELO ranking system used by chess leagues and tournaments. In Eller's vision, the player's ELO would be used to assess their capability as a security consultant, in particular their ability to identify and exploit vulnerabilities through a CTF. While this CTF-based global ranking system of security analysts never materialized before or after the Ghettohackers retired from CTF organization, the objective at the time seemed to be to root out unqualified and unfit consultants masquerading as hackers (BlackHat, 2004). The fact that the plan was never realized speaks to the challenges of engineering such a system at a global scale, but also the difficulty of instrumentalizing CTF as a tool to discipline the security industry's workforce. This incompatibility can be attributed to both the limitations of the attempts to gamify hacking through a purposive reframing of CTF as a form of professionalization and also to the subversive and resistive qualities of these games in relationship to hacker culture and its community.

WorkSec, the conference I attended the week the Cylance vulnerability story broke, hosts the Boss Battle CTF, a testament to the maturation of the cybersecurity industry over the intervening two decades since the Ghettohackers ran the Defcon CTF. The transformation speaks to the demand for information security labour in North America. Conference programming has a distinct focus on training, career mobility and is indicative of ways in which hacker knowledge via security research has been mobilized within the cybersecurity industry. The culture at WorkSec is emblematic of what Adrian Johns (2009) described as the conviviality of hacker culture (p.477) through its generous participatory emphasis on mentorship, career development and engagement with the discursive elements of security research and hacker culture.

Tickets are not sold for WorkSec: most attendees receive one through a donation or for free by volunteering in its programming. The conference's CTF the Boss Battle CTF (BBCTF), pairs junior members and recent hires with a veteran from the cybersecurity industry in a game which uses demanding and realistic scenarios to mentor players in "incidence response," how to handle a network intrusion by a malicious hacker. Just across from the CTF a separate conference hall is dedicated to helping attendees find work or get a better job. Throughout the conference speakers in this separate hall give recruitment pitches for large companies and talks about how to pursue mobility through promotion, certification and networking in an information security career.

When talks are not running, conference volunteers provide drop-in resume reviews as well as job interview preparation. Major security and technology companies ranging from boutique firms to Amazon and Microsoft have booths set up to recruit attendees, advertise openings and give away “conference swag”: t-shirts, stickers, bandanas and other branded merchandise. The generosity and supportive atmosphere around security work are central elements to the convivial atmosphere at WorkSec. The flow of social and economic capital at WorkSec is indicative of money coursing through the booming cybersecurity industry, but also emblematic of a grassroots effort by senior members of the hacker community to provide mentorship and support to new generations of cybersecurity workers. While hackers and their culture are often imagined as individualistic and anti-social WorkSec is indicative of the way in which aspects of care and communal spirit are mobilized within the hacker community to support and develop members of the security industry.

While it would be easy to conflate WorkSec as a conference organized by and for the information security industry, many of the organizers see it as a grassroots effort by the hacker community to support security practitioners. As Marty, one of the organizers of the CTF at WorkSec explains, “you know, the hacker community in part was manifested within these conferences but also other venues online. Whether it's IRC or you know, whatever other forums, I think these days is as much Facebook and Slack as anything else. But you know, that is the genesis of all this stuff.” Here Marty directly links the mutual networks of association hackers share over various platforms to most major information security and hacker conferences. The differences accentuated by the grassroots production of conferences by the hacker community were also touched on by Vince who compared WorkSec with Highball, another security conference which caters to managers and executives.

> Anyway, Highball is aimed at the CSO. It's aimed at the guy in the organization who writes the cheques. So, the vendors come out with all their sparkly boxes and all their neat little tools. And they want to sell them. Those guys in suits aren't going to WorkSec. Because WorkSec is free, or a donation. So, who's going to WorkSec? It's the guys who go to work to deal with the sparkly boxes that the CSO bought at Highball. So, you look at the talks at WorkSec, and they're about your day job. Either your new day job you

> want to get into or how to do your day job better. The real-world application, boots-on-the-ground stuff.

The context Vince provides here is valuable in demonstrating not only the stratification between management and workers in the information security industry but a conscientious acknowledgement of how patterns of production in the industry are shaped by management and the technologies they employ. In passing, many of my research participants referred to Highball as oriented towards management, vendors and elite hackers looking for audiences of investors for their security start-ups. Marty described Highball as "very much a corporate affair", while Pearson described the conference as having been "bought out", sold to corporate sponsors who had become the driving force in its programming and its reason for being. To this end, many of my research participants were at pains to emphasize the prohibitively expensive and commensurately glossy reputation of Highball within the continuum of security conferences, often establishing that it was distinct from other hacker conferences which were grassroots organizations.

Of the three competitions I observed for this study, the Boss Battle CTF (BBCTF) at WorkSec is likely to be perceived as the most realistic or as having the highest degree of verisimilitude in representing real-world information security practises. Groups of players known as "blue teams"[31] must defend their computer network from the "Red Team" a group of professional offensive hackers who have already compromised the systems used in the game. The network the Blue Teams defend utilizes both Windows and Linux terminals, various business applications and other network services designed by the event organizers to be likely to be representative of those used in an enterprise environment. Blue Teams are scored on their ability to detect intrusions, represented by "beacons" discovering and disabling these programs and preventing the Red Team from accessing the technology again. Increasing the realism, the game even features non-player actors representing business users who will score the Blue Team

[31] Industry parlance for information security analysts and administrators responsible for protecting the operational IT and business infrastructure.

on their ability to address a service outage caused by the hackers or to bring new vulnerable systems online that the Red Team will attack.

Given its emphasis on reproducing the work of network and security analysis, one could make the case that the BBCTF and many other CTF competitions could be understood as an example of what Jeremy Woodcock and Mark Johnson describe as "gamification-from-above", an "imposition of systems or regulation, surveillance and standardization" (p.534) to instrumentalize the systems used by games to discipline players through professionalization. In this case, scoring individuals on their ability to defend a realistic enterprise system from a team of attackers interfering with its operation is used to represent the working conditions of the information security industry. At the same time, the BBCTF utilizes elements of mentorship, camaraderie, as well as humour and absurdity to teach players valuable lessons about working in the security industry that extend beyond the disciplinary tools to develop players' abilities. It teaches them to cope with managerial and workplace culture, the social conditions of the cybersecurity industry to prevent common forms of harm.

One unique element of the BBCTF is that nine players on each Blue Team were paired with an experienced security professional, the team's "captain," for the competition. Prior to the event, the Bitflippers' captain held regular team meetings to strategize for the upcoming CTF. As Alice, one of the members of the Bitflippers explained, the team meetings and CTF preparation exposed her to useful training materials often guided by expert insight:

> So, there are a couple of things that our team leader […] kind of guided us down to terms of what we should be looking for and how we can try part of the environments during competition. So, I was looking up different Linux things like how to turn off IPv6. How to audit ICMP, using like IP tables.

While Alice works in digital forensics and incident response (DFIR), work analysis of information systems for signs of intrusion and forms of mitigation, preparation introduced her to resources available amongst the DFIR community on Twitter and important texts like the Blue Team Field Manual (Alan White & Ben Clark, 2017). In this way, mentorship at the BBCTF emphasized the discursive component of CTF in introducing players to relevant resources.

Similarly, Flynn describes how the team:

> created a GitHub repository and it made me, it gave me more of an insight of how GitHub is. How do you fork something? How you add something to a repository? So, for me personally it definitely, it helped me, because I definitely feel more confident in using and hosting stuff on GitHub.

Here Flynn notes how preparation for the event allowed her to develop a functional understanding of how she could integrate code repositories into her work as a security analyst. While we often think of technology workers as synonymous with coders, many security and IT roles only require participants to understand specific technical documents and the operations of systems such as firewalls, server logs and to work in a command line environment configuring certain programs with a text editor, but they often do not need to know how to code or use code repositories in their day-to-day duties. In these examples, both Flynn and Alice identify elements of the BBCTF that provided mentorship on the methodologies of security work or specific tools and platforms that allowed them to deepen their technical practise.

Important to Flynn was her observation that her captain, Wilf, prepared the team by drawing on "his prior experience." Of particular value, she noted, was his field-tested knowledge of practises, his willingness to describe "what has worked out for me in the past," as well as "what hasn't." A salient detail here is that the two share a workplace and Flynn, at least partially, works under Wilf who occupies a senior role at a civil agency. However, it was not the workplace, but the BBCTF where Flynn had better access to Wilf's strategic insights into running an information security program. When I interviewed Wilf, he indicated that his mentorship and coaching of early career security professionals focused on giving them time management and prioritization skills. Of particular importance was the sheer enormity of securing an entire organization's systems: "you're not going to be able to patch and defend everything," as this approach was unfeasible given the scarcity of time and effort, both in the game, but also faced by analysts in their day-to-day work. Instead, he argued that security practitioners needed to learn "how can you detect [intrusions] too? So, we put a lot [of CTF preparation] into detection, not just hardening."

As Marty explains this focus on intrusion detection is a discursive element of the BBCTF:

> In 2010 you know, we [security professionals] were worried about how, you know, are they going to break in? […] and it was over the next five years that the industry kind of came to the same general conclusion: that there's no stopping them [malicious hackers] if they want in, they will get in and you know, we're just the little Dutch Boy putting his fingers in the dike. We need to get past that. And so I would say that the evolution of [the BBCTF] just followed the industry in that, you know, it is very old hat to say 'Okay, you got to patch your stuff. You got to harden your system. Gotta do all that.' And then there's a degree of that to our game, [but there is also an emphasis on]: "great they're in. find them kick them out."

Both Marty and Wilf identify how their approach and design to the CTF needed to reflect contemporary practises in information security. Both note that the approach to the game needed to consider how effective play required both the ability to secure systems and also to perform surveillance of their use and access. As Marty & Wilf indicate this approach is grounded as much in the necessity to secure these systems as it is in efficacy, to use the time and effort available to a security analyst in the most useful way possible.

As part of his coaching, Wilf described using methodologies including the "MITRE ATT&CK" & Eisenhower matrices to identify "problems that are easy to solve and problems that are hard to solve […] if you solve the problem, it'll have a lot of impact, and in others, it won't be as much. So, you should be focusing on the things that you could do that are easy and have a lot of impact, like changing default credentials. Like, that's easy to that's easy to do [...] like anybody can do it. And anybody can also exploit it and like really take advantage of you in a horrible way." In coaching his teammates on methodologies like the ATT&K matrix (MITRE, 2018), Wilf indicated that it was not the technical skills which distinguished junior from senior colleagues, but their ability to analyze systems to identify high-priority and effective interventions. Prevalent amongst the information security industry workers is "employee burnout" an ongoing endemic of psychologically exhausted and demoralized information security staff. Commentators have described this burnout as the byproduct of demanding jobs which feature a high degree of uncertainty (as Marty observed), and do not offer a "healthy work life balance" (Mitchell, 2018). By structuring the BBCTF to simulate the same conditions as the industry its organizers and captains offer various strategies for coping with the workloads of security professionals, to work smarter rather than harder. Consequently, we can appreciate the ludification happening within WorkSec in communicating cultural norms and expectations around security work, efforts to shift notions of professionalization and the conditions of production within the security industry by communicating alternative, practitioner-oriented techniques.

However, not all of the educational objectives of a CTF are implemented cleanly. As discussed in earlier chapters, CTFs are widely understood as poor learning environments for the development of new skills. Terry, a member of the Bitflippers, the team I observed at the BBCTF, encapsulated the challenge of learning in a CTF environment:

> I think if I'm honest with myself, I always felt like I was just a little bit underwater. Like I was, you know, to take that metaphor a little further like often choking down lungfuls of water and air and gasping and not knowing what was going on. So, or questioning whether the work that I was doing was really helpful in the event. I don't think there was a really a moment where I was like, "boom, you came in the front door, and I smacked you down," you know, as far as like doing an awesome, awesome defense. It was more like, are the scripts that I haven't had enough practise at deploying running as best as I think they are, and it's not be helpful just to blindly rerun them, you know, in hopes of a better effect.

Prior to the event, Terry had been receiving some training in designing and running administrative scripts to harden Linux systems against attack. As his experience indicates, the limited information available to him in the CTF environment made it hard to empirically assess the success of his work. Similarly, Flynn, another member of the Bitflippers, described her increasing agitation to me as the Windows terminals she was entrusted to defend ground to a halt because of issues with the game's infrastructure, making it impossible for her to determine if she had properly secured these systems against the Red Team. These problems are worth highlighting because they demonstrate that while CTFs may have an educational function or purpose which could be used to train workers, their competitive environment relies on functional and informational asymmetries which are intrinsic to many forms of games; information and access to certain systems is deliberately predicated on scarcity. This scarcity as Flynn and Terry experienced can severely hamper educational outcomes, coupled with the fact that players aren't formally assessed through any kind of grade or certification when they finish. While CTFs like Boss Battle use many work-like forms of play, it's hard to make the case that these games serve a greater disciplinary function when security professionals can readily seek out a myriad of certifications and training to formally train them in specific technical skills to pad their resumes. As such, it is hard to make the claim that playing in a CTF is purely entrepreneurial but motivated by an enthusiasm for developing and refining practises as part of a player's professionalization.

Both Marty and Carl understood the frustration and difficulty built into the BBCTF. As the lead organizer Carl explains, "we want you to learn, we don't want you to rage quit, right? […] I think we actually had one of those this year [a player leaving the game prematurely out of frustration]. But that's not our intent." During observation, Carl explained to me that one of the challenges with making the CTF realistic was that it often caused players who felt stressed to drop out and so there was often pushback against creating environments within the game with a high degree of verisimilitude, that were limitations to how real the game could be. Speaking about the role of frustration in the game Marty described how "failure is important. You don't learn without failing. […] You got to get hands-on keys because you got to see what doesn't work and then figure out what does work." Here Marty makes an interesting point: the BBCTF's simulation provides players with a high degree of autonomy over the business environment they defend. The "keys" Marty describes is the rare opportunity to approach the work of protecting enterprise systems authoritatively and holistically, from the ground up as architects, rather than working in specific silos like analysis or security operations in systems which were often implemented before they started in their roles. This effort to empower or provide players with autonomy reflects Sherry Turkle's (1984) argument that many hackers seek out computers as an opportunity to reclaim control over their intellectual labour. In this case, the BBCTF provides players with the opportunity to experiment and research effective strategies for protecting systems that may elide their day-to-day duties. In a talk at the security conference USENIX, Haroon Meer, a well-respected security researcher, argued that defensive practitioners in cybersecurity should embrace "hackyness", creative techniques for defense, rather than ape or simply study the techniques of malicious hackers (Usenix, 2019). The BBCTF is complimentary to such an approach, insofar as it provides a unique aspect of simulation as play. Rather than reducing defense to a purely gamified form of labour, play reflects an ongoing discourse within the cybersecurity industry to engage in more novel forms of defense and to manage the working conditions commonly experienced in industry roles.

Given the amount of work that goes into the development of many CTFs, it may be surprising that few organizers are paid for their contributions, and that CTF organization and design is largely voluntary labour. In many cases, a conference or conference sponsors will fund the costs of running the CTF, but the organizers themselves are typically motivated by other factors than remuneration. When I asked Wilf his motivations for coaching and mentoring players in the CTF, his answer identified a degree of care which I hadn't anticipated:

> The more people interested in [security] I feel that's better really for the world. Like, you see everyday people get breached and just jacked around. It like really doesn't have to be that way. And yeah, the security talent in a lot of places is not that good unless you've worked for some crazy Silicon Valley place. [But] if you're working in something like not a technical company like then chances of them having like great security or not, not that good, but they need security. […] [Those organizations] handle a lot of money or like privacy-related types of stuff that you wouldn't want [exposed]. Like, that'd be really terrible if a lawyer or a doctor got hacked. Like, they probably have all kinds of really, like nasty data, that [could] hurt their clients, like hurt their patients. There's regulations for stuff like that, but what are the chances of, you know, some small legal firm in like a Midwestern city having a great security team?

Here Wilf establishes that one of his motivations for participating in a CTF is essentially a sense of civic duty. In recognizing not only the job shortage, but the asymmetries in talent between large technical firms and municipal organizations, Wilf associates his goal with developing the skills of practitioners working in more mundane environments rather than the technology industry, but who are responsible for protecting highly sensitive data and securing vital infrastructure for day-to-day life. Carl also identified similar sentiments, emphasizing the circulation of knowledge reflecting open-source practises: "the mission for BBCTF is simple: provide free training for the cyber security community through events like WorkSec and release to the public, the things we develop, for others to do the same." Marty provides a similar civic emphasis on his rationale for bringing the BBCTF to the WorkSec conference: "the philosophy of WorkSec is you know, exposing more people to the community and bringing in more people to the community. Whereas other conferences might be more exclusive, or have an exclusive cultural streak." Both Marty and Carl's responses identify an effort to sustain and grow the gift economy of the security public. The organizers of the BBCTF identify that there is a civic parameter to their work, in protecting their communities or growing the community of practise around security through inclusive games and the circulation of information.

As Marty describes and as I observed, victory is not particularly celebrated at the BBCTF and there is no awards ceremony like there are at many of the other competitions I attended. As Marty explained:

> We're very much trying to keep winning on almost a down low. […] We found it necessary because we quite often have to remind ourselves, what are we doing here and, you know, people on my staff will come up with awesome ideas. And sometimes the answer is, that'd be cool if we were competitive CTF where we just wanted to see who's the smartest person in the room?

As Marty explained players intrinsically understand their success through the experience of play and that there was no need to reward success outside of the game:

> sometimes they're surprised by the scoring engine versus what they feel like they're experiencing. And you know, sometimes it's aligned. And it does come down to the fact that it's, you know, perception is as much reality as anything.

What's remarkable about this response is that it emphasizes the degree to which enjoyment from the BBCTF, and perhaps most competitions, is procedural; realized through the experience of play rather than the realization of extrinsic objectives. As a result, at the BBCTF there is no need to celebrate the victors because they likely had a sense of their own success through the experience of playing the game. This philosophy also speaks to the closing procedures, where at the end of the game the BBCTF environments are slowly "burned down" by the Red Team who wipe the systems. For example, while I am observing Terry he logs into a Linux terminal he was defending whose command line has been wiped and only displays animated ASCII art of the "Party Parrot", text art of a bird coyly dancing as if to mock the viewer. In using these non-serious elements and in staging a game in such a way that the environment is ultimately unsalvageable for players, the BBCCTF elides essentializing victory as a serious outcome. At the end of the BBCTF, the Bitflippers emerge victorious, but the team looks partially deflated and very tired. Flynn and Terry crack some boutique IPA pale ale from a local brewery and clusters of the teammates commiserate their pyrrhic victory, others quietly leave. The game was stressful, unpleasant and by all accounts, no one has learned any new skills at the CTF over the last two days. Yet relationships were formed, lessons about the nature of security work and the practise of resiliency in network security were imparted, if fleetingly.

In providing guidance on the prioritization of security labour and emphasizing the occasional futility of information security work, there exists an obvious disciplinary objective in training security professionals to operate efficiently and resiliently. However, it could also be argued that this form of mentorship offers a form of care for participants, allowing them to develop practises which increases their assurance when working in an industry with a high degree of ambiguity and establish protective emotional boundaries around their expectations of work in the security industry. As many participants in the BBCTF indicated, the motivation behind this kind of work was to provide mentorship out of a sense of duty, either to the hacker community or in Wilf's case, out of a sense of civic duty. None of the CTF organizers or captains are paid for their contributions to the BBCTF, nor is it within the remit of their careers to provide this training.

Returning to Woodcock and Johnson's argument, it's worth evaluating if CTF constitutes gamification-from-above. Enacting "a terminological foreclosing of alternate possibilities" (p. 554) and if such forms of gamification are intended to discipline workers, making their work more efficient by narrowing the range of acceptable practises involved in labour. It's hard to malign the BBCTF with this critique of professionalization when it is motivated by a collective sense of communal and civic mentorship, much less its discursive focus on introducing players to the gift economy of hacker culture and security research which sustains information security work. Rather than dispute the argument made by Woodcock and Johnson, I propose that it can be troubled. As the authors themselves argue "context is therefore everything for 'gamification'" (p.553). In this case, context is the larger cultural milieux in which CTF is set. The game isn't intended to foreclose but to open up practice and understanding to practitioners who are often alienated from their intellectual labour. So instead of arguing that the BBCTF serves as either gamification-from-above or below, I would suggest that this competition is an example of the instrumentalization of playfulness to fit within the milieux and values of hacker culture. That through the process of ludification theorized by Grimes & Feenberg, it had already arrived at a state of rationalization which predates or is contemporaneous with much of the cybersecurity industry. Workers do not need to be disciplined if they have already bought into the core narrative set around CTF.

This understanding is figurative of a game in which the discursive qualities of security research are blended with the mentorship and gift economy of hacker culture. To this extent the game serves a reproductive function within hacker culture, inculcating players in the discursive knowledge produced in alignment with a vast amount of shared knowledge and culture shared online by the hacker community, not only in terms of information and software but also of votive and communal labour. In doing so, CTF and hacker conferences provide a shadow network, a ludic infrastructure, of support to practitioners which is perhaps somewhat unique as compared to many trades and professions given efforts to include and educate early career and aspiring labourers, instead of elites on the conference circuit or those with the exclusive connections and social mobility to attend Burning Man. In the rehearsals and through mentorship exchanges, players in CTF learn to think about their trade discursively, opening up new methods and techniques, and developing connections to other members and resources which sustains the rooting of these games within hacker culture. This sense of context within the hacker community, visible in and expressed by the members of the BBCTF organizing team I interviewed, speaks to a kind of resistance within the hacker community and hacker games to becoming instrumentalized purely as appendages of the information security industry. Rather, it is a reaction to the social conditions of labour in that industry.

6.3 CTFs as Cultural Infrastructure and in the Workplace

In considering the long history of CTF play there is often a rupture between those who believe it is a gateway to the development of new knowledge and skills contrasted against experts who argue that it has clear deficiencies as a learning environment (discussed in the second half of the last chapter). Given the social impact of CTF outside of pedagogical goals, like identity formation, it is worth considering what functions it does perform concerning the professionalization of its players. One recurring theme throughout my study was the relationship between CTF and/in the employment of participants and their relationships in the workplace. At the CrawlerCTF (CRCTF), I observed the Moths, whose members all worked together at a large web-development firm, Moth Corporate. Their parent company sponsored their admission to the CTF and the associated conference WebSec, paying for their travel and lodging for the competition as well; the team even played under the company name. Many other companies fielded their own teams at the CRCTF and the Moths were but one of three teams representing Moth Corporate at the event. The Moths I studied had a slight advantage over their co-workers, as the Moths were drawn from the ranks of the application security (appsec) team, while the others were mostly developers who did not specialize in security. As Brian explained, it is the job of the application security team to provide "security reviews of applications", running the company's "bug bounty program", "giving developers advice on how to […] solve security issues", "developing automated ways to deal with security issues or developing automated ways to detect those security issues so we can deal with them" and "an education piece" running the company's professional development program related to security, to help hundreds of the company's developers to identify and prevent the introduction of security issues in their own code. As a kind of case study, the Moths and their parent company are an interesting example of how CTFs serve as both a mode of knowledge transmission, but also how they function as cultural infrastructure within the security industry.

The part of his job duties that was particularly germane to our conversation was the training program Brian and his team oversaw at Moth Corporate. As Brian explained it, much of the training his team provides is a workshop

> Kinda like a CTF where we show a vulnerability type in an application. And then the participants are encouraged to look around that app for 10-15 minutes and find their own version of that vulnerability. And then they come up to the front and demo that vulnerability.

Brian and his team give away prizes, usually company-branded merchandise to teams of workshop participants who can demonstrate their vulnerability to other attendees. Brian noted that an interactive CTF-like model for workshops is “pretty useful” when compared to more passive models of security education “you can go up there and talk about how to write secure code, but showing somebody the consequence of not writing secure code is a lot more effective we’ve found.” The logic of this training is emblematic of the security public: by teaching his developers to think like hackers and to understand the technologies they use and produce through their vulnerabilities; Brian is also ensuring they can mitigate common contingencies that would expose customer data and transactions to risk.

Brian and his fellow team members Jean and Jonas also ran a CTF internal to their company which addressed relevant and common security issues with the technologies developers commonly used, complete with a scoreboard and prizes for the best players. Jean explained why this education was particularly effective: “I feel like there's a context here that needs to be kind of addressed with them [the developers]. Like with the technology we're using.” As Jean points out, this was more useful than paying developers to take generic security training courses or to figure it out for themselves: “I guess security courses are very broad or like they're with Java or PHP. That's not everyone's [use] case”, “I don't think there's a lot of resource like that, devs would be like super interested in to learn about security, and that is applicable to them.” Here, in particular, Jean emphasizes the degree to which the internal training program is scaffolded to the technologies used in the workplace. While neither Jean or Brian use the term constructivism here to describe their CTF-like training, nor might I expect them to, their pedagogical model reflects the same emphasis which that technique places on giving learners immediate and embodied knowledge of a subject. In particular, Jean and Brian’s program emphasized providing relevant and localized security education that could be immediately incorporated into the development work done at Moth Corporate.

In the technology industry, the practise of teaching developers about security risks in the technologies they produce falls into the practise of security education programmes. Typically approached in a cost-effect and compliance-based format, most organizations tend to utilize security education and training in fairly banal forms. Often security education takes the form of mandatory one-hour security awareness seminars or a mandate that employees must review a training module, usually a slide deck designed by a third-party compliance firm which provides the material through a learning management system. While such approaches to security education are widely loathed amongst white-collar workers, gamified approaches to security education in the workplace were not universally praised by everyone I interviewed either. Vish, who has a long history working in Silicon Valley-based firms, mentioned that one of the more prestigious companies he worked for sprung from former Defcon CTF organizers to provide a CTF-based security education workshop. As he explained despite the prestigious association of the organizer the CTF was not particularly compelling: “there’s a lot of fun things you can do, but I didn’t really feel the pressure”, “you’re looking for hidden fields in a JPEG or after a while it gets a little repetitive.” Vish, who works in application development, emphasized that the training was neither particularly compelling nor relevant to his work at the firm.

What’s interesting about contrasting Brian and Vish’s responses to the implementation of CTFs in the workplace for security education is the way in which it illustrates Morgan Ames’ critique of the way in which constructivist practices can be poorly deployed when they ignore locality (Ames, 2018). These experiences are connotative of the emphasis that constructivist pedagogy and scholarship have placed on context including Grimes and Field’s (2020) observation that “learning cultures” (p. 256) are situated in specific communities which significantly shapes their success and Karen Brennan and Raquel Jimenez’s (2020) argument that constructivist learning must be “meaningfully connected to one’s individual needs, not delivered in an abstract fashion that is inattentive to individual [and thus local] context” (p. 92). Much like the failure of corporately-sponsored hacking contests to appreciate hacker practice, an understanding of context and locality plays a major role in the success of CTF as a meaningful participatory exercise. To Grimes and Fields & Brennan and Jimenez’s point, Vish’s experience demonstrates how gamifying security education via a CTF is not a turnkey operation, and that a proscribed format of gamified security education runs the risk of being not fun at best and irrelevant at worst. By comparison, Brian and his team’s use of ‘CTF-like’ logic for workshops and company-wide internal competitions based on issues faced by developers at the company demonstrates how relevant and localized scaffolding ensures the veracity of the CTF for players at Moth Corporate.

For Brian this immediate and embodied style of training is a necessity given the scale of production at Moth Corporate: “there’s a team of like, 500 total developers,” as compared to the less than 20 members of his AppSec team, “the odds are stacked against us, so we have democratize it somehow.” In this sense, what Brian means by democratizing security education is rendering it participatory, immediate and accessible to his developers. During our interview Jean, a CTF designer and employee at Moth Corporate considered the benefits of using what could be considered a constructivist approach to security education against a traditional approach where the security team simply audits the work of developers. “[In] general you try not to be annoying as fuck and like just pointing out vulnerabilities” found amongst a developer’s code. He adds that such an approach would be implausible for his company: “we cannot look at like every project all the time, it's not scalable” due to the scarcity of security-team employees in comparison to the preponderance of developers regularly shipping code. Instead of relying on a highly centralized model of audit and authorization, Jean and Brian described the way the playful, CTF-like education program they developed allows their company to mitigate common vulnerabilities through the distribution closer to a model Brennan and Jimenez describe as “peer learning” rather than supervision (p. 92). These practises at Moth Corporate reflect larger industry-wide trends in projects like the Open Web Application Security’s (OWASP) Top 10 and MITRE’s ATT&K program (2020, p. 3) which “ensure” that businesses aren’t “distracted by minor risks while ignoring more serious risks that are less well understood” (OSWASP n.d.). Programs like OWASP and ATT&K encourage institutions to allocate their scarce security resources towards the elimination of high-impact, high-likelihood security risks first by educating their developers on common and relevant problems they are likely to encounter in routine work. In this way, Moth Corporate’s security team is providing similar meaningful scaffolding for security education within their organization that is immediate and intuitive to the experiences of their audience.

What became clear from my interviews with the Moths and CTF organizers who worked at Moth Corporate was the degree to which CTF also fulfilled a social role in the workplace, in addition to its use as an educational tool. While the Moths were predominantly comprised of members from the Appsec team, at least two of its players, Walt and Kennedy, were drawn from the developers. Despite their relatively ad-hoc composition, the Moths fared impressively with a top 10 finish in the final rankings of a CTF comprised of over 100 other teams, including more renowned CTF teams. Brian attributed his team's success to their ability to draw qualified players from across the company: "I don't want to brag but those people attended my workshop and did my CTF so [laughs] literally we picked those people by looking at the internal CTF and being like "You know the top 5? Ask them if they want to come to CRCRTF."" This practise at Moth Corporate corresponds with sociologist Fred Turner's theorization that such casual, but labour-like activities make "visible" their participants whose work is "transformed into the basis of individual reputations and communal intimacy" (p. 90). As Brian explained, the internal company-wide CTF was not only an effective education tool but created a source of information which identified who possessed remarkable security skills.

Brian's statement indicates the way in which engagement and participation distinguished players by encoding them with certain values relevant to security work. During our interview he described how the CTF allowed him to identify members of the development team he could approach to help him remediate problems.

> **Alex:** Would you say then that your internal CTF creates visibility into the workforce of whose got, sort of security aptitude or mindset?
>
> **Brian:** Oh yeah, yeah, if I were ever hiring internally, I would look at that leaderboard to figure out who to hire [laughs]. Cause we have a lot of a lot of really tough challenges on there, there's like some crypto ones, there's web, there's all that kind of categories, *it's a good yardstick* [my emphasis added]. […] It's easier to come to them and be like "hey I know you have some vague knowledge of security so I can just explain this thing to you in security jargon" instead of having to put it through my human filter.

In this way, CTF served as its own kind of language within the conditions of production at Moth Corporate, allowing Brian to discard the cumbersome "human filter" and communicate directly with someone who speaks the language of information security. As Brian explained, the visibility created through the CTF-like training was a two-way street:

> "and it kind of also puts our face out there, because security people aren't naturally uh, [Brian adopts a hushed, sarcastic intonation] I don't know if you've noticed naturally the

> most, they don't advertise their presence, too much. They [security team members] are very like introverted right? So, we kind of have to have these structured ways for people to uh… for people to meet the people who are dealin' with security at their company."

In this sense, CTF created a culture of visibility at Moth Corporate, which was frequently identified by its application security team members as a useful tool for internally recruiting capable parties to address security issues. As I have emphasized in other research, videogames have long created cultures of visibility around their play and their architecture, which is uniquely suited to the quantization of skill particularly amongst meritocratic cultures (Cybulski, 2014).

Amongst the application security team, Brian wasn't the only person to identify the way in which CTF play identified security-minded developers amongst his co-workers. As he and other members of his team described, the company adopted a kind of procedure around CTFs which employees participated in, organizing debriefing sessions following the event. Morgan, a well-respected hacker from his work in bug bounty programs described how playing in a CTF with the Moths was useful to him in building his reputation at his place of work:

> Sitting down [at a CTF] with [the Moths] I think that occurred in October and I had joined in June and so it was an opportunity to demonstrate that I actually knew what I was doing. So, you know I was able to A) capture flags from a web application perspective and then when we do the debrief, I was able to show how I did that using tools, and I think the team got a better understanding of kind of what my skills were. And I think that helped, and I remember a few people reaching out after the fact. It was just kind of like, they were interested in the fact that you know I was able to do all I was able to do with Burpsuite as opposed to my own custom tools or scripting, or that kind of thing. […] Having those relationships and being able to reach out to people and be like "how did you solve this challenge" and learn from people after the fact.

In Morgan's explanation, CTF performance became shorthand for competence and skill that allowed him to commute his status as a recent hire by signalling to his capability with certain security technologies. Throughout our interviews, both Morgan and Brian emphasized how participation in the CTF was an indicator of capability amongst their peers in application security. While we were walking for lunch Morgan explained that he also kept track of who on his team provided debriefs of CTF challenges and what skills were involved in solving those problems, so that he could turn to them if security issues were identified in relevant technologies the company uses. Morgan and Brian’s explanation of how CTF encoded skill, ascribes aptitude onto their co-workers in a way which is consistent with Michael Burawoy’s (1982) theory of “social codes” which emerge out of games in workplace environments, a term which identifies how certain behaviours in these games are ascribed common values on the job such as competence or trustworthiness (p. 79). It suggests an underlying privilege of CTF play is to be encoded, a potential to be made visible, recognized as skilled by engaging in the unwaged labour of CTF while other colleagues may have comparable skills but may be restricted by responsibilities or opportunities for access due to personal circumstances.

The use of CTFs as a social code in the workplace was evident outside of Moth Corporate as well. When I was observing the BBCTF Flynn noted that in her current job, she reported to Wilf, and both worked in a division of their organization which was led by someone known for organizing a CTF at another major hacker conference. When I asked Flynn, who was early in her career having only graduated college a year prior, if she felt pressure to participate in CTFs to fit into her company’s culture she turned the proposition of the question around:

> I don't think so. I feel like that's already been proven, but I know it’s definitely nice to see someone and I definitely feel like I respect [those] who do stuff outside in their outside life and take that time. So, I definitely think that, maybe, that they could probably feel likewise. That they see me doing more extracurricular stuff that is definitely important to my manager for sure, he sees that and takes value in that. But, mostly doing the CTF was for myself. And it was just very fortunate that me and my captain already worked well together and I was very fortunate to work on a team with him because of his experience. He definitely had, he's definitely up there. He won't say it, but he's up there!

Aside from challenging my assumptions about the social dynamics of her workplace, two elements of this response are interesting. First, Flynn emphasizes that CTF engagement amongst her co-workers impressed *her* with their commitment to maintaining their level of understanding and practise, that participating in these games was emblematic of their engagement with the field of security which was commensurate with her respect of their capability. This is significant as it indicates that the rationalization of play is not purely a downward phenomena, used to discipline/self-discipline less skilled participants, but speaks to a cultural economy in which play and engagement with hacker culture, ascribes expertise and status to participants. Second, Flynn identified that her shared engagement with Wilf in the CTF created an opportunity for a kind of informal mentorship with someone she had identified as possessing a discursive and ongoing engagement with her field of practise. As she indicates in this response, this close working relationship allowed Flynn to appreciate the depth of her co-worker's practise, a recognition that his proficiency was deeper that those skills he applied in the workplace. Given the often-atomistic social conditions of contemporary white-collar labour, where on-the-job training and apprenticeship is minimized in favour of hiring experienced candidates, Flynn's mentorship with Wilf via CTF signals how this game and by extension hacker culture, produces more convivial social conditions amongst workers in the security industry where knowledge and practise can be exchanged via extracurricular activities.

Walt, one of the members of the Moths I interviewed works as a mobile developer, coding the smartphone application and platform used by his company. Walt's expertise with Ruby on Rails gave his team an advantage in the internal CTF and as a result "my team ended up coming first and that CTF we sort of got like, I guess like prizes, whatever. They were just like, like sweaters and stuff. But from there, that's actually when Brian asked me if I wanted to come to the [CRCTF]." Walt described using his engagement with the company's internal CTF to gain a level of recognition and further his mobility within the company.

> I guess the takeaway from that is that basically doing the CTF sort of instilled confidence in them that I was somebody who would be able to handle being on their competitive team. It sort-of like gave me a name at Moth Corporate, somebody like who does CTF and who has […] these ideas about security and experience with mobile.

As a result, he and a select few other players were given a seat at the table for the company's most skilled CTF team. Walt's interview responses independently confirmed assertions made by both Brian and Morgan, that the CTF has been used to identify members of the development team who could be entrusted with security tasks. To this end, Walt could probably be characterized as something of a striver. A recent graduate, Walt had quickly been promoted from one corporate office to another and described participating in numerous activities at Moth Corporate, industry conferences and at his university which gave him a reputation as a skilled developer. In the time this dissertation was written Walt had already moved on to a more lucrative position at a new company, using his reputation at Moth Corporate to transition into a more prestigious job.

Michael Burawoy theorized how many games associated with workplaces often produced a social order, a kind of hierarchy amongst workers/players which identified reliable producers, but also those who demonstrated an understanding of material considerations and conditions of that production and could impose certain artificial rules on their production to align it with this game. In those workplaces Burawoy described playing this game as 'making out' and notes that skilled play often distinguished workers who were self-disciplined and often occupied positions of seniority and often respect amongst their colleagues, often having access to optimal assignments or tasks (p. 35). In a similar fashion, CTF communicates a candidates' desire to 'make out' in the security public, to engage with the self-disciplining logic of engaging in entrepreneurial activities which allow a participant to maintain a discursive understanding of ongoing developments in security research and hacking, but also to signal to their aptitude.

Only a handful of the CTF designers and participants I spoke to outside of educational institutions, where constructivist pedagogical methods are more common, described using gamified hacker exercises in the workplace to the extent the Moths did. So, ultimately Moth Corporate's practises around CTF are likely something of an outlier, which I serendipitously stumbled upon in the course of my fieldwork. With that being said, the way CTFs suffused work culture at Moth Corporate is figurative of the way in which this game is not limited to a gamified form of security education, its significance to modes of production, sociality and identity within an institution. Both Walt and Flynn's experiences speak to different roles that CTF can have in the workplace, where one used it as a way to gain recognition, while the other used it to deepen their social connections and practise with their co-workers. What's important about these observations is that they emphasize the difficulty of totalizing the laborious activity at the heart of CTF, that it does not fit neatly into a purely self-interested or altruistic activity. Through participation in the CTF both are possible, conditions afforded by both the design of the game and the community it is situated within.

6.4 Recruitment and Exclusion in CTF

Interviewing Brian about how he used some of the information from his company's CTF to recruit security ambassadors allowed him to relay an unexpected anecdote.

> **Alex:** Have you ever seen the movie The Last Starfighter?
>
> **Brian:** No.
>
> **Alex:** It's a movie about an arcade game that secretly recruits a person to fight in an intergalactic alien war.
>
> **Brian:** [laughs] I've had Google do that to me with Google search, I don't know if you've heard about that. For a while, they were trying to recruit engineers via Google search.
>
> **Alex:** So, you got one of those recruitment notices in your searches?
>
> **Brian:** Yeah, it kinda folded down and it was like "do you want to try our game" and it was a bunch of coding challenges, it was super frickin weird, but same kind of thing!

Whether Google's secretive practise of recruiting engineers by surveilling search queries might raise some ethical questions (documented by Dishman, 2017), this exchange reflects a kind of hacker folklore common to CTFs. If there was one story I heard over-and-over again prior to this study, it was that the winners of the Defcon CTF were often approached by the highest levels of the U.S. national security apparatus to work as hackers for America's government or tapped for lucrative work as an employee of its national security contractors. Vince, one CTF organizer. relayed this exact piece of folklore in an interview: "I've never talked to anyone who's got this but it's rumoured that you win the CTF at DEF CON and [Vince flashes finger quotes conspiratorially] "they" offer you jobs." While I similarly could not confirm this legend, I did appreciate Vince's candour in describing this legend for me to transcribe. Throughout my fieldwork and interviews, I encountered many examples of CTFs being used to recruit or screen prospective job seekers, which speaks to the degree to which this game has been instrumentalized by the security industry to identify valuable workers through a game involving hacking.

While CTFs serve as a kind of cultural infrastructure, they also have much more direct implications for how some players are recruited by firms. At the CRCTF, a local videogame studio which sponsors the event left recruitment flyers for a vacant security analyst position beside the pizza, knowing that viable candidates would likely be in attendance. As Guy, one of the CTF's organizers explained, in the French-Canadian community of hackers it was not uncommon to have local businesses sponsor the events and recruit from CTFs:

> They recruit these guys because you know, you have people basically saying, like, "I do this on weekends, and I enjoy it. I like problem solving!" and you know, and so they are close to the talent pool by, you know, being sponsors or being present in that scene.

For Guy, the consequences of hiring CTF players was obvious "you [will] have awesome developers, if you're able to attract the ones that are playing in these competitions, right?" Similar to Brian's comments, Guy notes that this kind of extracurricular engagement often acts as a signifier of not only capability but of desirability. As a social infrastructure a candidate's presence at a CTF communicates their willingness to 'make out,' as Burawoy (1982) might put it; engaging in entrepreneurial forms of training and networking that distinguishes an employee or prospective employee based on the kinds of value they can produce.

Leaving recruitment flyers around pizzas as a recruitment strategy was the tip of the iceberg at the CRCTF. As Max, the CRCTF's organizer explained "we also have companies that actually register a team, but fill like three spots with interviewees", adding, "we see this every year […] there's probably one or two teams that do this." This was confirmed by the CEO of one company at the event that sponsors the CTF; Max introduced me to the CEO of MammothSec during the competition and while the officer declined to be interviewed, he did explain his positive opinion in some detail while I took notes. Both Max and the CEO of MammothSec sought to emphasize to me that performance, an applicant's ability to solve challenges, was not the primary rationale behind sending prospective employees to the event. While Max indicated that a CTF could demonstrate how "people produce well and you know, deliver on time" the most important characteristic that he and many employers were more interested in was a candidate's ability to produce conditions of "psychological safety" which he defined as "so, you know, no blame, you know, no-blame culture, positiveness, transparency and all that." He concluded, "so they kind of recruit people through the CTF because they can see them not only on a skillset level but also on the communication level and on a team interaction level."

Max suggested this approach to hiring produced immediate insights: “you can see immediately, there's a great social fit if there's a great technical fit.” This rectified a traditional gap in hiring processes: “it's not the HR, that's going to be sitting there with a person, it's going to be the eventual colleagues or this person.” In this sense, Max emphasized that the primary qualities on which a prospect was evaluated was their interpersonal & communications skills and their ability to comport themselves in a competitive environment, a stand-in for stressful and time-demanding scenarios working in security (a similar rationale to what was described by the organizers of the BBCTF). In some ways, this approach signals a less managerial hiring process, with feedback coming from prospective colleagues. However, it is interesting that even though he emphasizes social skills as the primary determinant in a prospect’s CTF performance during their application, Max repeatedly refers to the way in which CTF performance still reflects technical capability, suggesting that technical skills were still evaluated, if less overtly.

Max himself was of two minds on the practice of using a CTF in a job interview. While he acknowledged that, “I think it is a very good idea for an interview,” he also described the practise of having job candidates play in a CTF, which runs the course of an entire weekend “harsh.” In clarifying his position, he noted: “I feel that requiring 48 hours of CTF as an interview is just it's not the way interviews should be conducted. So, I think it's too intense.” Max added that the time demands often meant that prospects often dropped out of the CTF early and that some teams/companies who used this method had occasionally tried to skirt CTF policy which enforces static team rosters by rotating another candidate into the event discreetly. In providing these contradictory comments, Max wrestled with the implications: “on the employer side, you know, you get the best experience” out of “your interview” by having a candidate hack and interact with company employees. From a candidate’s perspective, Max argued: “I think especially in an industry where you lack talent, putting people under this kind of pressure to interview them is probably at the end of these might be not very appealing.” It’s clear here that Max is wrestling between the functional, but also managerial logic applied to his game against his empathy for candidates. In this last comment, Max considers the demands against the candidate, but also provides a holistic perspective on the industry, indicating that such a practise might also turn away qualified applicants unwilling to speculate on spending a weekend playing a CTF to secure employment.

The practise of compelling a job candidate to partake in a CTF is an example of what Gina Neff (2012) described as "venture labor", the downloading of investments in "time, energy, human capital, and other personal resources" by workers in order to manage the risks traditionally borne by the companies they work for (p. 16). Instead of hiring a candidate purely based on their qualifications and accepting the risk that the new hire may not be a good cultural fit, the company has candidates demonstrate their candidacy by playing in a CTF as a stand-in for a work environment. Spending a weekend playing in a laborious CTF, particularly when they might otherwise be resting and or attending to domestic duties after the workweek's worth of work at another job, not to mention the demands against the company's existing employees at the CTF who must provide some sort of report or analysis of the candidate's performance. What can be extrapolated from my interview with Max is that CTF, like many other aspects of hacker culture, including hackathons and other autodidactic forms of learning, are occasionally instrumentalized by the security industry to mitigate the risk of hiring, often at a candidate's expense.

When I informally polled the Moths at the CRCTF on their disposition towards using a CTF in the hiring process, about half dissented, some observing that such a process would be too time-consuming. The assenting side, on the other hand, was quick to remind me that it is not uncommon for prospective employees in the technology industry to be subject to long-form interviews involving various tests of their coding and software conceptualization abilities. Those in favour were mostly younger employees. A majority of the CTF players I interviewed and observed were young, between the ages of 18-30, either pursuing an advanced degree or at an early stage in their career. Few spoke to demands against their time outside of their professional lives or training. As Ochre explained, CTF engagement was almost commensurate with leisure time associated with pursuing education:

> [Our team had] a lot of good people that were playing a lot for a year: in doing their master's thesis, [or] while they were working on their master's thesis for two years during their master's degree. But after that they were leaving for a job and they had no time anymore for playing.

Ochre also noted that in the United States where a PhD tended to last 5-6 years rather than 4 years in Europe, many American teams were better developed as players because students had more time for competitions and could mature their hacking skills. Guy indicated a slightly different time frame, but a similar pattern with his own experience in CTF: “we were playing a lot after university was probably my peak. So right before the kids but after university, and then you know, when the kids were born, then my participation kind of declined.” Both Guy and Ochre’s comments describe how the ability to participate in CTFs was closely tied to the availability of leisure time for themselves and other players, often weighed against economic and domestic demands like jobs and a family. As Wilf described, the discursive quality of CTF required him to keep abreast of new developments in the field: “it's harder to train for that”, noting “[I'm] getting, like old and have a family and stuff’ and that “simply physically preparing in some kind of schedule or whatever at the CTF” was often less feasible with demands against his time. It’s not surprising to suggest that hackers might have economic or domestic responsibilities which precede their time to hack, but what is interesting about these remarks and experiences is the way such responsibilities were often observed to displace the laborious play of CTF, often weighed against other forms of paternal and domestic labour.

At least two CTF participants I interviewed identified specific arrangements they shared with their domestic partners regarding the career expectation they participate in hacker events. Over a dinner break at the CRCTF, Morgan, a member of the Moths who was skilled in discovering vulnerabilities as part of his gig-work in bug bounty programs, relayed to me the understanding he and his wife shared about the kinds of hacking he did outside of work. Morgan’s wife managed a majority of caregiving responsibilities for their two children as a stay-at-home mom, while Morgan’s lucrative job in application security was the primary source of income for his family. In recognition of her constant attention to their children, he indicated that outside of work hours, he wanted to relieve her of as many parenting duties as possible. As a consequence, Morgan described how playing in CTFs was unusual for him, indicating that if he was going to take time away from his family to hack outside of work hours, he and his wife had an understanding it would be used to moonlight as a bug bounty hunter, pulling down a second income to pay for luxuries or vacations. Here there is an expectation that if extracurricular hacking is to be performed, then it should at least serve the immediate material benefit of the family.

Balancing the kind of professional development and networking that happens at a CTF with domestic responsibilities was similarly a topic of concern for Terry, whose wife also works in the technology industry.

> My partner and I very much support each other in our efforts to attend conferences [laughs]. And I'm kind of chuckling to myself because we both agree that going to a conference is a little bit like a vacation. Because while you're there and you don’t have to put in a full day of work afterwards, you don't have any kids that are dependent on you or, you know, frankly, any partners who are also dependent on you. So, you can go home and you can take a nap, you can go to a movie, you know, you could wake up at 6 am and go for two-hour exercise if you can afford to be at the conference by nine or something. So, we get that. And that's important because it means that we can have alone time or if our colleagues or friends are also there, it means we can have social time. […] And that's all fine because there's going to be a *quid pro quo* [emphasis mine] around that for us to go to our respective conferences. […] Given the relationship I have with my partner or the understanding I have, if it was going to be like a 10-or-12-hour day, I would honestly, I'd probably just get a hotel room in town. and just be like, I'm going to a conference. I'm not, I'm not here, I'm not accessible, because otherwise there's this assumption that I'm going to be able to get back into for dinner or to tuck the kids in.

Here Terry notes that he and his partner had a mutual understanding that conferences, which take one member of the household outside the home for a period of time, resulted in a break from domestic responsibilities. Their “quid pro quo” arrangement alludes to the fact that there was a clear expectation that such absences from domestic responsibilities would be evenly distributed between the two.

Terry and Morgan’s arrangements with their partners are indicative of a consciousness of these entrepreneurial and extracurricular demands of working in the technology industry. These domestic patterns speak to Kathi Week’s (2011) observation of how “the space of production reaches beyond the discrete workplace and the relations of production extend, beyond the specific employment relation” to make productive demands of technology workers outside their jobs. Such demands create a need for these workers to denote an “arbitrary distinction between” “productive” and “reproductive” labour or “remunerated life and non-remunerated life” between their working and domestic lives (p. 142). In light of Green’s earlier comments about the desire for professionalization amongst hackers in the 1990s who were having families, economic validation is certainly the most obvious, but consideration of how these jobs might afford domestic responsibilities might be considered too. Terry and Morgan’s understandings or arrangements reflect an expectation that the social conditions of professionalized labour in the security industry will allow for domestic stability, to leave space for domestic labour and parenting. The existence of these arrangements identifies a common perception of downward pressure in the technology industry, what Lily Irani (2015) described as a kind of entrepreneurial instrumentalization of hacker events, to build workplace relationships or keep the skills on their CV fresh through events like CTF.

None of the CTF participants I spoke to described their efforts to strike a balance between their extracurricular activities and domestic expectations in begrudging tones. Both Terry and Morgan indicated a strong desire to be supportive husbands and available fathers. Terry, in particular, spoke cynically of common conditions of labour in the technology industry, encountering job descriptions which indicated: "you're gonna work and really fast-paced environment with, you know, really hard-working people." Based on his experience working in Silicon Valley-based firms, Terry understood this kind of job description as: “code for more than 40 hours a week. And that's all code for, “I'm not gonna work there”” adding in his own rationale: “even if you were paying me 5, 10, 15% above market rate that doesn't give me back, you know, time with my kid who's, you know, young and doing things that they won't do ever again. So that becomes really important to me.” Terry and Morgan’s desire to be present seems to reflect larger demographic trends for fathers with full-time jobs to seek greater domestic presence and availability for parenting duties as well as to perform maternal support (Cooklin et al, 2016, p.1615, Joshi, 2021). In light of the shift in working conditions in white-collar information work, many parents, fathers included, reported greater job satisfaction when being able to flexibly attend to parenting duties while working from the home (Arntz et al., 2022). In reconciling the assumptions that they perform entrepreneurial duties (professional development and networking) outside of working with their desire to be available fathers, Terry and Morgan's comments indicate that despite their inculcation in hacker culture the identity does not totalize their patterns for work and if anything, signals expectations that their work should accommodate parenting and domestic life as a condition of their employment. Due to the lack of female research participants, it's hard to say if women are similarly able to expect or demand that their professional lives in the cybersecurity industry take account of their role as parents, or if such an expectation is gendered with women invisibly shouldering the brunt of domestic labour due to cultural norms around parenting. In any case, it's clear that cybersecurity workers are conscious of the degree to which training, education and other extracurricular activities have been commodified as an integral part of the social fabric of technology work.

MammothSec wasn't the only company using CTFs as part of its hiring or recruitment processes. Moving from the CTF floor in a convention centre back to Team Alpha's hotel room while observing them at the Danger Days CTF (DDCTF) I noted a foreign element out of place amongst the mostly shorts and t-shirt crowd. Clad in military-style haircuts, golf shirts and creased chinos a squad of recruiters from a major U.S. military contractor milled about the suite while dozens of open pizza boxes lined the hotel room bar and Alpha members munched on slices during a lunch break from the CTF. One of the contractor's employees had recognized a member of Team Alpha on the CTF floor and approached him: "He was like, dude, I am sending you guys all lunch. Just let me tell them I am hiring." Evidently, the pizzas were delivered with an in-person recruitment pitch. The very soldierly-looking recruiters chatted with Alpha's members about the perks of working for one of the many Maryland and Virginia-based defense firms. Military contractors support U.S. government cyberdefense, but also offensive operations, supplying vulnerabilities, which the NSA budgeted 25 million dollars for in 2013 (Perloth, 2021, p.192), software to automate exploitation, support personnel and other tooling that allows the American military to perform surveillance and other acts of digital espionage as part of its multi-billion-dollar intelligence budget. The most recent year, 2013, that such figures were made available estimated that the CIA and NSA's "black budget" was somewhere in the realm of $52.6 billion dollars, which likely includes the money paid by these intelligence agencies to their contractors in support of their work (Gellman & Miller, 2013). So, the pizza was a trifling cost to get access to Alpha's excellent hackers, many of whom performed the most technically demanding and sophisticated forms of hacking I witnessed in this study. In this sense, there was some credence to the folklore that top security firms recruited at prominent CTF competitions. In reality, it wasn’t winning, but simply qualifying for the event that signalled a player’s aptitude.

Being sought after by the military-industrial complex is prestigious for some but alludes to issues of nationalism which permeates hiring practises in the cybersecurity industry for others. As Qais, a member of Team Alpha was widely recognized as a skilled hacker by his peers and even by potential recruiters, explained to me:

> A lot of people would like would like to hire me if I was a U.S. citizen, is generally what they, they keep on saying. Like […] they want [security] clearance and I don't want to deal with that stuff. Or companies just don't want to do the whole HR paperwork.

Qais also notes that this isn’t just preference, but enforced by restrictive policy:

> There's also like all these the companies that come in and they're like: “we would demand US citizens only for hiring.” So, it's very discouraging seeing that constantly. Especially being a man from the Middle East.

It wasn’t only companies and policies which had discouraged Qais from working in the security industry:

> When I was an undergrad, there was a professor, not a security professor, who explicitly said that I should give up on security because I cannot get a job [because of his nationality]. I am not kidding about that, as almost verbatim cold there.

The temerity which Qais ascribes to this statement identifies both the general nationalist sentiment of restrictive work conditions in the cybersecurity industry, but also the degree to which this discourse is common knowledge in the industry and amongst industry-adjacent roles including the education sector. The point here is not that Qais was excluded from CTF as a result of his nationality/race, but his awareness of the factors had resulted in his exclusion from one of the perks of high-level study of information security research and CTF play, lucrative employment in the military-industrial complex.

It should be noted that Qais was not completely excluded from employment and job placement opportunities in the U.S. During our interview he noted many positive workplace experiences he had in the cybersecurity industry in the country where he studied, but that the exclusionary practises common to national security work and restrictive work permissions had impacted his career mobility. As Qais explained, these practises also had a corollary on his social life. When many of his friends and colleagues were recruited out of university by high-security organizations he found himself isolated: “I've had people who, because they're just so hooked on like, they want to get the government contracts or job where they have top secret clearance, etc., etc., etc., that they will cut off all contact with any foreigner.”

Qais’ experience reflects national security policy in the U.S. for obtaining security clearances under the Defense Counterintelligence and Security Agency (DCSA), part of the Department of Defense which conducts background investigations for the government and security industry contractors. While the DCSA’s policy to disclose foreign contacts does not exclude clearance applicants, it does require rigorous reporting of foreign-born contacts. Qais’ experience reflects an internalization of that policy expressed as a general social paranoia and general aversion to foreigners. This paranoia and internalization of the secrecy amongst high-security workers in the cybersecurity industry, as Qais explained, and the culture of confidentiality, affected existing friendships as well: “then they're like, we can't talk about work in front of you. And I know, I know, they're not trying to be offensive, but like, it's kind of like, man, this is shitty!” In hacker culture where exploring interesting problems is the lifeblood of the community, being cut out of those conversations for national security and secrecy’s sake was a serious blow to Qais’ ability to participate in conversation with colleagues. In this explanation, Qais drew an interesting contrast:

> But in general, like a lot of the hacker community, per se, not that corporate part, but like the hacker community I've noticed are more open, they don't care where I'm from. And if anything, they just get a general interest but how it is in [Qais’ birthplace].

This comparison is significant for two reasons: the most immediate being that Qais’ peers within the hacker community are less concerned about his race/nationality. The quote suggests that despite the meritocratic culture amongst hackers it was filtered or distinct from industry practises. This addresses the second reason why this quote is interesting as Qais delineates the hacker community from the security industry, but still ascribes a parallelized relationship, where there exists a clear overlap of practise and community consistent with the conceptualization of the security public as a formation which amalgamates the two.

The delineation of nationality within the security public identified by these experiences speaks to the way in which hacking has become legitimized as part of the security industry. While Matt Goerzen and Gabriella Coleman (2022) have recently emphasized the careful campaign of "linguistic, rhetorical and mediatic labour" by hackers to assert their professional legitimacy (p. 8) there are also material relationships that reflect national security discourses which have distinguished and elevated hackers within the technology industry and in public discourse. Qais' experience demonstrates the way in which the cybersecurity industry, through nationalist economic and security discourses, filters membership to a large sector of that industry through citizenship and race; structuring economic access and identity within the security public. What's important then about this structuring effect, is that the national security apparatus and discourse directly influence which individuals have access to lucrative and prestigious employment. Added to this, many prominent hackers within the cybersecurity industry have openly disclosed their former ties to the U.S. national security state, from Charlie Miller, a former NSA employee well known for hacking cars, to Robert M. Lee, an industrial security expert and former member of Cybercom & the U.S. Airforce's cyber operations. Even Mudge, the prominent member of the group the L0pht, while certainly regarded as a skilled hacker for his merits, has his legitimacy constantly filtered through his former employment at DARPA in books (Menn 2019), press releases and speaker biographies where he is described.

In these cases, security clearances, combined with affiliation to prestigious national security institutions, have allowed certain hackers to attain positions of authority, access and large public platforms on social media. Ultimately what's significant about this observation is the way in which professionalization and legitimacy are potentially constrained by nationality within the security industry. While scholars have identified the ways in which a hacker must operate within certain ascribed ethical parameters to be considered suitable for employment (Slayton, 2017; Tanczer, 2021), eligibility for employment based on nationality and access to certain labour markets also structures legitimacy within the security public. In its own way, industrial interest in CTF speaks to such a distinction: by attending local events many players are connoting their own eligibility within local/national markets and deploying skills which are of interest to local security concerns (such as specific concentrations of technology industries, web applications, like at the CRCTF for example) and national security discourses.

In many of my interviews, I asked players if there were any questions they thought I should have asked about CTF. After interviewing one CTF player, Claude, who participated in the DDCTF, he caught me off guard with a question about the meritocratic nature of CTF play.

> Are you familiar with survival bias? […] So, I think about hacker culture I think – the one that sticks around and the one that hacks back, the "learn by yourself" kind of challenge and they've proved their skills. They've worked. But that doesn't mean people who are not there [at the Danger Days CTF] are unfit to be good security professionals! Or good CTF players it just means that they didn't pass this challenge. […] You don't really belong or you're not really accepted as long as you don't prove that you're able to do certain things by yourself. […] I definitely had friends or contacts who like just throw people at challenges and say "come back when you have solved that" and that was their way of teaching or organizing a social [group] – like a security club.

Claude's comments surprised me, as it was one of the first and few times in this study a participant uttered a stringent critique of the hacker and CTF community that was generalizable. Usually, if a participant had a complaint it applied to a specific CTF, person or challenge. Here Claude is criticizing the operational logic of CTF as an arbitrary indicator of a player's skill, calling attention to the artifice of CTF challenges as being representative of real security issues or their relevance to becoming a security professional. During our interview he admitted a feeling of loneliness in struggling to find opportunities for mentorship and camaraderie, taking issue with the way in which CTFs often encourages individualist approaches rather than cooperation and mentorship.

The arbitrary quality of CTF and the sense of belonging it provoked was also observed by Pearson:

> I think that some of the people ended up moving away because they didn't feel very qualified either. So even you know, even on this apparently rocket ship ride to the moon.

> […] Some people left and went to become solar panel installers in Hawaii you know, even though […] [we] had all this contact and access and skill and it wasn't what they needed.

Here Pearson, whose cohort had seen tremendous success in the security industry, partly as a result of their success in CTF play and organization, noted that ultimately the entrepreneurial quality of CTF often left some members struggling to keep up. Pearson acknowledged that some questioned, "if the mountain, we were climbing was worth it?" What's interesting about Claude and Pearson's comments is the way they question the idea that success in CTF is generalizable, that a player's success and by extension their sense of belonging to the game's culture (and by extension, hacker culture) translates to professional success.

If we are to think about this arbitrary quality of CTF play identified by Claude and Pearson, it calls into question the role that such a game could objectively play in representation within the workplace, particularly if those who do play are considered to have 'survived' its filtering process. One group underrepresented in this study and within the CTF community broadly were women and in interviewing them it became clear that certain elements of CTF play and organization had impacted their engagement with the game and hacker culture broadly. For example, Dana described two incidents that discouraged her from attending hacker conferences in general, observing "there's definitely been times at DEF CON where women didn't exactly feel welcome." At one event she described feeling unsafe after an incident where "I encountered somebody after hours, and we kind of got physical in a way I wasn't comfortable with", attributing this behaviour to the culture at the conference. Another incident she referenced "was that infamous year where they had a card where you're supposed to go around and bribe" Defcon's volunteer security team (the "Goons") with a card that says "show your boobs" "which is not inclusive. And that was official Defcon. Okay? Handed out with the badge." The incident described by Dana occurred in 2011 when Def Con handed out a "goon bribe card" a kind-of scavenger hunt contest which came with the lanyard used to attend the conference. The goon bribe cards compelled female participants to "bribe" a Goon by showing them their breasts, and in turn, they would be rewarded with a prize, usually conference merchandise (hexadecim8, 2016). As Dana explained, her experiences at the conference conveyed a general lack of safety and respect for women at the event, and she decided only to return after friends vouched for changes to its culture and policies.

While Defcon has instituted many policy changes which it enforces using a committee known as the transparency board, the hacker conference does have a history of misogyny and sexism, which can account for the underrepresentation of women in the event and its flagship CTF. The first CTF at Def Con 4 in 1996 ceded the floor to "Strippercon" a conference-sanctioned event in the evening where nude dancers performed and wrestled for attendees. During an interview with one player at an early CTF he described encountering a user-submitted CTF challenge where players were compelled to hack a server riddled with pornography. In a podcast interview, Defcon CTF veteran Dr. Giovanni Vigna describes how a woman on his team Shellphish was frequently verbally harassed or subject to unwanted attention by Defcon attendees during a competition in 2009 (CTF Radiooo, 2020). These incidences point to a pattern of behaviour which has often led, as Dana attested to, women feeling unsafe or unwelcome at the conference and by extension at its influential CTF. Added to this problem many CTF teams take a laissez-faire approach to recruitment, which often reproduces a gender disparity amongst teams. Tara, a player on a team with over 50 members based in the U.S., described how there were more nationals from a mid-sized European country amongst her cohort than there were women, which she coyly described as a "homogenous" concentration given the gender distribution of the population. In Tara's analysis "cultures breed themselves" and in the absence of any policy to recruit women and rectify this disparity, the status quo for her team was to be largely composed of men. Dana and Tara's observations inform the way we can think of survivorship bias within the CTF community: those likely to play in a CTF and therefore to be recruited through one occupy a very specific configuration of players who have passed through certain cultural and communal filters. For a woman, being able to sustain one's affiliation with a conference or team despite these issues requires an effort to persist against cultural and institutional forces which are hostile or at least indifferent to their presence.

Conclusion

7 Hacking for Access to the Social

Understanding how "the stories we tell ourselves about ourselves" (Geertz, x) emerge is a murky process. When we seek to explain historical change, particularly as a process of meaning-making, we are fundamentally attempting to characterize the conclusion of a transitory period that we can rationalize in the present, but whose outcome could not have been easily predicted during the same period. For example, throughout this dissertation, I have evoked the spectre of hacker contests as a good example of a playful practice within the hacker community that failed and was roundly rejected by hackers themselves. *Why?* The hacker contest offered hackers the opportunity to compete for money, in some cases a small fortune at a time when hacking was largely unwaged! Such contests let hackers use their skills in subversion against real-world technologies, to prove themselves and to do it for a corporate audience who conferred legitimacy onto hackers by sanctioning such an event in the first place! Instead, CTF, a sideshow for a LAN party held at a hacker conference, with virtually no prize money, no corporate audience and in many cases using made-up challenges supplanted the hacker challenge. *Again, why?*

The simple answer is because hackers *wanted to* participate in CTFs. The complex answer, that this dissertation has presented, speaks to the authenticity of CTF as a game constituted by and for the hacker community, whose practices, play and design reflects shared values and meaning amongst its participants. To really "hack" something promises an approach to the material substrate of technologies, to engage with technical artefacts with a degree of latitude required to decompose and subvert sociotechnical systems, in order to find their weaknesses (as I describe in Chapter 4). This approach to security research is as much playful as it is scientific, stimulating the intellectual imagination of hackers who find a kind of pleasure in analyzing and reconfiguring the functions of technologies to undermine their protections. Security research cannot be purely reduced to the aesthetics of subversion due to the way in which hacker practices engage with the empirical foundations of computing as a form of technical experimentation (as I describe in Chapter 5). In contrast to hacker challenges, CTF commands the attention of hackers not because it offers them the opportunity to simply subvert a technology, but because it offers them a meaningful engagement with this technology and the attendant joy that comes from identifying vulnerabilities through rigorous experimentation. As a game, CTF is as much a ritual enacted through play which demonstrates their capabilities, as it is a story which hackers tell themselves to justify their approach to technology, by demonstrating its veracity. Hacker challenges do not sit well with either the ritual or the narrative due to their well-documented limitations.

In the past, CTF had served as an exposition of hacker talent when it was hard to hack anything in public without the threat of legal recrimination. In the present age of corporately certified ethical hackers, LinkedIn and bug bounties offering to pay a hacker cash for discovering and reporting vulnerabilities, it seems like the CTF would be outmoded, a relic of a time when hackers were part of the literal underground. Despite these changes to the valuation of hackers and their tradecraft, CTF enjoys greater prominence in the present moment, with an expanding player base and surging in popularity even though there is rarely, if ever, prize money offered and few obvious material rewards. Speaking to this tension, many of the research participants I engaged with in this study regularly get paid bug bounty programs or have full-time gigs as penetration testers with six-figure salaries, but will then play in or organize a CTF over the weekend, often emulating the same kind of hacking they do in their day-jobs. *Who has the time for all this hacking?* What I'm getting at here is that the techniques, tools and methodologies of hacking might be laborious, but hacking itself cannot be fully rationalized/totalized as work by hackers themselves. *Again, why?*

The simple answer to that question is that the pleasurable qualities of security research, both aesthetic and empirical, help to explain some of the appeal to hacking as leisure. The complex answer discussed throughout this dissertation is that hacking something at a CTF isn't just about a laborious process of producing contingent behaviour, it promises visibility, prestige and intellectual recognition by one's peers through the structure of the game. Often this prestige translates into career mobility, free beer and conference swag, or status (discussed in Chapter 6). The identity of hackers is heavily shaped by the social capital mobilized through their vibrant communities. Communal structures have long been sustained by a vast gift economy shaped by votive labour and the open exchange of information, which includes CTF competitions. Being a good hacker, as described by many of my research participants, isn't defined solely by technical acumen, or the ability to subvert technologies, but rather by the desire to participate in communal modes of engagement regarding security research sharing knowledge, tools and events/experiences, a recurring theme in my discussion with research participants.

Scholars discussed in this dissertation have defined the material and immaterial aspects of this communal behaviour: Gordon Meyer (1989) described information networks which sustain the hacker community as “mutual infrastructure” while Fred Turner (2009) described communal gift economies amongst technical workers as “cultural infrastructure.” Such explanations resonate with hacker culture’s gift economy, as much as they do with a ludic infrastructure at work in a CTF competition which uses a heuristic style of challenge design to encourage its participants to recirculate, appropriate and incorporate the knowledge, technologies and practices created by other hackers into their own playful activities. Academics quote, paraphrase and cite. Security researchers playing in a CTF read write-ups, fork Github repositories and follow challenge designers on Twitter. CTF play and hacker practice by extension is therefore as much about hacking as it is about the circulation of social capital within the hacker community. The game is expertly utilized as a discursive means to this end at beginner-level events to introduce new hackers to common practices as it is in high-level competitions to communicate cutting-edge techniques to subject matter experts.

The mode of communal engagement, the ludic infrastructure of CTF is, as it has been in the past, an ongoing site of struggle and contestation, which has certain changes, enclosures and efforts at privatization. While practices like hacker contests have been rejected, as discussed in Chapter 6, CTF has been influenced by paradigms including gender and race, corporate entrepreneurial practices and the discourse of the national security state. The influence of these paradigms is indicative of the way in which knowledge, technical resources and prestige are not evenly distributed in the hacker community. What it means to be a good hacker is socially constructed through recurring systems of association, meaning making and narrative, processes which CTF competitions excel at producing, for better or for worse. As a result, not everyone accesses CTF at its most elite register. Some thrive while their peers merely survive and even renowned hackers quit often in frustration or out of isolation. Certain hackers have access to prestigious communities, while others struggle to find the mentorship required to participate in a game with such a high learning curve. In this way, CTF is as much about skill, as it is about the access to and the navigation of social capital and the channels through which it flows.

While CTF competitions might embrace the logic of meritocracy in their execution, the rules and scoring system which structure a game, and the identities of hackers are demonstrably not constructed through an identical meritocratic process of achievement and recognition. As I've articulated throughout this dissertation, the hacker identity as constituted by its history, practices and values is heavily shaped through access to social and material capital, to leisure time and the computing resources required for mastery. Often construed as eremitic, the hacker identity is, in fact, deeply connected to larger economic, political and social systems and projects, many of which hackers have reacted to through their own idiosyncratic approaches ranging from free and open-source software to hacktivism and the community/fellowship shared amongst these technologists. By analyzing CTF competitions, I have called attention to similar linkages, analyzing a hacker game to explicate the material presence of larger systems and their prevailing logics in rituals of play. By doing so, I have sought to articulate how hacking, specifically security research, is in continuity, rather than an exception to existing cultural formations we understand already. CTF functions as a constant negotiation of the blurry boundaries between play and work, concisely because the game provides access to a social world larger than the sum of its co-constituted elements: shared experiences, shared systems of meaning and a shared enjoyment of technical practice.

a. Future Areas of Study in Capture the Flag

One of the main limitations of this study was the format and function of a doctoral thesis itself. While I have shoehorned a tremendous amount of historiography and historical analysis into this thesis through the literature review, there was a history of CTF that I captured in interviews and gleaned from archival research that described the emerging contours of the hacker community and the valuation of security research in the 1990s. While I did write extensively about some of this in earlier chapter drafts, much of this material could not be presented in a succinct way that advanced the distinct research objectives of this dissertation coherently. The ur-histories and early histories of CTF are largely unexplored and at risk of erasure due to the absence of primary documents, the relative age of the participants (some now entering seniority), pervasive link rot and the deprecation of early-web proprietary file formats (when was the last time you used RealPlayer to stream audio?). In future research, or perhaps a book, I'd like to document the histories of CTF that describe the many sites of cultural struggle and contestation informed by the hacker community and longstanding antagonisms which are now largely invisible, or moot, in the present day but represent significant narratives of cultural change around security research and the cybersecurity industry.

The second limitation of this study is the absence of non-male, non-white research participants, who occupied a small fraction of those contacted for this study. As I pointed out in the methods section this is, in part, due to the exploratory nature of the study which did not explicitly set priorities for inclusion, but it also speaks to my limited visibility into the larger CTF community at the outset of this study. Future studies, including my own, which are interested in greater representation amongst participants, might consider partnerships or work with organizations like the Diana Initiative,[32] or Blacks in Cybersecurity (BIC)[33] (as well as many others) which organize CTF competitions as part of a larger information security conference programming initiatives targeted at inclusion and representation. The events and CTF competitions run by these organizations would be an excellent place to situate a study to examine how cultures traditionally excluded from a largely male and largely Western hacker identity have begun using these games within their communities.

It was also through my current program of research that I noticed the beginnings of a major cultural shift within the security research arm of the hacker community: inclusion and representation have become a larger priority, but also the subject of debate and cultural skirmishes both online and at in-person conferences. While scholars like Leonie Tanczer (2016) and Christina Dunbar-Hester (2020) have written excellent material on issues of representation and diversity within the hacker community, many interesting policy and enforcement debates are happening at major information security and hacker conferences throughout North America in the present-day which warrant further attention for how they approach the topic of inclusion and social/restorative justice in the enforcement of policy at these conferences, particularly in light of the historically technomasculine and transgressive hacker identity. These skirmishes have called into question longstanding behaviours and practices within the hacker community. Policy

[32] https://www.dianainitiative.org/

[33] https://www.blacksincyberconf.com/

enforcement at conferences like Defcon and HOPE have and continue to push out former luminaries of the hacker community for problematic if not outright abusive behaviour. As such, probing the social conditions for these cultural changes, the discourse around them as well as material efforts to change conference programming and governance of these events. seems like a fertile area for studying a substantial cultural shift in the hacker community at large.

The final limitation of this study was that I simply collected too much data! While this is a good problem to have, I ran into material limitations in terms of time I could spend analyzing this information and well into the upper page limit I could spend attending to subjects pertaining to CTF that I thought were interesting and spoke to my limited research questions. I would have liked to spend more time discussing perceptions and understanding of cheating within CTF competitions. While we understand hackers as highly transgressive figures, many of the ways players described cheating challenged norms around the topic. As I described in Chapter 5, CTF organizations are still undergoing a major cultural shift in how they negotiate the practices considered essential to the hacker identity, particularly as they pertain to social forms of subversion. These and so many other cool things I encountered (open-source hacking tools created by signals intelligence agencies, memes, IRC channels, battery-powered conference badges made printed-circuit boards!) were just too hard to shoehorn into this dissertation.

b. Logging Out, Logging Off

In this study, I've identified many forms of research on CTF, wargames and other gamified information security exercises which attempt to quantify or explicate the efficacy of these games. Efforts to fully rationalize the CTF as an educational tool will likely remain the predominant trend for scholarship involving the game within academic circles, particularly those oriented towards STEM disciplines, as the game remains the focus of intense pedagogical instrumentalization for cybersecurity education. It is in that context that CTF risks being gamified in the common sense of the term. Filling the cybersecurity knowledge gap remains a hard-to-reach educational objective of world powers like the U.S. and China, who identify information security as a strategic priority of national significance for signals intelligence and national security, as well as smaller countries, provinces/states and municipalities, attempting to preserve digital statecraft under a deluge of cybercrime. In this context, CTF could easily become a story about a playful way to learn otherwise onerous subject matter.

I am hesitant to jump into the fray of quantifying or qualifying the efficacy of CTF because I see this approach as inherently reductive in understanding the broader cultural significance and potential of these competitions as a form of enculturation which makes it a unique form of gamified phenomena. Framing CTF as simply an educational pursuit, limiting it to a form of cybersecurity training detracts from examining the robust culture of CTF within the hacker community, which has used this game as both a tool of expression, but also as a tool of circulation amongst hackers, to point to other interesting subjects, methods and tools. As argued above, there are many gamic elements of CTF including time limits and scoring which can detract from their educational potential but make participation interesting and meaningful to both their players and designers.

Ultimately, I think a framing of CTF oriented purely toward training with an explicit focus on educational outcomes is also potentially harmful, threatening to collapse perceptions of the game within the community. Over-emphasizing CTF as a form of vocational training rather than an expressive, distinctly social instrument would not only make the game less dynamic but over time weaken the cultural economy which sustains the practice, orienting it away from the autonomous practices of its participants, enshrining a purely pedagogical rather than communicative values. In some ways, this harkens back to the concerns of figures within the hacker community who were worried that over time CTF would become watered-down and routinized into yet another certification within the cybersecurity industry, a resume item to be acknowledged, another compliance box to be checked off the list. In other ways, this concern reflects the fact that as a gamified activity, the most durable examples of CTF like the Defcon competition are oriented towards top-level practitionership and discursively require a constantly evolving technology skillset reflecting state-of-the-art knowledge and skills an area which traditional pedagogy struggles to teach. The level of depth and complexity that CTF has attained within the hacker community is sustained by a voluntaristic and energetic commitment to the discourse of vulnerability research and hacker practice, which continues to expand and experiment with the design and format of these events.

Finally, considering the geostrategic tensions around cybersecurity, it is worth considering what solutions exist to preserve the open exchange of security knowledge which the hacker community, embodied in part through CTF competitions continues to sustain. CTF and the hacker community that sustains it is one of the few global communities and activities that still brings security experts from nations in conflict into the same room under friendly pretences. Online it is not uncommon to see CTF players from the U.S., China, Russia and Europe engage in friendly exchanges over techniques, tools and write-ups used in competitions via platforms like Twitter, IRC and Discord. The same is true of in-person events, where a post-CTF afterparty gives way to long, sometimes drunken and enthusiastic conversations between players representing different nations about vulnerability research methodology and exploitation techniques. I do not pretend that CTF is a cure-all for geostrategic issues involving cybersecurity. But historically these kinds of free exchanges of scientific knowledge during events like the Cold War have been used to ease geopolitical tensions. As a knowledge-driven discipline, information security abides by the idiom ‘all ships rise with the tide’; the free exchange of cybersecurity knowledge has the potential to make the world a secure place by eliminating common and general threats to the privacy and security of computer users the world over. I sleep better knowing cybersecurity experts are sharing and honing their knowledge through playful activities like CTF and I wish more communities could follow the model of knowledge exchange and openness espoused by hackers in the security community. I’ll find a lot more time for CTFs myself now that this dissertation is finished.

References

adamd and Zardus. (2020, November 17). Shellphish History with Giovanni, Chris, and Davide. CTF Radiooo, Retrieved January 10, 2023, from https://ctfradi.ooo/2020/11/17/00B-Shellphish-History.html#4579f370

Aho, J. A. (1998). The things of the world: A social phenomenology. Praeger.

Aljanaki, Bountouridis, D., Burgoyne, J., Van Balen, J., Wiering, F., Honing, H., Veltkamp, R., & De Gloria, A. (2014). Designing Games with a Purpose for Data Collection in Music Research. Emotify and Hooked: Two Case Studies. In Lecture notes in computer science (pp. 29–40). Springer. https://doi.org/10.1007/978-3-319-12157-4_3

Ames, M. G. (2018). Hackers, Computers, and Cooperation: A Critical History of Logo and Constructionist Learning. PACMHCI, 2, 1–18.

Baird, B. J., Baird, L. L., & Ranauro, R. P. (1987). The moral cracker? Computers & Security, 6(6), 471–478. https://doi.org/10.1016/0167-4048(87)90028-9

Benkler, Y. (2006). The wealth of networks: How social production transforms markets and freedom. Yale University Press.

Berg, B. L. (2001). Qualitative research methods for the social sciences (4th ed). Allyn and Bacon.

Beltrán, Héctor. (2022). “Hacking, Computing Expertise, and Difference.” Just Tech. Accessed December 11, 2022. https://just-tech.ssrc.org/field-reviews/hacking-computing-expertise-and-difference/.

Bogost, 2011 http://bogost.com/writing/blog/gamification_is_bullshit/

Brandstätter, & Sommerer, C. (2016). Productive Gaming. Entertainment Computing - ICEC 2016, 260–265. https://doi.org/10.1007/978-3-319-46100-7_27

Brennan, Karen, and Raquel Jimenez. 2020. “The Scratch Educator Meetup: Useful Learning in a Playful Space.” In Designing Constructionist Futures: The Art, Theory, and Practice of Learning Designs, edited by Nathan Holbert, Matthew Berland, and Yasmin B. Kafai, 85–95. The MIT Press. https://doi.org/10.7551/mitpress/12091.001.0001.

Bretthauer, D. (2002). Open Source Software: A History. Information Technology and Libraries, 1(21), 3–10.

Brewer, G. & Shubik, M. (1979). The war game: a critique of military problem solving. Cambridge University Press.

Brinkmann, Svend. (2018). “The Interview” in Denzin, N. K., & Lincoln, Y. S. The SAGE Handbook of Qualitative Research, 1694, pp. 997-1038.

Brown, J. J. (2008). From Friday to Sunday: The hacker ethic and shifting notions of labour, leisure and intellectual property. Leisure Studies, 27(4), 395–409. https://doi.org/10.1080/02614360802334922

Buckleitner, W. (1999). The State of Children’s Software Evaluation - Yesterday, Today, and in the 21st Century. 10.

Burawoy, M. (1982). Manufacturing Consent. University of Chicago Press.

C-46 - Criminal Code, Parliament of Canada, RSC 1985, c C-46 (2022).

Caronia, L. (2018). The phenomenological turn in education. The legacy of Piero Bertolini's theory. Ricerche Di Pedagogia e Didattica. Journal of Theories and Research in Education, Vol 13, pp. 1-22. https://doi.org/10.6092/ISSN.1970-2221/8600

Charsky, D. (2010). From Edutainment to Serious Games: A Change in the Use of Game Characteristics. Games and Culture, 5(2), 177–198. https://doi.org/10.1177/1555412009354727

Coleman, G. (2010). The Hacker Conference: A Ritual Condensation and Celebration of a Lifeworld. Anthropological Quarterly, 83(1), 47–72. https://doi.org/10.1353/anq.0.0112

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

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

Conrad, Misenar, S., Feldman, J., & Simon, B. (2016). CISSP study guide (Third edition.). Syngress.

Crozier, M. (2010). The bureaucratic phenomenon. Transaction Publishers.

Cybulski, A. D. (2014). Enclosures at Play: Surveillance in the Code and Culture of Videogames. Surveillance & Society, 12(3), 427–432.

Dafermos, G., & Söderberg, J. (2009). The hacker movement as a continuation of labour struggle. Capital & Class, 33(1), 53–73. https://doi.org/10.1177/030981680909700104

Deem, R. (1982). Women, leisure and inequality. Leisure Studies, 1(1), 29–46. https://doi.org/10.1080/02614368200390031

Delfanti, A. (2021). The warehouse: Workers and robots at Amazon. Pluto Press.

Denning, Dorothy E. 1990. "Concerning Hackers Who Break into Computer Systems." In Proceedings of the 13th National Computer Security Conference, 653–64. Washington D.C. https://faculty.nps.edu/dedennin/publications/ConcerningHackers-NCSC.txt

Denzin, N. K. (1978). Sociological methods: A sourcebook (2d ed). McGraw-Hill.

Denzin, N. K. (1997). Interpretive ethnography: Ethnographic practises for the 21st century. Sage Publications.

Desjarlais, R., & Jason Throop, C. (2011). Phenomenological Approaches in Anthropology. Annual Review of Anthropology, 40(1), 87–102. https://doi.org/10.1146/annurev-anthro-092010-153345

Dishman, L. (2015, August 28). Google's Secret Strategy To Recruit Engineers. Fast Company. https://www.fastcompany.com/3050451/googles-secret-strategy-to-recruit-engineers

Dunbar-Hester, C. (2020). Hacking Diversity: The Politics of Inclusion in Open Technology Cultures. Princeton University Press.

Eagle, C. (2013). Computer Security Competitions: Expanding Educational Outcomes. IEEE Security & Privacy, 11(4), 69–71. https://doi.org/10.1109/MSP.2013.83

Egliston, B. (2020). ‘Seeing isn’t doing’: Examining tensions between bodies, videogames and technologies ‘beyond’ the game. New Media & Society, 22(6), 984–1003. https://doi.org/10.1177/1461444819875078

Eichberg, H. (2018). Play in Philosophy and Social Thought (S. H. Larsen, Ed.; 1st ed.). Routledge. https://doi.org/10.4324/9780429452109

Electronic Communications Privacy Act of 1986 (ECPA), 18 U.S.C. §§ 2510-2523

Eley, G. (2008). A crooked line: From cultural history to the history of society. Univ. of Michigan Press.

Eller, Riley. (2004). “Black Hat Briefings, Japan 2004 [Audio] Presentations from the Security Conference: Riley ‘Caezar’ Eller: Capture the Flag Games: Measuring Skill with Hacking Contests (English) on Apple Podcasts.” Apple Podcasts. Accessed December 23, 2022. https://podcasts.apple.com/us/podcast/riley-caezar-eller-capture-the-flag-games-measuring/id213956835?i=1000013763357.

Eve, M. P. (2021). Warez: The Infrastructure and Aesthetics of Piracy (1st ed.). punctum books. https://doi.org/10.53288/0339.1.00

Feiertag, R. J., & Neumann, P. G. (1979). The foundations of a provably secure operating system (PSOS). 1979 International Workshop on Managing Requirements Knowledge (MARK), 329–334. https://doi.org/10.1109/MARK.1979.8817256

Fizek, S., & Dippel, A. (2019). Laborious Playgrounds: Citizen science games as new modes of work/play in the digital age. In R. Glas, S. Lammes, M. de Lange, J. Raessens, & I. de Vries (Eds.), The playful citizen: Civic engagement in a mediatized culture (pp. 255–274). Amsterdam University Press.

Gee, J. P. (2003). What video games have to teach us about learning and literacy. Palgrave Macmillan.

Gee, J. P. (2004). Situated Language and Learning. Routledge.

Geertz, C. (1973). The Interpretation of Cultures: Selected Essays. Basic Books.

Girard, C., Ecalle, J., & Magnan, A. (2013). Serious games as new educational tools: How effective are they? A meta-analysis of recent studies: Serious games as educational tools. Journal of Computer Assisted Learning, 29(3), 207–219. https://doi.org/10.1111/j.1365-2729.2012.00489.x

Goerzen, M., & Coleman, G. (2022). The Rise of the Professional Security Hacker. Data & Society, Special Report, 1–126.

Gollman, D. (2007). Security Models. In J. Bergstra & K. de Leeuw (Eds.), The History of Information Security: A Comprehensive Handbook (pp. 623–635). Elsevier.

Gregory. (2021). CDPSE Certified Data Privacy Solutions Engineer All-In-One Exam Guide. McGraw-Hill Education.

Grimes, Sara M., and Andrew Feenberg. 2009. “Rationalizing Play: A Critical Theory of Digital Gaming.” The Information Society 25 (2): 105–18. https://doi.org/10.1080/01972240802701643.

Grimes, S., & Fields, D. A. (2015). Children's Media Making, but Not Sharing: The Potential and Limitations of Child-Specific DIY Media Websites. Media International Australia, 154(1), 112–122. https://doi.org/10.1177/1329878X1515400114

H.R.4718—Computer Fraud and Abuse Act of 1986, H.R.4718, 99th Congress, 2nd Session, 1213 (1986). https://www.govinfo.gov/app/details/STATUTE-100/STATUTE-100-Pg1213/summary

Hapgood, F. (1993). Up the Infinite Corridor. Addison-Wesley Pub. Co.

Holliday, A. (2007). Doing and Writing Qualitative Research. SAGE Publications Ltd. https://doi.org/10.4135/9781446287958

Huang, J., Yan, E., Cheung, G., Nagappan, N., & Zimmermann, T. (2017). Master Maker: Understanding Gaming Skill Through Practise and Habit from Gameplay Behaviour. Topics in Cognitive Science, 9(2), 437–466. https://doi.org/10.1111/tops.12251

Hexadecim8. (2016, August 13). When Will DEFCON Stop Being A Massive Sexist Cringe-Fest? Medium. https://medium.com/@hexadecim8/when-will-defcon-stop-being-a-massive-sexist-cringe-fest-cd9d58ccb549

Hughes, W. J. (1984). Report 98-894 / H.R. 5616: Counterfeit access device and computer fraud abuse act., H.R. 5616, 98th Congress of the United States, 2nd, 98-894 1. https://www.congress.gov/bill/98th-congress/house-bill/5616/all-info

huku, and argp. (2012). "The Art of Exploitation." Phrack Magazine. April 14, 2012. http://phrack.org/issues/68/13.html.

Huizinga, J. (1944). Homo Ludens, Switzerland: Routledge.

Husserl, Edmund. 1983. Ideas: A General Introduction to Pure Phenomenology. Translated by W.R. Boyce Gibson. Boston.

Hutton, E. F. (1983, January 17). Dialing for Data—Illegally. Newsweek, 101(3), 54.

Irani, L. (2015). Hackathons and the making of entrepreneurial citizenship. Science, Technology, & Human Values, 40(5), 799–824.

Jackson, M. (Ed.). (1996). Things as they are: New directions in phenomenological anthropology. Indiana University Press.

Jenkins, H. (2009). Confronting the Challenges of Participatory Culture: Media Education for the 21st Century, MIT Press, Cambridge, MA.

Johns, A. (2009). From Phreaking to Fudding. In Piracy: The intellectual property wars from Gutenberg to Gates (pp. 463–496). University of Chicago Press.

Johnston, J. R. (2009). Technological Turf Wars: A case study of the Computer Antivirus Industry. Temple University Press.

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

Juul, J. (2005). Half-real: Video Games Between Real Rules and Fictional Worlds. MIT Press.

Kafai, Y. B., & Burke, Q. (2015). Constructionist Gaming: Understanding the Benefits of Making Games for Learning. Educational Psychologist, 50(4), 313–334. https://doi.org/10.1080/00461520.2015.1124022

Kafai, Y. B., & Fields, D. A. (2013). Connected play: Tweens in a virtual world. The MIT Press.

Kafai, Y. B., & Resnick, M. (Eds.). (1996). Constructionism in Practise. Routledge.

Kalthoff, H. (2013). Field notes: Ethnographic writing reconsidered. Distinktion: Journal of Social Theory, 14(3), 271–283. https://doi.org/10.1080/1600910X.2013.838976

Kane, Jennifer. (August 27, 2018) 2019 "What Were the Top Drugs Police Seized at Burning Man Last Year?" Reno Gazette Journal. Accessed December 23, 2022. https://www.rgj.com/story/life/arts/burning-man/2018/08/27/burning-man-top-drugs-police-seized-festival-2017/1086004002/.

Kelty, C. (2008). Two Bits: The Cultural Significance of Free Software. Duke University Press.

Kelty, C. M. (2010, December 19). Limn: The Morris Worm. Limn. https://limn.it/articles/the-morris-worm/

Kiernan, C. R. (2017). Agents Of Dreamland. St Martin's Press.

Kim, A. S., & Ko, A. J. (2017). A Pedagogical Analysis of Online Coding Tutorials. Proceedings of the 2017 ACM SIGCSE Technical Symposium on Computer Science Education, 321–326. https://doi.org/10.1145/3017680.3017728

Kirkpatrick, G. (2013). Computer games and the social imaginary. Polity Press.

Knight, P. T. (2002). Small-Scale Research. SAGE Publications Ltd.

Kocurek, Carly A. 2015. Coin-Operated Americans: Rebooting Boyhood at the Video Game Arcade. Minneapolis, MN: University of Minnesota Press.

Kubitschko, S. (2017). "There Simply Is No Unified Hacker Movement." Why We Should Consider the Plurality of Hacker and Maker Cultures. Digital Culture & Society, 3(1), 185–196. https://doi.org/10.14361/dcs-2017-0112

Landwehr, Carl E. 2007. "Revolution through Competition?" IEEE Security & Privacy 5 (6): 3–4. https://doi.org/10.1109/MSP.2007.174.

Lasker, L., Parkes, W. F., Green, W., & Badham, J. (1982). Script: WarGames REVISED FINAL DRAFT [Film Script]. https://secureservercdn.net/198.71.233.96/p2z.144.myftpupload.com/pdf/WarGames.pdf

Levy, S. (2010). Hackers. O'Reilly Media.

Li, Vickie. 2019. "Binary Exploitation: Buffer Overflows." Medium (blog). October 21, 2019. https://vickieli.medium.com/binary-exploitation-buffer-overflows-a9dc63e8b546.

Library of Congress. (1998). The Digital Millennium Copyright Act of 1998: U.S. Copyright Office summary. Washington, D.C.: Copyright Office, Library of Congress.

Lipner, S. B. (2015). The Birth and Death of the Orange Book. IEEE Annals of the History of Computing, 37(2), 19–31. https://doi.org/10.1109/MAHC.2015.27

Marbach, W. D., Resener, M., Carey, J., Sandza, R., Rogers, M., Conant, J., & Agrest, S. (1983, May 9). Beware: Hackers at Play. Newsweek, 102(10), 42–48.

Markku, R., Wasiak, P., & Botz, D. (2015). Crack Intros: Piracy, Creativity and Communication. International Journal of Communication, 9, 798–817.

Markoff, J. (1988, November 9). The Computer Jam: How It Came About. New York Times, D10.

Mascot History. (n.d.). Division of Student Life - MIT. Retrieved December 7, 2021, from https://studentlife.mit.edu/cac/event-services-spaces/adventures-tim-beaver/mascot-history

Mason, W., & Clauset, A. (2013). Friends FTW! Friendship, Collaboration and Competition in Halo: Reach. Proceedings of the 2013 Conference on Computer Supported Cooperative Work - CSCW '13, 375. https://doi.org/10.1145/2441776.2441820

Menn, J. (2019). Cult of the Dead Cow: How the original hacking supergroup might just save the world. Public Affairs.

Meyer, G. (1989). The Social organization of the computer underground [Master's Thesis, Northern Illinois University]. https://apps.dtic.mil/sti/pdfs/ADA390834.pdf

Middleton, B. (2017). A History of Cyber Security Attacks: 1980 to Present. Auerbach Publications.

Mihalik, A. D. (1999, May 11). School Mascots: A beaver, a seal, and an engineer. The Tech, 6, from http://tech.mit.edu/V119/PDF/V119-N26.pdf

Mueller, G. (2016). Piracy as Labour Struggle. TripleC: Communication, Capitalism & Critique, 14(1), 333–345.

National Bureau of Standards. (1980). Federal Information Processing Standards Publication: Guidelines for security of computer applications (NBS FIPS 73). National Bureau of Standards. https://doi.org/10.6028/NBS.FIPS.73

Nguyen, C. T. (2019). The right way to play a game. Game Studies, 19(1). http://gamestudies.org/1901/articles/nguyen

Oberhaus, D. (2019, May 14). Who Killed the American Demoscene? Vice. https://www.vice.com/en/article/j5wgp7/who-killed-the-american-demoscene-synchrony-demoparty

Owens, K., Fulton, A., Jones, L., & Carlisle, M. (n.d.). pico-Boo!: How to avoid scaring students away in a CTF competition. p.1-6.

Page, B. (1988, November 7). A Report on the Internet Worm. Ryerson University, Electrical Engineering Department. https://www.ee.ryerson.ca/~elf/hack/iworm.html

Papert, S. (1986). Constructionism: A New Opportunity for Elementary Science Education. The National Science Foundation.

Parker, D. B. (1976). Computer abuse perpetrators and vulnerabilities of computer systems. Proceedings of the June 7-10, 1976, National Computer Conference and Exposition on - AFIPS '76, 65. https://doi.org/10.1145/1499799.1499810

Parker, D. B. (2002). Toward a New Framework for Information Security. In S. Bosworth & M. E. Kabay (Eds.), Computer security handbook 4 (4th ed, p. 5.1-5.19). John Wiley & Sons.

Pauly, D., & Greenberg, P. (1976, August 9). The Computer Bandits. Newsweek, 88(6), 58 & 61.

Peterson, T. F. (2011). Nightwork: A history of hacks and pranks at MIT. MIT Press.

Piaget, J. (1951). Play, dreams and imitation in childhood. https://www.taylorfrancis.com/books/e/9781136318030

Piaget, J. (1971). The theory of stages in cognitive development. In D. R. Green, M. P. Ford, & G. B. Flamer, *Measurement and Piaget.* McGraw-Hill.

Pöial, J. (2021). Challenges of Teaching Programming in StackOverflow Era. In Educating Engineers for Future Industrial Revolutions (pp. 703–710). Springer International Publishing. https://doi.org/10.1007/978-3-030-68198-2_65

RampantKitten: An Iranian Surveillance Operation unraveled. (2020, September 18). Check Point Software. https://blog.checkpoint.com/2020/09/18/rampantkitten-an-iranian-surveillance-operation-unraveled/

Reed, S. K. (1977). Automatic data processing risk assessment (NBS IR 77-1228; 0 ed., p. NBS IR 77-1228). National Bureau of Standards. https://doi.org/10.6028/NBS.IR.77-1228

Romero, M., Usart, M., & Ott, M. (2015). Can Serious Games Contribute to Developing and Sustaining 21st Century Skills? Games and Culture, 10(2), 148–177. https://doi.org/10.1177/1555412014548919

Rowlinson, M. (2005). Historical Research Methods. In E. F. Holton & R. A. Swanson (Eds.), Research in organizations: Foundations and methods of inquiry (pp. 294–312).

Ruthberg, Z. G. (1978). Audit and evaluation of computer security II (p. 220) [Conference Proceedings]. National Institute of Standards.

Saari, A. I., Renz, G., Davis, P., & Abel, M. G. (2020). The Influence of Age on Firefighter Combat Challenge Performance and Exercise Training Habits. Journal of Strength and Conditioning Research, 34(9), 2500–2506. https://doi.org/10.1519/JSC.0000000000003714

Saldaña, J. (2013). The coding manual for qualitative researchers (2nd ed). SAGE.

Samson, P. R. (1960). An Abridged Dictionary of the TMRC Language. http://www.gricer.com/tmrc/dictionary1960.html

Schrøder, K., Drotner, K., Kline, S., & Murray, C. (Eds.). (2003). Researching Audiences. Arnold.

Scully-Blaker, R. (2014). A Practised Practise: Speedrunning Through Space With de Certeau and Virilio. Game Studies, 14(1). http://gamestudies.org/1401/articles/scullyblaker

Security Contest Winter 2013-2014 FAQ. (2014, March 4). Telegram. https://core.telegram.org/contestfaq

Shade, Leslie Regan, and Jenna Jacobson. 2015. “Hungry for the Job: Gender, Unpaid Internships, and the Creative Industries.” The Sociological Review 63 (1_suppl): 188–205. https://doi.org/10.1111/1467-954X.12249.

Slayton, R. (2016). Framing Computer Security and Privacy, 1967-1992. In T. Misa (Ed.), Communities of Computing: Computer Science and Society in the ACM (pp. 283–323). ACM Press.

Slayton, Rebecca. 2017. “Limn: The Paradoxical Authority of the Certified Ethical Hacker.” Limn. February 14, 2017. https://limn.it/articles/the-paradoxical-authority-of-the-certified-ethical-hacker/.

Spafford, E. H. (1992). Are Computer Hacker Break-ins Ethical? Journal of Systems Software, 17, 41–47.

Statler, M., Heracleous, L., & Jacobs, C. D. (2011). Serious Play as a Practise of Paradox. The Journal of Applied Behavioural Science, 47(2), 236–256. https://doi.org/10.1177/0021886311398453

Steier, R. (1990). News track. Communications of the ACM, 33(5), 477–478. https://doi.org/10.1145/78607.316056

Steinkuehler, C., & Duncan, S. (2008). Scientific Habits of Mind in Virtual Worlds. Journal of Science Education and Technology, 17(6), 530–543. https://doi.org/10.1007/s10956-008-9120-8

Steinmetz, K. F. (2015). Craft(y)ness: An Ethnographic Study of Hacking. British Journal of Criminology, 55(1), 125–145. https://doi.org/10.1093/bjc/azu061

Sterling, B. (1993). The Hacker Crackdown: Law and disorder on the electronic frontier. Bantam.

Stoll, C. (1989). The Cuckoo’s Egg. Doubleday.

Strouse, J. (1982, June 14). Cash in the Chips. Newsweek, 99(24), 94a–94b.

Sundaram, Ravi. 2009. *Pirate Modernity : Delhi’s Media Urbanism*. London, UK: Routledge.

Tanczer, L. M. (2020). 50 shades of hacking: How IT and cybersecurity industry actors perceive good, bad, and former hackers. Contemporary Security Policy, 41(1), 108–128. https://doi.org/10.1080/13523260.2019.1669336

The NASA Heritage of Creativity: 2003 Annual Report of the NASA Inventions & Contributions Board (p. 1-18). (2003). NASA. https://www.nasa.gov/pdf/251093main_The_NASA_Heritage_Of_Creativity.pdf

Turkle, S. (1984). The Second Self: Computers and the Human Spirit (Twentieth Anniversary Edition). MIT Press.

Turner, F. (2006). From Counterculture to Cyberculture: Stewart Brand, the Whole Earth Network, and the Rise of Digital Utopianism. University of Chicago Press.

Turner, F. (2009). Burning Man at Google: A cultural infrastructure for new media production. 11(1 & 2), 73–94.

Van Maanen, J. (2011). Ethnography as Work: Some Rules of Engagement: Ethnography as Work. Journal of Management Studies, 48(1), 218–234. https://doi.org/10.1111/j.1467-6486.2010.00980.x

Votipka, D., Zhang, E., & Mazurek, M. L. (2021). HackEd: A Pedagogical Analysis of Online Vulnerability Discovery Exercises. 2021 IEEE Symposium on Security and Privacy (SP), 1268–1285. https://doi.org/10.1109/SP40001.2021.00092

Vu, W. (2019, January 2). The Ghost of Exploits Past: A Deep Dive into the Morris Worm | Rapid7 Blog. Rapid7. https://www.rapid7.com/blog/post/2019/01/02/the-ghost-of-exploits-past-a-deep-dive-into-the-morris-worm/

Wagner, M. G. (2006). On the Scientific Relevance of eSports. Proceedings of the 2006 International Conference on Internet Computing & Conference on Computer Games Development, ICOMP, 1–5.

Walford, G. (2009). The practise of writing ethnographic fieldnotes. Ethnography and Education, 4(2), 117–130. https://doi.org/10.1080/17457820902972713

Walter, Bo Kampmann. 2003. “Game Studies - Playing and Gaming: Reflections and Classifications.” Game Studies 3 (1). http://www.gamestudies.org/0301/walther/.

Wasiak, P. (2012). ‘Illegal Guys’ A History of Digital Subcultures in Europe during the 1980s. Studies in Contemporary History, 9, 257–276.

Weizenbaum, J. (1976). Computer power and human reason: From judgment to calculation. Freeman.

Williams, J. (2016, December 28). Our Fight to Rein In the CFAA: 2016 in Review. Electronic Frontier Foundation. https://www.eff.org/deeplinks/2016/12/our-fight-rein-cfaa-2016-review

Winter Contest Ends. (2014, March 4). Telegram. https://telegram.org/blog/winter-contest-ends

Wood. (2001). Can Software Support Children’s Vocabulary Development? Language Learning & Technology, 5(1), 166–166.

Woolf, N. H., & Silver, C. (2017). Qualitative Analysis Using NVivo: The Five-Level QDA® Method (1st ed.). Routledge. https://doi.org/10.4324/9781315181660

Wouters, P., van Nimwegen, C., van Oostendorp, H., & van der Spek, E. D. (2013). A meta-analysis of the cognitive and motivational effects of serious games. Journal of Educational Psychology, 105(2), 249–265. https://doi.org/10.1037/a0031311

Wright, S. H. (1998, March 18). Building 20’s last engineering project: A time capsule. MIT News | Massachusetts Institute of Technology. https://news.mit.edu/1998/capsule-0318

Wynn, D., & Williams, C. K. (2012). Principles for Conducting Critical Realist Case Study Research in Information Systems. MIS Quarterly, 36(3), 787–810.

Xie, Tianyi, Yuanyuan Zhang, Juanru Li, Hui Liu, and Dawu Gu. 2016. “New Exploit Methods against Ptmalloc of GLIBC.” In 2016 IEEE Trustcom/BigDataSE/ISPA, 646–53. Tianjin, China: IEEE. https://doi.org/10.1109/TrustCom.2016.0121.

Young, M. F., Slota, S., Cutter, A. B., Jalette, G., Mullin, G., Lai, B., Simeoni, Z., Tran, M., & Yukhymenko, M. (2012). Our Princess Is in Another Castle: A Review of Trends in Serious Gaming for Education. Review of Educational Research, 82(1), 61–89. https://doi.org/10.3102/0034654312436980

“OWASP Risk Rating Methodology | OWASP Foundation.” n.d. Accessed December 23, 2022. https://owasp.org/www-community/OWASP_Risk_Rating_Methodology.

Appendices

Appendix A: Teams, Organizers and Players

CTF: The Danger Days CTF (DDCTF)
Event: Danger Days
Style: Attack & Defend
Organizers:
Mikhail
Dylan
Fraser
Elliot
Pawel

Players Team: Team Alpha
Claudio
Hollis
Daniel
Qais
Hyun
Xingzhe
Dave
Tony
Leon
Franco
Mallory
Tim
Ochre
Claude
Dana
Tara

CTF: The Boss Battle CTF
Event: WorkSec
Organizers:
Vince
Marty
Carl
Vish

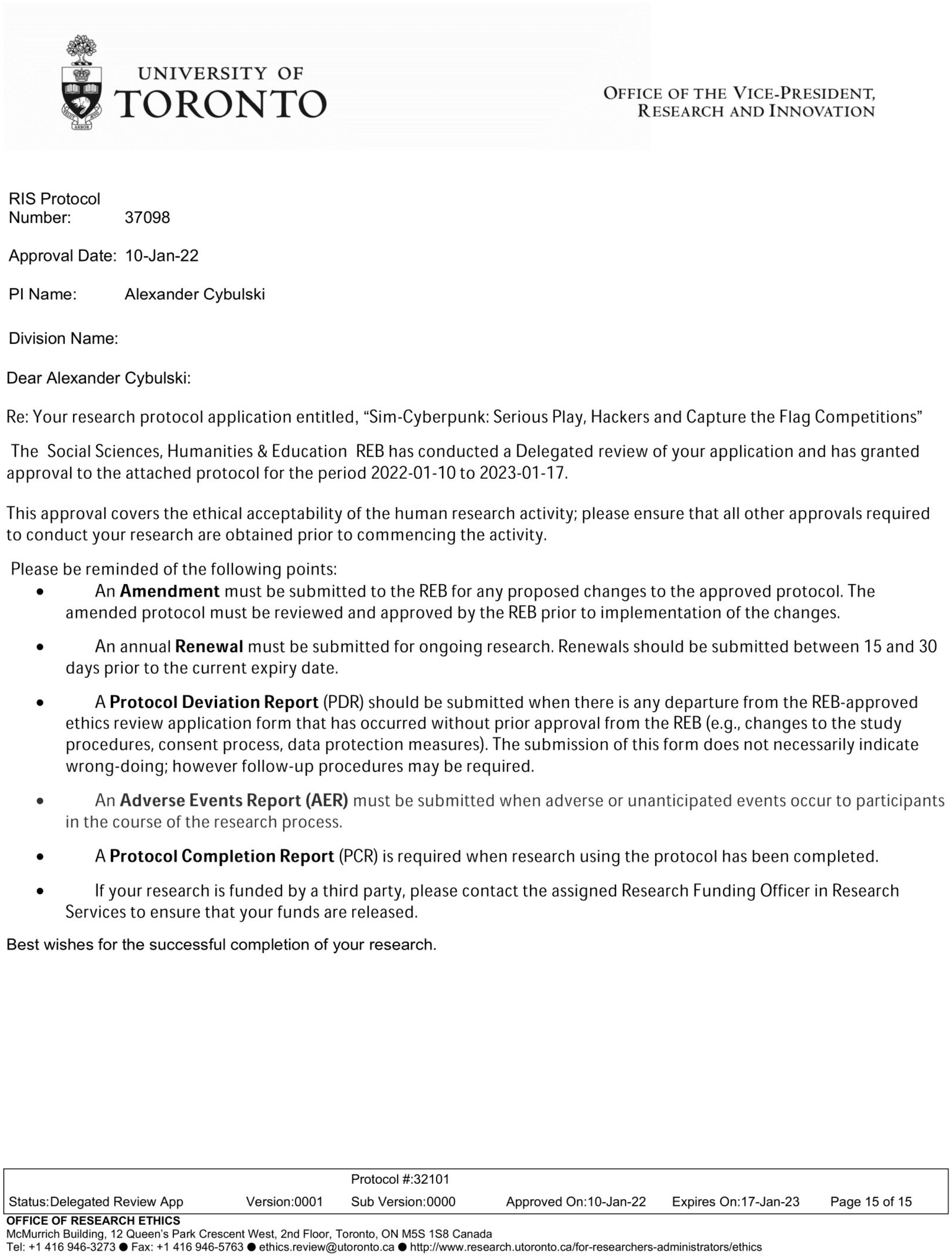
Player Team: The Bitflippers
Members:
Flynn
Wilf
Alice
Terry

CTF: The Crawler CTF (CRCTF)
Event: WebSec
Organizers:
Guy
Jean
Fred
Max

Player Team: The Moths
Morgan
Jonah
Walt
Brian
Kennedy

Unaffiliated Organizers & Designers:
Pearson
Conroy
Bruce
Green
Dorsett
Kurt

Appendix B: Office of Research Ethics – Approval Form



UNIVERSITY OF TORONTO

OFFICE OF THE VICE-PRESIDENT,
RESEARCH AND INNOVATION

RIS Protocol Number:	37098
Approval Date:	10-Jan-22
PI Name:	Alexander Cybulski
Division Name:	

Dear Alexander Cybulski:

Re: Your research protocol application entitled, “Sim-Cyberpunk: Serious Play, Hackers and Capture the Flag Competitions”

The Social Sciences, Humanities & Education REB has conducted a Delegated review of your application and has granted approval to the attached protocol for the period 2022-01-10 to 2023-01-17.

This approval covers the ethical acceptability of the human research activity; please ensure that all other approvals required to conduct your research are obtained prior to commencing the activity.

Please be reminded of the following points:

- An **Amendment** must be submitted to the REB for any proposed changes to the approved protocol. The amended protocol must be reviewed and approved by the REB prior to implementation of the changes.
- An annual **Renewal** must be submitted for ongoing research. Renewals should be submitted between 15 and 30 days prior to the current expiry date.
- A **Protocol Deviation Report** (PDR) should be submitted when there is any departure from the REB-approved ethics review application form that has occurred without prior approval from the REB (e.g., changes to the study procedures, consent process, data protection measures). The submission of this form does not necessarily indicate wrong-doing; however follow-up procedures may be required.
- An **Adverse Events Report (AER)** must be submitted when adverse or unanticipated events occur to participants in the course of the research process.
- A **Protocol Completion Report** (PCR) is required when research using the protocol has been completed.
- If your research is funded by a third party, please contact the assigned Research Funding Officer in Research Services to ensure that your funds are released.

Best wishes for the successful completion of your research.

Protocol #:32101
Status:Delegated Review App Version:0001 Sub Version:0000 Approved On:10-Jan-22 Expires On:17-Jan-23 Page 15 of 15
OFFICE OF RESEARCH ETHICS
McMurrich Building, 12 Queen's Park Crescent West, 2nd Floor, Toronto, ON M5S 1S8 Canada
Tel: +1 416 946-3273 ● Fax: +1 416 946-5763 ● ethics.review@utoronto.ca ● http://www.research.utoronto.ca/for-researchers-administrators/ethics

Copyright Acknowledgements