Technoethics and Sensemaking: Risk Assessment and Knowledge Management of Ethical Hacking in a Sociotechnical Society

by

Baha Abu-Shaqra

A thesis submitted

in partial fulfillment of the requirements for the

degree of Doctor of Philosophy in Electronic Business

Faculty of Engineering

University of Ottawa

Abstract

Cyber attacks by domestic and foreign threat actors are increasing in frequency and sophistication. Cyber adversaries exploit a cybersecurity skill/knowledge gap and an open society, undermining the information security/privacy of citizens and businesses and eroding trust in governments, thus threatening social and political stability. The use of open digital hacking technologies in ethical hacking in higher education and within broader society raises ethical, technical, social, and political challenges for liberal democracies. Programs teaching ethical hacking in higher education are steadily growing but there is a concern that teaching students hacking skills increases crime risk to society by drawing students toward criminal acts. A cybersecurity skill gap undermines the security/viability of business and government institutions. The thesis presents an examination of opportunities and risks involved in using AI powered intelligence gathering/surveillance technologies in ethical hacking teaching practices in Canada. Taking a qualitative exploratory case study approach, technoethical inquiry theory (Bunge-Luppicini) and Weick's sensemaking model were applied as a sociotechnical theory (STEI-KW) to explore ethical hacking teaching practices in two Canadian universities. In-depth interviews with ethical hacking university experts, industry practitioners, and policy experts, and a document review were conducted. Findings pointed to a skill/knowledge gap in ethical hacking literature regarding the meanings, ethics, values, skills/knowledge, roles and responsibilities, and practices of ethical hacking and ethical hackers which underlies an identity and legitimacy crisis for professional ethical hacking practitioners; and a Teaching vs Practice cybersecurity skill gap in ethical hacking curricula. Two main S&T innovation risk mitigation initiatives were explored: An OSINT Analyst cybersecurity role and associated body of knowledge foundation framework as an interdisciplinary research area, and a networked centre of excellence of ethical hacking

communities of practice as a knowledge management and governance/policy innovation approach focusing on the systematization and standardization of an ethical hacking body of knowledge.

Dedication

to mom and dad.

Acknowledgements

If I have succeeded it is by standing on the shoulders of giants. A lot of work goes into a PhD thesis. A collective thanks to all those who contributed to the success of the thesis, and my apologies to those I cannot identify because of a confidentiality clause.

It is impossible for me to express in words my gratitude to my PhD thesis supervisor, and before that my MA thesis supervisor, Professor Rocci Luppicini. I consider myself very lucky for the tremendous privilege and honour of learning from him and following in his footsteps in the field of Technoethics and the pioneering work of Mario Bunge especially with regard to technology assessment and grounding of technology in historical and theoretical context. Professor Luppicini's constructivist approach to supervision and teaching saw him giving me wings and letting me fly. For example, the idea of "the intertwinement of technology and society in complex sociotechnical systems" and that "we do sociology" were explicitly from him. On a professional practice level, Professor Luppicini taught me the way to deal with your doubters is to try to win them over to your side.

Thank you also to my distinguished thesis advisory committee members for their priceless guidance and contribution to the intellectual development of the thesis over the past four years. Special thanks to Professor Liam Peyton, my supervisor for "area two" of the interdisciplinary PhD in E-Business program. Your support made all the difference. I am infinitely grateful. Coming from the humanities and arts into an engineering discipline, I felt like a fish out of the water. Professor Peyton challenged me to step out of my comfort zone and plunge into technical scholarship on computer and network hacking. The idea of studying ethical hacking as penetration testing and the idea of interviewing "those who teach and those who practice" ethical hacking were from him.

A special thanks also goes to Professor André Vellino, my third distinguished TAC member, whose intellectual contribution, while perhaps a bit more subtle, has undeniably advanced my research. His comments helped me connect the dots. For example, his references to "falsifiability," "viability," and SoK pointed me straight to the scientific method and its centrality for my thesis, as a key component of a social science approach to studying technology in society. Thank you so much.

I also wish to extend a profound gratitude to the thesis examiners Professor Anabel Quan-Haase and Professor Hussein Al Osman for their very helpful feedback. Professor Quan-Haase's many contributions to the intellectual development of the thesis included her pioneering STS textbook "Technology and society" (2016) which made it possible for me to piece it all together--how my work (Bunge's conception of technology as social technology/sociotechnology and social systems as sociotechnical systems) fits into the tradition of STS and SCOT. Her detailed discussion of the thesis's contribution to the advancement of knowledge helped me appreciate the important implications of the thesis regarding theory, methods, and practice across disciplines. The most central contribution to the extant literature on hacking is that the thesis sheds light on ethical hacking meanings, theories, and social relevance, she said. My gratitude and admiration for her and her scholarship are off the charts.

Professor Al Osman helped me strengthen my empirical case study analysis by pointing me to data sources that would help me better understand ethical hacking teaching practices in higher education, especially, he said I should look into the program requirements and course descriptions of software engineering for a more holistic analysis. Further, his question during the oral defence "Who should teach ethical hacking?" set me off in the right direction to plan for future career opportunities. Thank you so much.

The author would like to thank the interview participants of this study for their generous time and expert contribution. Their participation was essential, and I am extremely grateful for their generosity in sharing their time and insights into ethical hacking teaching practices and effective governance in society. Finally, I would like to express my deepest appreciation to my loving family for believing in me and supporting me. Your help was indispensable. To my parents, brothers and sisters: Thank you from the bottom of my heart.

Table of Contents

List of Figures

List of Tables

Acronyms and Abbreviations

BoK: Body of Knowledge

EDP: Ethical Design Principles (e.g., EDP-STEI-KW)

CE: Computer Engineering

CS: Computer Science

CSE: Communications Security Establishment

NCE: Networks of Centres of Excellence

S&S: Science and Technology

SCOT: Social Construction of Technology

SE: Software Engineering

SSP-DMG: Science, Society and Policy Decision-Making Grid

ST: Sociotechnical

STEI-KW: Open, Scientific, Knowledge-Making Sociotechnical Society; Technology

STS: Science and Technology Studies

TEI: Technoethical Inquiry Theory

Chapter 1: Introduction

Hundreds of data breaches happen every year in higher education despite regulatory requirements to protect students' data, says the U.S. Department of Education (n.d.). For example, FERPA (Family Educational Rights and Privacy Act) requires an "educational agency or institution" to use "reasonable methods" to ensure that "school officials obtain access to only those education records in which they have legitimate educational interests" and that an "educational agency or institution that does not use physical or technological access controls must ensure that its administrative policy for controlling access to education records is effective" (34 CFR § 99.31). The disclosure of student information potentially violates FERPA and can expose students to "a host of negative consequences such as identity theft, fraud, and extortion" (U.S. Department of Education, n.d.). A government funded analysis of cyber-attacks against universities and colleges in the UK suggests staff or students are the more likely culprits of committing hacking crimes than is organized crime (Coughlan, 2018). The analysis focused on the timing of 850 attacks on the British academic network in 2017-2018. It concluded there are "suspicions that staff or students could be in the frame" (Coughlan, 2018), a finding that mirrors broader social trends of hacking crime being predominately an insider's attack. A "clear pattern" of attacks concentrated during term times and during the working day point to students or staff as the more likely perpetrators of hacking crime (Coughlan, 2018).

Cyber attacks on information assets in the private and public sectors is a growing and evolving threat, warns Public Safety Canada (2013A, 2013B, 2013C). The evolution of cyber-attack tools and techniques has accelerated dangerously in the recent past (PSC, 2013A, The Threat, para. 1). The frequency of hacking attacks increases year after year. And every year

"those seeking to infiltrate, exploit or attack our cyber systems are more sophisticated and better resourced than the year before" (PSC, 2013A, Introduction, para. 5).

> Cyber attacks include the unintentional or unauthorized access, use, manipulation, interruption or destruction (via electronic means) of electronic information and/or the electronic and physical infrastructure used to process, communicate and/or store that information. The severity of the cyber attack determines the appropriate level of response and/or mitigation measures: i.e., cyber security. (PSA, 2013A)

The increasing reliance on cyber technologies makes Canadians "more vulnerable to those who attack our digital infrastructure to undermine our national security, economic prosperity, and way of life" (Public Safety Canada, 2013A). Cyber warfare involves "actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption" (Clarke, Richard A., 2010). Cyber warfare acts against government or business interests can take the form of espionage or propaganda, or they can involve sabotage (e.g., Stuxnet), malware attacks on financial institutions (e.g., WannaCry and Petya), DDoS attacks, or attacks on power grids and critical infrastructure such as national defence facilities and hospitals.

Cybercrime costs worldwide are projected to grow from US$3 trillion in 2015 to US$6 trillion by 2021. Global spending on cybersecurity products and services for defending against cybercrime is expected to exceed US$1 trillion between 2017 and 2021 (Morgan, 2018).

> Cybercrime, also called computer crime, the use of a computer as an instrument to further illegal ends, such as committing fraud, trafficking in child pornography and intellectual property, stealing identities, or violating privacy. Cybercrime, especially through the

> Internet, has grown in importance as the computer has become central to commerce, entertainment, and government. (Britannica Online Encyclopedia, 2013)

Luppicini (2014) finds a myriad of cybercrime varieties exists and continues to arise, and highlights three areas of cybercrime threat to society: 1) Cyber theft and cyber fraud, including identity theft, information theft, intellectual property theft, and identity fraud; 2) cyber terrorism (e.g., Eid, 2010; Minei & Matusitz, 2011; Rid, 2012) and cyber espionage (e.g., Lin & Luppicini, 2011); and 3) cyberbullying (e.g., Thompson & Cupples, 2008). U.S. losses to ransomware have jumped from US$25 million in 2014 to over US$8 billion in 2018 with no signs of slowing down. Intellectual property theft in the US costs taxpayers around US$11 billion annually (CSIS & McAfee, 2018).

The cybersecurity risk continues to rise as businesses increase their dependence on IT, IoT devices, and mobile and wireless technology, making information security the most pressing IT concern for organizations today. Cybersecurity will be the main focus of this decade, says Germany's defense minister. Cyber attacks are the greatest challenge threatening global stability, Ursula von der Leyen told CNBC (Paganini, 2018). Network and data breaches "are happening so often it's now a question of 'when,' not 'if,' a business organization will face a security incident. At the same time, the United States is facing an acute shortage of cybersecurity experts" (Cyber Fasttrack, 2019). Information security can be understood as a process of applying security controls to protect the confidentiality, integrity, and availability (CIA) of information assets within information systems (Dhillon, 2007; Engebretson, 2011; Reynolds, 2012; Stamp, 2011; Sterling, 1993). For this thesis, cybersecurity is information security concerned with protecting the CIA of privileged information within "Cyberspace" (see Figure 1: The 15 Layer Cyber Terrain Model).

1.1. Cybersecurity Threats

The Communications Security Establishment (CSE) keeps a close watch on the cybersecurity threat environment facing Canadian individuals, businesses, and broader society. The CSE (2018) identifies two key cybersecurity threat areas to broader society: "Increasing Cyber Threat Exposure" due to the expanding interconnectedness of ICTs and their digital integration with industrial control systems, making an attack on critical infrastructure more likely/risky, and "Public Institutions and Sensitive Information" (the targeting of sensitive information and essential services institutions--governments, higher education, hospitals, etc. by malicious hackers). The CSE (2018) identifies "Data Breaches," including commercial espionage and social engineering, and "Exploiting Trusted Relationships" as two key cybersecurity threat areas to businesses. Finally, the CSE (2018) identifies "Cybercrime" and "Malicious Online Influence Activity" as two key cybersecurity threat areas to individuals.

Key findings of the CSE's National Cyber Threat Assessment 2018 are 1) society is facing an "Increasing Cyber Threat Exposure." "Canadians' exposure to cyber threats increases with the growing number of Internet-connected devices" (CSE, 2018, p. 11); 2) cybercrime is the cyber threat that Canadians and Canadian businesses are most likely to encounter in 2019; and 3) cyber threat consequences at the broad social level can be "severe and wide-reaching" with the potential to compromise public safety and national security, for example, by targeting Canadian critical infrastructure At the businesses level, cyber attacks can result in reputational damage, productivity loss, intellectual property theft, large-scale theft of personal information, operational disruptions (e.g., to the financial sector), and recovery expenses. And at the individual level, consequences of a cyber attack can span financial or privacy damage. Table 1: Cybersecurity

Threats Facing Individuals, Businesses, and Society summarizes the cyber threat environment in terms of Cybercrime, Political interference, and Cyber surveillance (hereafter surveillance).

Discussion of the cybersecurity threat in this thesis focuses on 1) the increasing cyber threat exposure as a broad societal threat, 2) cybercrime as the cyber threat that Canadians and Canadian businesses most likely to encounter in 2019, and 3) surveillance as a growing cyber threat to the privacy of individuals (to their information security and their political autonomy).

Table 1: Cybersecurity Threats Facing Individuals, Businesses, and Society (CSE, 2018)

Threat/Motivation	Social	Business	Individual
Cybercrime	1) Increasing Cyber Threat Exposure: "Canadians' exposure to cyber threats increases with the growing number of Internet-connected devices" (CSE, 2018 p. 11). "As the number and variety of devices used to support, monitor, and control critical infrastructure become more interconnected, the likelihood of cyber threat actors disrupting critical infrastructure has increased" (CSE, 2018, p. 23). 2) Public Institutions and Sensitive Information: Cyber threat activity "against public institutions—such as government departments, universities, and hospitals—is likely to persist because of the	Data Breaches (CSE, 2018): Data breaches Commercial espionage/commercial data theft Whaling/social engineering "Canadian businesses, especially those active in strategic sectors of the economy, are subject to cyber espionage aimed at stealing intellectual property and other commercially sensitive information." This cyber threat activity "can harm Canada's competitive business advantage and undermine our strategic position in global markets" (CSE, 2018, p. 19). "Foreign and domestic adversaries target higher education institutions that have military and government contracts" (McNamara March 15, 2019). The top higher education information security risks in Canada and the U.S. that are a priority for IT in 2016 (Grama & Vogel, 2017): (1) phishing and social engineering; (2) end-user awareness, training, and education;	Cybercrime: Information theft Theft of personal and financial information is lucrative for cybercriminals and is very likely to increase (CSE, 2018). Cybercriminals profit at the expense of Canadians by obtaining account login credentials, credit card details, and other personal information. They exploit this information to directly steal money, to resell information on cybercrime marketplaces, to commit fraud, or for extortion. (CSE, 2018, p. 11)

	essential nature of the services and the sensitivity of the information they manage" (CSE, 2018, p. 26).	(3) limited resources for the information security program (i.e., too much work and not enough time or people); and (4) addressing regulatory requirements.	
Political interference Cyber warfare Cyberterrorism	State propaganda Trolling Mis/dis-information (e.g., Russian interference in the US general election in 2016) DDoS/CIA attacks on critical infrastructure such as the power grid, defence facilities, and health services.	Cyber warfare can involve sabotage (e.g., Stuxnet); Malware attacks on financial institutions (e.g., WannaCry and Petya ransomware) attributed to North Korea.	Malicious Online Influence Activity Cyber threat actors can amplify or suppress social media content using botnets, which automate online interactions and share content with unsuspecting users (CSE, 2018). By spreading their preferred content among large numbers of paid and legitimate users, cyber threat actors can promote their specific point of view and potentially influence Canadians. (CSE, 2018, p. 15)
Cyber surveillance (Surveillance)	Opportunities: State surveillance (domestic surveillance) State intelligence (foreign surveillance) Threats: Espionage Terrorism Democracy (political autonomy)	Opportunities: Domestic: Innovation vs Privacy Foreign: International trade/business in BI Threats: Domestic: Innovation vs Privacy (duet of century) Foreign: Espionage Information theft/crime Sabotage Cyber campaigns launched by hackers from one country targeting firms of another country resulting in the theft of business information "such as bid prices, contracts and information related to mergers and acquisitions" (Onag, 2018).	Opportunities: Countersurveillance (securing personal privacy and autonomy) Threats: Domestic: Spying Foreign: International political economy, e.g., Facebook's Cambridge-Analytica data scandal

1.1.1. Increasing cyber threat exposure.

The increasing interconnectedness of society raises security risks to critical infrastructure and industrial control (IC) systems. Public institutions are likely to face an increasing risk of exposure to crime or state-sponsored or business espionage operations because of the essential nature of the services and the sensitivity of the information they manage. The exposure of Canadians to cyber threats "increases with the growing number of Internet-connected devices, such as televisions, home appliances, thermostats, and cars. Manufacturers have rushed to connect more types of devices to the Internet, often prioritizing ease of use over security" (CSE, 2018, p. 11). "As the number and variety of devices used to support, monitor, and control critical infrastructure become more interconnected, the likelihood of cyber threat actors disrupting critical infrastructure has increased" (p. 23). WannaCry is a good example of how malware can pose serious risk to critical infrastructure. The CSE and partner agencies attributed the WannaCry ransomware to North Korean cyber threat actors (CSE, 2018). In May 2017, WannaCry hit hard infecting more than 200,000 vulnerable computers in at least 100 countries. Notably, the ransomware spread to 25 facilities in a national health organization that provides emergency services. The incident forced the cancellation of over 19,000 appointments, including surgeries (CSE, 2018, p. 17).

Cybersecurity risk for public institutions, such as government departments, universities, and hospitals--is likely to persist "because of the essential nature of the services and the sensitivity of the information they manage." Public institutions are also "attractive to cyber threat actors because of their close connections with businesses and Canadians. Public institutions hold valuable intellectual property, sometimes belonging to partner organizations such as research centres or private firms" (CSE, 2018, p. 26).

1.1.2. Cybercrime at the business level.

Cybercrime, especially data breaches, will be the top threat facing businesses of all sizes in 2019. Key sources of security threat for businesses are whaling, large databases, and commercial espionage. Cyber threat actors are increasingly using the whaling social engineering technique against businesses. This term refers to spear-phishing aimed specifically at senior executives or other high-profile recipients with privileged access to company resources. Whaling occurs when an executive with authority to issue large payments receives a message appearing to come from a relevant department or employee, urging them to direct funds to an account controlled by a cyber threat actor. This type of social engineering can lead to major financial losses and reputational damage. Like other social engineering techniques, whaling is designed to exploit predictable human behaviour (CSE, 2018, p. 17). Large databases containing personal information such as names, addresses, phone numbers, financial details, and employment information are valuable to cyber threat actors. In 2019 large databases "will almost certainly remain attractive targets for cyber threat actors seeking to sell information or support state-sponsored espionage. "Cyber threat actors target Canadian businesses for their data about customers, partners and suppliers, financial information and payment systems, and proprietary information. Stolen information is held for ransom, sold, or used to gain a competitive advantage. Canadian businesses, especially those active in strategic sectors of the economy, are subject to cyber espionage "aimed at stealing intellectual property and other commercially sensitive information" Cyber threat actors "target commercial information so they can copy existing products, undercut competition, or gain an advantage in business negotiations" (CSE, 2018 p. 18). "We have observed some adversarial nation-states advance their defence and

technology sectors by conducting cyber commercial espionage around the world, including in Canada" (p. 19).

1.1.3. Cybercrime at the individual level.

Cybercriminals continue "to adapt and improve their cyber capabilities to steal, commit fraud, or extort money from Canadians" CSE, 2018, p. 11). Over two-thirds of Canadian adults were subject to cybercrime in 2012 (PSC, 2013B). Identity theft is an increasingly common cyber threat targeting personal and private information, including intellectual property theft, whereby a malicious actor impersonates someone else to take advantage of their access privileges to vital information. Identity theft costs Canadians nearly $1.9 billion each year (PSC, 2013A). Stealing personal and financial information is lucrative for cybercriminals and is very likely to increase. Cybercriminals profit at the expense of Canadians by obtaining account login credentials, credit card details, and other personal information. They exploit this information to directly steal money, to resell information on cybercrime marketplaces, to commit fraud, or for extortion (CSE, 2018, p. 11).

1.1.4. Surveillance: Invading privacy.

Cybercrime and cyber surveillance are both threats to the privacy of citizens (an infringement on their privacy rights). In cybercrime, a privacy attack is an information security "confidentiality" attack--that is, surveillance is a threat to the confidentiality of user data, such as PII, access credentials, sensitive documents, personal letters, etc. This is a technical definition of privacy. In state and business surveillance operations, a privacy attack is an attack on the liberty/autonomy of citizens--that is, surveillance is a threat to the social sensibility of one's right

to a reasonable expectation of privacy. Citizens have a “reasonable expectation of privacy” when they share information online. Canadian privacy law has long been reliant on the principle of “reasonable expectation of privacy.” Similarly, in the U.S. citizens have an “expectation of privacy.” More broadly and internationally, people have “a right to privacy.” This is a social definition of privacy. The United Nations General Assembly recognized the right to personal privacy as a universal human right in The Universal Declaration of Human Rights manifesto on December 10th, 1948. Article 12 says, “No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.”

1.1.4.1. State surveillance.

Nation states run external and internal (foreign and domestic) security intelligence operations to support national security and political stability. The two operational domains of state surveillance are foreign surveillance and domestic surveillance.

Foreign surveillance.

There are three key security and intelligence agencies in Canada: CSIS, CSE, and CFINTCOM--that is, the Canadian Security Intelligence Service (CSIS), Canada’s primary national intelligence service, operating under the Public Safety portfolio; and the Communications Security Establishment (CSE) and the Canadian Forces Intelligence Command (CFINTCOM), both operating under the National Defence portfolio. CSE provides foreign signals intelligence (SIGINT) to the Government of Canada in response to the priorities the

government has identified. CSE's mandate and authorities as defined in the National Defence Act require CSE to: 1) Acquire and use information from the global information infrastructure for the purpose of providing foreign intelligence, in accordance with Government of Canada intelligence priorities; 2) provide advice, guidance and services to help ensure the protection of electronic information and of information infrastructures of importance to the Government of Canada; and 3) provide technical and operational assistance to federal law enforcement and security agencies in the performance of their lawful duties (Foreign signals intelligence, CSE, 2019). SIGINT is "the interception and analysis of communications and other electronic signals." Today, "the world of signals intelligence includes any form of electronic communications, such as telephone calls and text messages, computer and internet communications, and satellite signals" (Foreign signals intelligence, CSE, 2019). SIGINT is one of several primary intelligence disciplines (Rosenbach, Peritz, & LeBeau, 2009, pp. 12-13):

- SIGINT, or Signals Intelligence, which involves the interception of COMINT (Communications Intelligence) and ELINT (Electronic Intelligence).
- HUMINT, or Human Intelligence, which is gathered from human sources, typically through clandestine operations.
- GEOINT, or Geospatial Intelligence, which is based on the visual representation of activities on Earth.
- MASINT, or Measurement and Signatures Intelligence, obtained by analyzing data such as missile plume signatures and uranium particles in the air.
- OSINT, or open source intelligence, which gathers intelligence from public sources such as the Internet, public documents, media, etc.).

The US National Security Agency (NSA) is a national-level intelligence agency of the U.S. Department of Defense, operating under the authority of the Director of National Intelligence. NSA is responsible for "global monitoring, collection, and processing of information and data for foreign and domestic intelligence and counterintelligence purposes." NSA consists of two branches: 1) Signals intelligence (SIGINT) and 2) cybersecurity (formerly information assurance). The NSA is responsible for providing foreign signals intelligence (SIGINT) to policy-makers and military forces. SIGINT plays a vital role in national security "by providing America's leaders with critical information they need" to defend the U.S., "save lives, and advance U.S. goals and alliances globally" (NSA, n.d.). NSA's cybersecurity branch works to prevent foreign nations from gaining access to sensitive or classified national security information--that is, to protect the U.S. communications networks and information systems (NSA, n.d.).

Domestic surveillance.

On one hand, governments/police and law enforcement agencies employ open source intelligence technologies to maintain national security and political stability, including to protect the public against crime or terrorism. Surveillance technologies that gather intelligence (useful or actionable knowledge) help policymakers/governments counter domestic and foreign threats, for example, via data mined from social media and keyword analysis to understand domestic and foreign public views on different subjects. Governments use algorithm and AI/ML (hereafter AI) based digital surveillance technologies to gather intelligence in attempts to intervene before crimes are committed, which falls under the banner of intelligence-led policing (Koops, 2013), for example, by monitoring social media platforms for certain keywords and pictures to help

prevent crimes before they escalate or to assist in criminal investigations, child crime, kidnapping, homicide, terrorist threats, and high-level computer intrusions.

On the other hand, surveillance is a growing cyber threat to the privacy rights of citizens. The ability of digital surveillance technologies to track the location and activities of users--generally, to profile users--has turned them into a formidable tool in the hands of police states and authoritarian governments eager to monitor and control activities that threaten power structures including activities of human rights activists. AI "enables large-scale surveillance of often vulnerable populations" (Shoker, 2019). The Edward Snowden revelations highlighted the extent of domestic state surveillance in the U.S. and the extent of business-state political economic collusion. Snowden revealed that the CSE used free airport Wi-Fi service to spy on the communications of all travelers using the Wi-Fi service and to track them after they had left the airport, all without a warrant. The number of Canadians affected by this surveillance is unknown. While some surveillance technologies are useful or beneficial, left to the unregulated market forces, surveillance has come to threaten the core of the liberal political tradition especially the autonomy of citizens and their freedom from political economic oppressive influence (e.g., manipulation of behavior).

1.1.4.2. Business surveillance.

A distinction can be made between business intelligence (BI) and business surveillance. Corporations gather intelligence to help them predict technology or social or regulation trends that can affect their current operations and future growth. According to Forrester Research, BI is "a set of methodologies, processes, architectures, and technologies that transform raw data into meaningful and useful information used to enable more effective strategic, tactical, and

operational insights and decision-making" (Evelson & Nicolson, 2008). Thus, BI can encompass information management (data integration, data quality, data warehousing, master-data management, and text- and content-analytics). BI systems combine data gathering, data storage, and knowledge management "with analysis to evaluate complex corporate and competitive information for presentation to planners and decision maker, with the objective of improving the timeliness and the quality of the input to the decision process" (Springer-Verlag Berlin Heidelberg, 2008).

Competitive intelligence and business analytics can be understood as sub-sets of BI. BI and competitive intelligence both support decision making. BI uses technologies, processes, and applications to analyze internal and external structured data and business processes, while competitive intelligence gathers and analyzes information situating a company vis-à-vis its competitors. Business analytics focuses on statistics, prediction, and optimization, rather than the reporting functionality.

Surveillance technologies are becoming increasingly sophisticated and prevalent and are being developed to detect and respond to behavioral patterns in real time. Surveillance technologies are wide ranging and begin with the core Internet communications protocol "IP," or more broadly the Internet protocol suit TCP/IP, and how it governs and structures communications on computer networks. IP addresses are comprised of two parts: Network address and host address (a host is a specific device on a network). Open source intelligence/surveillance technologies are widely used in the field of advertising. The advertising industry is based on collecting user data, on profiling users according to behavioral patterns or choices so as to micro-target them with effective messages. For example, cookies, or persistent identifiers are used in web browsers to track user activities. Third-party cookies enable

companies to track users across different media platforms. The data broker industry aggregates user data from across public platforms then sells them to marketing and advertising companies. For example, Acxiom Corporation, Little Rock, Arkansas, USA, operates twenty-three thousand computer servers that collect, collate, and analyze more than 50 trillion unique data transactions every year and have amassed profiles on over 700 million consumers worldwide (Goodman, 2016). While BI can be understood to refer to ethical sales and marketing practices, including assessment of the business risk environment, business surveillance is associated with intrusive intelligence gathering techniques that transgress the privacy rights of users of ICTs (the citizens).

Business surveillance applies the same data mining and analysis technologies and techniques of BI to profile users through data aggregated from social media and public records allowing retailers to micro-target and influence or manipulate user behavior. A "shockingly extensive, robust, and profitable surveillance architecture" (Schneier, 2015, p. 56) has emerged out of this technological infrastructure, and is behind the trend of privacy breakdown during the past five years equivalent to "an environmental calamity" (Thompson, 2019), such that even the Canadian Minister of Innovation said, "Canadians are rightfully concerned about reports of data breaches, misuse of personal information by large companies, election interference, and online hate related to mass tragedies" (Bains, 2019).

The information which NSA whistleblower Snowden revealed regarding "the extent of governmental surveillance and the close relationship between traditionally distinct public and private entities has damaged systemic trust in a profound way" (Shull, 2019). Attacks on the privacy of citizens represent a political threat in a society where political stability rests on deeply held and long-practiced set of core liberal values of personal liberty, individualism (autonomy), and freedom, rooted in the ideals of the Enlightenment revolution and the Scientific Revolution,

and a breach to the social contract forming the basis of the liberal political tradition. Citizens in liberal democracies are seeing their privacy rights squeezed from all sides—government, business, and malicious actors--eroding trust in government. The challenge for regulators and policymakers is: Is the data collection process of personal/private data ethical? Is intelligence gathering or knowledge making in support of business innovation ethical? What decision-making and technology governance frameworks are available to guide ethical technology governance?

Surveillance can be understood as a phase in the penetration testing process--as a phase of intelligence gathering or knowledge making. This study focuses on the intelligence gathering phases of OSINT or reconnaissance, network enumeration, and port scanning (what NIST, 2008, calls the discovery phase). Businesses use AI/ML powered intelligence gathering technologies to expand their capacity to mine and process business intelligence for growth, and in IT governance of network security. AI based OSINT technologies are used extensively by hackers and penetration testers to gather intelligence about a specific online target. Automated OSINT tools can be used to harvest data from social networks, including names, online handles, jobs, friends, likes/dislikes, locations, pictures, etc. (McLaughlin, 2012). Recon-ng and Maltego are data management tools designed to facilitate the process of gathering, analyzing, and organizing OSINT. Network enumeration and scanning technologies are being increasingly deployed to achieve “continuous testing,” and “network awareness” and to ensure that polices are followed (e.g., Snort and p0f in IDS/IPS applications). Other AI powered tools for OSINT gathering include FOCA and Cree.py in addition to Google custom searches.

AI is used in cybersecurity applications that include pattern recognition (e.g., to identify phishing emails based on content or sender information), anomaly detection (e.g., detecting unusual activity with applications in fraud detection for online banking), natural language

processing (converting unstructured text such as a webpage into structured intelligence), and predictive analytics (processing data and identifying patterns in order to make predictions and to identify outliers). AI enables human analysts to collect and analyze large data sets that would otherwise be insurmountable, that is, AI can be used to enhance intelligence operations. In ML the computer learns by itself. ML can be understood as a subcategory of AI that enables computers to learn without being explicitly programmed with predefined rules. ML is

> the scientific study of algorithms and statistical models that computer systems use to carry out tasks without explicit instructions, such as by using pattern recognition and inference … Machine learning algorithms build a mathematical model based on sample data, known as "training data", in order to make predictions or decisions without being explicitly programmed to do so. (Bishop, 2006)

Other subcategories of AI beside ML include machine vision, natural language processing (NLP) and machine translation, robotics, and purpose-driven and autonomous machines. Algorithms are the building blocks that make up machine learning and artificial intelligence. "An algorithm can either be a sequence of simple if → then statements or a sequence of more complex mathematical equations." ML algorithms include mathematical equations and operations (rules) such as for linear regression, decision trees, etc. But there is a difference between ML and AI, and it relates to the nature of the input data. "Machine learning is a set of algorithms that is fed with structured data in order to complete a task without being programmed how to do so. A credit card fraud detection algorithm is a good example of machine learning" (Bishop, 2006).

1.2. Social Digitization

Kool, Timmer, Royakkers, and van Est (2017) of the Dutch Rathenau Instituut argue that the digitization of society has entered a cybernetic phase, thanks to a host of emergent technological innovations in computing and communications together generating a new wave of digitization. The concept of digitization refers to a large cluster of digital technologies such as robotics, the Internet of Things, artificial intelligence and algorithms, and big data. Artificial intelligence is becoming ubiquitous, increasingly finding its way into more and more software applications, and involves giving computer systems a form of intelligence, such as learning and autonomous decision making, and thus supports a myriad of emerging and disruptive technological innovations (e.g., smart environments, robotics, and network monitoring). "Urgent Upgrade: Protect Public Values in Our Digitized Society" explores the ethical and societal challenges of digitization and the challenges of the governance landscape in the Netherlands. "We investigated which technologies are expected to shape digital society in the coming years, and which social and ethical challenges they will bring" (p. 116). The analysis involved an examination of the role of the scientific community and knowledge institutions, institutions responsible for protecting human rights, civil society, and "the roles of policy makers and politicians in agenda setting, in political decision making, and in the implementation of policy" (p. 11).

The analysis investigated the ethical and social issues that arise in the material, biological, socio-cultural and digital worlds and focused on eight technology areas that "best illustrate a wide range of the impact of the new wave of digitization" (p. 23)--that is, IoT and robotics; biometrics and persuasive technology; digital platforms, augmented reality, virtual reality and social media; and artificial intelligence, algorithms and big data (see Table 2).

Table 2: Technology Areas in The Four Worlds (Kool et al., 2017, p. 45)

Material world	Biological world	Socio-cultural world	Digital world
Robotics	Persuasive technology	Platforms	Artificial intelligence
Internet of Things	Multimodal biometrics	VR/AR and social media	Big data and algorithms

Although "digitization has been going on for decades," recently it has become "easier to intervene real time in the physical world at an increasingly detailed level." This "ushered in a new phase in the development of the digital society; a phase in which a cybernetic loop exists between the physical and the digital world" (p. 44). This means,

> processes in the physical world are measured, the resulting data is analysed, and then real time intervention takes place based on that data analysis. The impact of the intervention can subsequently be measured, analysed and adjusted, before rejoining the following cybernetic loop cycle. (p. 44)

Kool et al. (2017) see "a return to the so-called 'cybernetic thinking' that attracted interest in the 1950s and 1960s." In cybernetics "biological, social and cognitive processes can be understood in terms of information processes and systems, and thus digitally programmed and controlled" (p. 44). Based on the various phases in the cybernetic loop--collection, analysis, and application--the authors "see various ethical and social issues emerging" related to the development of technology that require attention in the coming years. The new wave of digitization is "leading to a world in which continuous feedback and realtime management and control are increasingly important principles for a range of services." This exerts "a strain on important public values" such as privacy, equity and equality, autonomy and human dignity. These values are clustered into seven topics (see Table 3: Overview of Ethical and Societal

Issues Related to Digitization). Analysis of the scientific literature on technologies revealed several recurring themes – "privacy, autonomy, security, controlling technology, human dignity, equity and inequality, and power relations" (Kool et al., 2017, p. 47).

Table 3: Overview of Ethical and Societal Issues Related to Digitization (Kool et al., 2017, p. 8)

Central topic	Issues
Privacy	Data protection, privacy, mental privacy, spatial privacy, surveillance, function creep
Autonomy	Freedom of choice, freedom of expression, manipulation, paternalism
Safety and security	Information security, identity fraud, physical safety
Control over technology	Control and transparency of algorithms, responsibility, accountability, unpredictability
Human dignity	Dehumanization, instrumentalization, deskilling, desocialization, unemployment
Equity and equality	Discrimination, exclusion, equal treatment, unfair bias, stigmatization
Balances of power	Unfair competition, exploitation, shifting relations consumers and businesses, government and businesses

Kool et al. (2017) argue that while initially digitization processes consisted of "the large-scale collection of data on the physical, biological and social world," a new wave of digitization characterized by continuous, cybernetic, feedback loops is focused on the large-scale analysis and application of that data. Nowadays "we can analyse this data on a large scale and apply the acquired knowledge directly in the real world" (p. 43). On one hand, real-time intervention and cybernetic (re)directing can be beneficial to society in various sectors--e.g., self-driving cars that update their digital maps through experience (learning). On the other hand, "Take for example social media users' newsfeeds, which social media companies are now 'customizing' based on their monitoring and analysis of these same users' surfing behaviour" (Kool et al., 2017, p. 25). Surveillance capitalism "commodifies personal clicking behavior" -- "it unilaterally claims

private human experience as a free source of raw material" (Thompson, 2019). Social media sites are "calibrated" for user engagement and interaction. Surveillance can influence user behavior in complex ways, including unconsciously--hitting either the information security or the political autonomy of citizens. Data surveillance "can unconsciously influence a user's identity, and lead to 'filter bubbles', in which the system only suggests news, information and contacts that match the user's previous behaviour, choices and interests" (Kool et al., 2017, p. 10).

Kool et al. (2017) conclude that "the far-reaching digitization of society is raising fundamental ethical and societal issues." Government and society "are not adequately equipped to deal with these issues" (p. 26). The governance system "needs to be upgraded if it is to "safeguard our public values and fundamental rights in the digital age now and in the future." This upgrading "requires that all parties – government, business and civil society – take action to keep digitization on the right track" (p. 26).

1.2.1. Digital transformation of higher education.

"In the context of sweeping social, economic, technological, and demographic changes," writes EDUCAUSE (2019), digital transformation (DT) is "a series of deep and coordinated culture, workforce, and technology shifts that enable new educational and operating models and transform an institution's operations, strategic directions, and value proposition." Social digitization and DT (which can be understood as a subcategory of social digitalization) are forms of social (sociotechnical) evolution. These sociotechnical shifts are transforming how businesses and society work. The intertwinement of technology and society within DT (Luppicini, 2020) promises new business opportunities and business models that capitalize on the technological infrastructure underlying a new wave of social digitization. DT is to be studied at the intersection

of “culture, workforce, and technology”--or society and technology--especially in light of how citizens in liberal democracies use (or should use) ICTs and social media. A new phase in the development of the digital society rests on self-correcting cybernetic loops operating in real time (real-time monitoring) existing between the physical and the digital worlds, that is, on the hybridization or convergence of the physical and digital worlds (Kool et al., 2017). AI, 5G, and IoT technologies have created systemic vulnerabilities relating to information security/privacy--especially increased risk of exposure to cybercrime and surveillance. Increasing exposure risk due to increasing interconnectedness (expansion of the attack surface) on an internationalized and globalized ICT network has brought ordinary Canadians to the forefront of the sociopolitical cybersecurity battle. Citizen information security awareness needs to span technical, as well as legal, social and political contexts governing or regulating the use of open hacking technologies.

What skills/knowledge and governance frameworks are needed to leverage opportunities and reduce risks of hacking technology use? Sociotechnical shifts create a need for IT governance frameworks regarding technology use, political decision making, and protecting social values at stake, notably privacy rights (the information security and political autonomy of individuals). Technology induced workplace shifts create a need for security training--they raise a need for new skills/knowledge/education, including technical (emergent technologies) and social education (including legal and political contexts). Addressing the emerging national and international challenges of a rising and increasingly more complex and internationalized cybersecurity threat landscape will require a broader approach to education “which may not be achieved through dedicated cybersecurity programs” (Radziwill, Romano, Shorter, & Benton, 2015, p. 5). Sociopolitical changes “are introducing new expectations of the current and entering workforce at the same time that they are bringing their own shifting expectations of the

workplace. All these changes are creating new opportunities and threats and demanding a reinvention of human resource management" (EDUCAUSE, 2019). Professional ethical hackers increasingly need a strong interdisciplinary foundation to cybersecurity education and governance. "Penetration testing is a highly technical and complex field. An ethical hacker requires deep knowledge across many areas, including, but not limited to software, hardware, networking, and even human behavior" (Thomas, Burmeister, & Low, 2018, p. 3). Cyber defense research teams increasingly need skills/knowledge beyond computer science, electrical engineering, software and hardware security, "but also political theory, institutional theory, behavioral science, deterrence theory, ethics, international law, international relations, and additional social sciences" (Kallberg & Thuraisingham, 2012, p. 2).

1.3. Cybersecurity Vulnerabilities

Canadian society has two key systemic vulnerabilities: A cybersecurity skill/knowledge gap and its nature as an open society. Criminals and other malicious threat actors seek to exploit these vulnerabilities which represent a national security risk spanning cybercrime, terrorism, economic welfare, and diplomatic (foreign influence). Programs teaching ethical hacking in higher education are steadily growing but student convictions for hacking crime is on the rise, cybersecurity risk in broader society is escalating, and the cybersecurity skill gap is getting worse--an estimated 3.5 million cybersecurity jobs will go unfilled by 2021 and fewer than one in four of the candidates who apply are qualified (Winick, 2018). There is a concern that teaching students hacking skills increases crime risk to society by drawing students toward criminal acts. Applying the precautionary principle: There is a concern that not teaching students hacking skills increases crime risk to society due to students' inability to use/understand hacking

technologies and how to protect themselves against them; there is a concern that not teaching students the necessary hacking skills lies behind a cybersecurity skill gap. Hence the thesis explores key societal cybersecurity risks (threats and vulnerabilities) and associated hacking technologies and skills which students may misuse in the current cyber threat landscape or which students need to learn to protect their privacy and to defend against future business or national cyber threats. Hence we can understand the risk of digital hacking technology use in ethical hacking teaching practices (in teaching students hacking skills) in the broader social cybersecurity context of threats to the information security/privacy rights of citizens from cybercrime and from political economic surveillance.

1.3.1. An open, scientific, knowledge-making society.

The thesis conceptualizes Canadian society as an open, scientific, knowledge-making sociotechnical society concerned with self-governance for survival in a changing environment (Bacon; Beer, 1984; Bunge, 1975, 1977, 1979, 1999; Descartes; Dewey, 1912, 1938/2018, 1984; Hume, 1748/1902; James; Popper, 1957, 1966, 2003, 2014; Weick, 1969/1979, 1995). See Table 4: The Epistemological Roots of STEI-KW as a Sociotechnical Theory of Society and Table 5: STEI-KW and Society.

Stehr (2002) says, “Contemporary society may be described as a knowledge society based on the extensive penetration of all its spheres of life and institutions by scientific and technological knowledge” (cited in Luppicini, 2010, p. 13). The concept of the knowledge society has recent roots in economics. The “placement of knowledge at the center of economic and societal growth is a relatively recent phenomenon marked by a shift in the modern world from an industrial age to an information age. In developed countries like the United States, this

shift occurred in the 1960s and 1970s with the rise of the knowledge-based economy" (p. 14). The focus on knowledge in society spearheaded in economics would spread to other disciplines and fields "under a variety of terms such as post-industrial society (Bell, 1976), postmodern society (Lyotard, 1984), posthuman society (Fukuyama, 2007), information society (Garnham, 2004), network society (Barney, 2003), and information age (Castells, 2000)" (p. 14).

Knowledge society is the most suitable term available for a technoethical inquiry, argues Luppicini (2010). First, while information/network society tend to focus on ICT, which is one aspect of technology and technique that does not address environmental or economic considerations, knowledge is "more closely aligned with organized aspects of human life and society where science and technology are influential, such as knowledge management and knowledge economy." Second, "given the importance attributed to tacit and explicit knowledge building activity as core to organizational development, the knowledge society is a better fit to describe organized forms of scientific and technological activity over competing terms." Third, while the knowledge society metaphor "accommodates technoethical concerns outside the scope of developed nations where networked technologies are widespread," the network society metaphor does not (Luppicini, 2010, p. 15). Individuals, communities, and organizations in a knowledge society produce knowledge-intensive work. A knowledge society generates, shares and makes available to all society members knowledge that may be used to improve the human condition. A knowledge society transforms information into resources that allow society to take effective action (Castelfranchi, 2007). A knowledge society promotes human rights and offers inclusive and universal access to all knowledge creation. The UNESCO World Report establishes four essential principles for developing an equitable knowledge society: Cultural diversity, Equal access to education, Universal access to information (in the public domain), and

Freedom of expression (United Nations Educational, Scientific and Cultural Organization, 2005). The concept of a knowledge society encapsulates a society's ethics and values--knowledge is a social construction comprised of facts and values inextricably intertwined.

In what ways are we a knowledge-making society? Two key defining characteristics of the emergent sociotechnical society are: Cybernetic digitization and a knowledge-driven economy. Cybernetic digitization (see Kool et al., 2017) refers to the convergence/hybridization of the digital and physical worlds through continuous, cybernetic feedback loops (real-time monitoring and adaptation). The cybernetic phase of social digitization, that is, the sociotechnical change it imagines, corresponds to an understanding of the Fourth Industrial Revolution as a social transformation involving social, political, cultural, and economic changes unfolding over the 21st century. Building on the ubiquity of digital technologies of the Third Industrial or Digital Revolution, the Fourth Industrial Revolution "will be driven largely by the convergence of digital, biological, and physical innovations" (Schwab, 2018). "It means that processes in the physical world are measured, the resulting data is analysed, and then real time intervention takes place based on that data analysis." The impact of the intervention "can subsequently be measured, analysed and adjusted, before rejoining the following cybernetic loop cycle" (Kool et al., 2017, p. 43)--that is, surveillance whereby companies track user actions, profiling them, and on that basis show real-time "appropriate" information, products, or prices.

1.4. A Knowledge-Driven Economy

Today, "five of the six most valuable publicly traded companies in the world deal in data," wrote Canadian Minister of Innovation Bains (2019) in a LinkedIn post (Innovation and

Privacy: the Duet of the Century). “Data-driven innovation will allow companies to grow and create good middle-class jobs for Canadians.”

> thanks to digitization, we can now collect and analyze data in previously unimaginable ways. And the value that can be derived through digital means – from artificial intelligence to machine learning – has made data the most valuable resource in the world. (Bains, 2019, LinkedIn)

AI/ML and digitization, especially the ability to mine and analyze large amounts of data and turn it into useful or actionable knowledge, has accelerated and intensified value creation from data. A new wave of digitization is focused on the large-scale analysis and application of that data on the physical, biological and social worlds (Kool et al., 2017). AI processing of information automates knowledge making and decision making--that is, AI can autonomously make decisions/construct knowledge. Data are raw facts lacking in meaning and social value. Information is data processed or arranged to give meaning but lacking value or emotion attached to it. Once humans interact with the information to use it in some social context, it is imbued with value and becomes knowledge (and wisdom with time). AI automates and accelerates the conversion of raw data to useful knowledge. Society’s ability to extract value from surveillance data has made privacy and innovation “the duet of the century” (Bains, 2019).

> Given this new reality, how do we protect people’s privacy and the security of their data, while preserving and even improving the competitiveness of Canadian innovators in this data-driven economy? For many people, this sounds like a zero-sum game. Sacrifice privacy for innovation, or let innovation suffer in the name of privacy. But these should not be competing priorities. In fact, we can only reach our full innovative potential if we

> build a strong foundation of trust on which our digital economy can flourish. Data-driven businesses rely on their users' trust and confidence. (Bains, 2019)

Minister Bains's (2019) comment is the beginning of the thread for the ensuing analysis. The first point to take to heart is that data is "the most valuable resource in the world." Data is the principal cybersecurity asset that needs protection, which makes cybersecurity top of mind for citizens, governments, and business. The National Cyber Security Strategy released in June 2018 recognized that "cyber security is the companion to innovation and the protector of prosperity" and cybersecurity is now an essential element to a functioning innovation economy (PSC, 2019). But a finer point needs to be made on the idea of a data-driven economy (Bains, 2019). It is a knowledge-driven economy. Knowledge as useful or actionable intelligence rather than mere data is the real source of value creation and now that AI can "make knowledge" it has opened doors for value creation/business models around value creation from mining and processing large amounts of data, especially personal "private browsing and clicking behavior" or "raw human experience" (Thompson, 2019).

The challenge for regulators and policymakers is: Is the data collection process of private data ethical? Is intelligence gathering or knowledge making in support of business innovation ethical? What decision-making and technology governance frameworks are available to guide ethical intelligence gathering? Does it produce knowledge that mirrors society? That is to say, does it produce knowledge in an ethical way?

1.5. A Crisis of Trust

"We can't afford to miss the boat on properly regulating the digital sphere, so that citizens can trust that their data is safe, and businesses can use data to innovate" (Bains, 2019)

"A future attack on the financial system's network infrastructure, or on a big bank, could trigger the next global economic crisis" (Orol, 2019). Cyberspace "presents both threats and opportunities—at the same time—and the collective challenge is to advance policy that can best maximize the opportunities while mitigating the threats in a constantly changing global environment" (Shull, 2019, p. 5). Trends indicate that the cybersecurity risk is escalating, or has escalated, from a risk status to a crisis situation. A multi-stakeholder prognosis of the cybersecurity governance landscape sees a crisis of trust at the personal, business and social levels threatening political and social stability. The essay series "Governing Cyberspace during a Crisis in Trust" by the Centre for International Governance Innovation (2019) takes a broad view of cybersecurity and addresses a range of topics, from the governance of emerging technology, including artificial intelligence and quantum computers, to the dark web and cyber weapons (Shull, 2019). A multi-perspective, multi-stakeholder analysis into regulation of AI in cyberspace--the conflicting interests/values regarding regulation of AI use in society/among societal sectors and institutions are elaborated. A more optimistic prognosis perhaps is that the world is at a turning point–the world may be heading to a crisis resembling the 2008 financial crisis in the heel of the financial services boom in the 1990s and 2000s.

> A crisis in the system could have profoundly damaging outcomes: cyber warfare, state surveillance, privacy invasion, data breaches, large economic and personal-income losses, and a global loss of trust. These risks are exacerbated by an East-West geopolitical divide: the United States and China are competing head-to-head for supremacy in the data realm, and everyone else is caught in the middle. (Fay, 2019)

1.6. Thesis Rationale, Research Questions, and Theoretical Framework

The escalating cybersecurity risk has governments and policymakers grappling for solutions. AI powered hacking technologies present both opportunities and threats in higher education and in broader society. There is a need for ethical governance--a need to effectively govern or regulate the use of digital hacking technologies in ethical hacking teaching practices in a global context to leverage the social and economic benefits that emergent and transformative technologies promise, while ensuring that the risks to the privacy rights and well-being and interests of Canadian citizens are minimized.

The thesis analyzes technology in the science and technology studies (STS) tradition. STS "is an interdisciplinary field concerned with the study of how scientific and technological changes intersect with society" (Quan-Haase, 2016, p. 51). An STS approach sees technology as a social construction reflecting and embodying social relations and cultural and political values. "Technology is both the driving force behind societal change as well as the output of our technological imagination. It is this dichotomy that we want to present." (p. ix). A deterministic approach to understanding the role of technology in transforming society can be utopian or dystopian. In technological determinism (e.g., traditional Marxism), technology shapes social interaction and systems of thought. By contrast, a critical approach sees technology as dialectic and value-laden (value as constitutive of technology). The outcome of society is the result of interaction between technology and humans and human systems in unpredictable ways. Technology "cannot be thought of as neutral because it is imbued with the values present from the culture from which it originated" (Feenberg, 1991, cited in Quan-Haase, 2016).

Technology is from the Greek word technología meaning systematic treatment. Technology has been studied as material substance, as knowledge, as practice, as technique, as

value, and as society. On the latter theme, for Baudrillard and Gane (1993), technology does not merely transform the world, "it becomes the world" (Quan-Haase, 2016, p. 44). For Marcuse (1982), technology is "a social process" of which social technologies, including communication and transportation, are a partial factor (p. 138). While early scholars in STS (Ellul & Vanderburg, 1964, 1981; Mumford, 1967, 1981) saw technology as an independent force dominating society, today STS analyzes technology in its unique social context of "complex societal influences and social constructs, entailing a host of political, ethical, and general theoretical questions" (Quan-Haase, 2016). Society and technology are closely interwoven and mutually shape each other (Bijker, 2009; Bijker et al., 1999)--cultural, social, political, economic, technological factors are integrated in social change. Within the field of STS, social change occurs as a blending of technological and social processes at various societal levels--individual, group, and macro levels (national and global). The two prominent approaches of STS are social construction of technology and actor network theory (ANT). STS theorists writing in the social construction of technology tradition, notably Bijker and Pinch, see human action as shaping technology. "Social constructivists argue that a technological object can acquire different uses and values according the social context in which it is placed" (Quan-Haase, 2016, pp. 52-52). The social construction of technology approach is used to understand technical change, the design of tools, and the technology-society relationship. STS theorists writing in the ANT tradition examine and describe the relationships and practices of actors. The theory focuses on how relationships between actors are constructed and practiced within a particular social context.

The thesis adopts the STS approach of the social construction of technology based on the following assumptions. First, ethical hacking is a social phenomenon, especially penetration

testing (in information security testing/IT security governance). Second, technology is understood as sociotechnology (Bunge, 1975, 1977, 1999) or social technology or social technological ontologies. Technology can be understood as the various ways a society constructs its social artefacts. The field of STS "emphasizes that artifacts are socially constructed, mirroring the society that produces them. At the same time, tools shape society itself, as well as its values, norms and practices" (Quan-Haase, 2016, p. 43). Third, technology is theorized as a knowledge-making epistemology (i.e., STEI-KW)--liberal empirical pragmatism epistemology of knowledge as a social construction, based on a philosophical understanding of the scientific method (Bacon; Beer, 1984; Bunge, 1975, 1977, 1979, 1999; Descartes; Dewey, 1912, 1938/2018, 1984; Hume, 1748/1902; James; Popper, 1957, 1966, 2003, 2014) within social science (the STS tradition). Hence, we can study technology as we would study social phenomena, applying the scientific method (see EDP-STEI-KW). STS approaches reject deterministic assumptions about technology's effect on society and call for holistic approaches and qualitative methods to studying technology and its role is social change, such as case studies, interviews, and ethnography (Bijker et al., 1999).

The use of digital hacking technologies in ethical hacking teaching practices in higher education and within broader society raises ethical, technical, social, and political challenges for liberal democracies--intelligent and intelligence gathering technologies present opportunities but also raise ethical and governance challenges regarding their use. The thesis presents an examination of opportunities and risks involved in using digital hacking technologies, especially AI based open hacking technologies, in teaching students hacking skills. More and more CS (computer science), CE (computer engineering), and SE (software engineering) programs are teaching ethical hacking in higher education. Paradoxically, teaching students hacking skills is a

double-edged sword: It can raise as well as lower crime risk to society. There is a concern that students may use the skills learned in university outside of class maliciously. Literature research revealed “little guidance in preparing students to responsibly use hacking skills learned in college” (Pike, 2013, p. 69).

Confusion arising from differences in perceptions among experts, industry practitioners, and policymakers regarding what constitutes ethical hacking teaching practices, what constitutes hacking skills, what is the risk to society of teaching students hacking skills, and how to mitigate these risks stifles innovation and effective educational policy development and implementation, which perpetuates the security risk. Exploring ethical hacking in a ST society begins with exploring ethical hacking teaching practices in higher education as the foremost knowledge-making institution in society and the bridge between education and the workplace. The thesis examined the following four research questions: RQ1 What constitutes ethical hacking teaching practices? RQ2 What constitutes hacking skills? RQ3 What is the risk to society of teaching students hacking skills (risks vs opportunities)? And RQ4 How to mitigate the risk of students misusing the hacking skills learned in college or university later in life in criminal activities? (See Table 6: The Meaning of ‘What constitutes ethical hacking teaching practices?’)

As Luppicini (2010) points out, it is precisely due to “the propagation of powerful new scientific and technical advances” within the knowledge society that “there is a need for a study of social and ethical aspects of such advances to leverage benefits and guard against the misuse of new tools and knowledge” (p. 14). While the impacts of AI use in surveillance on society are not clear, also not clear is how to study AI technology sociologically, which is an ethical governance challenge. The thesis applied STEI-KW as an overarching theoretical framework for an interdisciplinary approach to studying ethical hacking technology use and governance in

society. Karl Weick's (1969/1979, 1995) sensemaking model was used as a social constructivist theory of knowledge construction. STEI-KW was applied in four ways. First, STEI-KW was applied as a social systems theory to conceptualize Canadian society an open, scientific, knowledge-making sociotechnical society. The field of STS "emphasizes that artifacts are socially constructed, mirroring the society that produces them" (Quan-Haase, 2016, p. 43). Hence, "ethical hacking" skills/knowledge taught in higher education should mirror society as an open, scientific, knowledge-making society. Second, STEI-KW was applied as a knowledge-making epistemology or "technology" in the STS social construction of technology tradition--as an analytical lens for ethical hacking or penetration testing, in particular the intelligence gathering phase or "discovery phase" (NIST, 2008) of the penetration testing process. Third, STEI-KW was applied to examine ethical hacking teaching practices (pedagogy as communication). Fourth, STEI-DMG was applied as a technology assessment framework: An integrative approach to decision making. STEI-DMG is based on the 5 steps of TEI (Luppicini, 2010, p. 73). The ethical aspects of technology and "how technology shapes a society are studied by assessing ethical uses of technology in order to influence technological development and improve daily life in a society" (Luppicini & So, p. 114). Cybersecurity risk governance is a systemic problem that needs a holistic approach. STEI-DMG provides an appropriate holistic social system (social and technical aspects) framework for examining ethical hacking technology use and governance in Canadian society. STEI-DMG integrates research, societal/key stakeholder values/interests/perspectives, and key ethical perspectives in technology use assessment. The exploratory qualitative case study approach was followed (Creswell, 2003, 2007; Stake, 1995; Yin, 1994, 2003).

Table 8: RQs, Data Collection, and Theoretical Frameworks

RQ1 What constitutes ethical hacking teaching practices? (The focus of Chapter 4: Findings)	Systematic literature review (SLR), organizational documentation, and in-depth interviews.	STEI-KW (Case studies)	Synthesis: Who are ethical hackers and what do they do--meanings, ethics, values, skills/knowledge, roles and responsibilities, and practices of professional ethical hacking practitioners. Table 9: Hacking Skills Coding Table (Network Penetration Testing) Table 10: Professional Ethical Hackers Coding Table Table 14: Profiles of Hackers
RQ2 What constitutes hacking skills? (The focus of Chapter 4: Findings)	SLR, organizational documentation, and in-depth interviews.	STEI-KW (Case studies)	
RQ3 What is the risk to society of teaching students hacking skills (risks vs opportunities)? (The focus of Chapter 5: Advanced Analysis)	In-depth interviews and narrative literature review (with input from RQs 1 and 2 SLR).	STEI-DMG (technology assessment)	Synthesis: Teaching ethical hacking skillset (see Framework pp. 144-145) -- including Teaching vs Practice insights What "ethical hacking" is taught in CS/CE/SE majors in higher education; and is it ethical? Table 11: Ethical Hacking Skills/Knowledge High-Level Concepts in CS/CE/SE Programs Analysis of pedagogy as communication (using STEI-KW) Technology impact assessment (using STEI-DMG)
RQ4 How to mitigate the risk of students misusing the hacking skills learned in	In-depth interviews and narrative literature review	EDP-STEI-KW and SSP-DMG	Synthesis: S&T innovation risk mitigation initiatives:

college or university later in life in criminal activities? (The focus of Chapter 5: Advanced Analysis)	(with input from RQs 1 and 2 SLR).		Ethical teaching: OSINT Analyst cybersecurity role and associated BoK foundation framework Ethical governance: • Professionalization of ethical hacking practice/practitioners • A public policy initiative: A NCE of ethical hacking communities of practice, technology assessment (STEI-DMG), and policy innovation (SSP-DMG)

1.7. Thesis Objectives

Four objectives were pursued. The first thesis objective was to explore who are ethical hackers and what do they do (RQ1 and RQ2) as a synthesis of a basic or foundational profile for professional ethical hackers. While the number of academic programs teaching ethical hacking in higher education continues to rise, and the number of ethical hacking practitioners has grown steadily, this growth has not been mirrored with a similar growth in scholarly research focusing on the attributes of professional ethical hackers--meanings, ethics, values, skills/knowledge, roles and responsibilities, and practices of professional ethical hacking practitioners in a ST society. There is no consensus on what is ethical hacking or what it should be and what are the skills and competencies required to successfully function at the various levels of the profession. The continuing lack of agreement on the scope and purpose of the ethical hacking profession continues to challenge its value and perceptions within organizations--stifling suitable educational policy development. The uncertainty surrounding the meaning and value of ethical hacking in society can deter future students from pursuing a career in ethical hacking, harming

national security and the economy. Standardized skills/knowledge competencies of ethical hacking professionals will enable higher education, professional IT security associations, and employers to establish appropriate programs and curricula for educating and training new practitioners in the field.

The limited research on the topic of ethical hacking has created a gap in knowledge and skills regarding what is expected from those seeking to enter the information security field, and what hacking skills are actually taught in computer science and computer engineering programs. Confusion arising from differences in perceptions among experts, industry practitioners, and policymakers regarding what constitutes ethical hacking teaching practices, what constitutes hacking skills, the risk to society of misusing hacking skills and technologies, and how to mitigate these risks stifles innovation and effective educational policy development and implementation, which perpetuates the security risk. To help counter the confusion, the thesis sketches out a profile of professional ethical hacking practitioners to help us understand who are professional ethical hackers and what do they do (so as to design effective ethical hacking teaching practices): Foundational understandings/definitions regarding the meanings, ethics, values, skills/knowledge, roles and responsibilities, and practices.

The second thesis objective was to explore what "ethical hacking" is taught in CS/CE/SE programs at two Canadian universities as case studies in focus and is it ethical--does it mirror society/does it meet society's needs? (RQ1 and RQ3.) The third thesis objective was to perform an impact assessment using STEI-DMG to inform policy development and ethical decision making regarding the use of technology in society. The fourth thesis objective was to explore suitable S&T innovation risk mitigation initiatives (RQ4). Applying ethical design principles derived from STEI-KW (i.e., EDP-STEI-KW) the thesis makes recommendations for ethical

design of ethical hacking teaching practices and recommendations for ethical governance of ethical hacking in society.

1.8. Thesis Overview

The introduction chapter presented the broad social problem of rising student hacking crime and the cybersecurity skill gap--both social phenomena are indicative of an underlying cybersecurity skill/knowledge gap in higher education and a need for ethical and innovative approaches to address the skill/knowledge gap. A discussion of social digitization and DT furnished an outline of the technological infrastructure shaping the behavior of ICT users and disrupting business models, and creating systemic vulnerabilities. The cyber threat environment was elaborated, and this was followed by a discussion of society's key systemic vulnerabilities. The research questions and theoretical framework was followed by an explanation of the thesis objectives. Chapter 2 (Literature Review) presents synthesis of the key concepts drawn from the topic and theories, explains the epistemological roots and the theoretical framework and how it is used in the thesis with justification. Chapter 3 (Method) covers the methodological approach, data collection and analysis, coding and the analytic strategy, and data validation protocols. Chapter 4 (Findings) discusses the key themes from RQ1 and RQ2. Chapter 5 (Advanced Analysis) discusses the key themes from RQ3 and RQ4--that is, technology assessment and case studies (RQ3), and mitigation or S&T innovation initiatives (RQ4). Chapter 6 (Conclusion) summarizes the key thesis findings and explains the study limitations, contribution to knowledge, and future research direction.

Chapter 2: Literature Review

2.1. Introduction

This chapter covers two areas. “Part 1: Information Security Risk Governance” covers the technical, theoretical, and regulatory context of ethical hacking applications in information security testing and governance at the organizational and state levels. Key concepts relating to information security management and governance (with emphasis on higher education in Canada) were explained: A representation of the physical and logical network layers and the security areas they represent within “cyberspace”; the classes of network attacks on information confidentiality, integrity, and availability; definitions of information security; information security risk assessment and IA/IT governance frameworks; key information security risk governance/mitigation strategies; and finally, the cybersecurity regulatory landscape in Canada and the U.S. especially regulatory frameworks affecting privacy in higher education. “Part 2: Theoretical Framework” covers the theoretical framework (STEI-KW), its epistemological roots, and how it was applied in the thesis. Bunge’s (1979) systemism and Popper’s (1966) Open Society theories were explained, then Bunge’s (1975, 1977, 1999) conception of sociotechnology or social technology was discussed within the STS SCOT tradition (Quan-Haase, 2016). A non-justificationist theory of science that underlies a constructivist epistemology of knowledge making was discussed. Then ethical design principles were synthesized drawing on a non-justificationist view of the scientific method and an empirical pragmatic liberal epistemology of knowledge making. Finally, Weick’s (1969/1979, 1995) sensemaking model as a constructivist theory of knowledge making was discussed.

2.2. Part 1: Information Security Risk Governance

The terms information security, cybersecurity, Internet security, computer security, and network security have intersecting and evolving meanings, but generally refer to processes of implementing security controls including IA/IT governance frameworks to protect the confidentiality, integrity, and availability of privileged information as well as the technological infrastructure of a computer network or system against unauthorized access or manipulation (Anderson, 2003; Blakley, McDermott & Geer, 2001; Cherdantseva & Hilton, 2013; CNSS, 2010; ISACA, 2008; ISO/IEC 27000:2009; Venter & Eloff, 2003). Sensitive data should be protected based on the potential impact of a loss of confidentiality, integrity, or availability. Confidentiality "refers to protecting information from being accessed by unauthorized parties." Integrity "refers to ensuring the authenticity of information—that information is not altered, and that the source of the information is genuine." Availability of information means that information is accessible by authorized users. Protection measures (security controls) tend to focus on two key areas: Mitigating known vulnerabilities and implementing the principle of least privilege whereby only the required functionality to each authorized user is granted. Information security is "a risk management discipline, whose job is to manage the cost of information risk to the business" (Blakley et al., 2001). Information security,

- "preserves the confidentiality, integrity and availability of information" (ISO/IEC 27000:2009);
- is concerned with "authenticity, accountability, non-repudiation and reliability" (ISO/IEC 27000:2009 sees CIA as properties of information);
- ensures that "only authorized users (confidentiality) have access to accurate and complete information (integrity) when required (availability)" (ISACA, 2008);

- is concerned with both the protection of information as well as the of technological infrastructure or information systems (Cherdantseva & Hilton, 2013; CNSS, 2010);
- is concerned with access to information (CNSS, 201; ISACA, 2008); and
- aims to provide assurance "that information risks and controls are in balance" (Anderson, J., 2003);

Other key information security concepts include privacy, authenticity and trustworthiness, non-repudiation, accountability and auditability, and reliability (Cherdantseva & Hilton, 2013; ISO/IEC 27000:2009). The broad pragmatic goal of information security management is to prevent or to reduce the probability of unauthorized access or damage to valued information assets to an acceptable risk level through risk mitigation strategies that involve management controls (ensuring security policies are implemented), technical controls (e.g., use of intrusion detection techniques), and operational controls (best practices/standard operating procedures are followed by humans). Information security threats most commonly rated as a concern in higher education in Norther America are as follows. Confidentiality attacks: Exposure of confidential or sensitive information (79%), Integrity attacks: Unauthorized or accidental modification of data (29%), Availability attacks: Loss of availability or sabotage of systems (16%), and mixed threat attacks: Email viruses, ransomware, or other malware (31%), and Unauthorized, malicious network/system access (27%) (EDUCAUSE Information Security Almanac, April 2019, p. 2).

Information security governance is the top-level enterprise business function accountable for information security under the rubric of IT governance (NCC 2005 IT Governance). The IT department is a customer of the information security governance business function or service, (e.g., HR, Finance). IT security as integrated with enterprise-wide risk management

policy/framework (IT security risk management) operates within the information security governance framework. Information security is a specialized function within business organizations focused on securing an organization's information assets against unauthorized access or damage. An information security professional from IT ensures an institution's IT system is operating in a way that meets varied regulatory requirements. IT security is a stakeholder level concern within enterprises and is concerned with Internet access and identity and access management, and the technological infrastructure of the IT network and its smooth operation. Information security governance is concerned with defining security policy and aligning security strategy with business strategy. Information Systems are comprised of hardware, software, and communications "with the purpose to help identify and apply information security industry standards, as mechanisms of protection and prevention, at three levels or layers: Physical, personal and organizational" (Cherdantseva & Hilton, 2013). Areas for which central IT most commonly has primary responsibility in higher education are Network security (94%), Monitoring (88%), Communications security (86%), and Identity management (83%) (EDUCAUSE Information Security Almanac, April 2019).

2.2.1. Understanding information security risk.

A standard definition of risk is the potential to lose something of value. Another definition involves the exposure to danger. In information security, risk is typically understood as threat times vulnerability times impact (the likelihood that a threat will exploit a vulnerability resulting in a business impact), or threat times vulnerability with an overlay of control effectiveness or velocity. A cybersecurity risk manager should determine what is the suitable definition. A key challenge is prioritizing risk for optimal investment in countermeasures. A well-

understood list of risks must be matched with a list of suitable mitigations for those risks. A risk can be accepted (evaluate if the cost of the countermeasure outweighs the possible cost of loss due to the threat), mitigated (implement safeguards and countermeasures to eliminate vulnerabilities or block threats), or transferred (place the cost of the threat to another business function or unit) (Stewart, 2012).

A risk-based approach allows an organization to prioritize the vulnerabilities identified and focus its efforts on the risks that are the most significant to its operations. The first step in identifying business risks should be to understand the business as a society, as a social system--its identity, corporate vision, social/community relations, and values. Clause 4 of ISO 22301 calls for understanding internal and external environments, including an organization's activities, functions, services, and the organization's risk appetite (ISO 22301 Portal: Societal security - Business continuity management system, 2015). Businesses need to evaluate information security risks for the purposes of insurance underwriting and resource allocation; or if they are attempting to comply with HIPPAA, PCI, and other regulations, they will perform a risk assessment periodically. Risk assessment "identifies risks generated by the possibility of threats acting on vulnerabilities, and what can be done to mitigate each one" (PCI DSS Risk Assessment Guidelines, 2005). Several major regulatory frameworks, including HIPAA, PCI, and SSAE 16, require businesses to perform periodic risk assessment. A popular definition of risk management by ISO Guide 73:2009:

> In ideal risk management, a prioritization process is followed whereby the risks with the greatest loss (or impact) and the greatest probability of occurring are handled first, and risks with lower probability of occurrence and lower loss are handled in descending order. In practice the process of assessing overall risk can be difficult, and balancing

resources used to mitigate between risks with a high probability of occurrence but lower loss versus a risk with high loss but lower probability of occurrence can often be mishandled.

EC-Council defines four attack categories or "the various types of attacks a hacker could attempt" (Walker, 2017, p. 25): Operating system, application-level attacks, shrink-wrap code attacks, and misconfiguration attacks. The thesis conceptualizes cybersecurity as information security concerned with protecting the CIA of privileged information within "Cyberspace" (i.e., layers 2-11 of The 15 Layer Cyber Terrain Model, Riley, 2014A): Persona Layer #11 is concerned with user identity and authentication security and is concerned with managing (securing) information related to user ID, email accounts, phone numbers, and other PII and access codes to digital services (typically on the Internet) via suitable identity and access management controls. The biggest threat to compromising data confidentiality at this level is social engineering schemes. Software Application Layer #10 is concerned with application security (e.g., browsers, Office products, etc.). The two common attack types on web apps are cross-site scripting and SQL injections. Application-level attacks "are attacks on the actual programming code and software logic of an application. Although most people are cognizant of securing their OS and network, it's amazing how often they discount the applications running on their OS and network" (Walker, 2017, p. 25). Many applications on a network are not tested for vulnerabilities during their development and contain vulnerability "built into them" (p. 25). Shrink-wrap code attacks "take advantage of the built-in code and scripts most off-the-shelf applications come with … These scripts and code pieces are designed to make installation and administration easier but can lead to vulnerabilities if not managed appropriately" (p. 25). Operating System Layer #9 is concerned with host security and vendor software QA/security

(Windows, Android, iOS, etc.). Regular security patching is the key mitigation security control for this layer and the previous layer (OS). Operating system (OS) attacks generally target "the common mistake many people make when installing operating systems—accepting and leaving all the defaults. Administrator accounts with no passwords, all ports left open, and guest accounts (the list could go on forever) are examples of settings the installer may forget about" (p. 25). Further, operating systems "are never released fully secure—they can't be, if you ever plan on releasing them within a timeframe of actual use—so the potential for an old vulnerability in newly installed operating systems is always a plus for the ethical hacker" (p. 25). Logical Layer (Communications Ports and Protocols) #7-2 is part of host security, network security, and infrastructure security or the Data Link layer, the home of misconfiguration vulnerabilities. The "Internet" column in Riley (2014A) is the Internet protocol suite, which is a conceptual model and set of communications protocols used in the Internet and similar computer networks governing communications. It is commonly known as TCP/IP because the foundational protocols in the suite are the Transmission Control Protocol and the Internet Protocol. Misconfiguration attacks,

> take advantage of systems that are, on purpose or by accident, not configured appropriately for security. Remember the triangle earlier and the maxim "As security increases, ease of use and functionality decrease"? This type of attack takes advantage of the administrator who simply wants to make things as easy as possible for the users. Perhaps to do so, the admin will leave security settings at the lowest possible level, enable every service, and open all firewall ports. It's easier for the users but creates another gold mine for the hacker. (Walker, 2017, p. 25)

2.2.2. Key information security risk mitigation best practices.

From what I've seen, bad patching habits excluded, (configuration mistakes) seems to be one of the more common ways of introducing malware or vulnerabilities into a system. From a research and teaching perspective, I am interested in hacking, provided that the objective of the work is to inform defence design (i.e. identifying classes of attacks, rather than specific vulnerabilities in specific software releases). Otherwise the hacking 'discipline' could be categorized as a class of "bug-fixing" or software testing, it seems to me. (PPT15, personal communication, November 29, 2018). Key strategic and tactical risk mitigation best practices that are not mutually exclusive include,

- Avoiding misconfiguration gaffes

A vulnerability is "a software or hardware bug or misconfiguration that a malicious individual can gain unauthorized access to exploit" (Snedaker & McCrie, 2011, p. 4). The first counter-threat sword for IT is to update software with security patches regularly against known vulnerabilities. Secondly, is to avoid misconfiguration mistakes. Vulnerabilities exploited by penetration testing include: "Misconfigurations (insecure default settings), Kernel Flaws, Buffer Overflows, Insufficient Input Validation, Symbolic Links, File Descriptor Attacks, Race Conditions, and Incorrect File and Directory Permissions" (NIST SP 800-115, p. 4-5). Network misconfigurations are a common source of network security vulnerabilities. Key configuration mistakes include missing security patches (around 95% of cyber attacks exploit known vulnerabilities), default credentials (leaving default usernames and passwords unconfigured for databases, installations and devices), easy and reused passwords, turned off logging, insecure services or protocols (FTP, Telnet, HTTP), outdated encryption protocols (SSL v2 is considered

insecure and was superseded by SSL v3 in 1996), and exposed remote desktop services and default ports (implement defense in depth IA approaches).

> Any external-facing device that's connected to the internet should have layers upon layers of protection to combat attempts to gain access from simple methods like a brute-force attack. Services like Remote Desktop Protocol (RDP), a proprietary protocol developed by Microsoft, can provide administrators an interface to control computers remotely. Increasingly though, cybercriminals have taken to leveraging this exposed protocol when it's not configured properly. (Bandos, 2019)

- Implementing the principle of least privilege (through identity and access management controls; functionality vs security)

To reduce the threat exposure to an organization--secure network configuration: Develop a strategy to remove or disable unnecessary functionality from systems and to quickly patch known vulnerabilities. Implement the principle of least privilege whereby only the required functionality to each authorized user is granted. IT security should tweak access privileges to what is necessary and sufficient, that is, implement the principle of least privilege. The system should offer only the required functionality to each authorized user. For example, a web server that runs as the administrative user (root or admin) can have the privilege to remove files and users. The principle of least privilege "is widely recognized as an important design consideration in enhancing the protection of data and functionality from faults (fault tolerance) and malicious behavior (computer security)." Benefits of applying the principle include system stability, security, and ease of deployment of new apps/services (Saltzer & Schroeder, 1975).

- Implementing QA (software development)/IA (network security) approaches to information security using a suitable IT governance framework

IT should emphasize a holistic audit approach to information security. IA can be understood as a structured approach to align strategic organizational objectives with information use routines to ensure information security. IA is concerned with the system processing the information flow and storage and includes rules and regulations, performance objectives and oversight, compliance and audit/governance frameworks.

- Implementing defense in depth (e.g., layered security)

IT should take adopt several information security tactics for defense in depth--e.g., security awareness training, installing firewalls, continuous network monitoring, access control and authentication, anti-virus encryption and VPN, server integrity, and periodic auditing.

- Implementing open security and security by design frameworks/technologies

For Linus Trevor, proper security means that everyone is allowed to know and understand the design because it is secure. With many people looking at a computer code, it improves the odds that any flaws will be found sooner (Linus's law), which could be more efficient than testing. Eric S. Raymond famously said referring to Linus's law, "given enough eyeballs, all bugs are shallow." Presenting the code to multiple developers with the purpose of reaching consensus about its acceptance is a simple form of software reviewing.

2.2.3. IT governance.

Underlying various IA/IT security governance frameworks for information security governance such as ISO/IEC 27001 and PCI DSS are five strategies involving a risk-based approach to security management: Asset valuation, identifying threats, identifying vulnerabilities, risk profiling (measuring the risk), and risk mitigation (Cobb, 2019). This risk-based approach "allows an organization to correctly prioritize the vulnerabilities it's identified

and focus its efforts on the risks that are the most significant to its operations." A risk-based security strategy "identifies the true risks to an organization's most valuable assets and prioritizes spending to mitigate those risks to an acceptable level." A risk-based information security strategy "enables an organization to develop more practical and realistic security goals and spend its resources in a more effective way. It also delivers compliance, not as an end in itself, but as natural consequence of a robust and optimized security posture" (Cobb, 2019).

Steps of the Information Security Risk-Based Management Approach (Adapted from Cobb, 2019)

Step	Key processes
Asset valuation	Determine what are the organization's key information assets, where they are stored, and who owns them. When determining the value of assets, include "any business impact and costs associated with the confidentiality, integrity or availability of a compromised asset in an evaluation, such as lost revenue from an order-entry system going down or the reputational damage caused by a website being hacked." This way of evaluating assets "ensures those that are most important to the day-to-day continuity of the organization are given the highest priority when it comes to security."
Identifying threats	Identify who may want to steal or damage the organization's key information (or mission critical) assets, why, and how they may do it. This includes "competitors, hostile nations, disgruntled employees or clients, terrorists and activists, as well as non-hostile threats, such as an untrained employee." Also consider natural disasters such as floods and fire. Assign a threat level to each identified threat based on the likelihood of it occurring and the estimated impact/cost.
Identifying vulnerabilities	Automated vulnerability scanning tools are used by penetration testers to identify software and network vulnerabilities. Physical vulnerabilities may also need to be enumerated. Finally, there are "also vulnerabilities associated with employees, contractors and suppliers such as being susceptible to social engineering-based attacks."
Risk profiling	Risk profiling begins after an organization's assets, threats, and vulnerabilities have been identified. "Risk can be thought of as the likelihood that a threat will exploit a vulnerability resulting in a business impact." Risk profiling "evaluates existing controls and safeguards and measures risk for each asset-threat-vulnerability and then assigns it a risk score. These scores are based on a combination of the threat level and the impact on the organization should the risk actually occur."

Risk mitigation	"Once each risk has been assessed, a decision is made to treat, transfer, tolerate or terminate it. Each decision should be documented along with the reasons that led to the decision." Once mitigation measures are implemented "carry out tests to simulate key threats to ensure the new security controls do actually mitigate the most dangerous risks."

Several frameworks and tools exist to help with evaluating assets, threat levels, and risk scores. NIST's Risk Management Framework is commonly used to quantify operational risk--to help "ensure that an enterprise understands the true risks to the key assets behind its day-to-day operations and how best to mitigate them" (Cobb, 2019). The Risk Management Framework (NIST SP 800-37) as a cybersecurity risk management framework within organizations integrates information security and risk management activities into the system development life cycle (the second step of the RMF is to select the appropriate subset of security controls from the control catalog in NIST SP 800-53). NIST's RMF Revision 2 published in December of 2018 "takes a more holistic approach to the risk management process," integrates privacy and adds RMF to SDLC. It also "includes information on aligning the RMF with NIST's Cybersecurity Framework (CSF), supply chain and security engineering." Most commonly deployed information security standards or frameworks in higher education are: NIST 800-53/FISMA (33%), NIST Cybersecurity Framework (32%), and NIST 800-171 (31%) (EDUCAUSE Almanac, 2019).

According to EDUCAUSE, a U.S. based nonprofit association that helps higher education elevate the impact of IT, with community of over 100,000 members spanning 45 countries, information security was the number one IT governance issue in 2016. The top higher education information security risks that were a priority for IT in 2016 were 1) phishing and social engineering; 2) end-user awareness, training, and education; 3) limited resources for the

information security program (i.e., too much work and not enough time or people); and 4) addressing regulatory requirements (Grama & Vogel, 2017).

Information Security Risk in Higher Education (Adapted from EDUCAUSE, 2019)

1) Phishing and Social Engineering	"Over the past two decades, phishing scams have become more sophisticated and harder to detect." While traditional phishing messages "sought access to an end user's institutional access credentials (e.g., username and password)," today "ransomware and threats of extortion are common in phishing messages, leaving end users to wonder if they have to actually pay the ransom."
2) End-User Awareness, Training, and Education	End-user awareness, training, and education "is critical as campuses combat persistent threats and try to make faculty, students, and staff more aware of the current risks." While "the majority of U.S. institutions (74%) require information security training for faculty and staff, those programs tend to be leanly staffed with small budgets."
3) Limited Resources for the Information Security Program	The 2015 EDUCAUSE Core Data Service survey covering all US higher education institutions showed that about 2 percent of total central IT spending is allocated for information security and that there is 0.1 central IT information security FTEs per 1,000 institutional FTEs (full time equivalents). About 55% of surveyed respondents said the security awareness budget for 2016 was less than 5K; and about 25% said they do not know; 15% said between 5-25k; and 7% said between 25-50k; and less than 1% said between 50 and 100K. "With limited resources, higher education institutions must be creative and collaborative in addressing information security awareness needs."
4) Addressing Regulatory Requirements	The regulatory environment impacting higher education IT systems is complex. Data protection in higher education IT systems is

	governed by a patchwork of different federal and/or state laws rather than by one national data protection law. Student data are traditionally protected by the Family Educational Rights and Privacy Act of 1974 (FERPA) "although some types of student data, when it is held in healthcare IT systems, may be protected by the Health Insurance Portability and Accountability Act of 1996 (HIPAA)." In addition, some types of student and institutional employee financial data may be protected by the Gramm Leach Bliley Act (GLBA). State laws may have data-breach notification requirements, and contractual agreements may have their own list of security technological controls that must be implemented and validated in IT systems. (Grama & Vogel, 2017)

A cybersecurity policy provides guidance for the protection of information assets, IT assets, and infrastructures. A cybersecurity risk governance policy identifies stakeholders, assets and threats, and procedures to assess vulnerabilities and risks and procedures to mitigate risks and manage incidents. Stakeholders should be identified at all levels in the business hierarchy, which may include businesses, services, groups, or feature teams. In addition, external stakeholders such as customers, governments, and investors should be identified. An information security policy is based on a combination of appropriate legislation, such as FISMA; applicable standards, such as NIST Federal Information Processing Standards (FIPS); and internal compliance requirements. Information security policy is an essential component of information security governance.

IT governance policies tell administrators, users and operators how to use information technology to ensure information security within organizations. Information security policies

aggregate directives, rules, and practices that prescribe how an organization manages, protects, and distributes information. An organization's information security policies are typically high-level policies covering a large number of security controls. An information security policy at the institutional level should address the fundamentals of the institution's information security governance structure, including information security roles and responsibilities, rules of behavior that users are expected to follow, and minimum repercussions for noncompliance. Further, organizational policies should include an access control policy outlining the access available to employees in regards to an organization's data and information systems (e.g., based on NIST's Access Control and Implementation Guides); an incident response policy, remote access policy, email and communication policy, and disaster recovery policy.

IT governance frameworks are used to create value for organizations by streamlining or structuring activities so as to meet certain performance and regulatory requirements related to risk governance by aligning strategic goals with operations. IT governance is a framework "that provides a structure for organizations to ensure that IT investments support business objectives." IT governance emphasizes a strategic alignment between IT activities and business goals, value creation, and performance management. NIST describes IT governance as "the process of establishing and maintaining a framework to provide assurance that information security strategies are aligned with and support business objectives, are consistent with applicable laws and regulations through adherence to policies and internal controls, and provide assignment of responsibility, all in an effort to manage risk." ISO 38500 IT governance standard Corporate Governance of Information Technology defines IT Governance as three activities: Evaluate, Direct, and Monitor. While in the business world the definition of IT governance has been focused on managing performance and creating value, in the academic world the focus has been

on “specifying the decision rights and accountability framework to encourage desirable behavior in the use of IT” (Weill & Ross, 2004). Benefits of information security governance include 1) Increased predictability and reduced uncertainty of business operations; 2) Protection from the potential for civil and legal liability; 3) Structure to optimize the allocation of resources/prioritize risks; 4) Assurance of security policy compliance; 5) Foundation for effective risk management; and 6) Accountability for safeguarding information (EDUCASUE, 2019).

Governance, risk and compliance (GRC) is an IT governance model or framework for managing an organization’s overall governance, enterprise risk management and compliance with various regulations. GRC offers a structured approach to aligning IT activities with business goals while effectively managing risk and meeting compliance requirements. GRC is a top-level framework for coordinating technical solutions, business cooperation and buy-in, and meeting regulatory requirements. It should be very similar to a business plan. Organizations consult frameworks for guidance in developing and refining their GRC policy rather than creating one from scratch. “Frameworks and standards provide building blocks that organizations can tailor to their environment. According to Grama, COBIT, COSO and ITIL are the big players in many different industries.” Key IT governance frameworks include:

•ITIL: Customizable framework designed around documents and processes to deliver an IT governance/life-cycle framework

•COBIT 5: Governance and management of enterprise IT

•COSO: Guidance on governance and operational performance through internal control

•CMMI: Delivering value by building capability in people and processes

•ISO/IEC 38500:2015: International standard of governance for corporate information technology

•IT Governance: Developing a Successful Governance Strategy (ISACA)

Table 7: IT Security Governance and IT Security Management (Adapted from Educause.edu)

IT Security Governance (doing the right thing)	IT Security Management (doing things right)
Oversight--to ensure that risks are adequately mitigated	Implementation--ensures that controls are implemented to mitigate risks
Authorizes decision rights	Authorized to make decisions to mitigate risks
Enact policy (setting a course)	Enforce policy (steering)
Accountability--specifies the accountability framework	Responsibility
Strategic planning--ensures that security strategies are aligned with business objectives and consistent with regulations	Project planning--recommends security strategies
Resource allocation	Resource utilization

2.2.4. Cybersecurity regulatory environment.

Canada's most visible commitments to cybersecurity governance include Canada cybersecurity strategy 2010, Canadian Cyber Incident Response Centre (CCIRC), Counter-terrorism Strategy, RCMP Cybercrime Strategy 2015, National Strategy for Critical Infrastructure, and Action Plan for Critical Infrastructure (2014-2017). Relevant US regulations that govern ethical hacking include, the guidelines, standards, and laws that govern ethical hacking include FISMA, the Electronics Communications Privacy Act, PATRIOT Act, Privacy Act of 1974, Cyber Intelligence Sharing and Protection Act (CISPA), Consumer Data Security and Notification Act, and Computer Security Act of 1987. Further, the Health Insurance

Portability and Accountability Act (HIPAA) has five key subsections: Electronic Transaction and Code Sets, Privacy Rule, Security Rule, National Identifier Requirements, and Enforcement (Walker, 2017).

Important Cybersecurity Regulations

	International Standards	National or Regional Standards	Organizational Standards or Guidelines
IT Security Management	ISO 13335, ISO 13569, ISO 17799, ISO 27001, ISO 27002	BS 7799-2, NIST Standards	ACSI-33, COBIT Security Baseline, ENV12924, ISF Standard of Good Practice, SAS 70
IT Governance	ISO 38500:2008	COSO Internal Control -Integrated Framework	COBIT, ITIL, BITS
Compliance		Sarbanes-Oxley Act, Privacy Act, Trade Practices Act	Basel II, FFIEC Handbook, Gramm-Leach-Bliley Act, BSA, FACTA, GISRA, CA Bill 1386, PCI DSS, FISMA
Privacy		Directive 95/46-European Union, ETS no. 108 - Council of Europe, PIPEDA -Canada, Privacy Act 1988 - Australia, Specter-Leahy Personal Data Privacy and Security Act 2005 - USA, Personal Information Protection Act No. 57 - Japan	
Risk Management	ISO 27005	AS/NZS 4360, COSO Enterprise Risk Management, MoR, NIST Standard 800-30	

Security Metrics	ISO 27004	NIST Standards	Web Security Threat Classification, ISECOM, CVSS
Security Evaluation	ISO 15408, ISO 27001	NIST Standards - FIPS, NSA IAM / IEM	PCI DSS
Security Testing		NIST Standard- 800-42	OWASP, OSSTMM, CHECK, ISACA, ISSAF, CREST

2.3. Part 2: Theoretical Framework

2.3.1. STEI-KW as a sociotechnical theory of society: The epistemological roots.

For Mario Bunge (1975, 1977, 1999), ethics and technology are social constructions (social technologies). Ethics can be conceived of as a branch of technology. Ethical inquiries can be treated as technological inquiries are treated. Researchers can evaluate moral rules or statements as they would technological rules: Moral rules ought to be fashioned as rules of conduct deriving from scientific statements and value judgements. In his seminal essay, "Towards a Technoethics," Bunge (1975, 1977) offers three lessons moral philosophy can learn from contemporary technology. First, the classical distinction between what is and what ought to be can no longer be maintained. Second, facts and values become blended in action. In decision theory, for example, values and facts (statistical data) together guide decision making. Third, moral norms can no longer be considered immutable or infallible and separate from facts or knowledge; knowledge and practical experience or experimentation inform values, and vice versa.

Bunge (1975, 1977) presents a value theory that can serve as a basis for weighing means, goals, and side effects, and thus form a basis for a pragmatic decision-making framework. Bunge (1975, 1977) suggests three technoethical rules for the researcher: 1) Evaluate goals jointly with side effects; 2) match the means and the goal technically and morally, and employ only worthy

practical means and optimal knowledge; and 3) eschew any action where the output fails to balance the input because it is either inefficient or unfair. The concepts of efficiency and fairness can be understood as competing social values. Rather than being rigid ontologies, for Bunge (1975, 1977), they represent socially constructed technologies or social values with pragmatic utility--an overarching goal of improvement and success. Fairness, like efficiency, is instrumental, not an end in and of itself. The end is improvement and success. Bunge's (1975, 1977) pragmatic value theory was further developed by Rocci Luppicini (2010, p. 73) into a problem-solving inquiry approach within a systems framework and framed as the five steps of Technoethical inquiry theory (TEI). TEI assesses technology—its use and value—by weighing the potential benefits against the potential costs with emphasis on efficiency and fairness. As such, TEI provides an ethics-based (pragmatic) decision-making model.

Step 1: Evaluate the intended ends and possible side effects to discern overall value;

Step 2: Compare the means and intended ends in terms of technical and nontechnical aspects (moral, social);

Step 3: Reject any action where the output (overall value) does not balance the input in terms of efficiency and fairness;

Step 4: Explore relevant information connected to the perceived effectiveness and ethical dimensions of technology use; and

Step 5: Consider technological relations at a variety of levels.

Table 4: The Epistemological Roots of STEI-KW as a Sociotechnical Theory of Society

	Epistemology	Ontology	Theory application
Sensemaking (Karl Weick,	Empirical pragmatism	Constructivism; knowledge is contextual and	Communities of Practice as a knowledge management process.

1969/1979, 1995)		common knowledge is iterative.	
TEI (Luppicini, 2010)	Empirical pragmatism: Ontologically dissolving of the rational-empirical divide.	Instrumental reason; constructivism; knowledge is part fact part value.	Decision making is broad based, inclusive; knowledge gathering is multi-disciplinary and multi-stakeholder.

TEI incorporates a broad-based multi-perspective, multi-stakeholder knowledge gathering epistemology for decision making. However, it needs an explicit social systems theory and a political theory. To address the theoretical gap, STEI-KW incorporates Bunge's (1979) theory of systemism to account for social relations within a systems framework and Popper's (1966) political philosophy augmented with a historical understanding of core liberal values emerging from the Enlightenment and scientific revolutions for a political ideology--that is, the sociopolitical values that are the glue holding a society in cohesion. Popper's (1966, 2016) political philosophy of an "Open Society," a staunch defense of liberalism (in opposition to totalitarianism) based on his philosophy of science known as critical rationalism, is used. Bunge's (1979) systemism directs our attention to society as an open system as a starting point for the sociological structural-behavioral analysis of the thesis. What are the key properties of Canadian society as a sociotechnical system and what is the underlying structure and values shaping behavior? Canada is presented as an open, scientific, knowledge-making sociotechnical society concerned with self-governance for survival in a changing environment (Bacon; Beer, 1984; Bunge, 1975, 1977, 1979, 1999; Descartes; Dewey, 1912, 1938/2018, 1984; Hume, 1748/1902; James; Popper, 1957, 1966, 2003, 2014; Weick, 1969/1979, 1995). See Table 4: The Epistemological Roots of STEI-KW as a Sociotechnical Theory of Society and Table 5: STEI-KW and Society. The researcher's assumptions regarding Canadian society (Canada as a

pragmatic liberal society) are based on his personal experience and are framed as a carefully defined academic idea.

Following Luppicini (2005), Bunge (1999), Boyd (2004), and Winch (1990), technology is anchored in a philosophy of science. “Any worthwhile study of society must be philosophical in character and any worthwhile philosophy must be concerned with the nature of human society,” argues Winch (1990, cited in Luppicini, 2005, p. 104). Based on a Boyd (2004) and Luppicini (2005) approach to a comprehensive systems definition of technology, a social sciences approach, a view from outside a technical or engineering field of technology by social scientists seeks to ground the definition of technology in theoretical and historical contexts (in a social science context). Such theoretical grounding ought to integrate an understanding of technology within a philosophy of science. “Comprehensive” refers to the holistic and transdisciplinary approach followed to define technology in society--to the social science approach of grounding technology in historical and theoretical context. Luppicini (2005) frames educational technology in a social science context to articulate a systems definition of educational technology in society “for guiding activities connected to current and future developments in Educational Technology.”

> This is accomplished by (1) discussing influences outside the field of Educational Technology that impacted its conceptual development, (2) discussing influences within the field of Educational Technology that impacted its conceptual development, and (3) articulating a systems definition of Educational Technology in Society. (Luppicini, 2005, p. 103)

Consequently, Luppicini (2005) defines Educational Technology in Society as,

> a goal oriented problem-solving systems approach utilizing tools, techniques, theories, and methods from multiple knowledge domains, to: (1) design, develop, and evaluate, human and mechanical resources efficiently and effectively in order to facilitate and leverage all aspects of learning, and (2) guide change agency and transformation of educational systems and practices in order to contribute to influencing change in society. (p. 108)

Applying step (3), theoretical grounding of technology within social sciences, gives rise to STEI-KW as a knowledge-making epistemology (an adaptation of the Boyd-Luppicini comprehensive systems definition approach). STEI-KW provides an appropriate holistic social system (social and technical aspects) framework for examining ethical hacking technology use and governance.

2.3.2. Systemism.

Bunge's (1979) systemism is a social systems theory grounded in theoretical sociology. Every theoretical view of society has two components, ontological and methodological. The ontological concerns the nature of society and the methodological concerns the way to study it. Individualism and holism are both inadequate frameworks for studying societies. Individualism ignores social relations and the emergent properties of any society such as social cohesion and social mobility. A society is understood as "a collection of individuals and every property of it is a resultant or aggregation of properties of its members (individualism, atomism, or reductionism)." Holism, in comparison, refuses to analyze social relations and emergent properties, and loses sight of the individual. A society is understood as "a totality transcending its membership and is endowed with properties that cannot be traced back to either the properties of

its members or the interactions among the latter (holism or collectivism).” On ontological grounds, a society is “neither a mere aggregate of individuals nor a supraindividual entity: it is a system of interconnected individuals”; society has systemic or global properties; and interaction between two societies is an individual-individual affair where “each individual occupies a definite place in his society. And social change is a change in the social structure of a society - hence a change at both the societal and the individual levels” (p. 16). On methodological grounds, 1) The proper study of society is “the study of the socially relevant features of the individual as well as the research into the properties and changes of society as a whole”; 2) The explanation of social facts “must be in terms of individuals and groups as well as their interactions”; and 3) “Sociological hypotheses and theories are to be tested against social and historical data.” Systemism lacks the aforementioned ontological and methodological defects and “combines the desirable features of the previous views, in particular the hard-nosedness of individualism with the holistic emphasis on totality and emergence” (p. 14).

A society can be viewed as “a system of interrelated individuals sharing an environment while some of its properties are aggregations of properties of its components, others derive from the relationships among the latter” (Bunge, 1979, p. 13). A society σ is representable as an ordered triple (Composition of σ, Environment of σ, Structure of σ), where the structure of σ is the collection of relations (in particular connections) among components of σ. A society can be thus construed as its membership together with its structure. A society is thus “neither a mere ‘sum’ (aggregate) of individuals nor a Platonic idea (i.e., an institution) transcending them.” A society is “a concrete system of individuals beating social relations among themselves and is therefore representable as a certain relational structure” (p. 14). Every society is comprised of social subsystems, such as the health system, the school system, and the political system. Every

social system "can be analyzed into a number of subsystems each of which performs a certain function (i.e., is characterized by a peculiar subset of social relations or of transformation relations)." The "entire membership of any given society is distributed among its various subsystems, with all of its individual members belonging to several subsystems at a time" (p. 25).

Bunge (1979) theorizes institutions as sets of social systems. An F-sector of a society is "the set of all social subsystems (schools) performing a certain function F (e.g. the set of all schools)" (p. 24). An F-institution is defined as the family of all F-sectors. An institution is "the set of all F-sectors for a given F." Thus, "the set of all state systems is called Government, the collection of all school sectors School, the set of all trade unions Organized Labor, the set of all postal systems Mail, and so on" (p. 27). The institutional rules "reflect the way the subsystems function optimally or, if preferred, they are prescriptions for operating the system in an efficient manner (i.e. for attaining its goals or rather those of whom the system serves)" (p. 28).

2.3.3. The social construction of technology.

The thesis studies the social construction of technology in the STS tradition. STS "is an interdisciplinary field concerned with the study of how scientific and technological changes intersect with society" (Quan-Haase, 2016, p. 51). The thesis approach is based on the following assumptions. First, ethical hacking is a social phenomenon, especially penetration testing (in information security testing and IT security governance). Second, a ST approach to the study of technology sees society and technology as closely interwoven and mutually shaping each other (Bijker, 2009; Bijker et al., 1999). Writing on sociotechnical change, Bijker wrote: "Society is not determined by technology, nor is technology determined by society. Both emerge as two

sides of the sociotechnical coin" (Bijker & Wiebe, 1997). Following Bunge (1975, 1977, 1999), a ST approach to studying technological social change conceptualizes how the social and the technological intertwine to form a complex ST society. Within the field of STS, social change occurs as a blending of technological and social processes at various societal levels--individual, group, and macro levels (national and global). Third, technology can be understood as the various ways a society constructs its social artefacts. Following Bunge (1975, 1977, 1999), technology is conceptualized as sociotechnology or social technology or social technological ontologies. Bunge's conception of technology as socially constructed technologies is used to focus the sociological analysis on society's key structural (openness) and behavioral (trusting and knowledge-making behaviors) properties governing or pertaining to the use of digital hacking technology in society. The field of STS "emphasizes that artifacts are socially constructed, mirroring the society that produces them. At the same time, tools shape society itself, as well as its values, norms and practices" (Quan-Haase, 20016, p. 43), hence, hacking skills taught in higher education should mirror society as an open, scientific, knowledge making society (i.e., embody and reflect society's values and key structural and behavioral properties).

Fourth, the thesis conceptualizes technology as a knowledge-making epistemology (STEI-KW), of knowledge as a social construction or social technology based on an understanding of the scientific method (Bacon; Beer, 1984; Bunge, 1975, 1977, 1979, 1999; Descartes; Dewey, 1912, 1938/2018, 1984; Hume, 1748/1902; James; Popper, 1957, 1966, 2003, 2014)--that is, as a liberal empirical pragmatic theory of knowledge construction. Hence, we can study technology as we would study social phenomena, applying the scientific method. When the scientific method is understood as an epistemology of social construction of knowledge (empirical pragmatism), technology is seen as applied science, as a social construct that has

context-dependent emergent properties (including social meaning, use, and value). It follows, the meaning of a technology is interdependent on its use in its social context; the technology and its meaning mutually arise (ontologically) and shape one another--the social and the technological intertwine to define and redefine each other--they are conceptually interlocked in the human mind around their utility. Thus it becomes unrealistic to extricate a technology from its social context and consequences of its use, including the emotions it provokes. We can conceive of technological ontologies in that sense. The social construction of technology and its value/ethics mutually arise and co-evolve (ontologically), influenced by the environment, in the human mind and in society in the form of physical artifacts or tools. And from here we can say open liberal values (liberal values of an open society) become inscribed in technology or designed onto it, and the process is reciprocal--the technology becomes an agent of social change. This can be understood as how the theoretical framework STEI-KW conceptualizes technological agency in complex sociotechnical systems--it is considered at the conception level, the level of knowledge construction, rather than at the design or deployment levels. Values and ethics are thus a key design consideration of technology.

Open as a value and as a concept associated with society and with its identity becomes a structuring ontology and context for emergent technologies (ontologies). Open becomes constitutive of new knowledge and new ideas that stem from the same conceptual root--“open” branches off into new technological ontologies. Society structured the Internet, a U.S. invention, as open as a manifestation (an ontology) of its own values, societal norms, and structure. The Internet was introduced into society and it rapidly integrated with it because it embodied society’s cultural values and structure, and in turn the Internet began to structure an open society. This analytical approach pinpoints society’s contradictory properties--structural and behavioral

properties that are accentuated by technology use. STEI-KW is suitable for the analysis/design of hacking technology use/governance in society because it draws attention to the key systemic properties of a society representing its vulnerabilities as well as its strengths. The properties of open, scientific, and knowledge-making society are both society's biggest strengths and vulnerabilities.

Table 5: STEI-KW and Society

Core liberal values	Scientific method (Bacon; Beer, 1984; Bunge, 1975, 1977, 1979, 1999; Descartes; Dewey, 1912, 1938/2018, 1984; Hume, 1748/1902; James; Popper, 1957, 1966, 2003, 2014)	Open Society (Popper, 1966)	Sociological analysis: Properties of a sociotechnical society
Reason Rationalism can lead to human improvement (progress) and is the most legitimate mode of thinking.	Non-Justificationism: Falsifiability (Popper), pragmatic fallibilism (Peirce), instrumentalism (Dewey and James), and Bunge's fallibilism (systems as useful paradigms). Empirical inductivism is illogical (Hume); Deductive reasoning is circular. Both inductive and deductive approaches cannot provide knowledge certainty.	Critical rationalism; All knowledge is tentative.	Knowledge making (empirical pragmatism) Communication: Social construction of knowledge (constructivism). Technology as applied science--as a social construction (Bunge, 1966, 1975, 1977, 1998).
Skepticism and science Enlightenment intellectuals were	Methodological skepticism: Uncertainty about the truthfulness of knowledge claims.	An open society has non-deterministic, emergent properties.	Scientific: Uncertainty/risk accepting society (trusting behavior).

skeptical of the divine right of kings and monarchies, scientific claims about the natural world, the nature of reality, and religious doctrine.	Mitigate methodological skepticism by process transparency. The scientific method strives to reduce uncertainty (move us closer to the truth).	Scientific society as opposed to magical, tribal, or theist. Falsifiability; positivist empiricist verificationism creates inconsistencies.	Behavioral: Scientific method values and ethics underlying the behavior of citizens in a ST society. Uncertainty about knowledge can be associated with pluralism.
Liberty: Personal liberty, individualism (autonomy), and freedom. All individuals are equal and have basic rights. Freedom of conscience (thought or choice) and individuals should be free to act without oppressive restriction. Classical liberalism is grounded in a belief in reason and an aversion to coercion (Butler, 2015). Legitimate political power "is based on the consent of the people and is obligated to be representative of the people's will" (Abernethy, 2016).	Open systems evolve; are non-deterministic; and have emergent properties (Beer, Bunge, Dewey, Popper).	Open Society: A liberal society ("liberal democracies") Individualistic as opposed to collectivist, pluralistic as opposed to monolithic, abstract as opposed to tribal, and autonomous as opposed to totalitarian.	Open society Structural: Open society and open technologies. Freedom fosters uncertainty and the fragmentation of opinion--a property of pluralistic societies.

2.3.4. Of an open liberal society.

Austrian-born British philosopher Karl Popper developed the concept of open society as discussed in this thesis during WWII. The Open Society and its Enemies (1966) and The Poverty of Historicism (1957) lay out Popper's political philosophy and represent what Popper saw as his "war effort," penned in response to the rise of fascism in Europe and in his native Austria in the 1920s and 1930s (Popper, 2005). Open Society does not frame an open liberal society as some kind of utopian state. Liberal society is fundamentally contradictory, non-deterministically unfolding within a historical process of reconciling facts and standards as "one of the bases of the liberal tradition" (Popper, 1966, p. 743/804). Popper sought to underscore a scientific philosophy to political, social, and historical analysis, applying his philosophy of science, critical rationalism, to offer an epistemological critique of totalitarianism, understood in contrast to liberalism, and of deterministic social and historical views.

Two key points can help define Popper's (1966) theory of an open society. The first point relates to Popper's reading of social evolution, of society becoming increasingly more individualistic and anxious as it comes to accept the uncertainty associated with an abstract society (a society marked by impersonal social relations). The second point relates to Popper's epistemological critique of political practices and of historicism, notably of the philosophy and social sciences of Plato, Hegel, and Marx. Popper saw an open society as the outcome of a social evolutionary process that has come to characterize western societies since at least the Scientific Revolution and which involves a fundamental shift in social structure, where the comforts of certainty, a structured life, and the "group spirit of tribalism" found in closed societies is replaced by anxiety, the cost of freedom and individualism--evolution from a tribalistic, hierarchical, conformist, or closed society, to an individualistic, abstract, and humanistic open

society which he identified with liberalism. The beginnings of an open society, which Popper traces to the classical Greeks, was marked by a growing distinction between natural and human-made laws, and an increase in personal responsibility for moral choices. As opposed to a "magical or tribal or collectivist society," an open society is one "in which individuals are confronted with personal decisions." The ensuing anxiety is a worthwhile price to pay for the benefits of living in an open society, namely freedom and social progress. "It is the price we have to pay for being human" (Open Society Vol. 1, 176).

Popper levels an epistemological critique of political practices and of deterministic views of historical development or "historicism." Lay at the roots of totalitarianism a methodological blind spot, a lack of critical perspective, regarding political practices and deterministic histories. A scientific approach to knowledge construction can only offer tentative judgments. Critical rationalism is a philosophical critique of certainty, its defining logic is skepticism toward knowledge claims. The falsifiability approach to the criticism of knowledge claims suggests we can only approach the truth rationally by reducing our ignorance about the verisimilitude of knowledge claims. One cannot make deterministic predictions about the future, not only because pure reason, inductivist empiricism, and positivist empiricist verificationism are illogical and/or reductionist, for example, they ignore the role of the observer as an active agent in the construction of knowledge and the personal values embodied therein, but also because these values themselves and the supposed facts, as well as what it means to do science and the purpose and social value of a scientific inquiry are all emergent concepts (Kuhn, 2012, famously described the process of the social construction of new scientific paradigms).

Historicists who claimed or presumed a grasp of "the laws of historical development" are misguided in their analysis because they took a deterministic approach to predict the future.

Plato, Hegel, and Marx believed history unfolded in a certain direction to an end point. Historicism posits that history is governed by immutable historical laws or principles. For Hegel, history would come to an end when all the internal contradictions in human ideas were finally resolved through the gradual unfolding of reason. Marx's dialectical materialism inverted Hegel's idealism and predicted history would end when the capitalist modes of production create social unrest due to massive social inequalities to the point of provoking a working-class revolution.

> The productive power unleashed by new technologies and factory production under capitalism was ultimately incompatible with capitalism as an economic and political system, which was marked by inefficiency, instability and injustice. Marx predicted that these flaws would inevitably lead to revolution followed by establishment of communist society. This final stage of human development would be one of material abundance and true freedom and equality for all. (Gorton, n.d.)

For Popper, a scientific approach to politics would direct one to the process of political change, instead of fixating on the character or personality of politicians (e.g., who should rule), as the only rational political approach to safeguarding liberalism, that is, to achieve peaceful, bloodless political change. "What has to be done if ever the people vote to establish a dictatorship?" Popper (2016) wrote in an op-ed (reprint) to the Economist. What if someone took office through the ballot box elections but then hijacked the democratic process. This can be avoided by instilling a fail-safe mechanism into the political change process (he advocated a two-party system, such as found in Great Britain). The problem of modern liberal democracies is not "who should rule?" Popper (2016) argued that a rational political theory should address an

epistemological problem of government, namely, “how is the state to be constituted so that bad rulers can be got rid of without bloodshed, without violence?”

The Enlightenment (the Age of Reason) was an intellectual-social movement emphasizing reason, skepticism and science, and liberty and the rule of law that took place in Europe and later in the United States and Canada during the late 17th and early 18th century. Liberalism as it has emerged from the ideals of the Enlightenment holds certain values that underlie a political philosophy (liberalism) characteristic of the identity and political culture of western nations. The core liberal values are reason, skepticism and science, and liberty. These liberal values would begin to cement through Enlightenment philosophers as a distinct political ideology, perhaps foremost among them is English philosopher John Locke, often considered the father of liberalism. Locke’s social contract theory inspired the United States Declaration of Independence. Other key Enlightenment figures associated with social contract theory include Hobbes and Rousseau. John Stuart Mill’s “conception of liberty justified the freedom of the individual in opposition to unlimited state and social control.” These core liberal values have become entrenched in western political culture and form the basis of today’s conceptions of what constitutes civil rights, human rights, civil liberties, and political freedoms, including the right to free speech and individualism (autonomy). In that vein, the privacy of personal and privileged information (against breaches by covert digital surveillance by government or business agents, in breach of trust or social contract and privacy regulations), and freedom from political interference, manipulation, and intimidation (through targeted propaganda, disinformation, or social trolling), protects the autonomy of individuals and keeps them free from undue political or political economic oppressive restriction--that is, protects their personal liberties.

2.3.5. The scientific method.

The scientific method can be traced back to the Scientific Revolution (17th to late 18th century) and especially to the classical rationalism of French philosopher René Descartes and the classical empiricism of his contemporary English philosopher Francis Bacon. The Scientific Revolution began in Europe around the end of the Renaissance period and continued through the late 18th century, ushering in the Enlightenment. The publication of Nicolaus Copernicus' On the Revolutions of the Heavenly Spheres in 1543 is often cited as marking the beginning of the Scientific Revolution (Stanford Encyclopedia of Philosophy). Descartes and Bacon, widely considered the founders of the scientific method, introduced systematic doubt to scientific inquiry. Both philosophers believed that the way to the truth lies in the application of reason--rational (Descartes) and empirical (Bacon) (Duignan, 2019). Rather than through religious doctrine or emotions, a rationalist would rely on reason and logic to acquire true knowledge about the world. For Descartes, pure reason was the only reliable means to gain knowledge, and the senses had to be doubted--the real world can be accessed and described through logic (dualist realism or mind-matter split). In search of certainty, Descartes (*Meditations on First Philosophy*) discards all belief in things which were not absolutely certain, and then proceeds to establish what can be known for certain, which he concluded was his ability to think--hence, "Je pense, donc je suis." Cartesian doubt is methodological. It uses doubt as a route to certain knowledge by finding those things which could not be doubted. In comparison, Bacon took it that all knowledge was attainable through the senses. Often regarded as the father of empiricism, Bacon believed that scientific or objective knowledge (ideally the truth--it is not clear Bacon believed he could necessarily arrive at the truth with certainty through his observationalist-inductivist approach) can be gained based only on inductive reasoning and careful observation of events in

nature. Importantly, he argued, scientific knowledge can be achieved by use of a skeptical and methodical approach whereby scientists aim to avoid misleading themselves. Bacon's method of scientific inquiry was methodical and iterative, and skeptical of a scientist's lapse into misleading themselves. The Baconian method (in *Novum Organum*) sought to link cause and effect of a phenomenon by careful observation and an iterative process of elimination. He reasoned: If X is seen to arise in the presence of Y time and time again, while it is not seen to arise in the presence of Z time and time again, we can make a scientific claim by inductive reasoning that Y causes X. Next, the scientist may gather additional data or use existing data and the new axioms to establish additional axioms. The process is repeated in a stepwise manner to build an increasingly complex base of knowledge, one which is always supported by observed facts, or more generally, empirical data.

2.3.6. A non-justificationist theory of science.

Since Descartes and Bacon, two key paradigms in the philosophy of science that can be considered critical of previous philosophies would come to dominate our understanding of the scientific method, the critical rationalism of Karl Popper (1957, 1966, 2003, 2014) and the classical American pragmatism of John Dewey and William James. Along with Bunge, they all espoused a non-justificationist view of knowledge claims. The key points to elaborate in these philosophies pertain to the scientific method and knowledge claims to the truth, or broadly to objective knowledge, and the picture that emerges about the nature of knowledge. Critical rationalism and its key analytic probe, the falsifiability criterion, are situated within a brief discussion of the birth and evolution of the scientific method during the Scientific Revolution and through the Enlightenment age up to modern times. Attention is given to the essence of the

scientific method, and its relationship to the Enlightenment ideals of liberalism, what the thesis calls core liberal values.

2.3.6.1. Critical rationalism.

Critical rationalism is an epistemological philosophy advanced by Popper in The Open Society and its Enemies (2013), The Logic of Scientific Discovery (2002), Conjectures and Refutations (2014), The Myth of the Framework (2014), and Unended Quest (2005). Popper considered that the strongest motivation for scientific discovery was the search for truth, and sought to determine how truth can be ascribed to scientific knowledge claims. Popper's philosophy of science and political philosophy is anchored in his critical rationalism and its key concept of falsifiability, that one can only criticize knowledge claims not positively verify them or rationally (in the classical sense) justify them.

A scientific hypothesis must be falsifiable. According to the falsification criterion, only tentative refutation or criticism can be made to support claims about the truthfulness of attained knowledge; knowledge claims can only be verified indirectly, by pointing to outcomes of an experiment that conflict with predictions deduced from the hypothesis. An unlikely theory that conflicts with current observation and is thus false (e.g., all swans are white) is considered to be better than one which fits observations but is highly probable (e.g., all swans have a color). The logic is that it is better a theory can be shown to be wrong and we know it than presumed right and we do not know it (Marsh, 1994). In that sense, the utility of the scientific method is that it gets us closer to the truth.

For Popper, the truthfulness of knowledge claims cannot be justified through pure reason or through empirical induction (shown to be illogical by Hume) or verified by the positivist

empiricist approach of logical positivists. Deductive reasoning is circular since the premises already contain the claim of the conclusion. Hume had shown that inductive reasoning is illogical, since "it requires inductive reasoning to arrive at the premises for the principle of inductive reasoning, and therefore the justification for inductive reasoning is a circular argument" (1748/1902). Verificationism holds that a statement must, in principle, be empirically verifiable for it be both meaningful and scientific. Popper argued that with their verificationism doctrine logical positivists had mixed two different philosophical problems, that of meaning and that of demarcation. For Popper, falsifiability is the suitable criterion of demarcation of science; and while falsificationism is only concerned with meaningful statements, non-falsifiable statements are not necessarily meaningless.

2.3.6.2. Empirical pragmatism.

For logical positivists, scientific knowledge provided a literal description of objective fact and excluded lived qualitative experience as providing access to the natural world. "Nature as objectified justified nature as an object of value-free human manipulation" (Rosenthal & Buchholz, 2000A, p.38). The mind-matter split implicit in the traditional understanding of scientific study is illusory. For the pragmatist, humans are within nature not outside of it and causally linked to it. Humans are active, creative agents who through meanings help structure the objects of knowledge and who thus cannot be separated from the world known (Rosenthal & Buchholz, 2000A). John Dewey used Heisenberg's principle of intermediacy to argue, "what is known is seen to be a product in which the act of observation plays a necessary role. Knowing is seen to be a participant in what is finally known" (Dewey, 1984, p. 163). Human activity partially constitutes the nature people experience. For pragmatism,

> with its emphasis on broad empiricism and ontological emergence, both facts and values emerge as wedded dimensions of complex contexts which cannot be dissected into atomic bits. The entire fact-value problem as it has emerged from the past tradition of moral philosophy is misguided from the start. (Rosenthal & Buchholz, 2000A, p.46)

Empirical pragmatism (Dewey and James) can be understood to integrate the basic insights of empirical and rational thinking. Empiricism can be understood as the view that all knowledge has its source in sensory experience (Talisse & Aikin, 2008)--all hypotheses must be tested against observations of the natural world rather than resting solely on a priori reasoning, intuition, or revelation. For pragmatism, the end of action is satisfaction and adjustment. Pragmatists are generally concerned with how to make actions more successful (Talisse & Aikin, 2008). Pragmatic theories are rooted in Peirce's pragmatic maxim, which is the starting point for clarifying the meanings of difficult concepts within pragmatism, such as truth, belief, certainty, and knowledge, in viewing them as outcomes of an inquiry:

> Consider what effects that might conceivably have practical bearings you conceive the objects of your conception to have. Then, your conception of those effects is the whole of your conception of the object.

Pragmatism's alternative to knowledge justification (fallibilism) is inquiry. A pragmatic theory of knowledge is concerned with the utility of knowledge, as opposed to its truthfulness. For Dewey (1938/2018), truth or knowledge (warranted assertions) are the outcome of a problem-solving inquiry: "The best definition of truth from the logical standpoint which is known to me is that by Peirce."

> The opinion which is fated to be ultimately agreed to by all who investigate is what we mean by the truth, and the object represented in this opinion is the real [CP 5.407]. (Dewey, 343 n).

In *Logic: The Theory of Inquiry*, Dewey (1938/2018) gave the following definition of inquiry: "Inquiry is the controlled or directed transformation of an indeterminate situation into one that is so determinate in its constituent distinctions and relations as to convert the elements of the original situation into a unified whole" (p. 108). Instrumentalism is the view that the point of scientific theories is to generate reliable predictions. For Dewey the utility of a theory is a matter of its problem-solving power. According to Dewey's constructivist philosophy, humans construct knowledge and meaning from their experiences: Knowledge is subjective and contextual, more precisely, intersubjective, and the viability of beliefs trumps their truthfulness. The notion of knowledge as justified true belief is thus rejected in favor of a more pragmatic approach to knowledge claims--a non-justificationist view of scientific knowledge claims. Dewey's constructivism is an epistemological theory according to which knowledge is not a description of an independent nature or reality, but a construction, the outcome of interactions between a system and its environment. His theory of knowledge accounts for both the subjective (individual) and intersubjective (sociocultural) dimensions of the construction of knowledge. For Dewey (1912, p. 23), perception is a temporal act, a process of choosing.

> Dewey's 'transactional realism' (Sleeper, 1986) locates the act of construction (of objects) in the organism-environment transaction, and it is precisely because of this that Dewey is able to circumvent the (epistemological) choice between idealistic construction and realistic representation. (Biesta & Vanderstraeten, 1997, p. 3)

Since the activities of the organism are a constitutive element of the constructed objects, this suggests that every organism constructs its own reality, implying that "Dewey can only reconcile constructivism and realism at the cost of a radical and fundamental subjectivism" (p. 3).

Popper contrasted his critical rationalism with uncritical or comprehensive rationalism or the justificationist view that only what can be proven by reason or experience should be accepted as scientific knowledge (Wettersten, n.d.). Popper's fallibilism holds that though theories (bold conjectures or guesses) could never be positively justified, they may still be rationally accepted provided repeated attempts to falsify them have failed. Fallibilism is the general idea that propositions concerning empirical knowledge can be accepted even though their truthfulness cannot be proven with certainty. Empirical pragmatism holds that general view of knowledge (i.e., Pierce's pragmatic fallibilism and Dewey's and James's instrumentalism)--all beliefs and theories are best treated as working hypotheses which may need to be refined, revised, or rejected in light of future inquiries. This pragmatic orientation to knowledge claims can be seen in Bunge's philosophy of science, where fallibilism is seen is his use of systems or frameworks.

The scientific method as understood today retains its essence as an exercise in human agency (as opposed to religious doctrine) and its purpose to discover the truth--and although it is doubtful the scientific method can ever generate immutable truths (or that we would know it, since the observer constructs knowledge intersubjectively from sensory inputs, based on past experiences), it can still be useful in generating useful knowledge and testable hypotheses used in making predictions about future events. Scientific knowledge claims are tentative, subject to continuous testing or verification by observation and experimentation.

There are scientific method principles, and there is the process of the scientific method. The scientific method principles involve careful, skeptical observations, formulating hypotheses based on the observations via induction, experimental and measurement-based testing of deductions drawn from the hypotheses, and refinement or rejection of the hypotheses based on experimental findings. Applying scientific method principles is a philosophical angle related to justificationist and positivist verification claims to knowledge. According to the justificationist view, only what can be proven by reason or experience should be accepted as truth. Positivist verificationism says the truth of knowledge claims can be verified by positivist empirical testing or observation, and it stands in opposition to Popper's falsifiability approach, which says whether by reason or through observation or measurement, no certainty can ever be made about the truthfulness of knowledge claims--the best you can do is to make a tentative judgement. The iterative process in the form of steps of the scientific method can be thus outlined: Define a question, Gather information and resources, Form an explanatory hypothesis, Test the hypothesis by performing an experiment and collecting data in a reproducible manner, Analyze the data, Interpret the data and draw conclusions that serve as a starting point for new hypotheses, and Publish the findings/results.

2.3.7. Scientific method and trust.

The philosophy of human knowledge (epistemology) includes views on empiricism, rationalism and skepticism. While philosophical skepticism is an approach that questions the possibility of certainty in knowledge, methodological skepticism is an approach that subjects all knowledge claims to scrutiny to sort out true from false claims. Religious skepticism can be understood as a form of philosophical skepticism. For Tillich (2001, *Dynamics of Faith)*, doubt

is an element of faith. Those who commit their lives and themselves to a great cause or notion, an "ultimate concern," have to live with a nagging doubt, an existential doubt, whether they have made the right choice in life--whether this ultimate concern of theirs (e.g., a religion) is the real deal, the truth, or whether they are fooling themselves or wasting their lives. Tillich says those who decide to accept a religion as true are taking a risk, "the risk of faith." It is because they have doubt ("existential doubt") that they are able to perform this act of faith (i.e., take a risk). There is always the risk of faith because of existential doubt: Is it really worthwhile? Attitudinal doubt, Tillich says, exists when someone is despairing or cynical of the truth to the point that they become indifferent to finding it.

A scientific society accepts uncertainty as a sociocultural political value in analogy to how scientists accept uncertainty about the truthfulness of knowledge claims derived from scientific inquiries, that is, methodological skepticism. Trust can be understood as a subset of risk, as risk accepting--more specifically, trust can be defined as acceptable uncertainty or acceptable vulnerability. A ST society is accepting of political risk, which is a form of trust. According to Hofstede's (1980, 2001) National Culture 6-D Model, Canada and western nations generally score on the lower end of the Uncertainty Avoidance dimension.

Scientific method and an open society: The open system as a biological metaphor is a form of scientific (analogical) reasoning. Open systems (as biological systems) are non-deterministic and change (adapt) in response to a changing environment.

Scientific method and uncertainty and innovation: The key step in applied (methodical) creative thinking is the suspension of judgment about the likelihood or rationality of explored or imagined ideas during brainstorming for solutions to a stated problem (e.g., the Simplex applied creativity model by Basadur, 1998).

Scientific method and uncertainty and critical thinking: A non-critical thinker would decontextualize information from human agency, that is, ignore the constitutive role of values/interests/emotions in constructing knowledge. Such reasoning (seen in logical positivism) was rejected by non-justificationist views of knowledge claims. For the pragmatist, one cannot extricate fact from value within knowledge claims. A critical thinker understands that knowledge is socially constructed, technology is socially constructed, and "the scientific method" likewise is socially constructed and provisional.

Scientific method and security testing: Information security testing and the scientific method have two nascent streams. One is more academically oriented focusing on the systemization of knowledge (e.g., Herley & Van Oorschot, 2017, 2018; Van Oorschot, 2017), and the other stream more practice oriented focusing on the science of security (e.g., Riley, 2014B). Two key concepts are involved, applying scientific method principles (about what the scientific method entails--its logic, its underlying philosophy of knowledge), and systematization which aims to organize or standardize a body of knowledge to make it more amenable to collaborative use, peer review, and development.

Inductive and deductive reasoning: An experiment is conducted to determine whether observations agree with or conflict with the predictions of a hypothesis (Popper, 2003). If the results of an experiment confirm the predictions made by a hypothesis, the hypothesis is deemed more likely to be correct but remains suspect, subject to further testing. If over time a hypothesis becomes well supported, a general theory may be developed. Inductive reasoning involves trying to find a pattern in data or measurements to infer a hypothesis. Inductive inferences have observations as premises and theories as conclusions. The key skill related to inductive reasoning is the detection of patterns in data or behavior, which is helpful when the security researcher is

trying to discover new vulnerabilities. Deductive reasoning involves using an axiom or a general rule to compute the value of an unknown variable, or testing the agreement of test results against a hypothesis.

2.3.8. Scientific method design principles.

These principles inform ethical design principles for ethical hacking teaching practices in higher education and for ethical governance of hacking technologies use in society. Ethical design means designing systems of knowledge making should be carried out following the scientific method. A scientific method to generate knowledge should be,

1. Pragmatic: efficient and fair based on risk-benefit and/or cost-benefit analysis incorporating key societal sectors (knowledge users/technology exploiters) values/interests and facts (collaborative) throughout the project (from setting goals to knowledge sharing and exploitation);
2. A problem-solving inquiry that seeks useful and practical knowledge/solutions to real world problems;
3. A valid method (produces “truthful” knowledge) subject to continuous verification and modification;
4. Skeptical--hence creative/innovative, and critical (knowledge is socially constructed and provisional);
5. Based on or incorporates scientific method principles, hence methodical (quality assurance is built in the process) and systematic (standardized process to achieve maximum clarity and to facilitate collaboration and peer review);

6. Iterative to continuously incorporate the latest social and scientific discoveries, understandings, technologies, or paradigms; and to ensure method validity;
7. Transparent as a proxy for justification of knowledge claims, to counter researcher bias, and to help verify method validity (e.g., through reproducibility)--through publication, and generally sharing of knowledge;
8. Communal (e.g., communities of practice as a knowledge management approach) to incorporate the values and interests (hence buy-in) of the research community and the broader community of knowledge or technology users in the design and decision-making process; to produce useful/viable knowledge (since knowledge is intersubjective); to be inclusive (hence fair); and to reduce equivocality about the meanings and value of produced knowledge (hence reduce the risk of hacking);
9. Collaborative to produce common objective knowledge;
10. Explicit about sociopolitical values inscribed into technology design to reduce equivocality and the risk of hacking crime, and as a liberal counter-threat sword;
11. In tune with the nature and needs of society as an open, scientific, knowledge-making ST system.

2.3.9. Ethical design principles.

STEI-KW can be used to derive guidelines or insights to incorporate in designing ethical ST processes (incorporating social engineering, including nudging, and management science concepts, including from scientific method design principles), that is, the EDP-STEI-KW framework. A ST society as framed in this thesis is an open, scientific, knowledge-making society concerned with self-governance. EDP-STEI-KW: Ethical design principles for ethical

hacking education and for ethical governance of hacking technologies use in a ST society (used in conjunction with Table 5: STEI-KW and Society). EDP-STEI-KW incorporates scientific method design principles in the design process. It is a framework to help analyze/design societal teaching practices and governance of hacking technology use to improve cybersecurity governance at individual, organizational, and social levels.

Ethical design principles for ethical hacking teaching practices in higher education.

Ethical design means ethical hacking teaching practices are designed to address societal needs--in tune with social properties (society's nature): Open, scientific, knowledge-making society concerned with self-governance.

1) Open ST society

Open society (Popper, 1966) and open technologies (open technological ontologies, Bunge, 1966, 1975, 1977, 1998).

Open values (core liberal values): Reason, skepticism and science, and liberty. (Technology as value/open technological ontologies.)

2) Scientific behavior and underlying values/ethics

Trusting behavior and underlying scientific method values:

Two key concepts are involved, applying scientific method principles (about what the scientific method entails--its logic, its underlying philosophy of knowledge), and systematization which aims to organize or standardize a body of knowledge to make it more amenable to collaborative use, peer review, and development.

Scientific method and trust: A scientific society accepts uncertainty as a sociopolitical value in analogy to how scientists accept uncertainty about the truthfulness of knowledge claims

derived from scientific inquiries, that is, methodological skepticism. Trust can be understood as a subset of risk, as risk accepting--more specifically, trust can be defined as acceptable uncertainty or acceptable vulnerability.

Scientific method and uncertainty and innovation: The key step in applied (methodical) creative thinking is the suspension of judgment about the likelihood or rationality of explored or imagined ideas during brainstorming for solutions to a stated problem (e.g., the Simplex applied creativity model by Basadur, 1998).

Scientific method and uncertainty and critical thinking: For the pragmatist, one cannot ontologically extricate fact from value within knowledge claims. A critical thinker understands that knowledge is socially constructed, technology is socially constructed, and "the scientific method" likewise is socially constructed and provisional.

3) Knowledge-making behavior and underlying values/ethics

As per STEI-KW, constructed knowledge is interdisciplinary, empirical pragmatic ethical decision making is "democratic"--broad based, multi-stakeholder, multi-perspective, incorporating multi-disciplinary research, from a systems perspective, whereby the values/ethics of key societal sectors/key stakeholder groups are incorporated into decision making at every step of the innovation process; further, values and ethics are a key design consideration of "technology"--broadly understood to include knowledge construction and knowledge management processes.

Empirical: Hands on or practical exercises.

Empirical pragmatic: Constructivist problem-solving inquiry approach; personal experience in learning.

Pragmatic: Practical, useful skills/knowledge from the perspectives of learners, business/industry, government, higher education, and civil society; the broad social (ethical, legal) consequences of misusing hacking technologies/skills, prevention, and mitigation beside vulnerability discovery.

Are social values/ethics explicit?

Are there formal understandings (consistency in the use of terms)?

Ethical design principles for governance of hacking technologies use in society.

Ethical governance means risk assessment and risk mitigation measures are designed to address societal needs--in tune with social properties (society's nature): Open, scientific, knowledge-making society concerned with self-governance.

- Governance: A process for policy decisions, to steer society as a whole, and for maintaining the system's identity. Accountable to the public.
- Key stakeholder groups/societal sectors involved in governance of hacking technologies use: Business/industry, government, higher education, and civil society (the public).
- Key social values to include in knowledge management (core liberal values in relation to information security): The right to the security/privacy of personal and privileged information; freedom of conscience/expression; freedom from undue political or political economic oppressive restriction, that is, protection of personal liberties.
- Canadian governance values: Trust, open knowledge, transparency in decision making, security/privacy, human rights (Canada's Digital Charter: Trust in a digital world); Equity, Diversity and Inclusion (EDI) in Research (Frontiers in Research Fund); democracy, innovation (Innovation, Science and Economic Development Canada); Transparency of

government spending and operations, open government, accountability (Treasury Board of Canada Secretariat)

- Corporate IT/IA governance values: Security-by-design (DevSecOps software development), privacy-by-design, iterative development process, agile SDLC, risk-based management (RMF).

Sociotechnical design: Security and privacy by design.

Piecemeal social engineering (Popper, 1966) strategies can be applied using the scientific method to analyze social systems in order to design the appropriate methods to achieve the desired results in the human subjects. Nudges can be used to influence social behavior without coercion, through positive reinforcement or environmental cues. One key tactic involves default settings which can be used to shield citizens from digital surveillance (when set to opt in rather than opt out of push notifications and geolocation services).

2.3.10. Weick's sensemaking model.

Weick's sensemaking model (1969, 1979, 1995, 2005; Weick, Sutcliffe, & Obstfeld, 2005) is a communication theory of knowledge making, the social construction of knowledge. Epistemological roots of sensemaking theory can be linked to phenomenology (broadly concerned with the subjectivity and intersubjectivity of human experiences) and general systems theory (broadly concerned with complex cybernetic systems). Two key concepts are, sensemaking happens as a result of iterative communication exchange between communication actors within an environment, and explicitness in communication (iterative communication cycles that turn tacit knowledge into explicit knowledge) improves the efficiency of the

sensemaking process, that is, it reduces uncertainty in the information environment. Equivocality is “the engine that motivates people to organize” (Sutcliffe & Obstfeld, 2005). Reducing equivocality (unpredictability) in the information environment happens through reducing uncertainty resulting from variances in perceptions among stakeholder groups (communication actors) through communication interaction opportunities to construct common knowledge/understandings. Interpersonal interaction among participants to construct common knowledge is the most effective way to reduce equivocality. Sensemaking is the process by which people give meaning to an experience. The point of sensemaking is to reduce equivocality. Participants organize processes of information exchange to make sense of equivocal information during which the meanings of terms and events are negotiated. The end product of sensemaking is common knowledge.

Human organizations engage in information processing to reduce equivocality of information. Through sharing information, participants jointly make sense of reality by reducing equivocality. Sensemaking describes how information is exchanged and processed between communication actors through interaction and iteration. Sensemaking involves three key strategies, enactment, selection, and retention of information. Sensemaking is relevant to new information (e.g., during learning) where uncertainty about meanings is introduced into an environment (Weick, 1995). In enactment, in equivocal environments in organizational systems, for example, an observer brackets interpretations of an event or message, building on past personal experiences and taking cues from their environment, then selects an interpretation (makes sense of the information) and then solidifies a meaning with time through iteration and interaction with others (feedback corrects or changes meanings). Human organizations exist in an information environment. A university or a classroom can be seen as an information

environment. Equivocality then is a problem of confusion not of ignorance. The remedy is to interact with others in the information environment in ongoing communication opportunities--behavior cycles (ongoing interpersonal interaction), or less preferably, assembly rules (written text); through social interaction and iteration the ambiguity of information is reduced, that is, common knowledge is socially constructed. Sensemaking it is a process of social construction of meanings, it is both subjective and intersubjective. Sensemaking starts with noticing and bracketing, is about labeling, is retrospective, is about presumption, is social and systemic, is about action, and is about organizing through communication (Weick, 1969, 1995).

2.4. Chapter Conclusion

This chapter covered two areas. "Part 1: Information Security Risk Governance" covered the technical, theoretical, and regulatory context of ethical hacking applications in information security testing and governance at the organizational and state levels. The key concepts relating to information security risk management and governance were explained. Information security was defined in relation to IT security, IA, and IT governance frameworks. Key concepts surrounding information security risk were explained. "Part 2: Theoretical Framework" covered the theoretical framework (STEI-KW), its epistemological roots, and how it was applied in the thesis. Bunge's (1979) systemism and Popper's (1966) Open Society theories were explained, then Bunge's (1975, 1977, 1999) conception of sociotechnology or social technology was discussed within the STS SCOT tradition (Quan-Haase, 2016). A non-justificationist theory of science that underlies a constructivist epistemology of knowledge making was discussed. Then ethical design principles were synthesized drawing on a non-justificationist view of the scientific method and an empirical pragmatic liberal epistemology of knowledge making. Finally, Weick's

(1969/1979, 1995) sensemaking model as a constructivist theory of knowledge making was discussed.

Chapter 3: Method

3.1. Introduction

The qualitative exploratory case study approach (Creswell, 2003, 2007; Stake, 1995; Yin, 1994, 2003) was followed to explore ethical hacking teaching practices in two Canadian universities as the case studies in focus. This chapter first addressed the research design and its suitability for addressing the thesis research questions. The research questions (RQs) were stated and linked to the theoretical framework (STEI-KW) and the topic of ethical hacking in society (see Table 8: RQs, Data Collection, and Theoretical Frameworks). Next, the rationale for the selection of the case studies, and the sampling strategy and criteria were addressed. Data collection and analysis procedures were then presented and followed by an explanation of the coding and analytic strategy. Finally, the methodology reliability and validity protocols were discussed.

3.2. The Case Study Methodology

Research design must address three concerns: Knowledge claims or theoretical perspectives, strategies of inquiry, and methods of data collection and analysis (Creswell, 2003, 2007). The thesis adopts a qualitative exploratory case study methodology using two Canadian universities as the case studies in focus. Qualitative research takes place in a natural setting which enables the researcher to develop a level of detail about the place or individual and to be involved in the experiences of the participants (Creswell, 2003; Rossman & Rallis, 1998). Throughout the "qualitative research process, the researchers keep focus on learning the meaning that the participants hold about the problem or issue, not the meaning that the researchers bring

to the research or writers from the literature" (Creswell, 2013, p. 47). A pragmatic knowledge claim to qualitative research is pluralistic and problem-centred, and is concerned with consequences of actions and real-world practice (Creswell, 2003). Two approaches are suitable for pragmatic research: Experimental and case study (Yin, 2003). Case studies allow researchers to explore a program, event, activity, process, or individuals in depth (Creswell, 2003). A case study deals with contextual variables and relies on multiple sources of evidence. It can be thought of as a comprehensive method, covering the logic of design, and data collection and analysis techniques. A case study,

> is an empirical inquiry that investigates a contemporary phenomenon within its real-life context, especially when the boundaries between phenomenon and context are not clearly evident. (Yin, 2003, p. 13)

Case analysis is a particularly appropriate method for the investigation of systems explanations of organizational functioning (Miller, 2009). It aligns with STEI and with Weick's sensemaking model in their systemic and pragmatic theoretical orientation regarding data collection and analysis, including triangulation via data derived from multiple stakeholder perspectives and the centrality of context and personal experience as sources of knowledge. The qualitative case study methodology is well suited for capturing the unique complexities of a single case (Stake, 1995), when the study focus is on operational links rather than on frequencies or incidences, when little control over events is expected, and when the focus of the study is on contemporary phenomena within a real-life context (Yin, 1994).

The qualitative exploratory case study methodology is particularly appropriate when there is a scarcity in the literature on the subject (Stebbins, 2011). Case study research is suitable to "either develop an in-depth understanding of a single case or explore an issue or problem

using the case as a specific illustration" (Creswell, 2013, p. 97). In a single instrumental case study (Stake, 1995), the researcher "focuses on an issue or concern, and then selects one bounded case to illustrate this issue" (cited in Creswell, 2013, p. 99). The thesis followed the instrumental case study approach.

3.3. Methodology Rationale

The case study (Stake, 1995; Yin, 1989) qualitative research method examines in depth purposeful samples to study a phenomenon such as ethical hacking. It exemplifies the researcher preference for depth, detail, and context, often working with smaller and more focused samples in comparison to the large samples of primary interest to statistical researchers. Exploratory research is suitable for problems or phenomena that are in the formative stages to help clarify primary issues surrounding the problem or to establish priorities, clarify trends or map a field and develop operational definitions (Shields & Rangarjan, 2013).

Qualitative research is iterative and adjustments and changes are a natural part of qualitative work. The qualitative researcher uses reasoning that is multifaceted and iterative "with a cycling back and forth from data collection and analysis to problem reformulation and back" (Creswell, 2003, p. 183). Qualitative research involves "an emergent and evolving design rather than tightly prefigured design" (Creswell, 2013, p. 46).

> The research process for qualitative researchers is emergent. This means that the initial plan for research cannot be tightly prescribed, and that all phases of the process may change or shift after the researchers enter the field and begin to collect data. (Creswell, 2013, p. 47)

3.4. Revisions and Justification for Revisions

Two key changes during the thesis development are notable. After the third interview, the RQs were revised and the theoretical lens for examining communication/pedagogical practices for the two case studies was substituted. In light of the fact that it became evident through the course of data collection that there are significant differences between interview participants and within literature about foundational concepts (definitions) regarding the meanings, ethics, values, skills/knowledge, roles and responsibilities, and practices of ethical hacking and ethical hackers, the focus of the analysis shifted toward establishing foundational understandings and definitions for these foundational concepts (hence "what constitutes" rather than "what are"). Open coding was performed during a first pass through the data for these foundational concepts.

The researcher substituted Stafford Beer's (1972/1981, 1979, 1980, 1984, 1985) management cybernetics model, the viable system model (VSM), with Weick's (1969/1979, 1995) sensemaking model when he noticed while going through the data collection and analysis that 1) he was using the VSM the same way he was trained to use the sensemaking model--"information variety" (VSM) can be substituted with "variances in perceptions" (Weick) about what constitutes ethical hacking and hacking skills, and "instruction" (VSM) can be substituted with "underlying communication practices" (Weick); and 2) that the substitution helps give more analytical insight (and emphasis) by invoking the need to make tacit sociopolitical values explicit as part of the thesis analysis and recommendations. It would quickly become apparent from data collection that there were no "ethical hacking" courses per se taught in the two participating research institutions or in higher education in general--ethical hacking related topics (in information security testing) are dispersed across disciplinary areas in various information security curricula (the thesis focused on CS, CE, and SE programs). Hence the analytical focus

ought to be on how knowledge is constructed versus how information or knowledge flows through an educational system (see Table 12: Applying KW and VSM in Communication Analysis).

Beer (1985) famously argued that "cybernetics is the science of effective organization" (p. ix). Beer pursued the VSM "through neurocybernetics and social science, through the invention and study of cybernetic machines, through the mathematics of sets and stochastic processes, and at all times through the OR (operations research) fieldwork in industry and government." The quest came to be known as "how systems are viable; that is, how they are 'capable of independent existence'" (Hilder, 1995). Beer argued that viable or autonomous systems have an underlying optimal organization (a specific structure with five specialized functions within it that ensure its survival in a changing environment through the regulatory process of homeostasis). The VSM prescribes optimal human organization--at least it starts with a description of the necessary and sufficient cybernetic subsystems of a human system, and analogies can be drawn from there to other types of systems that include non-human agents. The VSM is very "versatile"--it allows for a lot of creative ways to be theorized and applied. Brain of the Firm (1972/1981), The Heart of Enterprise (1979), and Diagnosing the System (1985) together establish the theoretical foundations of the VSM and its applications in management cybernetics. Every viable system contains and is contained in a viable system (viable systems in recursion are homologous). The cybernetic model of any viable system is comprised of five necessary and sufficient subsystems (Operations, Coordination, Optimization, Development, and Valuation)—the "management cybernetics" of the system—interactively involved in any organism or organization capable of maintaining its identity in a changing environment. Internal

and external analysis is performed to identify the modes of behaviour (practices) and relationships that constitute viability.

Original RQs:

RQ1 What are the current ethical hacking teaching practices in higher education in North America?

RQ2 What are the current challenges to effective open source information security management practices in higher education in North America?

RQ3 What are the potential benefits and challenges of establishing a networked centre of excellence of ethical hacking communities of practice in higher education?

Revised RQs:

RQ1 What constitutes ethical hacking teaching practices?

RQ2 What constitutes hacking skills?

RQ3 What is the risk to society of teaching students hacking skills (risks vs opportunities)?

RQ4 How to mitigate the risk of students misusing the hacking skills learned in college or university later in life in criminal activities?

3.5. Sampling Strategy and Criteria

The interview participants were recruited by email with the aid of a formal recruitment letter and a consent agreement to participate in the research. In-depth, semi-structured interviews were conducted within a set time (1 hour) at various university campus locations or by phone. The interview sessions were audio recorded and the relevant parts transcribed for accuracy. Further, hand-written notes were taken during the interviews. The sampling criteria for the

interview participants were as follows: Each of the interviewed university experts in information security penetration testing and industry practitioners (those with experience practicing ethical hacking or hiring ethical hackers) had a minimum of one-year experience in information security testing teaching and practice in higher education and in the IT industry respectively; or participants had at least one year experience in information security or IT policy or policy analysis in academia. Interview participants were sought out for their expert knowledge in 1) scholarly research in ethical hacking education and practice; 2) current practices and trends in ethical hacking education and practice; and 3) organizational communication practices in ethical hacking education or industry experience in practicing ethical hacking or mentoring or training or hiring ethical hackers. The participating universities were chosen because the needed expert knowledge was found there.

3.6. Data Collection and Analysis

The theoretical framework (STEI-KW) guided data collection and analysis. Structural and behavioral analysis of society as a social system points to society as a liberal open society founded on the ideals of the Scientific Revolution and the Enlightenment. Open hacking technologies are the focus of the study. This is justified on two accounts, 1) since sociotechnology is understood as social technologies or social technological ontologies, open society is ontologically co-extensive with open technology (emphasizing the nature of technology as a social construct); hacking skills are ontologically coextensive with hacking technologies, hacking methodologies, hacking values, and so on; and 2) since the key structural property of a ST society as theorized in the thesis is its open nature, studying digital hacking technologies at the intersection of society and technology means focusing on open hacking skills

and open hacking technologies. Put differently, according to the STS approach, hacking technologies as socially constructed are understood to mirror the society that produces them (society is theorized as open, scientific, and knowledge making), hence the focus on open hacking technologies.

Data collection and analysis consisted of systematic literature reviews (Jesson, Matheson, & Lacey, 2011; Okoli & Schabram, 2010), organizational documentation of two Canadian universities, and in-depth interviews with 14 interview participants (in addition to one participant who contributed via email) comprised of university experts and industry practitioners of ethical hacking and policy experts. Numerous secondary resources were consulted including governmental and business/industry resources, policy reports, industry white papers, and many websites. For research questions 1-2: Systematic literature reviews and organizational documentation were conducted comprised of about 50 pages of organizational documents available on public web pages of two Canadian universities. For research questions 3-4: Narrative literature reviews were conducted augmented with input from RQ1 and RQ2 SLRs. For research questions 1-4: In-depth interviews (Jackson, Gillis, & Verberg, 2011) were conducted with university experts, industry practitioners, and policy experts. RQs 1 and 2 are addressed in the Findings chapter. RQs 3 and 4 are addressed in the Advanced Analysis chapter. RQ3 is addressed under technology assessment and Teaching vs Practice (the case studies), while RQ4 is addressed under the risk mitigation discussion (recommendations). (SLRs for RQ1 and RQ2 have informed RQ3 and RQ4. Rather than conducting SLRs for RQ3 and RQ4, the researcher opted to focus on extant government and business/industry research/reports of clear and direct relevance to the thesis, e.g., CSE's, 2018, cyber threat assessment report, and Kool et

al.'s, 2017, state of the art research on social digitization, its key technologies, and potential impacts on society.)

A systematic literature review was conducted for RQ1 What constitutes ethical hacking teaching practices? Four key themes emerged: Professional ethical hacking is legal, Ethical hackers are trustworthy, What do ethical hackers do? and An identity and legitimacy crisis. A systematic literature review was conducted for RQ2 What constitutes hacking skills? Three key themes emerged: Steps of the penetration testing process, Open source penetration testing methodologies, and The penetration test report. Contribution to knowledge of RQ2 was delineated by the theoretical framework and focused on open/open source technologies. Further, RQ2 (hacking skills/knowledge) was subordinate to RQ1 (i.e., "who are ethical hackers and what do they do" included a synthesis of a foundational framework/profile for professional ethical hacking practitioners--the meanings, ethics, values, skills/knowledge, roles and responsibilities, and practices). A narrative literature review was conducted for RQ3 (risk assessment) focusing on pragmatic technology assessment using STEI-DMG, which is concerned with the ethics of teaching students hacking skills or the ethics of using hacking technologies in ethical hacking teaching practices in higher education (weighing opportunities against threats) invoking the precautionary principle (the risk of not teaching students hacking skills). Are the teaching practices in tune with societal needs and incorporate the interests/values of key societal sectors/stakeholder groups? Open coding was performed during a first pass through the data for what constitutes ethical hacking teaching practices. Coding coalesced around three main themes that are discussed within the broader Teaching vs Practice cybersecurity skill gap context: Teaching ethical hacking skillset, Pedagogy as Communication, and Technology Assessment: An Integrative Approach. A narrative literature review was conducted for RQ4 (risk mitigation)

focusing on S&T innovation initiatives. Applying EDP-STEI-KW to advise ethical design of ethical hacking teaching practices pointed to (recommendations) the role of OSINT Analyst, a novel cybersecurity role synthesized to meet the needs of society, and the foundation framework of a body of knowledge for the role. Applying EDP-STEI-KW to advise ethical governance of using digital hacking technologies in higher education and in broader society pointed to (recommendations) the professionalization of ethical hacking as an occupation/the licensing of professional ethical hacking practitioners, and to a public policy initiative comprised of a networked centre of excellence of ethical hacking communities of practice as a research and governance approach and the policy innovation decision making framework of SSP-DMG.

Organizational documentation consisted of 50 webpages concerning program course requirements and course descriptions of undergraduate courses in CS, CE, and SE programs (3 credit) courses taught in English for 2019-2020 at the two participating higher education institutions. Online course descriptions at the two participating research institutions were surveyed for technical and social hacking skills focusing on network penetration testing high-level concepts. Courses not directly teaching computer network skills were excluded from the analysis (courses with “security” or “secure” in their title were retained for examination given their direct relevance). Finally, the study focused on courses cross-referenced between the two participating universities. Program requirements for CS/CE/SE majors were examined for required courses in technical hacking skills and social hacking skills, the latter includes ethics and social science. Further, two courses were closely examined: The syllabus for a computer systems security course and the syllabus for a professional practice course for insights into communication practices (pedagogy as communication) and insights into what constitutes

professional practice. See Organizational Document Review. Finally, bachelor degree programs in CS/CE/SE disciplines were surveyed for inclusion of security majors/specializations.

Organizational Document Review

University 1 ~25 webpages	University 2 ~25 webpages
1. Ethical hacking skills in CS/CE/SE curricula: Technical and social hacking skills focusing on network security penetration testing: 1.1. Course descriptions (e.g., technologies/methods of intelligence gathering esp. using AI, including OSINT, network enumeration, and port scanning; and cyberspace and network protocols, classes of attacks, and best practices--e.g., identity and access management. 1.2. Program requirements (a holistic view of what is taught--ethics, scientific and sociopolitical values). 2. Professional practice courses	1. Common courses teaching networking skills. 2. Pedagogy as communication: A common course (a computer systems security course) was examined for variances in perceptions in knowledge and opportunities of common knowledge making.

In-depth, semi-structured interviews were conducted with 14 interview participants (in addition to one participant, PPT15, who contributed via email) between December 7, 2018 to

April 15, 2019: Four ethical hacking university experts, four ethical hacking industry practitioners, and six policy experts (see Interview Participants by Area of Expertise). In-depth interviews are typically done "to solicit people's descriptions and explanations of events taking place in their own environment" (Eid, 2011, p.10). Advantages of conducting in-depth interviews include more researcher control over the line of questioning, and the ability to obtain historical and primary information (Creswell, 2003). In-depth interviews allow researchers to collect the respondents' perceptions of their world. Interview quotations are used to illustrate key analytical points. Combining in-depth interviews with a document review enables the capturing of explicit as well as tacit knowledge surrounding organizational practices.

Interview Participants by Area of Expertise

Teaching:	Practice:	Policy experts (6)
Four university experts who teach ethical hacking (penetration testing) PPT3: University Professor of Computer Science and Software Engineering PPT8: University Professor of Computer Science PPT14: University Professor of Computer Science PPT15 (via email): University Professor of Computer Science and Software Engineering	Four industry practitioners who practice ethical hacking (penetration testing) or hire ethical hackers PPT11: Security Consultant with over 20 years of experience in ethical hacking/information security testing and management with the federal government and in the private sector PPT6: Sr. Business Support Analyst with a global leader in software security and business intelligence services (Big Data and CRM, Big Data and Security) PPT12: Security Expert with over 10 years of experience in ethical hacking/information security testing and management with the federal government PPT9 (American context): Security Professional with a global financial institution	PPT4 PPT5 PPT7 PPT13 PPT2 PPT10

3.7. Coding and the Analytic Strategy

Data analysis involves systematically organizing, integrating, and examining data, searching for patterns and relationships in the details. The "recursive process of analysis begins immediately with the first data-collection episode and continues throughout the study" (Jackson, Gillies, & Verberg, 2011, p. 242). "To analyze, we connect particular data to concepts, advance generalizations, and identify broad trends or themes. Analysis allows us to improve understanding, expand theory, and advance knowledge" (Neuman, 2011, p. 341). After coding, concept building, and emergence of key themes, analytic strategies are applied for the analysis of the data--strategies that link data to theory. In qualitative research, coding or "concept formation is an integral part of data analysis and begins during data collection"--conceptualization is a way to organize and make sense of data. The research questions provide a guide but the data analysis process often leads to new questions. Theory is used to interpret the findings (Neuman, 2011, p. 344). Data analysis means making conceptual connections of the data or searching for patterns in the data. "Once you identify a pattern, you need to interpret it in terms of a social theory or the setting in which it occurred. This allows you to move from the particular description from a historical event or social setting to a more general interpretation" (Neuman, 2011, p. 351).

Data coding was performed against the theoretical propositions (Yin, 1994) of STEI-KW. The illustrative pattern matching method (Neuman, 2010) was applied as the analytic strategy. The illustrative method anchors or illustrates theoretical concepts with empirical evidence. It applies theory to a concrete social setting and organizes data based on theory. "Preexisting theory can provide conceptual empty boxes that you fill with the empirical evidence" (Neuman, 2011, p. 353). In the pattern matching variation of this analytic strategy, patterns or concepts identified in the case studies are matched to those derived from theory.

Open coding was performed during a first pass through the data for the ethics, values, meanings, skills/knowledge, roles and responsibilities, and practices of professional ethical hackers and ethical hacking. The interviews were transcribed first, and two coding tables were created--Table 9: Hacking Skills Coding Table (Network Penetration Testing) and Table 10: Professional Ethical Hackers Coding Table. Open coding themes from the interviews, the literature reviews, and organizational documents were extracted and incorporated in the coding tables.

3.8. Reliability and Validity

Reliability and validity are concepts that address the truthfulness, credibility, or believability of findings (Neuman, 2010). Reliability refers to the replicability of a researcher's results–the extent to which another researcher can make similar observations under identical or very similar conditions (Creswell, 2003; Neuman, 2010; Stake, 1995; Stebbins, 2002; Yin, 1994). Reliability means dependability or consistency (Neuman, 2010). Researchers must be consistent in how they make observations; for example, through the use of explicit interview questions and research procedures (Neuman, 2010; Yin, 1994). Validity in exploratory research (credibility or trustworthiness) refers to whether a researcher can gain an accurate impression of a group, a process, or an activity, and how so (Stebbins, 2002). Validity suggests truthfulness. It refers to "how well an idea 'fits' with actual reality"; or "how well we measure social reality using our constructs about it" (Neuman, 2011, p. 175). Qualitative researchers are more interested in achieving authenticity than in realizing a single version of Truth (Neuman, 2010). Authenticity means, "offering a fair, honest, and balanced account of social life from the viewpoint of the people who live it every day" (Neuman, 2011, p. 181). Reliability requires

clarity about the followed procedures of data collection, analysis, and interpretation to ensure consistency. Hence researchers are encouraged to develop a case study protocol, keep an organized case study database, and maintain a chain of evidence (Yin, 1994). Reliability also requires clarity on the logic linking the data to the research propositions or questions, the operational measures used for the concepts or theories, and the criteria used to interpret the data (Yin, 1994). The thesis enhanced the reliability of the research methodology by providing details about the participant recruitment process, the data collection methods (the interviewing process and interview questions, as well as documentation gathering), and data analysis.

Saturation is a popular strategy for the trustworthiness of findings. Data saturation or information redundancy is the point at which no new themes or codes emerge from data. The researcher did not find it helpful to "operationalize" the concept of saturation to determine a priori the number of interview participants that would be sufficient to achieve coding reliability that somehow faithfully reflects the facts out there--as this presumes the researcher is not an active agent who interacts with the data subjectively and intersubjectively to construct knowledge that reflects "facts" inextricably mixed with values and interests. I agree with Braun and Clarke (2019) that while the concept of data/thematic saturation is "coherent with the neo-positivist, discovery-oriented, meaning excavation project of coding reliability types of TA," it is not consistent with the values and assumptions of reflexive thematic analysis. I agree with them that researchers using reflexive thematic analysis ought to "dwell with uncertainty and recognise that meaning is generated through interpretation of, not excavated from, data, and therefore judgements about 'how many' data items, and when to stop data collection, are inescapably situated and subjective, and cannot be determined (wholly) in advance of analysis." The researcher's approach to thematic analysis/to capture patterns of meaning across datasets was

reflexive, probably a mix of following a deductive way where “coding and theme development are directed by existing concepts (STEI-KW guided data collection and analysis) and, more importantly, following a constructivist way. A constructivist approach puts emphasis on sociocultural context and on personal experience as sources of knowledge. For the researcher, saturation as a milestone in data collection and analysis has to do more with self-awareness than with correspondence to facts or reality. The researcher does not believe they went out there and discovered the facts; rather, the researcher interacted with the data and interpreted it based on the researcher’s experiences in life and the broader social totality that shapes the researcher’s views and values.

The theoretical framework STEI-KW guided data collection and analysis. Further, the researcher’s past work and experience on the topic of ethical hacking helped them identify key themes. Systemism (Bunge, 1979) instructs that the proper study of society is “the study of the socially relevant features of the individual as well as the research into the properties and changes of society as a whole” (p. 14) and hence pointed the researcher to the need to understand the professional attributes of ethical hacking practitioners. The researcher went into the interviews searching for insights about the socially relevant features or professional attributes of ethical hackers that can serve as a basis for sketching out a professional practice profile--the meanings, ethics, values, skill/knowledge, roles and responsibilities, and practices, as open coding elements. Further, the researcher went into the data collection interviews looking for “ST hacking skills”--that is, for technical hacking skills and social hacking skills as two broad categories or themes when discussing ethical hacking technology use/teaching practices.

3.9. Data Validation Protocols

Method validation protocols include: 1) Triangulation of measure (Neuman, 2011) or triangulation of data (Yin, 1994): Different sources of data and different measures (perspectives) of ethical hacking practices are used in order to increase the validity of the study; 2) triangulation of method (Stake, 1995): Three data collection methods are used—in-depth interviews with subject matter experts and stakeholder groups within an organization, organizational documentation, and newspaper archival research; 3) triangulation of observers (Neuman, 2011) or member checking (Stake, 1995): Participants are consulted on the findings (the interview transcripts) so as to counter selective perception and interpretation and to ensure the accuracy of quotes; and 4) triangulation of theory (STEI-KW): Two complementary theoretical lenses, STEI and the KW, are used to situate organizational ethical hacking practices within the broader industry and social contexts.

3.10. Chapter Conclusion

This chapter first addressed the methodological justification for the thesis. It then explained the research design. This was followed by a statement about the rationale for the selection of the research site and sampling strategy. Data collection and analysis procedures were then discussed. An explanation of the implemented data validation protocols followed. Finally, the methodology reliability and validity protocols were discussed.

Chapter 4: Findings

4.1. Introduction

This chapter addressed RQ1 and RQ2: Who are ethical hackers and what do they do--that is, the meanings, ethics, values, skills/knowledge, roles and responsibilities, and practices of professional ethical hackers. The first part of this chapter focused on "RQ1 What constitutes ethical hacking teaching practices?" and sought to situate ethical hacking within the field of information security and to establish foundational understandings about ethical hacking as an interdisciplinary research area. Four key themes were discussed: Professional ethical hacking is legal, Ethical hackers are trustworthy, What do ethical hackers do? and An identity and legitimacy crisis. The second part of this chapter focused on "RQ2 What constitutes hacking skills?" and sought to map the language and key concepts surrounding ethical hacking as penetration testing. The scope covered themes focusing on open "technologies" as guided by the theoretical framework STEI-KW. Three key themes were discussed: Steps of the penetration testing process, Open source penetration testing methodologies, and The penetration test report.

4.2. RQ1 What Constitutes Ethical Hacking Teaching Practices?

This section explored RQ1 What constitutes ethical hacking teaching practices? While the number of academic programs teaching ethical hacking in higher education and the number of ethical hacking practitioners continue to grow, this growth has not been mirrored by a similar growth in scholarly research outlining the roles and responsibilities, and practices, and necessary knowledge and skills of professional ethical hacking practitioners in Canada. There is no consensus on what is ethical hacking or what it should be and what are the skills and

competencies required to function successfully at the various levels of the profession. A systematic literature review (Jesson, Matheson, & Lacey, 2011; Okoli & Schabram, 2010) of ethical hacking teaching practices was conducted to inform an inquiry into the professional attributes (professional profile) of ethical hackers (who they are and what they do), and what ethical hacking is taught in CS, CE, and SE programs in higher education (the latter is addressed in Advanced Analysis chapter). See Table 6: The Meaning of 'What constitutes ethical hacking teaching practices?,' Table 9: Hacking Skills Coding Table (Network Penetration Testing), and Table 10: Professional Ethical Hackers Coding Table.

This section aims to sketch out a portrait of professional ethical hackers and ethical hacking anchored in an understanding of the professional ethics, values, skills/knowledge, and practices of ethical hackers as penetration testers. Literature on ethical hacking spans a plurality of definitions and explanations. This thesis addressed a scarcity in empirical interdisciplinary research in ethical hacking as a research area. The discussion in this chapter focuses on exploring a comprehensive systems definition of ethical hacking based on the approach by Boyd (2004) and Luppicini (2005), that is, to render visible a systems definition of ethical hacking technology in society to guide ethical use and governance. Ethical hacking is defined from within the information security field and defined from outside the information security field, the social sciences and humanities perspective. The research database SCOPUS was used to locate relevant literature. The search strategy first identified 99 publications. These were reduced to 14 core peer-reviewed articles retained for the synthesis based on their relevance and quality, after applying the inclusion criteria, disregarding duplicates, and surveying the abstracts. The inclusion criteria specified peer-reviewed journal articles published between 2007 and 2019. The researcher sought a time frame of just over a decade and settled on 12 years. This excluded

unpublished research and research published before 2007, articles not directly addressing the research question, and articles lacking a rigorous methodology (see Table 13: Search Record for RQ1).

The 6 methodology steps are, Step 1 Define the research question, purpose, and scope: RQ1 What constitutes ethical hacking teaching practices? The purpose of the analysis is to inform an inquiry into how to teach hacking skills to higher education students in an ethical way. Step 2 Identify data sources: SCOPUS. Step 3 Conduct keyword search: The keyword search involved using synonyms from the RQ and subject terms to construct Boolean searches such that the search strings are appropriately derived from the research question. Step 4 Practical screening: 14 core peer-reviewed journals were retained for the synthesis based on their relevance and quality. Step 5 Data extraction: The core studies were organized into topic themes. Step 6 Synthesis. The data synthesis strategy involves collating and summarizing the results and findings of primary studies. The goal of this step is to present the extracted data from primary studies so that the results of the study are summarized. Four key themes were discussed: Professional ethical hacking is legal, Ethical hackers are trustworthy, What do ethical hackers do? and An identity and legitimacy crisis.

4.2.1. Professional ethical hacking is legal.

The key defining characteristic of penetration testing as ethical hacking is the legal imperative: Ethical hacking is unambiguously legal. Ethical hackers need prior authorization, a legally binding contract with the computer network owners before attempting to breach a computer network (Bodhani, 2013; Palmer, 2001; Young, Lixuan, & Prybutok, 2007). Much of the discussion around the various hat color codes of hackers revolves around this point. While an

ethical hacker is “authorised to break into supposedly ‘secure’ computer systems without malicious intent, but with the aim of discovering vulnerabilities in order to bring about improved protection,” a black-hat hacker is “someone who hacks with malicious intent and without authorisation” (Bodhani, 2013, p. 64). For Bodhani (2013), there is white, black, and a wide range of in-between ethical greys “who will search for vulnerable systems and inform the company but will hack without permission” (p. 65).

Bodhani (2013) presents 10 types of cyber hackers: White hats, black hats, grey hats, blue hats, elite hacker activist, script kiddies, spy hackers, cyber-terrorists and mobile hackers. But for Young et al. (2007), 9 of the 10 shades represent variations on the same theme: Illegal hacking. Computer hacking is either fully legal and authorized, or is an illegal activity. Presuming there is more than one type of acceptable hacking--authorized access--can give justification to illegal activity. Hackers often view themselves as modern-day Robin Hoods (Young et al., 2007). This Robin Hood mentality allows hackers “to deceive themselves and view their illegal activities as providing a service for the greater good. It also gives them cause to justify their activities should they be caught engaging in any illegal activities by blaming the victims” (p. 282).

The practices of professional ethical hackers are governed by a legal framework (Graves, 2010; Palmer, 2001). Ethical hackers have authorization to hack the target system. In recent years, hacking “is used most typically to describe a person who accesses computers and information stored on computers without first obtaining permission. Logan and Clarkson (2005) support that definition in describing hacking as accessing a system that one is either not authorized to access or one who accesses a system at a level beyond their authorization (Pashel, 2006). Hackers can be divided in to a number of groups some of which “are clearly ethical, others are clearly unethical, and still others exist in a gray area of sorts and whose ethics can be

debated" (Pashel, 2006, p. 197). White hats use their ability "in a manner that most would clearly define as ethical. Examples are employees who, with permission, attack a company's network in order to determine weaknesses, and law enforcement and intelligence agents who use their skill in the name of national security or to investigate and solve crimes." They have a duty to use their knowledge in such a way as "to benefit other people" (Pashel, 2006, p. 197). Pike (2013) draws a sharp distinction between white and black hats. A white-hat hacker is defined as "a hacker who is committed to full compliance with legal and regulatory statutes as well as published ethical frameworks that apply to the task at hand." In contrast, a black-hat hacker is "a hacker who either ignores or intentionally defies legal or regulatory statutes with presumably little interest in ethical frameworks" (p. 69). Logan and Clarkson (2005), Pashel (2006), Sharma and Sefchek (2007), Xu, Hu, and Zhang (2013), and Young et al. (2007) all more or less echo Pike's definition--essentially placing hacking and hackers at either side of the law.

It should be noted, legal does not necessarily equate with ethical. What constitutes legal practice is a political verdict aimed at preserving (reflecting or embodying) the interests and values of those who drafted or ratified the rules. The use of technology to construct knowledge via open AI based intelligence gathering technologies by adversaries has much to do with the efficient and fair use of the technology in society, and in a global system, with the equitable access to the technologies, but is also subject to the pressures of realities (e.g., scarcity of resources) and human nature and its basic need for security above all else. For example, offensive realism in IR suggests that defensive measures taken by one nation are seen as threatening or as a threat by adversarial nations. Nation states seek regional and global hegemony as the only rational choice to ensure survival. Mearsheimer (2001) says conflict between nations is inevitable. In the Liberalism perspective to IR, nations should come together

as responsible stakeholders and regulate the use of a technology in a collaborative manner that respects the values and interests of each.

4.2.2. Ethical hackers are trustworthy.

Harper et al (2011) are an important authority on what constitutes ethical hacking. We do not have to agree with them wholeheartedly, but their conception of ethical hackers underscores the centrality of trust in ethical hacking work. The title of their book, *Gray Hat Hacking: The Ethical Hacker's Handbook*, is a giveaway to their view, which is that white hat hackers are in fact grey hat hackers by necessity, by virtue of their practices. The ethics of ethical hacking includes the need to understand an adversary's tactics and recognizing the grey areas in security, they argue.

> Many times, while the ethical hacker is carrying out her procedures to gain total control of the network, she will pick up significant trophies along the way. These trophies can include the CEO's passwords, company trade-secret documentation, administrative passwords to all border routers, documents marked "confidential" held on the CFO's and CIO's laptops, or the combination to the company vault. The reason these trophies are collected along the way is so the decision makers understand the ramifications of these vulnerabilities … as soon as you show the CFO his next year's projections, or show the CIO all of the blueprints to the next year's product line, or tell the CEO that his password is "IAmWearingPanties," they will all want to learn more about the importance of a firewall and other countermeasures that should be put into place. (p. 11)

Andrasik (2016), and Thomas et al. (2018) make the same point as do Harper el al. (2011), that ethical hackers will sometimes unavoidably access privileged information. Andrasik (2016) adds that organizations hiring ethical hackers need to talk to references first:

> If a pen-test group is going to actively try to breach your defenses, you want to know their ethics are beyond reproach. That knowledge should come from somewhere other than a well-crafted website or canned testimonials— it should come from conversations with companies that have experienced a pen test by the group in question.

Thomas et al. (2018) argue that naturally "and to be effective, ethical hacking involves trying to gain access to a system to access confidential and sensitive information. This means, that a certain level of trust needs to be established between the ethical hacker and the party engaging them" (p. 3). The authors point out a fact that admittedly complicates the discussion (it is an important point to note, but lies outside the thesis scope):

> an ethical hacker needs to keep their knowledge of exploits up to date, and they will likely need to go "underground" to gain this knowledge (Conran 2014). Because ethical hackers may even utilize questionable means to gain intelligence it may result in a question of their professional ethics. (p. 4)

In contrast to a cracker, who is a malicious hacker, an ethical hacker "is someone who employs the same tools and techniques a criminal might use, with the customer's full support and approval, to help secure a network or system" (Walker, 2017, p. 29). According to the International Council of Electronic Commerce Consultants (EC-Council), an ethical hacker is "an individual who is usually employed with the organization and who can be trusted to undertake an attempt to penetrate networks and/or computer systems using the same methods and techniques as a Hacker." A Certified Ethical Hacker (EC-Council) is, "a skilled professional

who understands and knows how to look for weaknesses and vulnerabilities in target systems and uses the same knowledge and tools as a malicious hacker, but in a lawful and legitimate manner to assess the security posture of the target system(s).” EC-Council emphasizes that ethical hackers use the same knowledge and tools as a malicious hacker but in a lawful and legitimate manner, and that ethical hackers are trustworthy professionals who are employed within business and industry organizations to perform security testing processes. Graves (2010) and Palmer (2001) agree on the three attributes of trust, honouring the integrity of the client’s system, and on seeking prior permission from the client. Graves refers to these traits as professional. First and foremost, ethical hackers “must be completely trustworthy” (Palmer, 2001, p. 771). During an evaluation, “the ethical hacker often holds the ‘keys to the company,’ and therefore must be trusted to exercise tight control over any information about a target that could be misused” (p. 771). Second, ethical hackers should take “all precautions to do no harm to their systems during a pen test” (para. 1). Third, the imperative to obtain permission before attempting to access the computer network--the practices of professional ethical hackers are governed by a legal framework (Graves, 2010; Palmer, 2001). Ethical hackers should address both systemic vulnerabilities as well as preventive measures (Harris, 2007; Palmer, 2001). Several codes of conduct for information security professionals and ethical hackers exit. They are all voluntary and only applicable to individuals who are members or certified professionals of the respective association. The codes of ethics may contain similar directives but they are all different and include different levels of detail.

Key Codes of Conduct for Information Security Professionals (Adapted from Thomas et al., 2018, pp. 5-6)

Code of conduct	Key directives
CREST Code of Conduct	CREST is a not for profit organization that originated in the UK. It has active chapters across Europe, the Middle East, Africa and India (EMEA), the Americas, Asia, and Australia, and New Zealand. CREST's purpose is "to provide a level of assurance that organizations and their security staff have a level of competence and qualification in conducting security work such as penetration testing, threat intelligence or incident response (CREST, n.d.)." The CREST code of conduct is "fairly detailed and covers requirements such as ensuring regulatory obligations, adequate project management, competency, client interests, confidentiality, and ethics (CREST, 2016)."
EC-Council Code of Ethics	EC-Council is best known for its Certified Ethical Hacker (CEH) certification, which is recognized as a U.S. Department of Defence (DoD) 8570 cybersecurity certification. The EC-Council Code of Ethics requires "confidentiality of discovered information, ensuring that any process or software obtained is legal and ethical, ensuring proper authorization, adequate project management, continuing professional development, ethical conduct, and not being convicted of any crimes (EC-Council, n.d.)."
Global Information Assurance Certification (GIAC) Code of Ethics	GIAC provides several highly regarded certifications in the security industry which include penetration testing, security management, and digital forensic certifications. The GIAC Code of Ethics is comprised of four sections: Respect for the public, respect for the certification, respect for the employer, and respect for oneself. The code mandates that "professionals will take responsibility and act in the public's best

	interests, ensure ethical and lawful conduct"; maintain confidentiality, competency, accurate representation of skills and certifications "and avoiding conflicts of interest (GIAC, n.d.)."
ISACA Code of Professional Ethics	ISACA was established in 1969 and focuses on IT governance. It has over 140,000 members worldwide (ISACA, n.d.). ISACA provides training and certification for information security and cybersecurity professionals. The ISACA Code of Professional Ethics mandates that compliance with standards and procedures, due diligence, legal conduct and confidentiality, competency, and continuing professional development are maintained (ISACA, n.d).
ISC2 Code of Ethics	ISC2 is an international, not for profit organization with over 125,000 members in the information security profession (ISC2, n.d.). ISC2's Code of Ethics consists of four directives: Protecting society and public interest, acting honourably, honestly, justly, responsibly and legally, being competent, and advance to protect the profession (ISC2, n.d.).

4.2.3. What do ethical hackers do?

Defined from within the information security field the term ethical hacking most formally refers to penetration testing practices, and less formally to vulnerability assessment and risk assessment processes. The core work of professional ethical hackers involves performing security assessments or audits (vulnerability assessment, risk assessment, and threatscape analysis) and their cybersecurity role in organizations can be seen as "analysts" collecting and analyzing threat data and giving actionable recommendations to mitigate any security risks (putting threat intelligence into real-life risk context). Key practices of ethical hackers include 1) Risk assessment usually against known vulnerabilities/threats; 2) Discover unknown vulnerabilities/threats; 3) Compliance with privacy and security regulations and standards--

government regulations (e.g., Privacy Act, 1983; PIPEDA, 2000), industry regulations (e.g., PCI DSS, ISO/NIST), and in-house standard procedures and best practices; and 4) Audit performance of security controls.

The NIST Risk Management Guide defines risk assessment as "the process of identifying the risks to system security and determining the probability of occurrence, the resulting impact, and additional safeguards that would mitigate this impact" (Landoll & Landoll, 2005, p. 10). A vulnerability assessment is the process of identifying, quantifying, and prioritizing (ranking) the vulnerabilities in a system. Vulnerability assessments can include passive and active vulnerability scanning of network and operating systems. Vulnerability assessments usually covers network and infrastructure testing. Vulnerability scanning is performed before penetration testing. "A penetration test is a proactive and authorized attempt to evaluate the security of an IT infrastructure by safely attempting to exploit system vulnerabilities, including OS, service and application flaws, improper configurations, and even risky or illegal end-user behaviour.

> Tests are typically performed to systematically compromise servers, endpoints, web applications, wireless networks, network devices, mobile devices and other potential points of exposure. Testers may even attempt to use the compromised system to launch subsequent attacks at other internal resources, specifically by trying to incrementally achieve higher levels of security clearance and deeper access to electronic assets and information via privilege escalation. (Rodger, 2013, p. 41).

"A simple way to remember is that a technician runs a vulnerability scan while a hacker performs a penetration test" (Rodger, 2013, p. 48). (See Table 15: Vulnerability Scan and Penetration Test Comparison.) The "magic" part of a penetration test is exploiting a vulnerability discovered during the vulnerability assessment phase (Harper et al., 2011; Walker, 2017).

Penetration testing is “usually done by a person or party contracted by the target to pinpoint any weaknesses that they may have.” A penetration test is “a proactive and authorized attempt to evaluate the security of an IT infrastructure by safely attempting to exploit system vulnerabilities, including OS, service and application flaws, improper configurations” (Rodger, 2013, p. 41). The recommendations should tell the customer how to remediate the identified findings. Based on the type of auditing required, there are two main penetration testing types. In black box testing, the penetration tester has no prior knowledge of a company’s network, more closely replicating remote attacks. In white box testing, the testers typically have complete access to information about the application they are attacking, that is, the testers have a complete knowledge of the network. White box testing represents a worst-case scenario where the attacker has a complete knowledge of the network. A penetration test “is when ethical hackers do their magic. They can test many of the vulnerabilities identified during the vulnerability assessment to quantify the actual threat and risk posed by the vulnerability” (Harper el al., 2011, p. 11). Penetration testing includes probing for vulnerabilities as well as giving proof of concept for an attack--that is, testing or verifying a hypothesis. Pentesting (penetration testing) is a process of scientific inquiry.

“As soon as someone mentions the word ‘proof,’ or ‘I have proven security,’ I believe that person has no idea of how things work in practice. Because in practice we cannot prove security. It does not work that way.” (PPT14)

“You cannot prove that something is secure. You can only prove that you don’t know how to attack it.” (PPT10)

"You're thinking, 'Well, I want these people to defend my system.' They aren't the defenders ... They are the attackers. They figure out how to break things. And the skill of breaking things is not the skill of making things." (PPT8)

Two Key Ethical Hacking Paradigms

Strategy	Offensive security (testing)	Defensive security (testing)
	"Hacker powered security" (e.g., HackerOne and Bugcrowd)	Diligence SDLC/agile security DevSecOps/security-by-design Best practices, IA
Mindset	Attacker Adversarial Damage, break, deceive, trick	Defender Ally Protect/prevent/mitigate
Skillsets	How to penetrate an information system	How to protect an information system (risk assessment/governance skills)
Conflict of interests	Less or no conflict of interests	Conflict of interests (hackers are typically employees)
Related paradigms		Hygiene culture Security culture
Permission of system's owner	Authorized, legal	Authorized, legal
	Blackbox testing Black hat hacking Third party audit/auditor perspective of infosec governance (policies, procedures, plans, platforms, compliance, IA compliance, awareness, responsibilities/roles)	Whitebox testing White hat hacking
Authentication	Unauthenticated scan (outsider attack)	Authenticated scan (simulation of insider attack)

4.2.4. An identity and legitimacy crisis.

A view from outside of the information security field (i.e., from the social sciences and humanities) of how uses of the term hacking have influenced its conceptual development includes a view of the role of the mass media and law enforcement in changing the original positive connotation of the term hacking from around the late 1980s and through the early 1990s to connote unlawful or criminal acts (Coleman & Golub, 2008; Thomas, 2005), as well as an anthropological analysis (taxonomy) of various hacker ethic based on idioms and practices (Coleman & Golub, 2008) and the pioneering historical work of Steven Levy (1984) on hacker culture. Coleman and Golub (2008) saw various hacker ethic as representative of the subjective self. In that vein, they conceptualize three liberal moral expressions of hackers and hacking (cultural sensibilities or hacker ethics) revealed variably in the context of computer hacking: Cryptofreedom, free and open source software, and the hacker underground (see Table 14: Profiles of Hackers and Figure 2: Profiles of Hackers Graph).

Several social and historical factors underlie an identity and legitimacy crisis for professional ethical hacking practitioners. An identity crisis can be understood as a crisis of confusion regarding who are professional ethical hackers and what do they do (what is ethical hacking). A legitimacy crisis can be understood as a crisis of confusion regarding the ethics and values of professional ethical hackers, and regarding their value (contributions) to organizations and society at large. The following influences contribute to a confusion regarding the identity and legitimacy of professional ethical hackers, and hence pose problems for S&T innovation approaches to technology governance.

In the golden age of hacking, media began to frame criminal hackers as simply hackers (instead of the more accurate description of “criminal hackers”) thus associating hackers and

hacking per se in the public mind with malice and malevolence. Meanwhile, law enforcement in the golden age of hacking was influenced by a sense of "moral panic" regarding the rise of hacking and hackers and began transposing terms used for criminal acts in the physical world to the online world. Perhaps the media were taking their cues from law enforcement or perhaps they were experiencing an episode of moral panic themselves, or perhaps the media opted for brevity so they dropped the word "criminal" from what should have been "criminal hacking." Yet perhaps the word hacking on its own sounded more dramatic and more likely to capture the attention of viewers and listeners. Both the media and law enforcement demonized hacking and hackers and undermined the increasingly important role of hackers and hacking in society needed to ensure national security. The value of hacking and by extension teaching students to hack remains confused.

Ethical hacking as a profession suffers from delegitimization stemming from confusion and a corollary social stigma surrounding hackers, which is tied to historical and social developments. The meaning of the term ethical hacking can be understood in relation to the term hacking, as their history is intertwined. Hacking today "connotes pejorative attempts to gain unauthorized access to computers." When the term hacking was first introduced in the early 1960s, it was used to refer to a group of pioneering computer aficionados at Massachusetts Institute of Technology (Levy, 1984) who "typically had little respect for the silly rules that administrators like to impose, so they looked for ways around" (Stallman, 2001). In the 1960s to the 1970s, a hacker was "simply someone obsessed with understanding and mastering computer systems" (p. 602). A hacker (noun) meant,

> 1. A person who enjoys learning the details of computer systems and how to stretch their capabilities—as opposed to most users of computers, who prefer to learn only the

> minimum amount necessary. 2. One who programs enthusiastically or who enjoys programming rather than just theorizing about programming. (Palmer, 2001, p. 769)

The connotation of the term "hacker" would undergo a transformation in the late 1980s and early 1990s (Coleman & Golub, 2008; Thomas, 2005). Hacking and hackers became increasingly associated with computer intrusions and unauthorized telephone calls. By the early 1990s, the word hacking had begun acquiring a negative connotation. The mass media began using the term hacker to describe individuals who break into computers for fun, revenge, or profit, instead of the more accurate term of criminal hacking. Thomas (2005) traces the legacy of demonization of hackers to the rhetoric of media and law enforcement of the early 1990s. "In retrospect, the rhetoric of law enforcement and of other 'moral entrepreneurs' of the late 1980s and early 1990s can be seen as an example of how the symbolic manufacturing and pursuit of demons can lead to equally demonic excesses that may create ethical transgressions greater than those being controlled (p. 600). The responses of law enforcement in the golden age of hacking to incidents by computer hackers was "out of proportion to the threat" and reflected a "moral panic." It focused on selected incidents as "symbolic signposts" that illustrate how hacking "both constituted and reflected ironic ethical ambiguity between the enforcers of the law and those who transgressed it."

The origins of hacking "were grounded arguably in what the original participants saw as an ethical, even noble, pursuit. However, law enforcement agencies had a different metaphor, setting out on a mission to purify cyberspace from the invading vandal hordes" (Thomas, 2005, p. 603). An example of imposing familiar concepts on new behaviors can be seen in the ways in which legal concepts such as burglary, trespassing and theft, "terms that have a reasonably unequivocal meaning in a world of material objects – became opaque, even absurd, when applied

to cyberspace. Yet, prosecutors invariably used such legal terminology in their indictments." By "metaphorically invoking images of home intruders and thieves, legal rhetoric manipulated the meaning of hacking behavior to – some might say cynically– demonize the participants successfully. The indictments transformed 'bad acts' into formally sanctionable ones by creatively linking the act to more familiar predatory behaviors, such as 'breaking and entering' (e.g. US vs Robert J. Riggs and Craig Neidorf, 1990, 90-CR 0070 United States District Court, ND Ill. ED)" (Thomas, 2005, p. 601). Since hacker was originally meant as a compliment, computer security professionals prefer to use the terms intruder or cracker for hackers who have turned to the dark side.

The social stigma surrounding hacking harms society. Social stigma is both a consequence and a cause of the identity and legitimacy crisis: It undermines ethical hacking education (acting as a reinforcing feedback loop--ignorance fuels the stigma and the stigma leads to ignorance because the topic becomes a taboo) raising crime risk to society. The stigma from confusion surrounding the profession and the roles of professional ethical hackers in organizations and in society drives down student enrolment and the hiring of expert hackers as instructors and professors within higher education.

> Finding an academic who has those skills, they are few and far between. We have to be very careful about our professional standing. There is certain amount of negativity looked at to hacking in general. As a professional, if I say, "Yeah, I built my hacking skills," "Well, how did you do that? What did you break into?" There's a certain amount of stigma against hacking, whether it be ethical or not, and so, for an academic to gain the level of skills so they can teach about it adequately is a bit of a challenge. (PPT3)

Levy (1984) offered one of the earliest theorizations of hacker ethic (what hackers

thought it meant to be a hacker), particularly in the early decades of computer technology in the 1950s and 1960s (McConchie, 2015). Key hacker ethic principles are: 1) "The fundamental tenet of the hacker ethic is that information should be free, and that access to computers should be unrestricted" (McConchie, 2015, p. 879); 2) Hackers see the creative reuse and repurpposing of technology as a hands-on way of learning about the world and becoming self-directed and self-reliant individuals; 3) Hackers believe that information should be decentralized and authority mistrusted; and 4) Hackers believe that hacking, in itself, can make the world better through the free exchange of information and hacking skills (McConchie, 2015). The mistrust of authority structures hacker ideas about socialization and self-organization within hacker communities; the community of hackers presents itself as a meritocracy wherein hackers ought to be judged solely on hacking skills, "not bogus criteria such as degrees, age, race, or position" (Levy, 1984, p. 35).

4.3. RQ2 What Constitutes Hacking Skills?

This section explores RQ2 What constitutes hacking skills? A systematic literature review (Jesson, Matheson, & Lacey, 2011; Okoli & Schabram, 2010) of hacking skills was conducted to identify major themes in literature surrounding hacking skills. A systematic review of hacking skills in literature serves as a basis for mapping out the language and key concepts surrounding hacking skills and hacking technologies with emphasis on skills that mirror society (i.e., open/open source) in the context of exploring ethical hacking teaching practices in higher education (focusing on penetration testing in information security testing).

The research database SCOPUS was used to locate the relevant literature. The search strategy first identified 50 publications. These were reduced to 10 high-quality peer-reviewed articles on the basis of their research quality for the final synthesis after applying the inclusion

criteria, disregarding duplicates, and surveying the abstracts. The inclusion criteria specified peer-reviewed journal articles published between 2007 and 2019. Selection emphasized open source technologies and methodologies. This excluded unpublished research and research published before 2007, articles not directly addressing the research question, and articles lacking a rigorous methodology (see Table 16: Search Record for RQ2).

The 6 methodology steps are, Step 1 Define the research question, purpose, and scope: RQ2 What constitutes hacking skills? The purpose of the analysis is to map the language and key concepts surrounding ethical hacking as penetration testing. The scope covers themes surrounding hacking "technologies" and themes surrounding open and open source. Step 2 Identify data sources: SCOPUS. Step 3 Conduct keyword search: The keyword search involved using synonyms from the RQ and subject terms to construct Boolean searches such that the search strings are appropriately derived from the research question. Step 4 Practical screening: 10 core peer-reviewed journals were retained for the synthesis based on their relevance and quality. Step 5 Data extraction: The core studies were organized into topic themes. Step 6 Synthesis. The discussion and analysis in this section are based on an understanding of ethical hacking as penetration testing, which is the most formal definition of the term. Penetration testing as ethical hacking is discussed with focus on network security testing (see Table 9: Hacking Skills Coding Table (Network Penetration Testing)). Three key themes were discussed: Steps of the penetration testing process, Open source penetration testing methodologies, and The penetration test report.

4.3.1. Steps of the penetration testing process.

To conduct a security audit, first, the scope of the penetration testing or vulnerability

assessment operations is specified. Penetration tests should be seen as targeted exercises. The scope of test activities and test objectives, a schedule for the test activities, and the specific machines or applications to be tested are all specified upfront. Each test objective will have its own set of parameters and processes. In the words of NIST SP 800-115,

> In the planning phase, rules are identified, management approval is finalized and documented, and testing goals are set. The planning phase sets the groundwork for a successful penetration test. No actual testing occurs in this phase. (p. 5-2)

Walker (2017) proposes five main stages for a penetration test or "act of hacking": 1) Reconnaissance involves the steps taken to gather evidence and information on the target, 2) scanning and enumeration phase takes the information gathered in reconnaissance and applies tools and techniques to gather more in-depth information on the targets, 3) gaining access where "true attacks are leveled against the targets enumerated in the second phase," 4) maintaining access, where hackers attempt to ensure they have a way back into the compromised system, and 5) covering tracks, where "attackers attempt to conceal their success and avoid detection by security professionals" (p. 36). Faircloth (2011) proposes an iterative five stage reconnaissance phase: Intelligence Gathering, Footprinting, Human Recon, Verification, and Vitality. Table 17: Five Phases of Reconnaissance outlines the intelligence objectives, output (deliverables), and intelligence resources and tools for each phase. The last phase (Vitality) can be omitted in passive reconnaissance.

The thesis focuses on three key steps in the network penetration testing process (hence a three-step penetration testing framework): Reconnaissance, network enumeration, and port scanning--up to the point of levelling true attacks against network target systems. Each of these three phases can be either passive or active. There are two types or techniques of attacks: An

active attack threatens the confidentiality and integrity of data, and a passive attack threatens the confidentiality of data. The three key steps or phases of footprinting (reconnaissance), network enumeration, and port scanning (what NIST SP 800-115 calls the discovery phase) are intelligence gathering processes to prepare for an exploit strategy against a target. NIST SP 800-115 divides penetration testing into four main phases: Planning phase, Discovery phase (addressing Target Identification and Analysis Techniques), Attack phase (addressing Target Vulnerability Validation Techniques), and Reporting (see NIST SP 800-115, p. 5-2 for an in-depth discussion of the discovery phase). The three steps of the discovery phase represent successive stages of escalation in network access privileges. Reconnaissance uncovers information about a target company, such as its name and the identity of its partners, employee numbers, primary top-level domain names, and email address structure. Enumeration produces a narrowed-down list of specific IP addresses, port numbers, hostnames, and bulk lists of email addresses. Scanning gathers client-server level intelligence.

Key risk thresholds or milestones within the three-step penetration testing framework: 1) From footprinting/reconnaissance to network enumeration mark a change in network access authorization level (what is public and "open" and what is not) (e.g., lawful DNS-based data exfiltration from public sources vs unauthorized network access); 2) from network enumeration to active port scanning--active interference in network communication processes may cause delay or downtime (e.g., consumption of bandwidth during continuous active enumeration or monitoring, or during continuous penetration testing or to ensure network awareness within IT security governance), and traceability to penetration testers becomes a concern; and 3) from vulnerability assessment to "proof of concept" or the testing of security hypotheses regarding exploitable vulnerabilities within an information system. Penetration testing involves "launching

real attacks on real systems and data using tools and techniques commonly used by hackers" (NIST SP 800-115, p. 5-2). Most "ethical hacking" activities are in practice vulnerability assessment activities. Performing real attacks on real systems carries a higher risk that must be weighed carefully against the intended benefits. It must be justified on a cost-benefit basis by a security analyst with broad and interdisciplinary knowledge about the social threat landscape, human behavior, sociopolitical conflicts, in addition to the technical knowledge. Penetration testing can compromise data integrity or availability (accidental damage) or confidentiality (the penetration tester sees confidential information just by virtue of performing the test).

Penetration tests begin with an extensive information gathering phase. Open source information on the Internet can be used to build a profile of the target user or system. The vast majority of footprinting activity, also called OSINT, is passive in nature. Active recon involves social engineering and "anything that requires the hacker to interact with the organization" (Walker, 2017, p. 45). Social engineering is a threat that can exploit an ignorance (skill/knowledge gap) or credulity (lack of critical thinking/not understanding that reality is socially constructed) of the technology user (i.e., a gap in end-user security awareness) regarding the safe and ethical use of technology. Passive reconnaissance involves gathering information from the public domain in places like Internet registries, Google, newspapers, and public records. At this stage "the target does not even know generally that they are the subject of surveillance." The first step involves collating technical information on an organization's public-facing systems. "Internet registries, coupled with services such as Shodan or VPN Hunter, can highlight and identify an organization's Web servers, mail servers, remote access endpoints and many other Internet-facing devices." Methods include "gathering of competitive intelligence, using search engines, perusing social media sites, participating in the ever-popular dumpster dive,

gaining network ranges, and raiding DNS for information" (Walker, 2017, p. 44). A key argument is that there is no clear cutoff point between passive and active intelligence gathering techniques. Wheeler (2011) notes, "Although passive testing sounds harmless, beware that the definition of passive is not always consistent across the field. There are definitely gray areas to be aware of." The confusion includes whether the use of third parties for services is considered passive testing (e.g., Passive Information Gathering (Part 1), Ollmann, 2007), whether the process of testing can be traced back to the tester, and whether the information gathering can be performed without the knowledge of the organization under investigation (i.e., stealthy--the key emphasis here is that intelligence gathering does not draw attention and remains undetected).

Network enumeration involves the discovery of active hosts and devices on a network and mapping them to their IP addresses. Network enumeration involves gathering information about a network such as the hosts, connected devices, and usernames using protocols like ICMP and SNMP. "Once available hosts on a network have been found via networking enumeration, port scanning can be used to discover the services in use on specific ports." Port scanning refers to the process of sending packets to specific ports on a host in the network and analyzing the responses to learn details about its running network services and operating systems, software applications, thus locating potential vulnerabilities. Network enumeration and port scanning help testers map network services and topology to fine-tune their assault tactics. A tool like Nmap usually performs enumeration and scanning by launching custom TCP, UDP or ICMP packets against a given target. The target responds to the information requests in the form of a digital signature. This signature is key to identifying what software, protocols and OS is running the target device. Nmap scans can identify network services, operating system number and version, software applications, databases, and configurations, all with high probability. p0f is a passive

monitoring alternative to Nmap, a passive fingerprinting tool that does not generate network traffic, is used to analyze network traffic and identify patterns behind TCP/IP-based communications often blocked for Nmap active fingerprinting techniques. Passive fingerprinting uses sniffer traces from the remote system to determine the operating system of the remote host. p0f uses a fingerprinting technique "based on analyzing the structure of a TCP/IP packet to determine the operating system and other configuration properties of a remote host." It includes powerful network-level fingerprinting features, and the ability to analyze application-level payloads such as HTTP, and can be used for detecting NAT, proxy and load balancing setups (see Table 18: Pen Source/Free Tools—for Network Penetration Testing). Network penetration testing and exploitation techniques typically include: Bypassing firewalls, Router testing, IPS/IDS evasion, DNS footprinting, Open port scanning and testing, SSH attacks, Proxy Servers, Network vulnerabilities, and Application penetration testing (Cipher, n.d.).

Passive network sniffers, notably Snort, the de facto standard for IDS/IPS applications, can monitor and capture data packets passing through a given network in real time. "Sniffers operate at the data link layer of the network. Any data sent across the LAN is actually sent to each and every machine connected to the LAN. This is called passive since sniffers placed by the attackers passively wait for the data to be sent and capture them." "The most fundamental approaches to detecting cyber intrusions are to monitor server logs for signs of unauthorized access, to monitor firewall or router logs for abnormal events, and to monitor network performance for spikes in traffic" (EDUCAUSE, 2020). Placing a packet sniffer on a network in promiscuous mode allows a malicious intruder to capture and analyze all of the network traffic such as payloads containing confidential information. Treurniet (2004) used a proprietary tool developed at DRDC to analyze network traffic in 1999 to investigate whether "the information

obtained through active methods may also be obtained by passively listening to traffic." A network sniffer was "strategically placed on the network and the traffic is examined as it passes by. The behaviour of the traffic can be compared to an established policy for deviations" (p. 2). "Good agreement was found between the test program results and the documented network attributes" showing how passive scanning methods can be used in achieving network awareness without introducing unnecessary traffic (Treurniet, 2004, p. 2). See Table 19: Properties of a Network and Whether they Can Be Discovered Passively.

Effective network security requires real time awareness of the activities taking place on the network, to verify that the network policy is not being violated by any user or misconfiguration. A network can be periodically scanned to obtain real-time awareness. Active techniques to periodically scan the network have two disadvantages. First, they are intrusive, they introduce traffic into the network which consumes considerable bandwidth. Second, scanning can miss an activity, for example, when a specific port is probed with a specific protocol, because these look for a particular activity. These drawbacks can be addressed by using passive techniques where no traffic is introduced into the network. "Passive techniques have been in use in both defensive and offensive approaches for years but have only appeared recently in commercial products" (Treurniet, 2004, p. 1). "A sniffer is strategically placed on the network and the traffic is examined as it passes by. The behaviour of the traffic can be compared to an established policy for deviations" (Treurniet, 2004, p. iv). The passive technique can also identify information leaking form the network that could be used by malicious hackers. Attackers expect that active methods are used by organizations to test their own networks, so it "stands to reason, then, that more experienced attackers would also employ passive methods to obtain

network information" (Treurniet, 2004, p. 2). Thus continuous surveillance or monitoring can be achieved using passive network sniffers to assess the security of a network.

4.3.2. Open source penetration testing methodologies.

Markedly different testing methodologies are developed independently within the open source community. Key open source penetration testing methodologies include Open Source Security Testing Methodology Manual (OSSTMM) (Herzog, 2006), NIST 800-115 (2008) Technical Guide to Information Security Testing and Assessment, The Open Web Application Security Project (OWASP), The Penetration Testing Execution Standard (PTES), The Information System Security Assessment Framework (ISSAF), PCI-DSS v.1 2015 Penetration Testing Guide, and Communications Security Establishment/Royal Canadian Mounted Police, Harmonized Threat and Risk Assessment Methodology (CSE/RCMP, 2007) (see Bradbury, 2010; Faircloth, 2011; Goel & Mehtre, 2015; Shah & Mehtre, 2015; Valvis & Polemi, 2005). Key open source penetration testing methodologies discussed here are Open Source Security Testing Methodology Manual (OSSTMM 3.0), NIST Special Publication 800-115: Technical Guide to Information Security Testing and Assessment (NIST 800-115), and Communications Security Establishment/Royal Canadian Mounted Police, Harmonized Threat and Risk Assessment Methodology (CSE/RCMP, 2007). A comparative analysis of the three open source penetration testing methodologies offers insights into how they can integrate with a harmonized penetration testing methodology based on IA philosophy to information security (see Table 20: Information Security Assessment Methodologies).

The original Open Source Security Testing Methodology Manual (OSSTMM) is a peer-reviewed manual of security testing and analysis, "a methodology for a thorough security test,

known as an OSSTMM audit" by the Institute for Security and Open Methodologies (ISECOM), was published on December 18, 2000. The current version OSSTMM 3.0 was published on August 2, 2008. In version 3, OSSTMM encompasses tests from all channels: Human, Physical, Wireless, Telecommunications, and Data Networks. A set of security metrics used, Risk Assessment Values (RAVs), provide a tool that can provide a graphical representation of changes in state over time. The primary focus in version 3 has been to move away from solution-based testing, which assumes specific security solutions will be found in a scope and are required for security (like a firewall). Instead, the focus is on a metric for the attack surface (the exposure) of a target or scope, allowing for a factual metric with no bias (the risk-based approach). The purpose of NIST SP 800-115: Technical Guide to Information Security Testing and Assessment (September 2008) is "to provide guidelines for organizations on planning and conducting technical information security testing and assessments, analyzing findings, and developing mitigation strategies" (NIST, 2008, p. ES-1).

NIST SP 800-115 Section 4 Target Identification and Analysis Techniques focuses on "identifying active devices and their associated ports and services, and analyzing them for potential vulnerabilities" (p. 4-1). It includes Network Discovery which "uses a number of methods to discover active and responding hosts on a network, identify weaknesses, and learn how the network operates." Passive (examination) and active (testing) techniques discover devices and active hosts on a network. Passive techniques can use a network sniffer to monitor network traffic and record the IP addresses of the active hosts, and they can report which ports are in use and which operating systems on the network have been discovered--without sending out a single probing packet (p. 4-1). Section 4 also covers Network Port and Service Identification. "Some scanners can help identify the application running on a particular port

through a process called service identification" (p. 4-3). Banner grabbing involves "capturing banner information transmitted by the remote port when a connection is initiated. This information can include the application type, application version, and even OS type and version." The result of network discovery and network port and service identification is "a list of all active devices operating in the address space that responded to the port scanning tool, along with responding ports" (NIST, 2008, p. 4-3). Port scanners can identify active hosts, operating systems, ports, services, and applications, but they can not identify vulnerabilities. "To identify vulnerable services, the assessor compares identified version numbers of services with a list of known vulnerable versions, or performs automated vulnerability scanning" (p. 4-4).

Vulnerability scanners can be broadly divided in to two categories: Web application scanners, such as Acunetix, WebInspect, NetSparker; and network and infrastructure scanners like Nessus, Qualys, and Metasploit. Vulnerability scanners can check compliance with host application usage and security policies, identify hosts and open ports, identify known vulnerabilities, and provide information on how to mitigate discovered vulnerabilities. Vulnerability scanners often use their own proprietary methods for defining the risk levels. One scanner might use the levels low, medium, and high; another scanner might use the levels informational, low, medium, high, and critical, making it difficult to compare findings among multiple scanners. Vulnerability scanners rely on a repository of signatures which requires the assessors to update these signatures frequently to enable the scanner to recognize the latest vulnerabilities. NIST SP 800-115 Section 5 Target Vulnerability Validation Techniques focuses on using information produced from target identification and analysis to further explore the existence of potential vulnerabilities. The objective is to prove that a vulnerability exists, and to demonstrate the security exposures that occur when it is exploited" (p. 4-5).

The Harmonized Threat and Risk Assessment Methodology (TRA-1) by the Communications Security Establishment (CSE) and the Royal Canadian Mounted Police (RCMP) (CSE/RCMP, 2007) presents a flexible approach which can be automated and serves as a general framework for a harmonized penetration testing methodology by applying a project management frame (see Table 20: Information Security Assessment Methodologies). The TRA approach provides "a clear rationale for cost-effective risk mitigation strategies and safeguards to meet business requirements; and a transparent audit trail and record of risk management decisions to demonstrate due diligence and accountability, thereby satisfying statutory obligations and policy requirements" (CSE/RCMP, 2007, p. EO-2).

4.3.3. The penetration test report.

A vulnerability scanner "actively communicates with the target system, sends the malicious packets and analyses the results, which can then be exported to PDF, HTML, CSV and other formats" (Rasskazov, 2013, p. 58). Typical vulnerability management software obtains the results and provides a comprehensive dashboard to present the results. "It can build trends, sort the results by criticality, and keep additional records, for example business purpose of the system or location" (Rodger, 2013, p. 48). The software's reporting component can generate the compliance reports against widely used standards, for example PCI DSS, ISO 27001, or against the corporate policies, for example the percentage of computers with outdated software or weak password policy. Nexpose and other vendors include the vulnerability management software in the package with vulnerability scanners, while other vendors (e.g., Nessus) sell the software separately.

The penetration test report typically two sections: The executive summary and the

technical report. “Primarily, the pentesters and their work is judged by their report” (Velu, 2013, p. 7). Pen test report writers address key considerations: Who is the audience of the report (e.g., senior management or IT staff), the purpose of testing, necessary procedures are justified, and required actions stated clearly. “A report should present outcome of the whole project by including objectives, used methodology, successful exploits, root cause of those exploits and recommendations” (Chaudhary, 2013, p.18). The report will offer an assessment of technical risk, business risk, reputational risk, and compliance risk. The key part of a penetration testing is the findings: Customers will want to prioritize the remediation activities according to classification of the findings.

4.4. Chapter Conclusion

The first part of this chapter addressed RQ1 and sought to establish formal understandings about the identity of professional ethical hackers, their ethics and values, roles and responsibilities, and their practices, and their professional and social value, to counter legitimacy problems abundant in news media narratives and descriptions. Four key themes were addressed: Professional ethical hacking is legal, Ethical hackers are trustworthy, What do ethical hackers do? and An identity and legitimacy crisis. The second part of this chapter focused on RQ2 and sought to map the language and key concepts surrounding ethical hacking as penetration testing. The scope covered themes surrounding hacking technologies and themes surrounding open and open source. Penetration testing as ethical hacking was explained with emphasis on passive network security testing practices. Three key themes were addressed: Steps of the penetration testing process, Open source penetration testing methodologies, and The penetration test report.

Chapter 5: Advanced Analysis

5.1. Introduction

This chapter addresses RQ3 and RQ4 and focuses on S&T innovation risk governance of ethical hacking technology use in ethical hacking teaching practices in higher education in Canada. The first part of this chapter (risk assessment) addresses "RQ3 What is the risk to society of teaching students hacking skills?" To answer RQ3, ethical hacking teaching practices in higher education in Canada were explored at two societal levels, institutional and social. Ethical hacking is presently a grey academic disciplinary area. There is no broad consensus on what it is or what it should be. Confusion arising from differences in perceptions among experts, industry practitioners, and policymakers regarding what constitutes ethical hacking teaching practices, what constitutes hacking skills, what is the risk to society of teaching students hacking skills, and how to mitigate these risks stifles innovation and effective educational policy development and implementation, which perpetuates the security risk. The thesis explores what "ethical hacking" is taught in CS (computer science)/CE (computer engineering) /SE (software engineering) programs in two Canadian universities and is it ethical? STEI-DMG is used as a theoretical framework to guide a technology impact assessment, focusing on AI based intelligence gathering/surveillance technologies, to inform the ethical governance of technology use in society. STEI-DMG integrates into decision making research, ethical perspectives, and the interests/values of key societal stakeholder groups invested in teaching students hacking skills: Students of higher education, higher education, business/industry, government, and society.

The second part of this chapter (risk mitigation) addresses "RQ4 How to mitigate the risk

of students misusing the hacking skills learned in college or university later in life in criminal activities?" and focuses on exploring suitable S&T innovation risk governance initiatives. Under the banner of risk mitigation, recommendations were advanced by the thesis by applying the EDP-STEI-KW framework for ethical hacking teaching practices and ethical governance. Toward ethical design of teaching practices, the thesis recommends a novel OSINT Analyst cybersecurity role and associated body of knowledge (BoK) foundation framework. Toward ethical governance of hacking technology in society, the thesis recommends the professionalization of ethical hacking practitioners, accreditation/certification of ethical hacking skills, and a public policy initiative to govern or regulate the use of digital hacking technologies in ethical hacking teaching practices in higher education in Canada comprised of a networked centre of excellence of ethical hacking communities of practice as a research and governance approach focused on establishing effective ethical hacking teaching practices and addressing the cybersecurity skill gap, and a science, society and policy (policy innovation) decision making grid (see SSP-DMG: Research and governance knowledge management).

5.2. RQ3 What is the Risk to Society of Teaching Students Hacking Skills?

> Today, the already demanding task of companies to protect themselves against cyber threats is exacerbated by the phenomenon of the cyber security skill shortage, namely the lack of professionals with the knowledge and skills to perform a cyber security job. Companies would like to hire professionals in the cyber security sector but they are struggling to find them due to lack of skills. (Global Cyber Security Center, n.d.)

Contributing to a lack of skilled cybersecurity professionals worldwide, which is nearing 3 million globally according to the International Information Systems Security Certification

Consortium (ISC)², are a variety of factors, including rapid technology changes, hiring constraints, inadequate understanding of cybersecurity fundamentals, and the absence of a clear cyber career pathway for those entering the information security field (CISA, 2019).

> The amount of information can be overwhelming and conflicting. In addition, inconsistent language used in job titles and requirements can add to the uncertainty and discouragement. The limited understanding of prerequisite skills and knowledge required when entering the cybersecurity field, or advancing from an existing cyber role, is a significant hurdle. (CISA, 2019, p. 3)

While the cybersecurity risk continues to rise, Canada faces an acute shortage of cybersecurity experts. Programs teaching ethical hacking in higher education are steadily growing but there is a concern that students might use the attacks and vulnerability detection techniques outside of class maliciously (Hartley, 2006; Logan & Clarkson, 2005; Pashel, 2006; Pike, 2013; Sharma & Sefchek, 2007). Student "expulsions and convictions for hacking activities are on the rise and indicate that more needs to be done to protect students" (Pike, 2013, p. 69). Literature research revealed "little guidance in preparing students to responsibly use hacking skills learned in college" (Pike, 2013, p. 69). The ethical dilemma is that by possessing the same skills of criminals, students can better protect an IT system but there is a concern that teaching students hacking skills increases crime risk to society by drawing students toward criminal acts. Applying the precautionary principle: There is a concern that not teaching students hacking skills increases crime risk to society due to students' inability to protect themselves due to ignorance of emergent hacking technologies and how their use in society may pose a security or privacy risk. Further, there is a concern that not teaching students the necessary skills lies behind a cybersecurity skill gap.

5.2.1. Teaching ethical hacking skillset.

Ethical hacking as a broadly recognized curriculum or body of knowledge within the field of information security is not generally taught in higher education in CS, CE, and SE programs in Canada at the undergraduate level (the focus on the study). There is no evidence for a broad recognition that "ethical hacking" should be a subject matter with its own curriculum as a philosophy or a paradigm to teaching students hacking skills in higher education.

PPT11 says ethical hacking as an academic discipline is "non existent at this point. Needed, but non existent." "I hire a bunch of co-op students" to perform ethical hacking activities but "I've not seen anybody who's specifically done course work in ethical hacking." "I have not seen any professional development programs for it … the people that I work with that do ethical hacking tend to be people who have learned it on their own." Ethical hacking "is pretty much a black art that people learn kind of on their own." PPT11 says he does not think that higher education in Canada is teaching ethical hacking but it is something that is needed because currently it is a grey area.

> It's not like there's ethical hacking and there's non-ethical hacking … there's some grey spaces in the middle, and I think that by putting in place some kind of certification, or some kind of educational program, it helps delineate it better because I certainly know people who slide from the white hat a little bit to the grey, and back. It would be very helpful, I think, for some professional development programs to help kind of delineate what's needed out there, and bring it out of the shadows too. (PPT11)

"Ethical hacking" as an academic discipline remains a grey area. Curricula teaching ethical hacking skills variably make refence to cybersecurity, information security, IT security,

software security, Internet security, network security, and so on. Ethical hacking skills are taught in various CS/CE/SE curricula in the apparent absence of a broad strategic organizing or governing framework (e.g., see Canadian Cybersecurity Course Directory 2015 by SERENE-RISC, an NCE funded network of centre of excellence hosted by the Université de Montréal, Quebec.). Literature that focuses on ethical hacking as a professional practice in a Canadian context is lacking. There is no consensus on what is ethical hacking or what it should be and what are the skills and competencies required to function successfully at the various levels of the profession. Certification bodies have stepped to fill a gap left open by academia and are the sitting authority on what is ethical hacking or what it should be, as the various certification bodies see it (e.g., OSCP, CEH, PenTest+, and GPEN).

Industry certification has become a necessary credential recruiters look for in job applicants in information security. A survey by Global Knowledge in 2018 finds that 83 percent of IT professionals in the U.S. and Canada hold an IT certification; 44 percent of IT decision-makers say certifications result in employees performing work faster; 33 percent of IT decision-makers say certification results in more efficiency when implementing systems; and 23 percent of IT decision-makers say certification helps deploy products and services faster with fewer errors.

A broad framework of teaching ethical hacking skills in computer science and computer engineering undergraduate programs in higher education was construed based on in-depth interviews with ethical hacking university experts and industry practitioners (see Teaching Ethical Hacking Skillset Framework).

> The key idea is to teach students when they're designing networks, when they're designing software, these are vulnerabilities to watch out for, these are vulnerabilities to

> test for, but they're all the kinds of things that, if you are going to be a hacker, that you would need to know about, because you'd try to exploit those. And if you're an ethical hacker, you're going to try to exploit those just the same as if you're a black-hat hacker. (PPT3)

The discussion focuses on two skillsets, technical hacking skills and social hacking skills, and sheds light on the nature and potential causes of a Teaching vs Practice cybersecurity skill gap--that is, computer science and computer engineering programs should include more offensive hacking skills in the curricula, there is a need for hands-on experience/specializations in software and network security and security testing skills, and there is a need to establish credentials for ethical hacking practitioners through licensing/accreditation programs.

Teaching Ethical Hacking Skillset Framework

1. Technical hacking skills

1.1. Software security and software security testing

1.1.1. Vulnerability discovery and vulnerability assessment and knowledge of exploits, scripts, and viruses and how they work (PPT3, PPT8, PPT14, PPT6, PPT12).
1.1.2. Software coding and programing skills include knowledge of software languages, especially C, C++, and JavaScript (PPT3, PPT14, PPT12).

1.2. Network security and network security testing

Skills to protect a future employer's IT infrastructure or IT network system against unauthorized use or access, including how to test a company's defences (PPT3, PPT8, PPT14, PPT6, PPT12).

- Defense in depth (layered security to protect data/mission critical assets and information management system)
- A solid understanding of TCP/IP and network services
- Use of multiple information gathering techniques to identify and enumerate targets running various operating systems and services
- Ability to identify existing vulnerabilities and to execute organized attacks in a controlled manner

• Ability to identify and exploit XSS, SQL injection and file inclusion vulnerabilities in web applications
2. Social hacking skills 2.1. Countermeasures component 2.1.1. Prevention component: ethical-legal consequences 2.1.2. Teaching hacking skills as a comprehensive audit/as skills in QA/IA/IT governance frameworks (process focused) 2.2. Professionalism/Professional Practice in Society 2.2.1. Professional ethics 2.2.2. The social context (the social science context of technology use and professional practice) The sociopolitical and scientific values underlying the behavior of professional engineers The role of ethical hacking practitioners in historical and theoretical context

Interviewed ethical hacking university experts (PPT3, PPT8, and PPT14) discussed two approaches to teaching ethics to undergraduate students studying in CS/CE/SE programs: Countermeasures integrated with CS/CE/SE technical instruction, and as a separate course (e.g., professional practice). A two-prone approach to the instruction of social hacking skills includes instruction of a cybersecurity countermeasures component (the ethical-legal consequences of misusing hacking skills, and QA/IA approaches to information security), and instruction of Professionalism/Professional Practice in Society--as a program course requirement.

5.2.1.1. Software security and software security testing.

Software security testing practices include vulnerability discovery and vulnerability assessment and knowledge of what exploits exist and how they work, how viruses work, and how to write and execute scripts (PPT3, PPT8, PPT14, PPT6, PPT12). Software coding and programing skills include knowledge of software languages, especially C, C++, and JavaScript (PPT3, PPT14, PPT12).

PPT3 says teaching students secure software development means teaching them how to discover vulnerabilities and how to perform security testing.

> I teach about ethical hacking, and I say that it's valuable to learn the skills as a professional to be able to investigate your own software that you're developing to start with, to see if you can crack it, and that's a starting point, because you want to get your software to be defendable against people who are unscrupulous, and so for some testing purposes, you need to have basic hacking techniques to try and break into it and make sure that it's safe. (PPT3)

PPT14 says higher education should teach students how to "develop an awareness and expertise of what (hacking) tools are available" and "how exploits such as Metasploit, Nmap, etc. work" so as to be able to test their own products. "If you want to develop a good encryption algorithm, it's widely recognized that you need to know how to break cryptographic algorithms." PPT8 says the idea is to teach computer science students software skills so that "they become better developers. And they go out there and they build software with the recognition of the kind of ways their stuff can be exploited, and they know to avoid doing stupid things."

The second set of technical skills within the software security parcel refers to software coding or software programing skills. PPT14 says ethical hackers "must have knowledge of technical languages."

> The flaws that are exploited boil down to language-specific issues. You need to know C, even if you don't think C should be used in programming new systems. There is a large legacy base of C and C++ code that continues to be exploited. (PPT14)

Ethical hackers need to learn JavaScript because it is "inevitably used in web security exploits. JavaScript inserted into HTML pages as the basis for browser server interaction"

(PPT14). PPT12 adds, ethical hackers need knowledge of "a lot of different programming languages and with enough depth" that they can find implementation problems with them. Depending on "the depth of the ethical hacking exercise" ethical hackers may need "to be able to either edit or write shell scripts like something a system admin would do." "If you want to go really deep into it, you're going to want probably grab some binary files and do a reverse engineering on them … skills in terms of low-level skills like assembly language skills are very important." For PPT12, "a minimum toolkit" would be "a C, C++, a bit of java, Pearl, Python." Java "is mainly because of the server-side web, the middleware platforms. So, it's either doing ethical hacking or like a red alert, red-teaming on something which has a web front thing … This is where I see the Java, server side Java helpful." Python "is for all of the exploit development, the shell development. There's lots of libraries and toolkits … basically since 2008, 2009, Python became the defacto grand development language in the security field." "C, C++ is for the low-level applications, like understanding how the coding conventions work, for like when you're doing the assembly, the machine language assembly level" (PPT12).

5.2.1.2. Network security and network security testing.

The second broad area of technical hacking skills concerns equipping students with the necessary skills to protect their future employer's IT infrastructure or IT network system against unauthorized use or access, including how to test a company's defences. PPT14 says, to protect the IT system of their future employers, students would need to know what network hacking and testing tools are used in the wild, including

> vulnerability assessment tools like Nmap, things like Metasploit which have both the legitimate and non-legitimate uses. There's a tool called Netcat. Tools that allow you to

> do TCP/IP session hijacking. Tools that allow you to do ARP spoofing. There are very powerful toolkits that are available for free. And knowing how to use those is, I think, important. (PPT14)

PPT3 says students should know how to test a future employer's company defenses. "You might want to build skills to put yourself forward as a professional, to be able to say, Okay, this company, let's see if I can break into your systems using whatever tools I can, so that we can test its defenses." PPT6 says, students need skills related to "infrastructure layout" of a company's computer network. "On a basic level, you'd have a single layer of security, you have a firewall. And it's how do I get through that firewall? … then, as we get higher up, we start using packet sniffers … we basically look at interactions on the network."

5.2.1.3. The case for ethics instruction.

Pike (2013) is concerned whether college students of information security receive the necessary training to responsibly use hacking skills learned in college—that is, whether the academic training provides them with an environment where they gain the necessary experience and skills applying ethical principles. Literature research "revealed little guidance in preparing students to responsibly use hacking skills learned in college." It is not clear "that academic training environments provide students with an environment where they gain experience applying ethical practices" (Pike, 2013, p. 69). It is not clear students are receiving the necessary training to ensure that hacking skills and knowledge gained are not misused. Logan and Clarkson (2005) argue that computer science departments in higher education have been increasingly including information security content--hacking tools, methods, and other types of security testing and management skills "without much discussion of the potential for misuse or abuse by

students" (p. 157). "Universities should never assume that students learn ethical behavior, the laws on illegal network/computer access, outside (or before) their time at the university" (Logan & Clarkson, 2005, p. 160).

Pashel (2006) explored the ethics of teaching students how to hack at the university level and ways university computer security programs can help prevent the misuse of knowledge and skills gained in higher education. Overall, "instruction in ethical hacking would be a useful and critical component of computer security programs at universities" (p. 200). Given "the proper training in ethics and law, students who learn traditionally illegal computer skills in the course of studying computer security will use those skills for the greater good far more often than they will use them illegally and immorally" (p. 199). The key to effectively teaching students how to hack is in teaching them the ethical and legal implications of their skill, as well as the ramifications of misusing their skill (Pashel, 2006). "At present, few computing students are required to take ethics and law classes. It is unrealistic to expect these students to understand the full ramifications of their potentially illegal behavior if they are not schooled in these areas" (Pashel, 2006, p. 199). Students may not know clearly what is considered illegal. Students may not understand the ethical and social consequences of hacking. Universities "cannot assume that students are inherently ethical or knowledgeable and the likelihood that a student will use his newly acquired skills to commit a malevolent act will likely decrease dramatically when required to take computer ethics and law courses" (Pashel, 2006, p. 199).

Logan and Clarkson (2005) reviewed major requirements from the websites of the institutions listed on the National Security Administration website as Centers of Academic Excellence (CAE) in Information Assurance to determine whether universities required their computer science students to take a course in ethics and computer law. The NSA 2004 lists 59

universities that offer majors and have courses in information security to undergraduate and graduate levels. The analysis finds that 66% of them do not require undergraduate students to study ethical and/or legal issues as part of a degree program and 95% of all such institutions with graduate studies programs do not require ethics courses. “It is evident from these percentages that formal instruction in ethical and/or legal issues of computing is not a universal priority in CS curricula even in those institutions with a focus on security” (p. 160). Logan & Clarkson (2005) examined the syllabi for a variety of courses in security at CAEs and found that ethics about the use of computer facilities was not generally covered while unethical behaviour concerning cheating was fully explained in every syllabus.

Young et al. (2007) focused on the perceptions of active hackers recruited during a DefCon conference in Las Vegas about possible influence of social pressures as well as legal measures aimed at information security on their behaviour. Perception measures included moral disengagement, informal sanction, punishment severity, punishment certainty, and utility value. Moral disengagement refers to the cognitive processes that justify deviant conduct. Informal sanctions are reactions by others to the deviant behaviour of an individual. Punishment severity is the impact on an individual as a result of being publicly discovered engaging in an illegal or immoral act (e.g. prison time). Punishment certainty measures an individuals’ perception of the probability of being caught. A utility value perspective proposes that given a choice between two or more courses of action “a hacker will make a choice based on which provides the greatest level of gratification after consideration of the risks associated with the choices” (p. 283). The action of most interest was the decision to engage or not engage in illegal hacking. Previous research has shown that severity of punishment has little or no effect when the likelihood of punishment is low. Although punishment for hacking is severe, hackers may believe the chances

of being caught are low. Data was collected through handout surveys distributed to participants. The majority of the attendees were self-proclaimed hackers or people who have interest in hacking activities. Participation in the study was strictly voluntary. During the 3-day conference, 127 people filled out the survey. When asked if they had "participated in a hacking activity that would be considered outside the bound of that allowed by the courts system in the last year, 54 individuals (42.5%) answered yes" (Young et al., 2007, p. 283). The researchers regarded only the responses from the 54 respondents for the analysis. The respondents were asked to rate statements measuring the five dimensions of perception that are relevant to views on hacking.

The results of the study show that when compared to other attendees and the student population, hackers have a statistically significant higher level of moral disengagement. Hackers perceive that hacking is acceptable as long as no damage is done. Further, they believe hacking can help companies improve their defenses. Results suggest that hackers perceive a statistically significant lower level of informal sanctions against hacking; and that hackers perceive a statistically significant lower likelihood of getting caught. Further, while hackers and other conference attendees perceived the consequences of being caught engaging in illegal hacking activity as severe, students' perception of punishment severity was significantly lower than hackers and other conference attendee population. This is a noteworthy finding in light of the visual confirmation of the age group of the conference participants (hackers are mostly 12–28 years old). The overall results suggest that investments, tools and techniques that improve detection of security breaches and prosecution of hackers "may be more effective than increasing punishment and enacting more laws" (p. 286).

Xu et al. (2013) studied how computer hacking emerges in young people, why talented computer students become hackers, and how gray hats become black hats so as to "help schools,

universities, and society develop better policies and programs for addressing the phenomenon" (p. 65). Interviews with six known computer hackers in China addressed two main questions: How do hackers get started? and How and why do they evolve from innocent behaviour (such as curious exploration of school computer systems) to criminal acts (such as stealing intellectual property)? Three key insights emerged from the study. Firstly, computer hackers start out often as talented students, curious, exploratory, respected, and, importantly, fascinated by computers--not as delinquents or as social outcasts. "Our subjects indicated that many college students were involved in computer hacking, though only a small number ever become hackers who commit crimes using their skills, in college or after graduation. Most will find jobs in top-tier IT companies and information-security firms" (p. 70). There is "no guarantee our subjects, as students or as future employees, would not continue to use their increasingly sophisticated hacking skills to do harm." The primary constraining factor "seems to be their moral values and judgment about hacking" (p. 70). Secondly, "porous security, tolerance by teachers and school administrators, and association with like-minded individuals make for fertile ground in transforming young talents into hackers." Eliminating tolerance and "strengthening moral-value constraint appear to be the only manageable options in resisting hacking today" (pp. 73-74). Thirdly, moral values and judgment seem to be the only reliable differentiator between grey hats and black hats.

5.2.1.4. Countermeasures component.

Ethical hacking curricula should include a prevention component.

Ethical hacking curricula should include the ethical-legal consequences of misusing hacking skills learned in university as a prevention component integrated with the technical

instruction. Presently few computing students are required to study the ethical-legal consequences of misusing the hacking skills learned in college (Logan & Clarkson, 2005; Pashel, 2006). Interviewed university experts on ethical hacking said they teach ethics in an integrated way, that is, technical instruction is contextualized with the ethical-legal dimensions/consequences of misusing the skills. PPT3 says the ethical and legal components are a "key part of the course."

> We talk about a number of legal aspects broadly--liabilities, torts, contracts. In this case, we're talking mostly liability issues. Liability for leaving open vulnerabilities, and then of course there's the criminal aspect of, you have to make sure that you're not doing something that breaches the actual acts, teach about the various Acts that relate to information technology, privacy, security. PPT3

For PPT14, ethical hacking instruction entails teaching "the ethical side of it, what permissions you need, never to do this on someone's products or networks that you don't have permission for--all the things that if you want to retain the common understanding of ethical, you don't want to violate." Hackers "break in without permission. The number one rule has to be, never do this on a live system unless you have written permission from high senior officials" (PPT14). PPT8 says he talks to his computer science class about the potential ethical and legal consequences of misused talent. "I definitely spend at least a lecture talking about it … I tell them … I don't want to have to come bail you out." "You need the ethics," says PPT6, "because this is one industry where it's two sides of the same sword: ethical hacking, unethical hacking. Often, it's literally, do I have permission or not?" "I think every course needs ethics in it."

Ethical hacking should be taught as a comprehensive audit.

Hacking skills should be taught as a comprehensive audit using IA/IT governance approaches. “Many hacking books and classes are irresponsible. If these items are really being developed to help out the good guys, they should be developed and structured that way.” For Harris (2007), responsible hacking books should give information about how to break into systems as well as about defence and prevention measures.

> This means more than just showing how to exploit a vulnerability. These educational components should show the necessary countermeasures required to fight against these types of attacks, and how to implement preventive measures to help ensure that these vulnerabilities are not exploited. (Harris, 2007, The Controversy of Hacking Books, para. 3).

Universities are incorporating information security curricula at the undergraduate and graduate levels to address a national need for security education. The goals of such programs are “to reduce vulnerability in National Information Infrastructure by promoting higher education in information assurance and security, and to produce a growing number of professionals with information systems security expertise” (Sharma & Sefchek, 2007, p. 290). From the perspective of software security, CS programs should teach students hacking skills as skills in assurance (Radziwill et al., 2015). Students need to learn vulnerability discovery plus information security defense measures as part of a comprehensive audit. Students should be able to “perform vulnerability assessments on the entire spectrum of data assets: Applications, policies, procedures, and physical infrastructure,” but hacking performed on a network “should be part of a larger security audit process designed to reveal vulnerabilities and improve security policies and procedures” (Logan & Clarkson, 2005, p. 158).

5.2.1.5. Professionalism/Professional Practice in Society.

Professional ethics.

Three ethical hacking university experts mentioned professionalism as in professional ethics or a professional code of conduct that guides the behavior of professional engineers and computer scientists (PPT11, PPT3, PPT10). As a professional engineer, says PPT3, he is "bound by a number of codes of practice, of ethics." "As a professional engineer, I'm bound by the PEO code of ethics … I'm also bound by the software engineering code of ethics, the ACM code of ethics, the IEEE code of ethics, because I'm members of multiple societies that have codes." PPT3 says he teaches "five different codes of ethics. They are all broadly the same, but I teach about them to students."

> That is in the course calendar descriptions and it's also in our accreditation. We are accredited by CIPS, the Canadian Information Processing Society, and by the Canadian Engineering Accreditation Board, and both of those require us to teach students about ethics. (PPT3)

Emphasizing the importance of professional conduct (professional practice) for the industry/business side, PPT11 says, "It's the professionalism that large organizations are looking for to take you seriously."

The social context.

This area of ethical hacking instruction pertains to teaching the social science context of technology use and professional practice, and includes the sociopolitical and scientific values underlying the behavior of professional engineers and computer scientists and situating the role of ethical hacking practitioners in historical and theoretical context. The first point pertains to

following and teaching the scientific values of society, including a scientific approach to knowledge management/systematic thinking/systems thinking--and although not specifically cited by any of the interviewed participants, the second point pertains to teaching the sociopolitical values of society (open, scientific, knowledge-making society). PPT11 says the way to deal with the greyness in the academic discipline of ethical hacking is to teach following scientific values.

> It's kind of like when software engineering became an engineering discipline. There were a lot of coders that knew how to code, but they didn't have the mindset to approach it as a systematic large problem. I think ethical hacking is a very similar thing.

PPT11 adds, ethical hacking "has become more of an engineering type of discipline now. There's structure, there's rigor, there's tools out there that can be used for it … you need to systematically approach a problem, how to see if you can penetrate a system or not." It is "that systematic nature that most of the underground ethical hackers, or the small people, don't have because they've never had exposure to doing it in kind of an engineering mindset" (PPT11).

5.2.1.6. Teaching vs Practice insights.

The discussion focuses on two skillsets, technical hacking skills and social hacking skills, and sheds light on the nature and potential causes of a Teaching vs Practice cybersecurity skill gap--that is, computer science and computer engineering programs should include more offensive hacking skills in the curricula, there is a need for hands-on experience/specializations in software and network security and security testing skills, and there is a need to establish credentials for ethical hacking practitioners through licensing/accreditation programs.

PPT11 says programs in CS and CE in higher education should teach more offensive hacking skills. “The stuff you see in school is defensive that's being taught, how to secure systems.” For PPT12, teaching students hacking skills would entail teaching them how to find holes in software and network systems and how to conduct a full blown attack on an IT infrastructure or information management system. “For me, ethical hacking is done in an organization who wants to improve their security posture by doing full blown cybersecurity attacks on their infrastructure.”

> Basically finding holes in either the software infrastructure, could be the network infrastructure, could be the hardware involved as well. It could involve bad procedures which could lead eventually to a security hole and I would also include social hacking techniques as part of ethical hacking. (PPT12)

Interviewed participants from both camps--those who teach and those who practice ethical hacking or hire ethical hackers--supported a need to teach higher education students studying in CS and CE disciplines offensive hacking skills but with seemingly different levels of emphasis. Industry practitioners seemed generally more emphatic or explicit about the need for real-life offensive skills.

> If an organization wants to do it right … you want to get the people who could do it for malicious reasons. It's the same skill sets. If you don't have the same skill sets, the danger is adding it in such a way that would leave security holes or will leave potential attacks or potential attack surface which won't be revealed. (PPT12)

In comparison, university experts seemed less emphatic about the need to teach students more offensive hacking skills.

> As a professional engineer, I'm bound by the PEO code of ethics, and among the items in that, I shouldn't bring the profession into disrepute. So one has to be careful to be completely above-board, and make sure that one doesn't, for example, get bad press for teaching hacking. Because that could be considered to be bringing the profession into disrepute. I'm also bound by the software engineering code of ethics, the ACM code of ethics, the IEEE code of ethics … I'm bound by a number of codes of practice. (PPT3)

The university experts' general endorsement of teaching more offensive computer hacking skills can be construed from a combination of key words or expressions they used, and a seeming emphasis on certain defensive concepts such as vulnerability discovery, developing secure code, and security testing.

Interviewed ethical hacking university experts on teaching students offensive hacking skills

PPT3	PPT8	PPT14
Students "need to have basic hacking techniques to try and break into it and make sure that it's safe." "Okay, this company, let's see if I can break into your systems using whatever tools I can, so that we can test its defenses." "If you're an ethical hacker, you're going to try to exploit those just the same as if you're a black-hat hacker."	PPT8 supports teaching students "the mindset combined with knowledge." Ethical hackers have "an adversarial relationship with the developer of the application." Ethical hackers are "a professional adversary. That's what they are. They break the system. Good QA people have some commonality to this." "If you're going to design a good defense, you have to understand the offense. Because, if you don't understand how the offense is going to adapt and change in response to the defense, then you can't make it resilient."	"To develop a good encryption algorithm, it's widely recognized" that students "need to know how to break cryptographic algorithms"; if you don't know how to break (cryptographic algorithms), you don't know how … to protect (against them)." "I think if you don't have hands-on experience with the tools that are being used against you, you don't know how to defend against them."

Interviewed ethical hacking industry practitioners emphasized the necessity of hands on/specializations in cybersecurity skills.

> You need some hands-on experience, and that's where things like co-op programs come in. I've hired a number of co-op students, and if after two or three work terms, yes, they're market ready, but they need to have the hands-on, practical, in-the-field experience in security. (PPT11)

PPT6 says "right now, I mean, it's really hard to get that job right out of university because you don't have the skillsets or the experience … You have to do all these other certifications, and even then you're not necessarily ready, you're just kind of ready."

5.2.1.7. Ethical hacking high-level concepts.

Online course descriptions were surveyed for network security and network security testing ethical hacking (penetration testing) high-level concepts taught in CS/CE/SE curricula. Courses descriptions for select courses were surveyed for technical and social hacking skills against a provisional framework of skillsets, Ethical Hacking High-Level Concepts (3 Levels of Abstraction). The results are summarized in Table 11: Ethical Hacking Skills/Knowledge High-Level Concepts in CS/CE/SE Programs. The key highlights are,

- Ethical hacking techniques and skills regarding protecting information and technological infrastructure of information systems are dispersed across disciplinary areas within CS/CE/SE curricula.
- The most common concepts taught were Network protocols, TCP/IP model, and Access management, at about 70% of examined courses.

- The second most frequent concepts taught relate to defense in depth strategies access management/identity and access management, at about 50% of examined courses.
- The third most frequent concepts taught relate to IT security governance and the application of iterative, collaborative and holistic process management frameworks, including IA/QA approaches to IT security, and SDLC/agile software development approaches, both at about 35% of total examined courses.
- Less than 10% of surveyed courses (1/14) had any implicit reference to social hacking skills--that is, a course on designing secure computer systems (3 units) referenced "Ethical issues in computer security" which is a risk mitigation component (crime prevention component).

Ethical Hacking High-Level Concepts (3 Levels of Abstraction)

Technical hacking skills		
IT governance	Security/privacy policies and regulations and compliance	
IT security governance	IA/QA approaches to IT security	SDLC/agile software development/Design of security system and components DevSecOps/security-by-design
	Security testing	
	Security awareness	
Defense in depth	Access management	Access control Access and authentication IAM User security (passwords, identity, biometry)
	Social engineering	
	Application security	Cross site scripting attacks SQL injection attacks
	Operating system security	
	Layered security: IDS/IPS, firewalls, software security	

	Basic Cryptography and Tools	Cryptography, Key exchange, Security Policies; Encryption
Network protocols	Common network protocols Internet Protocol Suite (the TCP/IP protocol suite) The TCP/IP model and the OSI model	
Network enumeration and scanning techniques and technologies	Open technologies AI based intelligence gathering/surveillance technologies	
Types of network attacks (passive and active)		
Social hacking skills		
Risk mitigation component	Ethical-legal consequences/prevention component Audit/comprehensive approach to hacking education (vulnerability discovery and mitigation)	
Interdisciplinary educational lens (a social sciences content/context)	Social hacking values (tacit sociopolitical values made explicit) Philosophy of science/scientific method Science of security content	

Table 11: Ethical Hacking Skills/Knowledge High-Level Concepts in CS/CE/SE Programs

Course descriptions (numbers following the course code letters indicate program years. University 1 is the base of the table but corresponding courses in University 2 are identified)	Ethical hacking refences to elements in the "Ethical Hacking High-Level Concepts (3 Levels of Abstraction)" framework in course descriptions
CE3: An introductory course on data communications and networking (3 units)	Network protocols, TCP/IP model, Access management

CE4: A course on wireless networks (3 units)	Access management, Network protocols, TCP/IP model
CE4: A course on higher layer network protocols (3 units)	Common network protocols, TCP/IP model, OSI model
CE4: A course on network management of computer systems	Common network protocols, TCP/IP model, OSI model
CE4/CS4: A course on the secure design of computer systems (3 units)	Security policies--IT governance Security awareness--IT security governance User authentication--Defense in depth: Access management Application security mechanisms--Defense in depth: Application security Security of operating systems and software-- Defense in depth: Operating system security Encryption--Basic Cryptography and Tools: Encryption Firewalls-- Layered security: Firewalls Design of security system and components--IT security governance: IA/QA approaches to IT security, Security-by-design Devices for security analysis; sniffers, attack detectors--Network enumeration and scanning techniques and technologies Ethical issues in computer security--Risk mitigation component: Ethical-legal consequences/component
CS4: A course on computer networks protocols (3 units)	Common network protocols, TCP/IP model, OSI model

CS5: A course on cryptography and network security (3 units) Cross referenced to a corresponding course in University 2	Basic Cryptography and Tools: Cryptography, Key exchange Common network protocols, TCP/IP model, OSI model Access management: Access control, User Security (passwords, identity, biometry) Defense in depth: Layered security, Intrusions detection/intrusion prevention, firewalls, software security Types of network attacks (passive and active)
CS5: A course on authentication and software security (3 units) Cross referenced to a corresponding course in University 2	Defense in depth: Access management Access Control Access and authentication Common network protocols, TCP/IP model, OSI model IT security governance: IA/QA approaches to IT security SDLC/agile software development/Design of security system and components DevSecOps/security-by-design
CS5: A curse on computer security and usability (3 units) Cross referenced to a corresponding course in University 2	IT security governance: IA/QA approaches to IT security SDLC/agile software development/Design of security system and components DevSecOps/security-by-design
CS5: A course on the communication protocols of mobile and wireless networks (3 units) Cross referenced to a corresponding course in University 2	Common network protocols, TCP/IP model, OSI model
CS5: A course on wireless ad hoc networking (3 units) Cross referenced to a corresponding course in University 2	Common network protocols, TCP/IP model, OSI model, Access management

CS5: A course on evolving information networks (3 units) Cross referenced to a corresponding course in University 2	
CS5: A course on wireless networks and mobile computing (3 units) Cross referenced to a corresponding course in University 2	Common network protocols, TCP/IP model, OSI model, Access management
CS5: A course on data networks (3 units) Cross referenced to a corresponding course in University 2	Access management
SE4: A course on cloud systems and networks (3 units)	Access management (some aspects, e.g., cloud data center management and service provisioning)

5.2.1.8. Program requirements.

The study surveyed CS/CE/SE undergraduate programs in a Canadian university faculty of engineering for technical and social hacking courses taught and whether they were compulsory, optional, or elective. (There was no cybersecurity major or specialization within CS/CE/SE undergraduate programs at the same participating university.) The key highlights are,

- There were no "ethical hacking" courses per se taught in the explored Canadian universities.
- There was no requirement to teach a security course (in undergraduate CS/CE/SE programs). "Even though cybersecurity professionals are currently in high demand, specialized programs are limited, and nearly all computer science programs do not require cybersecurity coursework to graduate" (Radziwill et al., 2015).
- There was a compulsory ethics course, a professional practice course, taught to everyone in the CS/CE/SE programs at the faculty of engineering.
- There was no requirement to teach a social science course.

Program requirements at a Canadian university

Course/Program	CS Honours BSc in Computer Science (120 units)	CE BASc in Computer Engineering (129 units)	SE BASc in Software Engineering (129 units)
Technical hacking skills Ethical Hacking Cybersecurity AI/M/Algorithms	CS2: On data structures and algorithms (compulsory) CS3: On design and analysis of algorithms level I (compulsory)	CE4: On designing secure computer systems (elective) CS2: On data structures and algorithms (compulsory)	CE4: On designing secure computer systems (optional) CS2: On data structures and algorithms (compulsory) CS3: On design and analysis of algorithms level I (compulsory)

Social hacking skills Ethics: Professional ethics Professional conduct QA/IA/process-based quality governance frameworks Social science: Technology assessment	CS2: On professional practice (compulsory) Twelve course units of humanities or social sciences courses (electives)	A course on professional practice in IT and engineering (compulsory) History (year 2): On technology, society and environment (optional) Philosophy (year 2): On scientific thought and social values (optional)	SE2: On professional practice (compulsory) SE3: On software QA (compulsory) History (year 2): On technology, society and environment (elective)

5.2.2. Pedagogy as Communication

The second type of analysis constituted an examination of pedagogy as communication (sensemaking). Weick's sensemaking model was applied to explore variances in perceptions (inconsistencies in usage or application of words or concepts) in course content and underlying sensemaking opportunities (i.e., opportunities to construct common knowledge). The analysis focused on a CS course taught by two different instructors at a participating Canadian university who were also interviewed for the study, a course that is cross-referenced with the other participating university (as an equivalent or corresponding course).

The course syllabus for a computer systems security course taught by two interview participants (university professors teaching CS) at a Canadian university (PPT8 and PPT14) was selected for a closer examination of communication practices applying Weick's model. This allowed for the integration of interview data and organizational documentation in the analysis and assessment of whether there were differences in perceptions about what constitutes ethical hacking teaching practices and hacking skills. Other organizational document analysis focused on network security course descriptions for key skill themes--see Table 9: Hacking Skills Coding Table (Network Penetration Testing). Weick's sensemaking model was applied to explore variances in perceptions (inconsistencies in usage or application of words or concepts) in course

content/teaching practices and sensemaking opportunities (construction of common knowledge). The "STEI" part of STEI-KW was used to assess whether course technical and social content (and training) meet the needs of society--of open technologies/society technical and social knowledge pertaining to technology use in society taught, including tacit social values.

PPT8: Legal, ethical, and political content: There was no evidence of explicit refence to tacit open liberal political values or to ethical-legal consequences of misusing hacking skills.

PPT8: Sensemaking (Weick) opportunities: Communication routines/channels: Beside personal communication during class, the key nexus of communication with students was a wiki page at (link removed to ensure confidentiality) which is "the canonical source of information on this course." Students were advised to refer to it for updates: When significant changes are made to the document it will be either announced in lecture and/or posted in the course discussion forum. There were also online course discussions on (name of website removed for confidentiality). Students were advised to get an account on the wiki so that they can edit content--students were advised to email the course professor to get an account with their preferred username and email address.

PPT8: Constructivism: There was evidence of emphasis on hands-on exercises and training, for example, there was an "experience" scheduled for each week; further, there was evidence that students were given the opportunity to choose a topic for a comprehensive literature review assignment to develop their literature review or research proposal, start with a single research paper that they find interesting and that is related to distributed operating systems. PPT8 notes, "The only way you learn that is by doing … it takes practice, and it takes a certain mindset. The willingness, a stubbornness if anything."

PPT14: Legal, ethical, and political content: There was no evidence of explicit refence to tacit open liberal political values or to ethical-legal consequences of misusing hacking skills.

PPT14: Sensemaking (Weick) opportunities: Communication routines/channels: Beside personal communication during class, the key nexus of communication with students was OpenStack, in addition to the course's webpage at (link removed) and the lab's webpage at (link removed).

PPT14: Constructivism: There was evidence of emphasis on hands-on exercises and training, for example, there were 5 programming-based lab assignments, worth 8% each, two of them individual assignments, and two others are group assignments done in twos.

In conclusion, variances in perceptions: According to the course descriptions the key topics covered by PPT8 and PPT14 are the same: (description removed for confidentiality). The two universities explored as case studies are a seeming exception in that they seem to have synchronized the content of their courses (notably, courses are cross referenced in the program descriptions on the university websites).

The key area missing in the two examples is the non-technical content, specifically, the broader sociopolitical context, beside the lack of evidence of emphasis on the ethical and legal prevention components. This is especially relevant to a computer security course since cybersecurity is as much a social topic as it is a technical topic--it requires interdisciplinarity. Further, the course description did not indicate a holistic emphasis on cybersecurity education and mitigation (beside vulnerability discovery)--ethical hacking as an audit process--or an emphasis on IA/QA approaches to security governance. And, tacit scientific and sociopolitical values ought to be made explicit.

5.2.3. Technology Assessment: An Integrative Approach

STEI-DMG is applied as a social systems framework for identifying and analyzing the potential impacts of teaching students hacking skills to guide ethical decision making or ethical use governance through a comprehensive systems sociotechnical approach to technology assessment. An overarching pragmatic ethical assessment is applied to explore the risks and opportunities involved in teaching higher education students hacking skills--the potential benefits weighed against the potential costs and side effects, and the means weighed against the ends, to guide ethical decision making. Four ethical perspectives are integrated in the analysis: Duty/deontology, rights, virtue, and utilitarianism. Normative ethics is concerned with the standards and principles used to determine whether something is right or good, that is, the study of ethical action. It is a branch of philosophy that investigates the set of questions that arise when considering how one ought to act morally. While all ethical frameworks may result in the same or similar conclusions about what should be done, they will typically give different reasons for reaching those conclusions. The goal of ethical impact assessment is to facilitate rational public policy decision-making by articulating the ethical dimensions of any issue in a transparent manner. The findings integrate ethical perspectives/values/multi-disciplinary research and can be developed into policy (see STEI-DMG: Opportunities and Risks of Teaching Students Hacking Skills).

5.2.3.1. Ethical perspectives and frameworks.

Normative ethics is concerned with the standards and principles used to determine whether something is right or good, that is, the study of ethical action. It is a branch of philosophy that investigates the set of questions that arise when considering how one ought to act

morally. Four ethical perspectives are integrated for the analysis: Duty/deontology, rights, virtue, and utility (see Table 21: Ethical Frameworks). While all ethical frameworks may result in the same or similar conclusions about what should be done, they will typically give different reasons for reaching those conclusions.

Deontology asserts that an action is morally right if it is done out of a sense of duty. A duty perspective is generally concerned with the individual's obligations toward others (the collective). Duties are considered as "natural, universal, rational, and self-evident" (May, 2012, p. 22). In moral law "one performs an action because of an obligation to follow a set of standards or rules," hence people have a duty to obey moral guidelines. In deontology "actions are judged on the intrinsic character of the act rather than on its effects" (May, 2012, p. 22). For Kant, right actions are actions done without qualification. Kant invoked the categorical imperative to specify the universal character of duty: "One ought only to act such that the principle of one's act could become a universal law of human action in a world in which one would hope to live" (p. 22). What is right for one person is right for everyone. From this perspective improving the ethics of an organization would require developing universal ethical principles "rationally derived—that are enacted out a sense of duty or responsibility" (p. 23).

A rights perspective, like the duty perspective, universalizes ethics, hence rights are considered inalienable, such as rights ingrained in the U.S. Constitution. Human rights are granted naturally and cannot be altered because they are rationally self-evident. A rights perspective aims "to establish a social compact, or contract (hence, often called the contractarian alternative to deontology), of rights that are maintained between individuals and the community" (May, 2012, p. 24). For John Locke all persons are born with, and possess, basic natural rights, possessed by everyone equally. Rights constitute the basis by which actions of individuals and

institutions ought to be judged. For Locke, the social contract between people can only be maintained if human rights are developed, maintained, and preserved. For John Rawls, the standard for ethical action is based on a reasonable position. Rawls argued that rights can be determined by placing persons behind a veil of ignorance where they cannot anticipate how their own actions might affect them--such that no person can expect to either benefit or to be harmed any more than others. Both Locke and Rawls sought to create principles and practices of justice through rights. For both, no society can be just if it is devoid of rights for its people. From this perspective, improving the ethics of an organization would place emphasis on compliance and legally sanctioned rights, such as those stipulated in the US Equal Employment Opportunity Commission (EEOC) guidelines.

In virtue ethics, people have the duty to self-actualize and, therefore, should be granted the right to accomplish that self-actualization. All humans are born with inherent potential, and human development becomes a struggle for self-actualization. “An action is judged based on whether it allows for expression of full potential, thus creating benefits for both the individual and the community” (May, 2012, p. 26). The development of virtue is seen as requiring the cultivation of good habits that occur within a social realm--thereby ethics is seen to involve being a contributing member of a community. Society then “has an obligation to develop educational and learning opportunities for citizens to develop their full potential” (p. 27). A virtue is often seen as an internal capacity of humans that produces ethical behaviour. Plato identified justice, courage, temperance, and wisdom as the most important virtues. From this perspective, improving the ethics of an organization would focus on strengthening personal and institutional virtues in order to maximize human potential within and outside of the organization.

Consequentialism holds that an action is morally right if its consequences are beneficial and morally wrong if its consequences of are harmful. Utilitarianism holds that an action is morally wrong if its results are more harmful than beneficial. A utility perspective judges actions based on their consequences. For Bentham, a principle of utility is necessary in order to evaluate whether an action creates the greatest happiness in relation to other alternatives, considering both the immediate consequences as well as the long-term effects of actions. Similarly for John Stuart Mill the purpose of ethical action is "to achieve the greatest overall happiness for the greatest number and actions are evaluated by the extent to which they contribute to that end" (May, 2012, pp. 25-26). An ethical approach to utility "would require moving beyond traditional economic models of cost-benefit analysis to consider which decisions benefit the greatest number with the greatest good. As a result, organizations might have to consider the unintended and long-term consequences of their actions. Members of an organization drawing on utility-based ethics may ask these questions: Have we considered all alternative actions and selected the one that produces the greatest good or pleasure? How can we best serve the ends of the collective rather than the individual? What specific actions or general rules will either maximize or minimize "good"?

Table 21: Ethical Frameworks

Ethical perspective	Definition of ethical conduct	Ethical approach
1) Deontology (duty, obligation, or rule-based ethics.) In deontology, "actions are judged on the intrinsic character of the act rather than on its effects" (p. 22). What is right for one person is right for everyone.	Ethical conduct involves always doing the right thing: Never failing to do one's duty. For Kant, acting ethically means choosing to obey the universal moral law.	The duty approach: Which action respects social moral obligations or rules? "The ethical action is one taken from duty, that is, it is done precisely because

In moral law, "one performs an action because of an obligation to follow a set of standards or rules" (May, 2012, p. 22). From this perspective improving the ethics of an organization would require developing universal ethical principles "rationally derived—that are enacted out of a sense of duty or responsibility" (May, 2012, p. 23). Ethical obligations are the same for everyone (universal), and knowledge of what these obligations entail is arrived at by discovering rules of behavior that are not contradicted by reason. <In acting according to a law that we have discovered to be rational according to our own universal reason, we are acting autonomously (in a self-regulating fashion), and thus are bound by duty, a duty we have given ourselves as rational creatures. We thus freely choose (we will) to bind ourselves to the moral law.> (Kant's Moral Philosophy, Stanford Encyclopedia of Philosophy)		it is our obligation to perform the action" (Brown University, 2013).
2) Rights For John Locke all persons are born with and possess basic natural rights, possessed by everyone equally. For John Rawls, contractualism held that moral acts were those which people would all agree to if they were disinterested (deciding from behind a "veil of ignorance" unbiased by personal interest). Both Locke and Rawls sought to create principles and practices of justice through rights. For both, no society can be just if it is devoid of rights for its people. From this perspective, improving the ethics of an organization would place	The best ethical action is that which protects the ethical rights of those who are affected by the action.	The rights approach: Which action respects the rights of all who have a stake in the decision? The justice approach (social contract): Which action treats people equally or proportionately?

emphasis on compliance and legally sanctioned rights, such as those stipulated in the US Equal Employment Opportunity Commission (EEOC) guidelines. The Fairness or Justice Approach of Rawls argued along Kantian lines that just ethical principles are those that would be chosen by free and rational people in an initial situation of equality. This is based on a formulation of Kant's categorical imperative that says: "Act in such a way that you treat humanity, whether in your own person or in the person of another, always at the same time as an end and never simply as a means to an end."		
3) Virtue In virtue ethics, people have the duty to self-actualize and, therefore, should be granted the right to accomplish that self-actualization. All humans are born with inherent potential, and human development becomes a struggle for self-actualization. "An action is judged based on whether it allows for expression of full potential, thus creating benefits for both the individual and the community" (May, 2012, p. 26). The development of virtue is seen as requiring the cultivation of good habits that occur within a social realm--thereby ethics is seen to involve being a contributing member of a community. Society then "has an obligation to develop educational and learning opportunities for citizens to develop their full potential" (p. 27). A virtue is often seen as an internal capacity of humans that produces ethical behaviour. Plato identified justice, courage, temperance, and wisdom as the most important virtues.	Ethical conduct is whatever a fully virtuous person would do in the circumstances. "An action is judged based on whether it allows for expression of full potential, thus creating benefits for both the individual and the community" (May, 2012, p. 26).	The virtue approach: Which action leads me to act as the sort of person I should be? What are the character traits (either positive or negative) that might motivate us in a given situation?

From this perspective, improving the ethics of an organization would focus on strengthening personal and institutional virtues in order to maximize human potential within and outside of the organization.		
4) Utilitarian "All Utilitarians would abide by the principle of producing the most good with the least harm. A utility perspective judges actions based on their consequences. For Jeremy Bentham, a principle of utility is necessary in order to evaluate whether an action creates the greatest happiness in relation to other alternatives, considering both the immediate consequences as well as the long-term effects of actions. Similarly for John Stuart Mill the purpose of ethical action is "to achieve the greatest overall happiness for the greatest number and actions are evaluated by the extent to which they contribute to that end" (May, 2012, pp. 25-26). From this perspective, improving the ethics of an organization would seek to create change that will have positive consequences for the organization and its stakeholders. An ethical approach to utility "would require moving beyond traditional economic models of cost-benefit analysis to consider which decisions benefit the greatest number with the greatest good. As a result, organizations might have to consider the unintended and long-term consequences of their actions. Members of an organization drawing on utility-based ethics may ask these questions: Have we considered all alternative actions and	Ethical conduct is the action that will achieve the best consequences.	The utilitarian approach: Which action will produce the most good and do the least harm?

selected the one that produces the greatest good or pleasure? How can we best serve the ends of the collective rather than the individual? What specific actions or general rules will either maximize or minimize "good"?		

Analysis using STEI-DMG allows for an integrative approach to decision making and governance of AI based intelligence gathering ethical hacking technology, by leveraging interdisciplinary and multi-stakeholder knowledge needed to understand the sociotechnical complexity of ethical hacking technology use in society. A technology impact assessment was performed from key stakeholder perspectives against a sociotechnical social science (sociology) perspective framed within STS and focusing on ethical knowledge making/intelligence gathering technologies--focusing on OSINT and network enumeration and scanning intelligence gathering technologies and how they may undermine privacy (information security or confidentiality and political autonomy).

STEI-DMG: Opportunities and Risks of Teaching Students Hacking Skills

Sociotechnical (social science) perspective vs. Stakeholder perspective	Society		Business/industry	
Impact analysis	Intended ends	Possible side effects	Intended ends	Possible side effects
>Social	Address a cybersecurity skill/knowledge gap (a national vulnerability):	Rising student hacking crime.	• to address a cybersecurity skill gap: cybersecurity professionals are needed for IT security;	AI based intelligence technologies can be used in spying on businesses.

	• to reduce the risk of rising student hacking crime; • to address a cybersecurity skill gap that threatens stable business and government; and • to protect students by teaching social hacking skills (mitigation/ethical and legal consequences).		• to teach ethical hacking (penetration testing as information security testing) taught within an IT governance framework; and • to teach AI based intelligence/surveillance technologies especially network security and network awareness applications (to improve security and business performance, especially in BI applications). • CS/CE programs should teach students hacking skills with mitigation: 1) teach the ethical-legal consequences and 2) teach as assurance/IA/QA holistic audit approach to security management.	
>Technical				
>Ethics Duty	The duty approach: Which action respects social moral obligations or rules? Doing the right thing means teaching students the necessary ST hacking skills to empower them to protect themselves	There may be a tendency to underestimate the need to weigh the benefits against the potential risks of using the various hacking and	Support teaching students hacking skills because a vibrant economy needs it (to maintain the standard/quality of living.	Misuse of surveillance technologies in spying or in committing insider's data breaches.

	and to protect society--to support national security (to offer citizens "social contract" security/privacy them expect).	surveillance technologies --some are more dangerous than others--there is a need for a risk-based regulation.		
Rights	Teach students hacking skills because this respects their right to education that will help them succeed in life.	Students may commit crime or unethical acts. The risks have to be weighed against the potential benefits.	Businesses would like to find ethical hacking talent to remain in business.	Students to learn skills that meet the needs of business, correspondin g to ST changes.
Virtue	In virtue ethics, society "has an obligation to develop educational and learning opportunities for citizens to develop their full potential" (May, 2012, p. 27). Students ought to be given the opportunities to achieve self-actualization--they ought to be taught hacking skills to enable them to realize their full potential.	Because it emphasizes the importance of role models and education to ethical behavior, it can sometimes merely reinforce current cultural norms as the standard of ethical behavior. Emphasizing virtues can	Business should find channels to help students self-actualize in collaboration with academia, e.g., through cybersecurity talent competition, internships, and scholarships.	

		make it more difficult to resolve disputes, as there can often be more disagreement about virtuous traits than ethical actions.		
Utilitarianism	Utilitarians would argue that teaching students hacking skills is ethical because it reduces crime risk and thus produces the greatest amount of good with the least harm.	Some harm might be done and hence a need to consider how everyone's rights have been respected.	Teach students the skills the industry needs, as it produces the greatest good and least harm.	The risk to be weighed against the benefit.

Sociotechnical (social science) perspective vs. Stakeholder perspective	Higher education		Students	
Impact analysis	Intended ends	Possible side effects	Intended ends	Possible side effects
>Social	• to prepare college and university students with the skills and knowledge necessary for employme	Social stigma drives down enrollment in hacking disciplines and discourages professors from highlighting their hacking careers. News leaks about hacking activities can	• to help students become employable; • to prepare students for success in their future employment; • to help students protect data assets of future employers; and • to help students protect themselves	Students would commit hacking crime without realizing it if they are not clear on the

	nt (Weingarten & Hicks, 2018) as well as to equip them with skills and tools to investigate and think critically so as to be socially responsible, productive, and engaged citizens; • to "produce a growing number of professionals with information systems security expertise" (Sharma & Sefchek, 2007, p. 290); and • to "reduce vulnerability in National Information Infrastructure by promoting higher education in informatio	raise concerns about the reputation of institutions due to the social stigma associated with hacking activities.	against confidentiality and autonomy privacy attacks.	ramifications of hacking to themselves and to society.

	n assurance and security."			
>Technical	To protect higher education institutions—most attacks of data breaches are insider's.		To protect their employer: 1) Hacking skills are equivalent to audit skills "as both are designed to discover flaws in the protection of data and secure operation of a system"; 2) knowledge of hacking skills and practice improves security by informing network administrators how an exploit can be executed; and 3) a systems administrator must possess the same skills as the attacker to provide the best security defense (Logan & Clarkson, 2005, p. 157).	
>Ethics Duty	Higher education has a moral duty to teach hacking skills to students which will help students later on in their personal and professional lives.	Students may misuse the hacking skills they learned in unethical or unlawful acts.	Students have a moral duty to learn ethical hacking to be able to protect themselves, and the nation, and not to use the skills unlawfully or unethically.	The duty to learn hacking has to be measured against the student's right to self-actualization (they may not be interested in the topic of security).

Rights	The reputation and financial performance of the institution should not hurt by some bad press.	The risk of teaching should be weighed against the benefits of teaching students hacking skills.	Students have a right to good education to succeed later in life. Students have a universal right to learn hacking skills for self-protection, for employment (the right to work), a "the right to know"; the right to equal access to knowledge/skills/citizenship rights; and in general the right to self-actualize.	
Virtue	Higher education to develop teaching practices to help students develop their full potential" (p. 27). Students ought to be given the opportunities to achieve self-actualization--they ought to be taught hacking skills to enable them to realize their maximum potential. It can be argued that hacking for	Defense/countermeasures ought to be included in education	Students ought to be given the opportunities to achieve self-actualization.	

	the goal of self-actualization is ethical, if hackers do it to realize their full potential.			
Utilitarianism	Teaching students hacking skills helps national security and have a net positive contribution to society.	There is a need not to ignore fairness when teaching: are mitigation and countermeasures being taught? Are social as well as technical skills being taught (for effective education).	Students would be able to protect themselves and find work which supports an overall good of supporting national security.	

Sociotechnical (social science) perspective vs. Stakeholder perspective	Government	
Impact analysis	Intended ends	Possible side effects
>Social	Teach students the necessary skills to enhance national security: • to help Canada achieve its National Cyber Security Strategy 2018 policy goals: • security and resilience, • cyber innovation, and • leadership and collaboration (Shull, 2019). • to address a rising national need for security education--to reduce vulnerability in the national information infrastructure (Sharma & Sefchek, 2007, p. 290); • to secure the digital infrastructure in	Students would spy on the government as employees or as outsiders.

	light of a worsening crisis of trust.	
>Technical		
>Ethics Duty	The government has a moral duty to support teaching students hacking skills so as to protect the national security and political stability.	Some students may misuse the technology skills as an insider from outside government.
Rights	Government needs qualified citizens to safeguard national security.	
Virtue	Students ought to be given the opportunities to achieve self-actualization--they ought to be taught hacking skills to enable them to realize their maximum potential.	
Utilitarianism	Students should know the cyberthreat landscape and extent of politicization of personal communication (the expanding digital net has brought the citizens to forefront of the cybersecurity battle.	

Step 1: Evaluate the intended ends and possible side effects of teaching students hacking skills to discern overall value.

Intended ends of teaching students hacking skills.

From society's perspective, first, teaching students hacking skills helps Canada address a cybersecurity skill/knowledge gap, a national security vulnerability. Teaching students hacking skills aims to reduce crime risk to society, that is, to reduce the risk of students committing criminal acts (or perform unethical privacy breaches) with the skills acquired in an ethical hacking course (Logan & Clarkson, 2005; Pike, 2013; Sharma & Sefchek, 2007); and it aims to address a cybersecurity skill gap that threatens a stable business and government environment in a globalized ICT network that has politicized business and personal communication--it has brought society and what is social to the forefront of the battle for cybersecurity. Second,

teaching students hacking skills aims to help protects students from incarceration for committing hacking crime. “Student expulsions and convictions for hacking activities are on the rise and indicate that more needs to be done to protect students” (Pike, 2013, p. 69).

From the government’s perspective, teaching students hacking skills helps Canada achieve its national security objectives. First, the Government of Canada’s national cybersecurity efforts set out in the National Cyber Security Strategy released in June 2018 links security, innovation, and prosperity with focus on three policy themes (Shull, 2019, p. 5): 1) Security and resilience (to enhance cyber security capabilities to better protect Canadians and defend critical government and private sector systems); 2) cyber innovation (to position Canada as a global leader in cyber security); and 3) leadership and collaboration (to have the federal government of Canada lead work to shape the international cyber security environment in Canada’s favour). Second, Canada needs ethical hacking professionals with the necessary skills to address a rising national need for information security education--to reduce vulnerability in the national information infrastructure “by promoting higher education in information assurance and security, and to produce a growing number of professionals with information management systems security expertise” (Sharma & Sefchek, 2007, p. 290). Third, Canada needs future citizens and ethical hacking professionals able to secure the digital infrastructure so as to maintain a stable political system based on trust in light of a worsening crisis of trust.

From the students’ perspective, teaching students hacking skills pertains to four key objectives. First, to help students protect themselves against confidentiality and autonomy privacy attacks. “Courses have been designed to teach students to hack, with the implication that it is a necessary security practice and that it will improve employability as a network administrator charged with protecting valuable corporate assets” (Logan & Clarkson, 2005, p.

157). Second, to help students protect data assets and computer network infrastructure of future employers, as well as the national critical infrastructure. Teaching hacking as "a method of teaching students how to protect the data assets of future employers" (Logan & Clarkson, 2005, p. 157). Third, to help students become employable. Fourth, to prepare students for success in their future employment.

From the business/industry perspective, teaching students hacking skills aims to address a cybersecurity skill gap: Professional ethical hackers/cybersecurity professionals are needed for IT security with knowledge of user security awareness training as well as network security and network awareness (continuous monitoring of network traffic, e.g., using "sniffers"). Students need skills in IA/QA holistic approaches to security management. "From the perspective of software security, hacking skills specifically should be promoted as a means to develop skills in assurance, application design, and quality assurance" (Radziwill et al., 2015). They also need skills in AI based intelligence/surveillance technologies applications especially in network security/network awareness (including data mining and machine learning based information security testing and management applications).

From the perspective of higher education, the primary purpose of higher education is to prepare college and university students with the skills and knowledge necessary for employment (Weingarten & Hicks, 2018)--which means addressing a cybersecurity skill gap, the first key objective or interest--as well as to equip them with skills and tools to investigate and think critically so as to be socially responsible, productive, and engaged citizens, that is, to self-actualize. The second objective is, universities are incorporating information security courses at the undergraduate and graduate levels to address a national need for security education--to buttress national security, that is, "to produce a growing number of professionals with

information systems security expertise" so as to reduce vulnerability in critical infrastructure and to protect the digital infrastructure (Sharma & Sefchek, 2007, p. 290).

Possible side effects of teaching students hacking skills,

- Students would spy on the government as employees or as outsiders;
- Rising student hacking crime;
- Students would commit hacking crime without realizing it if they are not clear on the ramifications of hacking to themselves and to society;
- AI based intelligence technologies can be used in spying on businesses (compliance and legal culpability concerns); and
- Social stigma drives down enrollment in hacking disciplines and discourages professors from highlighting their hacking skills and careers. News leaks about hacking activities can raise concerns about the reputation of institutions due to the social stigma associated with hacking activities.

Step 2: Compare the means and intended ends in terms of technical and nontechnical aspects (moral, social).

Three key arguments have been used in justification for teaching hacking skills in information security courses at both the undergraduate and graduate levels: 1) Hacking skills are equivalent to audit skills "as both are designed to discover flaws in the protection of data and secure operation of a system"; 2) knowledge of hacking skills and practice improves security by informing network administrators how an exploit can be executed; and 3) a systems administrator must possess the same skills as the attacker to provide the best security defense (Logan & Clarkson, 2005, p. 157). Teaching hacking skills focuses on the need to better understand hackers and hacking attacks (Logan & Clarkson, 2005; Pike, 2013). By

understanding how to hack, a student understands how a hacker might attempt an attack a system, and can identify the signs of a security breach--enabling them to identify and correct security flaws. “The same tools and skills as hackers”: AI based intelligence/surveillance technologies especially in network security and network awareness applications (including data mining and machine learning)--e.g., applications in detecting cybersecurity threats (IDS/IPS or applications in network enumeration and port scanning) used in information security, in crime by criminals, and in political economic surveillance.

Step 3: Reject any action where the output (overall value) does not balance the input in terms of efficiency and fairness (overall assessment of technology use in society in terms of efficiency and fairness).

Intended ends of teaching students hacking skills--universities are incorporating ethical hacking skills at the undergraduate and graduate levels in computer science and computer engineering majors:

- To support national security by having a skilled population of ethical hacking professionals graduates of higher education;
- To protect (secure) the national ICT digital infrastructure;
- To prevent cyber attacks against national critical infrastructure;
- To lower crime risk to society: By empowering students with the necessary ST skills/ability to protect themselves (their privacy) on the ICT grid as well as to protect their future employer’s data assets and network infrastructure.
- To help students be employable;
- To help students achieve success with their future employers; and
- To address a cybersecurity skill gap.

- Duty perspective: Doing the right thing means teaching students the necessary ST hacking skills to empower them to protect themselves and to protect society--to support national security (to offer citizens "social contract" security/privacy them expect).
- Rights perspective: Teaching students hacking skills is ethical because this respects their right to education that will help them succeed in life.
- Virtue perspective: Society "has an obligation to develop educational and learning opportunities for citizens to develop their full potential" (May, 2012, p. 27). Students ought to be given the opportunities to achieve self-actualization--they ought to be taught hacking skills to enable them to realize their full potential.
- Utilitarian perspective: Teaching students hacking skills is ethical because it reduces crime risk and thus produces the greatest amount of good with the least harm.

Possible side effects of teaching students hacking skills,

- Students would spy on the government as employees or as outsiders;
- Rising student hacking crime;
- Students would commit hacking crime without realizing it if they are not clear on the ramifications of hacking to themselves and to society;
- AI based intelligence technologies can be used in spying on businesses (compliance and legal culpability concerns);
- Social stigma drives down enrollment in hacking disciplines and discourages professors from highlighting their hacking careers;
- Duty perspective: There may be a tendency to underestimate the need to weigh the benefits against the potential risks of using the various hacking and surveillance

technologies--some are more dangerous than others--there is a need for a risk-based regulation;

- Rights perspective: Students may commit crime or unethical acts. The risks have to be weighed against the potential benefits;
- Virtue perspective: Because it emphasizes the importance of role models and education to ethical behavior, it can sometimes merely reinforce current cultural norms as the standard of ethical behavior. Emphasizing virtues can make it more difficult to resolve disputes, as there can often be more disagreement about virtuous traits than ethical actions; and
- Utilitarian perspective: Some harm might be done and hence a need to consider how everyone's rights have been respected.

There is a need for pragmatism, for solutions that leverage the opportunities (intended ends/potential benefits) and reduce the risk (potential side effects) through a broad-based decision making/policymaking process, an integrative approach--that is, we need to regulate the use of emergent disruptive hacking technologies through a public policy taking a risk-based approach to decision making emphasizing innovation. An ethical impact assessment of technology use in society integrates research, stakeholder perspectives/interests and societal values--to inform effective policy development.

5.2.4. Recommendations.

Two sets of recommendations are presented. The first set of recommendations was synthesized from literature review, in-depth interviews, and the technology impact assessment performed using STEI-DMG and pertain to 1) the instruction method of ethical hacking: It should be holistic, interdisciplinary, there is a need to standardize/systematize an ethical hacking

body of knowledge, and a need to be explicit about tacit scientific and sociopolitical values; and 2) the technical and social hacking skills taught. The second set of recommendations was derived from theory (EDP-STEI-KW) and focused on S&T innovation risk mitigation initiatives.

The instruction method of ethical hacking.

The increasing exposure risk due to increasing interconnectedness (expansion of the attack surface) on an internationalized and globalized ICT network has brought ordinary Canadians to the forefront of the sociopolitical cybersecurity battle. Addressing the emerging national and international challenges of a rising and increasingly more complex and internationalized cybersecurity threat landscape will require a broader approach to education "which may not be achieved through dedicated cybersecurity programs" (Radziwill et al., 2015, p. 5). Sociopolitical changes "are introducing new expectations of the current and entering workforce at the same time that they are bringing their own shifting expectations of the workplace. All these changes are creating new opportunities and threats and demanding a reinvention of human resource management" (EDUCAUSE, 2019). Professional ethical hackers increasingly need a strong interdisciplinary foundation to cybersecurity education and governance. "Penetration testing is a highly technical and complex field. An ethical hacker requires deep knowledge across many areas, including, but not limited to software, hardware, networking, and even human behavior" (Thomas et al., 2018, p. 3). Cyber defense research teams increasingly need skills/knowledge beyond computer science, electrical engineering, software and hardware security, "but also political theory, institutional theory, behavioral science, deterrence theory, ethics, international law, international relations, and additional social sciences" (Kallberg & Thuraisingham 2012, p. 2).

Ethical hacking skills should be taught in a social science context, as it exists at the intersection of various disciplinary areas, taking an interdisciplinary approach. There is a need for an interdisciplinary approach to ethical hacking education that puts technical hacking skills and knowledge making in a broader sociopolitical perspective. Hence, ethical hacking skills can be taught within a STS sociotechnical framework. An interdisciplinary approach can help anchor the role of ethical hacking practitioners in historical and theoretical context. For Habash (2019), the composite engineer has a balanced mix of technical and social hacking skills. Further, higher education should take a holistic approach to cybersecurity education by giving the necessary information security education and training to higher education students for self-protection (against privacy attacks) by integrating ethical hacking teaching across all curricula or by offering students security awareness training where the credits are counted toward their total credit requirements (most data breaches are insider's).

There is a need for the systematization and standardization of ethical hacking knowledge in society. The standardization and systematization of ethical hacking as a body a knowledge open for scrutiny and peer review is analogous to how the open source community works and its philosophy (PPT11).

> If you have a proprietary set of skills, and a proprietary set of tools, and a proprietary set of methodology, it's not going to be widespread and shared, and improved across the industry.

But by "bringing it out in the open" by having "a standardized methodology of teaching, a standardized baseline of teaching, it allows the opportunity to be peer reviewed, and to be improved, and to be constantly updated" (PPT11).

Further, there is a need to make explicit what are tacit sociopolitical and scientific values shaping or governing the use of technology in society (especially, respecting the rule of law, the right to privacy and political autonomy, and the right to free expression without fear of retribution). Curricula should make explicit social values that constitute the broader social context of technology use and professional practice.

The technical and social hacking skills taught.

Higher education should teach more technical hacking skills. Hartley (2005), Logan and Clarkson (2005), Pashel (2006), Pike (2013), and Sharma and Sefchek (2007) all agreed, as did both ethical hacking experts and practitioners interviewed, that teaching students hacking skills has a net benefit to society.

Pike (2013) interviewed information security professionals for guidance on improving ethical hacking educational in higher education and found that support for integrating hacking into cybersecurity curricula was unanimous. A total of 206 interviews were conducted during three information security conferences in the Southwestern United States in the spring of 2013. All of the interviewees were self-proclaimed information security professionals with at least one year of experience. The 206 interviewees responded that ethical hacking should be included in cybersecurity courses at the university level. Most of the interviewees offered one or more recommendations to help protect students. Pike's (2013) recommendations were grouped into several categories: 1) Social interaction/support system, 2) Competition, 3) Recognition, and 4) Ongoing skills development. Most strikingly, respondents mentioned the need for positive social groups more often than any of the other recommendations. Group affiliation and teamwork was evident for both white-hat and black-hat hackers, and the importance of these affiliations was

evident. Pike (2013) proposes that the creation of "student peer groups that support white-hat hacking practices, with ethical and moral codes that are guided by the rule of law, will reduce the likelihood of student engagement in unethical activities" (p. 71).

The in-depth interviews shed light on the nature and potential causes of a Teaching vs Practice cybersecurity skill gap--that is, computer science and computer engineering programs should include more offensive hacking skills in the curricula, there is a need for hands-on experience/specializations in software and network security and security testing skills, and there is a need to establish credentials for ethical hacking practitioners through licensing/accreditation programs.

Higher education should teach more social hacking skills. CS/CE/SE programs should teach students hacking skills in conjunction with suitable mitigation countermeasures: The ethical-legal consequences of misusing hacking skills (a prevention component), and hacking should be taught as a comprehensive audit/skills in assurance (QA/IA approaches). From the perspective of software security, hacking skills "should be promoted as a means to develop skills in assurance, application design, and quality assurance" (Radziwill et al., 2015).

There was broad agreement among interviewed ethical hacking experts and practitioners on the need to teach ethics. PPT6 suggests a double-prone approach should be taken for ethics instruction in higher education in computer science and engineering disciplines. First, as a component of technical instruction. "I think every course needs ethics in it" (PPT6). Second, as a standalone course taught to all higher education students.

> I think we all have to take at university an intro to writing course in our undergrad, we all had to take it. English 1501 or whatever it was. Sure that's important … But the thing, to me, is, if you're a Canadian citizen at least, and you're in the English program, you've

graduated from an English school, which means you've written papers in your life. (PPT6)

5.3. RQ4 How to Mitigate the Risk of Students Misusing the Hacking Skills Learned in College or University Later in Life in Criminal Activities?

The S&T innovation pyramid (Androsoff, 2019) can be conceptualized thus, from top to bottom: Leadership and Policies, Policymaking Process and Platforms, and People and Skills. The second set of recommendations for effective ethical hacking teaching practices are derived from theory (EDP-STEI-KW) and focus on S&T innovation risk mitigation initiatives geared toward harmonizing knowledge and technology use within society, that is, with the nature of society and its scientific and sociopolitical values. Under the banner of risk mitigation, recommendations were advanced by the thesis by applying the EDP-STEI-KW framework for ethical hacking teaching practices and ethical governance. To help the standardization and systematization of an ethical hacking body of knowledge, an OSINT Analyst cybersecurity role and associated body of knowledge foundation framework are synthesized as a baseline skillset. Other S&T innovation initiatives include recommendations for the professionalization of ethical hacking practitioners/licensing/accreditation. A public policy initiative is explored to govern the use of intelligence/surveillance technologies in society comprised of a networked centre of excellence of ethical hacking communities of practice as a knowledge management and governance approach focusing on establishing effective ethical hacking teaching practices, and primarily the systematization of an ethical hacking body of knowledge.

5.3.1. Ethical design of ethical hacking teaching practices recommendations.

The cybersecurity role sketched out for an OSINT Analyst has no parallel in the field of information security, but is synthesized as a composite focusing on passive (confidentiality) network security penetration testing skills in the context of IT governance. OSINT analysts collect and analyze intelligence data using various software tools and techniques (e.g., passive and active intelligence gathering); they look for and identify patterns in data and network user behavior from evidence (collected data) and they interpret the findings and place them in social, economic, and political context. The two approaches to network vulnerability assessment are passive and active, and they span the activities leading up to the actual hacking phase of the ethical hacking process: Reconnaissance or footprinting, network enumeration, and port scanning. OSINT analysts are knowledgeable about both passive and active network surveillance and testing techniques (the focus of the discussion is on network penetration testing skills), but specialize in passive techniques, which often requires a higher level of technical knowledge and social hacking skills. Passive vulnerability assessment is the stuff of espionage.

OSINT analysis is typically performed using open source tools, resources, and methodologies. OSINT within ethical hacking (penetration testing) is typically discussed in the context of passive footprinting only, that is, nonintrusive intelligence gathering. However, the thesis seeks to carve out a more expansive and critical role for OSINT researchers, a specialization in passive information security testing techniques (intelligence gathering), increasingly relevant to the needs of society with the direction toward automation in data gathering and analysis (i.e., knowledge making), including of surveillance data, facilitated by an increasingly interconnected society and AI technologies. An OSINT analyst operates at the intersection of complex technical and social processes, and sometimes in a grey area. This

warrants attention for society, and this role fulfils this societal need for self-reflexivity (it embodies the information security contradictions in behavior and values within society).

OSINT Analyst Cybersecurity Role and BoK Foundation Framework.

1) Communication competency area:

The penetration test report writing.

2) Social competency area:

Table 4: The Epistemological Roots of STEI-KW as a Sociotechnical Theory of Society

Table 5: STEI-KW and Society

Scientific method design principles

Technology assessment for ethical decision making (STEI-DMG)

Table 22: The Dialectics of OSINT Gathering as Knowledge Making (Inscription of Tacit Values)

Properties of a ST Society (Analytical Elements)

Structural properties:	Open liberal society	Open society: Freedoms and social progress, individualism/autonomy, abstract social relations, personal responsibility, humanistic, peaceful unseating of rulers; Core liberal values (Enlightenment ideals): Personal liberty, individualism/autonomy, freedom; freedom of conscience (expression) without

		oppressive restriction; consent legitimates political power, equality/equal rights.
Behavioral properties:	Trusting	Risk accepting, scientific values (methodological skepticism and scientific process; critical rationalism).
	Knowledge-making	Empirical pragmatism (constructivism) and scientific method design principles.

3) Technical competency area:

Ethical Hacking High-Level Concepts (3 Levels of Abstraction)

Steps of the penetration test process

The RCMP/CSE harmonized penetration testing methodology

Cyberspace (Riley, 2014A) and types of network attacks

Active and passive intelligence gathering techniques and technologies

Applications of AI in information security testing/governance: Opportunities and risks (applications in IDS/IPS)

4) Legal competency area: Cybersecurity policies and regulations in Canada and the U.S. including privacy and security regulations: An understanding of the rules and regulations around information security within an international context regarding information security, security and privacy.

5) Management/Governance competency area:

Two Key Ethical Hacking Paradigms: Offensive vs Defensive Testing

Table 7: IT Security Governance and IT Security Management (Adapted from www.educause.edu)

IT governance/IA frameworks

Information security policy

Table 23: High-Level Network Security Risk Management Concepts

Policy Management (Prevention)	Operations (Monitoring & Response)
IT Security Governance Security Policies & Compliance Security Architecture & Design In depth security Continuous C&A Cyber Threat Intel Thread Modeling Risk Management Security Awareness Training Penetration Testing Vulnerability Assessment	SIEM (Security information and event management) Escalation Management Focused Ops Digital Forensics Continuous Monitoring and Assessment Situational Awareness SOC/NOC Monitoring (24x7) --security operations center/network operations center Incident Reporting, Detection, Response (CIRT) --Computer Incident Response Team Security Dashboard Security SLA/SLO Reporting

5.3.2. Ethical governance recommendations.

Two key S&T innovation initiatives are explored: 1) Professionalization of ethical hacking practitioners and accreditation/certification of ethical hacking skills (through a national level professional association of ethical hacking practitioners), and 2) a public policy initiative to govern or regulate the use of digital hacking technologies in ethical hacking teaching practices in higher education in Canada comprised of a networked centre of excellence of ethical hacking communities of practice as a research and governance approach focused on establishing effective

ethical hacking teaching practices and addressing the cybersecurity skill gap, and a science, society and policy decision making grid (see SSP-DMG: Research and governance knowledge management).

The Networks of Centres of Excellence program, an initiative of CIHR, NSERC and SSHRC, plays an important role in "mobilizing the best of Canada's research, translational, and entrepreneurial expertise and engaging Canadian and international partners from the private, public, and non-profit sectors, by de-risking their investments in network activities" (NCE, 2018). This way the program "helps to expand global knowledge" in the strategic area of cybersecurity and "enables the creation and implementation of multifaceted solutions to specific social and economic challenges, with the goal of helping build a more advanced, healthy, competitive and prosperous country" (NCE, 2018). The NCE program funds unique partnerships among universities, industry, government, and non-government organizations, aimed at solving critical social problems in need of a collaborative approach and a wide range of research expertise. NCEs are expected to 1) Support interdisciplinary research, the co-creation of new knowledge on critical social issues in a specific research area; 2) Train the next generation of highly qualified people; and 3) Engage partners in the design and execution of all network activities including knowledge creation, knowledge mobilization, and knowledge exploitation—including working with end users to facilitate the application of knowledge. NCEs are expected to be "challenge-focused and solution-driven"; NCEs support the creation of solutions to critical social problems through large scale academic-led research networks. NCEs leverage multidisciplinary expertise and resources from across Canada through collaboration to accelerate the co-creation of new knowledge and mobilization of knowledge in a specific research area on critical issues of intellectual, social, economic and cultural significance by "engaging partners

from multiple academic institutions, industry, government and not-for-profit organizations" (NCE, 2018).

The critical social problem of rising student hacking crime and the cybersecurity skill gap requires a collaborative approach and a wide range of research expertise involving experts, industry practitioners, policymakers, and non-government organizations. A networked centre of excellence of ethical hacking communities of practice is explored as a collaborative, international, multi-perspective research and governance (i.e., knowledge management) powerhouse that brings together broad-based expertise in ethical hacking and cybersecurity. The explored networked centre will lead a consortium of Canada's leading research institutions in academia, government, and industry, centres of expertise, and policy think tanks working in the various defense and education sectors relating to cybersecurity, focused on the ethical design of ethical hacking teaching practices in higher education and the ethical governance of hacking and surveillance technology use in higher education and in society. The centre's main objective would be to improve the governance of science, technology and innovation by integrating research, education and public engagement at every stage of innovation continuum--from developing science policy to improving how it is regulated to understanding its social implications. The prime task of the recommended NCE will be to lead a process of knowledge management including the systematization and standardization of an ethical hacking body of knowledge in Canada in a global context.

A center of excellence is a formal partnership between the host institution and other higher education institutions within Canada and internationally, and government, and industry organizations focused on research, research training, research promotion, and knowledge mobilization activities. A formal partnership is a

> bilateral or multilateral formal collaboration agreement between an applicant and one or more partner organizations, of which at least one must be a Canadian postsecondary institution and at least one must be different from the institution or organization that will administer the grant funds. Partnerships may be between academic institutions, or between one or more academic institutions and one or more non-academic partner organizations. These partner organizations agree and commit to work collaboratively to achieve shared goals for mutual benefit. (Social Sciences and Humanities Research Council, 2019)

Partner organizations "pool financial resources to de-risk investments and suggest an amount of funds required from SSHRC."

There are no minimum or maximum budgets for any application in this competition. It is expected that requested funds will be supplemented by cash and/or in-kind contributions from partners. Network funding is available in 5-year renewable cycles. The progress of each network will be assessed annually, and may result in continued funding, conditional funding, or the phasing out of a network before the end of the 5-year award term. (NCE, 2018)

A network "creates its own administration and governance to select and support research topics that align with its strategic objectives. As the R&D landscape evolves over the life of the network, it continuously grows to involve new individuals and groups who enable meeting new opportunities and challenges of this evolution."

The recommended NCE will address issues from the funding of the S&T enterprise, through its regulatory oversight to its social implications. The scope of research and governance activities spans three streams:

1) Science for policy (evidence-based decision making):

As a key thesis contribution toward establishing effective ethical hacking educational public policy, the thesis formulates formal understandings of ethical hacking teaching practices and hacking skills, including information security testing (vulnerability assessment, penetration testing, and social engineering).

2) Policy for science (science and innovation policy):

i) STEI is applied in conjunction with a comprehensive (pragmatist) technoethical analysis as an ethical decision-making framework regarding ethical hacking teaching practices in higher education.

ii) A centre is explored as a collaborative research and decision-making framework.

iii) A centre is explored as a funding approach of a S&T enterprise.

3) Technology assessment and governance (policy for technology):

i) The thesis presents a risk-benefit analysis of hacking technologies use in ethical hacking teaching practices in support of evidence-based decision making;

ii) Hard and soft governance approaches to the use of hacking technologies in ethical hacking teaching practices in higher education include,

a) outcome-oriented codes of ethics (Saner, 2004) incorporating ethical design and information assurance principles. The codes serve as a basis for a QA accreditation/audit framework for voluntary compliance (use of the codes of ethics);

b) a networked centre of excellence of ethical hacking communities of practice as an international, interdisciplinary, transformational, collaborative approach to research and governance; and

c) the proactive regulatory cooperation framework (Saner & Marchant, 2015) in support of governance by regulation.

Theorizing the explored expertise centre as a knowledge management and governance process using STEI-KW as a broad organizing conceptual framework and SSP-DMG as a policy innovation and decision-making framework, the thesis explored a social-technical risk-based approach to govern the use of digital hacking technologies in ethical hacking teaching practices in higher education to help strengthen Canada's ability to manage hacking crime risk to society in a global context.

SSP-DMG: Research and governance knowledge management

S&T Innovation spectrum/pyramid qualitative assessment for decision making on research initiatives	SSP goals	National cybersecurity goals (cybersecurity vision*)	Cybersecurity governance initiatives Public policy initiative
Science for policy News/discoveries	Science for decision making	Protecting the digital homeland	Formal understandings, OSINT Analyst and BoK
Policy for science Policy gap analysis	Skill development; Training of highly-qualified personnel; Science informed policy; DimensionsEDI	Establish effective ethical hacking teaching practices in Canada Government leadership needed on the cybersecurity risk governance	Professionalization initiative; public policy initiative Cybersecurity skill gap; rising student hacking crime Ethical dilemma (teaching hacking skills) Legitimacy and

			identity crisis affecting enrolment and teaching
Technology assessment Risk-benefit analysis	Science for decision making; Risk assessment; policy for science	Precautionary approach to teaching hacking skills in higher education	Risk vs opportunities analysis (STEI-KW)
Funding NCE/NFREF, The Natural Sciences and Engineering Research Council of Canada (NSERC), the Canadian Institutes of Health Research (CIHR), and the Social Sciences and Humanities Research Council of Canada (SSHRC)			NCE/NFRF funding; Centre of excellence of ethical hacking communities of practice
Assessment of project suitability: >Policy analysis (gaps/recommendations) >Level of novelty/leadership >Research theoretical frameworks >Skill development (training/education supported) >Funding options			

5.4. Chapter Conclusion

This chapter first addressed RQ3 by offering a technology impact assessment of teaching

students hacking skills using STEI-DMG, considering opportunities and risks, and the analysis was followed by recommendations. Then RQ4 was addressed: Two key S&T innovation initiatives were discussed under the banner of risk mitigation. This covered the recommendations: Ethical hacking education recommendations, and Ethical governance recommendations by applying the EDP-STEI-KW framework. Two key themes were discussed: OSINT Analyst cybersecurity role and associated body of knowledge foundation framework, and a public policy initiative to govern the use of hacking technologies in ethical hacking teaching practices in higher education comprised of networked centre of excellence of ethical hacking communities of practice and a policy analysis framework: SSP-DMG.

Chapter 6: Conclusion

6.1. Summary and Implications of the Findings

The thesis fills a gap that is of great public interest related to security risks and the implications for the public. The thesis research problem can be articulated thus: Confusion arising from differences in perceptions among experts, industry practitioners, and policymakers regarding what constitutes ethical hacking teaching practices, what constitutes hacking skills, the risk to society of misusing hacking skills and technologies, and how to mitigate these risks stifles innovation and effective educational policy development and implementation, which perpetuates the security risk.

Three key thesis objectives were pursued to address a cybersecurity skill/knowledge gap in higher education. The first objective was to explore who are ethical hackers and what do they do (RQ1 and RQ2). The key finding is an identity and legitimacy crisis for professional ethical hacking practitioners exists and is indicative of an underlying sociocultural confusion. To help counter the confusion, the thesis sketches out a profile of professional ethical hacking practitioners to help us understand who are professional ethical hackers and what do they do (so as to design effective ethical hacking teaching practices): Foundational understandings/definitions regarding the meanings, ethics, values, skills/knowledge, roles and responsibilities, and practices. The second thesis objective was to explore what "ethical hacking" is taught in CS/CE/SE programs in higher education in Canada, and is it ethical (RQ3). Three key themes were discussed: 1) Teaching ethical hacking skillset (three sub-themes were discussed, Teaching ethical hacking skillset, Ethical hacking high-level concepts, and Program requirements); 2) Pedagogy as Communication; and 3) Technology Assessment: An Integrative

Approach. The third thesis objective was to explore suitable S&T innovation risk mitigation solutions (RQ4). Theory-derived recommendations for effective ethical hacking teaching practices in society were presented. Applying ethical design principles derived from STEI-KW (i.e., EDP-STEI-KW) the thesis makes recommendations for ethical design of ethical hacking teaching practices and recommendations for ethical governance of hacking technologies in society.

6.2. Research Contributions

The thesis has important implications for theory, methods, and practice across disciplines. First, the most central contribution to the extant literature on hacking is that the thesis sheds light on ethical hacking meanings, theories, and social relevance. Foundational definitions/understandings: Meanings, ethics, values, skills/knowledge, roles and responsibilities, and practices of ethical hackers/ethical hacking--to address a literature gap and to address the identity and legitimacy crisis of professional ethical hacking practitioners. Second, the thesis proposes a new approach toward teaching ethical hacking, which will have direct impact on institutions of higher education. The two case studies provide in-depth understandings of the perspectives/skills, and views of ethical hacking and in particular on how experts see the ways to best mitigate the risk of students misusing the hacking skills learned in college or university later in life in criminal activities. The dissertation includes a literature review that comprehensively covers epistemology, science and technology studies, and theories. The thesis examines an interdisciplinary topic, ethical hacking, of practical relevance that affects institutions of higher education as well as average citizens. The thesis employs a constructivist approach grounded in STS and directly engages with key stakeholders including industry practitioners, university

experts, and think tank policy experts. STEI-KW as a design/audit model for ethical knowledge making (knowledge construction/autonomous decision making): STEI-KW can be applied to assess/audit or guide the design/integration of knowledge making or decision making in AI use that meets the needs of society.

One practical implication of the thesis is a set of recommendations for design of ethical teaching practices and ethical governance. The thesis explored S&T innovation initiatives (risk mitigation initiatives): The professionalization of ethical hacking practitioners (OSINT Analyst cybersecurity role professional profile as a baseline battery of skills), and a public policy initiative to govern the use of hacking skills was explored comprised of a networked centre of excellence as a research and governance approach, a science, society and policy decision making grid (SSP-DMG), and a STEI-DMG for technology assessment. Another practical implication of the thesis is that the thesis effectively bridged form the findings to important practical policy recommendations that can be implemented that directly inform teaching practices at institutions of higher education in Canada by making available a working model of ethical hacking professional training. A working model of ethical hacking professional training: The OSINT Analyst cybersecurity role/BoK framework as a model for the necessary skills of a professional ethical hacker suitable for undergraduate level education; and as a base model or a baseline skillset canon for security awareness training in higher education. Security awareness training can then be adapted (up-skilled or "down-skilled") according to user role/access privileges based on the OSINT Analyst model and the important work by Sabillon, Serra-Ruiz, and Cavaller (2019), "An Effective Cybersecurity Training Model to Support an Organizational Awareness Program: The Cybersecurity Awareness TRAining Model (CATRAM). A Case Study in Canada." CATRAM "can represent a substantial foundation for the implementation of any organizational

cybersecurity awareness program. CATRAM can also assess any awareness training model that is persistent and relevant with the current cyberthreat landscape" (p. 2).

6.3. Limitations of the Study

Strengths, limitations, and possibilities of ethical hacking as a social construct.

Theorizing ethical hacking as a social construct ultimately improves national security and public safety through improved knowledge management. It facilitates effective (fair and efficient) use/governance of technology in society. Key strengths of ethical hacking as a social construct include the following. First, as a social construct, as a standardized/systematized ethical hacking body of knowledge, it would reflect society/society's needs by integrating perspectives/interests/values of key societal/stakeholder groups thus help bridge the Teaching vs Practice cybersecurity skill gap. Second, ethical hacking as a social construct supports professional practice--it embodies or reflects the professional ethics and the sociological context of using technology (social structure, the scientific and sociopolitical values of society, and a vision for the role of professional ethical hacking practitioners in society). Third, it would improve the likelihood of success because it would be more likely to gain broad public acceptance.

To help the standardization and systematization of an ethical hacking body of knowledge, an OSINT Analyst cybersecurity role and associated body of knowledge foundation framework were synthesized as a baseline skillset of ethical hacking training/education. This standardization would help reduce confusion regarding ethical hacking and ethical hackers in society by facilitating the construction of common knowledge--especially when instruction is coupled with

making tacit values explicit. Reducing the confusion and hence the social stigma around hacking and hackers improves the education of ethical hacking/enrolment in ethical hacking programs.

The principle limitation would be its rather specificity for Canadian society--it needs development within an international and global governance framework. Key methodological limitations pertain to the validation of findings: The findings can be further validated via expanding the number of participating higher education institutions in future studies investigating ethical hacking teaching practices and the cybersecurity skill gap, and increasing the number of interview participants (expanding the sample size as well as incorporating the perspective of CS/CE/SE recent university graduates (especially regarding their views on skills around a Teaching vs Practice gap). Other study limitations include not performing a SWOT analysis of privacy regulations in Canada and the U.S.; and not including a more expanded analysis of AI applications in network security (intelligence gathering).

6.4. Future Research Directions

A leadership role that higher education should play in ethical hacking teaching.

To address a cybersecurity skill gap and rising crime risk to society including rising student hacking crime, higher education should lead the process of ethical hacking knowledge management in society by focusing on establishing effective ethical hacking teaches practices in higher education--specifically, by way of standardization and systematization of an ethical hacking body of knowledge and licensing and accreditation of skills of ethical hacking practitioners to establish credentials.

A networked centre of excellence of ethical hacking communities of practice as a knowledge management and governance approach (policy innovation) would investigate

nationwide the cybersecurity skill gap (the nature of the problem) and its underlying knowledge management/governance challenges/opportunities--for example, by interviewing university experts, industry practitioners, and policy experts to further develop the hacking skills framework and analysis presented in this thesis and shed further light on the nature and causes of the cybersecurity skill gap between teaching and practice (e.g., the need to teach more offensive skills, the need for hands on/specializations in cybersecurity, and the need to establish credentials that correspond to leading industry certifications and curricula/skills through joint collaborative programs. The explored centre would focus on bridging academia and business/industry (Teaching vs. Practice) through collaborative research and training programs that address specific skillsets or specializations in ethical hacking or cybersecurity testing skills. Other knowledge management activities would include leading knowledge co-creation, sharing, mobilization, and promotion of knowledge; and promotion and networking activities that engage and connect key stakeholder groups invested in teaching students hacking skills. Finally, the centre would mobilize knowledge through various publications, media and outreach initiatives (e.g., public forums) to disseminate knowledge, and provide training of highly qualified personnel and prepare the next generation of ethical hacking and cybersecurity professionals.

Who should teach ethical hacking?

First, professors of CS (computer science)/CE (computer engineering)/SE (software engineering) programs in higher education should teach ethical hacking: i) any course, since we need engineering education to integrate ethics/a social science perspective with the technical instruction of hacking skills. Ethics should be taught in the context of technology use in its social science context, integrated with the technical instruction (to train the composite engineer); ii) as

a standalone course; and iii) as a course available to all university and college freshman year students as an introductory course to cybersecurity. Second, IT departments of higher education as a holistic approach to IT security management would teach ethical hacking to students, staff, and faculty.

Ethical hacking as counter-surveillance.

What constitutes ethical hacking teaching practices with emphasis on "hacking" is understood as, what constitutes ethical OSINT gathering teaching practices, that is, what constitutes teaching students ethical OSINT gathering (teaching students to make knowledge/perform OSINT gathering in a responsible manner). Thus, ethical hacking is ethical knowledge making using OSINT technologies (OSINT gathering). This meaning of hacking is close to the meaning of surveillance (as intel gathering). The dialectics of empowerment and exploitation of using open hacking technologies (a critical political economic perspective) is located in the nexus of the knowledge making epistemology of STEI-KW as the site of conception of knowledge of contradictory values and agencies: Political economic when knowledge making is understood as free labor (e.g., see Gehl, 2014) and "liberalism" when knowledge making is understood as a counter-surveillance or counter-hegemonic act.

Table 22: The Dialectics of OSINT Gathering as Knowledge Making (Inscription of Tacit Values)

Technology as surveillance/hegemonic	Technology as countersurveillance/counterhegemonic
Political economic values	Liberal (core liberal values) open society (Popper, 1966) political values

	Scientific method (principles and process) Empirical pragmatism (framed as constructivism)

Governing technology in a globalized environment.

The use of technology to construct knowledge via open AI based intelligence gathering technologies by adversaries has much to do with the efficient and fair use of the technology in society, and in a global system to the equitable access to the technologies, but is also subject to the pressures of geopolitical realities and human nature and its basic need for security above all else. For example, offensive realism in IR suggests that defensive measures or acts taken by one nation are seen as threatening or as a threat by adversarial nations. Nation states seek regional and global hegemony as the only rational choice to ensure survival. For Mearsheimer (2001), conflict, at least between great powers, seems inevitable. In the Liberalism perspective to IR, nations should come together as responsible stakeholders and regulate the use of a technology in a collaborative manner that respects the needs and interests of each.

Canada can build on its global expertise and leadership in AI regulation. A "great push to digitize society has meant building inherent vulnerability into the core of the economic model. This is all taking place atop a deeply fragmented and underdeveloped system of global rules" (Shull, 2019, p. 4). According to Canada's Defence Policy, "Strong, Secure, Engaged," state and non-state actors "are increasingly pursuing their agendas using hybrid methods in the 'grey zone' that exists just below the threshold of armed conflict" (Shull, 2019, p. 7). A recent OECD (2019) study comparing national cybersecurity strategies in 10 OECD countries found that cybersecurity policy making is at a turning point. Cybersecurity "has been elevated among governmental policy priorities." But there is a global lack of frameworks to address the governance challenge. There are some initiatives to govern AI technologies taking a humanistic approach--such as by

OECD and Group 7, and Canada's Digital Charter: Trust in a digital world--but these frameworks need to incorporate a mechanism to harmonize and coordinate cybersecurity governance agreements across different cultures and political systems. The proactive regulatory cooperation framework (Saner & Marchant, 2015) can be applied as a policymaking framework to harmonize international regulations regarding the use of digital hacking technologies because it accounts for cultural, legal, social differences. Regulations would "differ among jurisdictions only when there are explicit reasons such as existing differences in cultural, social, ethical, political, legal, or physical environments" (p. 148). The framework can be applied to achieve coordinated, harmonized, and aligned regulations even if the regulatory route is not chosen as a governance approach. International regulatory coordination efforts vary in forms. Cooperation initiatives may involve sharing of certain data gathering and analysis functions "to provide a common evidentiary foundation for national regulations." Other approaches "may be directed to increasing communication and networking among national regulators to minimize divergent polices, nomenclatures, standards, and requirements." Such international regulatory cooperation initiatives can be global, multinational, regional, or bilateral (p. 148).

References

Abernethy, S. (2016). What was the Enlightenment? Retrieved August 1, 2019, from https://thefreelancehistorywriter.com/

Anderson, J. M. (2003). Why we need a new definition of information security. *Computers & Security. 22* (4): 308–313. doi:10.1016/S0167-4048(03)00407-3.

Andrasik, A. (August 19, 2016). In but not out: Protecting confidentiality during penetration testing GIAC (GSEC)Gold Certification. Retrieved December 20, 2019, from https://www.giac.org/paper/gsec/38727/out-protecting-confidentiality-penetration-testing/152285

Andress, J. (2014). *The basics of information security: Understanding the fundamentals of infosec in theory and practice*. Syngress. p. 240. ISBN 9780128008126.

Androsoff, R. (April 8, 2019). The digital government pyramid: Rethinking our institutions for the digital era. Retrieved December 20, 2019, from https://iog.ca/about/news/the-digital-government-pyramid-rethinking-our-institutions-for-the-digital-era/

Bains, N. (2019). Innovation and Privacy: The Duet of the Century. Retrieved August 1, 2019, from https://www.linkedin.com/pulse/innovation-privacy-duet-century-navdeep-bains/

Bandos, T. (May 8, 2019). Top 5 Configuration Mistakes against getting hacked. Retrieved December 20, 2019, from https://threatpost.com/top-5-configuration-mistakes-hackers/144457/

Basadur, M. (1998). *Simplex: A Flight to Creativity*. Buffalo, N.Y.: Creative Education Foundation Press.

Beer, S. (1972/1981). *Brain of the firm*. New York: Herder and Herder.

Beer, S. (1979). *The Heart of Enterprise*, John Wiley, London and New York. Reprinted with corrections 1988.

Beer, S. (1980). *Organizational change and development: A systems view*: Glenview: Scott-Foresman.

Beer, S. (1984). The viable system model: Its provenance, development, methodology and pathology. *Journal of the Operational Research Society, 35*(1), 7-25.

Beer, S. (1985). *Diagnosing the System for Organizations*; John Wiley, London and New York. Translated into Italian and Japanese. Reprinted 1988, 1990, 1991.

Biesta, G. & Vanderstraeten, R. (1997). Subjectivity and intersubjectivity in the construction of knowledge: A Deweyan approach. Paper presented at the Annual Conference of the British Educational Research Association (BERA) York, 11-14 September 1997. Retrieved August 14, 2019, from http://www.leeds.ac.uk/educol/documents/000000486.htm

Bijker, Wiebe E. (1997). *Of bicycles, bakelites, and bulbs: Toward a theory of sociotechnical change* (PDF). Cambridge, Massachusetts: MIT Press. p. 274. ISBN 9780262522274.

Bijker, W. E. (2009). *Social construction of technology*. In J. K. B. Oslon, SA Pederson & V. H. Hendricks (Eds.), A companion to the philosophy of technology (pp. 88-94). Malden, MA: Wiley-Blackwell.

Bijker, W. E., Hughes, T. P., & Pinch, T. J. (Eds.). (1999). *The social construction of technological systems: New directions in the sociology and history of technology*. MIT press.

Bishop, C. M. (2006), Pattern Recognition and Machine Learning, Springer, ISBN 978-0-387-31073-2

Blakley, B., McDermott, E., & Geer, D. (2001, September). Information security is information risk management. In Proceedings of the 2001 workshop on New security paradigms (pp. 97-104). ACM.

Bodhani, A. (2013). Bad... in a good way. *Engineering & Technology (17509637), 7*(12), 64-68.

Boyd, G. M. (2004). Conversation theory. *Handbook of research for educational communications and technology, 2*, 179-197.

Bradbury, D. (2010). Hands-on with metasploit express. *Network Security, 2010(7*), 7-11. doi:10.1016/S1353-4858(10)70092-1.

Braun, V. & Clarke, V. (2019). To saturate or not to saturate? Questioning data saturation as a useful concept for thematic analysis and sample-size rationales, Qualitative Research in Sport, Exercise and Health, DOI: 10.1080/2159676X.2019.1704846

Brown, M. (June 26, 2019). Student Data at Risk for Massive Exposure Through Breaches. Retrieved December 20, 2019, from https://edtechmagazine.com/higher/article/2019/06/lingering-security-gaps-higher-ed-student-data-breaches-remain-concern

Brown, S., Gommers, J., & Serrano, O. (2015). From cyber security information sharing to threat management. Paper presented at the WISCS 2015 - Proceedings of the 2nd ACM Workshop on Information Sharing and Collaborative Security, Co-Located with: CCS 2015, 43-49. doi:10.1145/2808128.2808133

Brown University. (2013). A Framework for Making Ethical Decisions. Retrieved January 20, 2020, from https://www.brown.edu/academics/science-and-technology-studies/framework-making-ethical-decisions

Bunge, M. (1966). Technology as applied science. In *Contributions to a Philosophy of Technology* (pp. 19-39). Springer.

Bunge, M. (1975). *Towards a technoethics*. Philosophic Exchange, 6(1), 3.

Bunge, M. (1977). *Towards a technoethics*, Monist, 60(1). 96-107.

Bunge, M. (1979). A systems concept of society: Beyond individualism and holism, *Theory and Decision, 10*(1), 13-30.

Bunge, M. (1998). Sociotechnology, in Bunge, Mario (ed.), *Social science under debate: a philosophical perspective*, Toronto, Ontario Buffalo, New York: University of Toronto Press, pp. 297, ISBN 9780802083579.

Bunge, M. (1999). *Social science under debate: A philosophical perspective*. University of Toronto Press.

Butler, E. (2015). Classical Liberalism–A Primer. London Publishing Partnership.

Castelfranchi, C. (2007). Six critical remarks on science and the construction of the knowledge society. *Journal of Science Communication, 6*(4), 1-3.

Centre for International Governance Innovation. (2019). Governing cyberspace during a crisis in trust. Retrieved January, 17, 2019, from https://www.cigionline.org/articles/governing-cyberspace-during-crisis-trust

Center for Strategic and International Studies (CSIS) and McAfee. (2018). The economic impact of cybercrime—No slowing down. Retrieved September 11, 2019, from https://www.mcafee.com/enterprise/en-us/solutions/lp/economics-cybercrime.html

Chaudhary, H. (2013). Writing an effective penetration testing report. *PenTest Magazine, 3*(7), pp. 18-29.

Cherdantseva, Y. & Hilton, J. (2013). Information security and information assurance. The discussion about the meaning, scope and goals. In: *Organizational, Legal, and Technological Dimensions of Information System Administrator.* Almeida F., Portela, I. (eds.). IGI Global Publishing.

Cipher. (n.d.). Reconnaissance, Intelligence Gathering or Open Source Intelligence (OSINT) Gathering. Retrieved January 21, 2020, from https://cipher.com/blog/the-types-of-pentests-you-must-know-about/

CISA (Cyber-infrastructure). (2019). Cybersecurity career paths and progression February 2019. Department of Homeland Security. Retrieved September 26, 2019, from https://niccs.us-cert.gov/sites/default/files/documents/pdf/cybersecurity%20career%20paths%20and%20progressionv2.pdf?trackDocs=cybersecurity%20career%20paths%20and%20progressionv2.pdf

Clarke, Richard A. (2010). *Cyber War*. HarperCollins. ISBN 9780061962233

CNSS (Committee on National Security Systems). (2010). National Information Assurance (IA) Glossary, CNSS Instruction No. 4009, 26 April 2010.

Cobb, M. (June 2019). 5 ways to achieve a risk-based security strategy. Retrieved December 20, 2019, from https://searchsecurity.techtarget.com/tip/5-ways-to-achieve-a-risk-based-security-strategy

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

Communications Security Establishment/Royal Canadian Mounted Police, Harmonized Threat and Risk Assessment Methodology (TRA-1, 2007). Retrieved January 4, 2017, from http://www.rcmp-grc.gc.ca/ts-st/pubs/tra-emr/index-eng.htm

Communications Security Establishment. (2018). National Cyber Threat Assessment 2018. Canadian Centre for Cyber Security. Retrieved August 1, 2019, from https://www.cyber.gc.ca/en/guidance/national-cyber-threat-assessment-2018

Conrad, J. (2012). Seeking help: The important role of ethical hackers. *Network Security*, 2012(8), 5-8.

Cooper, M. H. (2009). Information security training - What will you communicate? SIGUCCS'09 - Proceedings of the 2009 ACM SIGUCCS Fall Conference, pp. 217-221.

Coughlan, S. (14 September 2018). Students blamed for university and college cyber-attacks. Retrieved December 20, 2019, from https://www.bbc.com/news/education-45496714

Creswell, J. W., (2003), *Research design: Qualitative, quantitative, and mixed methods approaches.* Thousand Oaks: Sage Publications.

Creswell, J.W., (2007). *Qualitative inquiry and research design: Choosing among five approaches*. Thousand Oaks: Sage Publications.

Creswell, J. (2009). *Research design: Qualitative, quantitative, and mixed methods approaches*. SAGE Publications, Incorporated.

Creswell, J. W. (2013). *Research design: Qualitative, quantitative, and mixed methods approaches*. Sage publications.

Creswell, J. W., & Poth, C. N. (2016). *Qualitative inquiry and research design: Choosing among five approaches*. Sage publications.

Cyber Fasttrack. (2019). Fast-track your journey to a career in cybersecurity. Retrieved September 13, 2019, from cyber-fasttrack.org

Dean, S. (2016). 5 Cloud, Big Data, and Networking Platforms to Kickstart Your Open Source Career. Retrieved January 22, 2020, from https://www.linux.com/news/5-cloud-big-data-and-networking-platforms-kickstart-your-open-source-career

Dewey, J. (1984). The quest for certainty. In Jo Ann Boydston (Ed.), *The Later Works* (1981-1989) (pp. 144-152). Carbondale and Edwardsville: Southern Illinois University press.

Dewey, J. (1938/2018). *Logic-The theory of inquiry*. Read Books Ltd.

Dewey, J. (1912). Perception and organic action. *The Journal of Philosophy, Psychology and Scientific Methods, 9*(24), 645-668.

Dhillon, G. (2007). *Principles of information systems security: Text and cases*. NY: John Wiley & Sons.

Duignan, B. (March 29, 2019). Enlightenment. Encyclopedia Britannica. Retrieved August 3, 2019, from https://www.britannica.com/event/Enlightenment-European-history

Dupuy, J. (1986). The autonomy of social reality: On the contribution of systems theory to the theory of society. In: Elias L. Khalil & Kenneth E. Boulding eds., *Evolution, Order and Complexity.*

EDUCAUSE. (2019). Dx: Digital Transformation of Higher Education: What Is Digital Transformation? Retrieved December 11, 2019, from https://www.educause.edu/focus-areas-and-initiatives/digital-transformation

EDUCAUSE Information Security Almanac 2019. (April 10, 2019). Retrieved January 21, 2020, from https://library.educause.edu/resources/2019/4/the-educause-information-security-almanac-2019

EDUCAUSE. (2020). Intrusion Detection and Prevention. Retrieved January 31, 2020, from https://library.educause.edu/topics/cybersecurity/intrusion-detection-and-prevention

Eid, M. (2010). Cyber-Terrorism and Ethical Journalism: A Need for Rationalism. *International Journal of Technoethics (IJT), 1(*4), 1-19.

Eid, M. (Ed.). (2011). *Research methods in communication*. Boston, MA: Pearson.

Ellul, J. (1964). *The technological society*.

Ellul, J. (1981/1997). *Perspectives on our age: Jacques Ellul speaks on his life and work*. House of Anansi.

Engebretson, P. (2011). *The basics of hacking and penetration testing: Ethical hacking and penetration testing made easy*. [Books24x7 version] Retrieved March 26, 2013, from http://common.books24x7.com.proxy.bib.uottawa.ca/toc.aspx?bookid=44730

Evelson, B. & Nicolson, N. (2008). Topic overview: Business intelligence. Forrester Research. Retrieved January 17, 2020, from https://www.forrester.com/report/Topic+Overview+Business+Intelligence/-/E-RES39218

Faircloth, J. (2011). *Penetration tester's open source toolkit*. Penetration tester's open source toolkit. Retrieved from www.scopus.com

Foreign signals intelligence (CSE, 2019). Retrieved January 22, 2020, from https://www.cse-cst.gc.ca/en/inside-interieur/signals-renseignement

Fay, R. (May 28, 2019). The world faces a turning point on data and AI. Will we learn from the financial crisis? Retrieved September 24, 2019, from https://www.theglobeandmail.com/opinion/article-the-world-faces-a-turning-point-on-data-and-ai-will-we-learn-from-the/

Gallon, M., & Law, J. (1997). After the individual in society: Lessons on collectivity from science, technology and society. *Canadian journal of sociology, 22*(2).

Gehl, Robert W. (2014). Reverse Engineering Social Media: Software, Culture and Political Economy in New Media Capitalism. Philadelphia: Temple University Press.

Given, L. M., ed. (2008). *The sage encyclopedia of qualitative research methods*. SAGE Publications.

Global Cyber Security Center. (n.d.). Policy interventions and the cyber security skills shortage. Retrieved January 21, 2020, from https://gcsec.org/policy-interventions-and-the-cyber-security-skills-shortage/

Goel, J. N., & Mehtre, B. M. (2015). Vulnerability assessment and penetration testing as a cyber defence technology. Paper presented at the Procedia Computer Science, 57 710-715.

Goodman, M. (2016). *Future Crimes*. New York, NY: Anchor Books.

Gorton, W. (n.d.) Karl Popper: Political Philosophy. Internet Encyclopedia of Philosophy. Retrieved August 3, 2019, from https://www.iep.utm.edu/popp-pol/

Grama, J. & Vogel, V. (January 17, 2017). Information Security: Risky Business. Retrieved October 28, 2019, from https://er.educause.edu/articles/2017/1/information-security-risky-business

Graves, K. (2010). *CEH certified ethical hacker study guide*. John Wiley & Sons.

Habash, R. (2019). Professional Practice in Engineering and Computing: Preparing for Future Careers. CRC Press.

Harper, A., Harris, S., Ness, J., Eagle, C., Lenkey, G., & Williams, T. (2011). *Gray hat hacking: The ethical hacker's handbook*, third edition. McGraw-Hill/Osborne. Retrieved June 7, 2013, from http://common.books24x7.com.proxy.bib.uottawa.ca/toc.aspx?bookid=40079

Harris, S., Harper, A., Eagle, C., & Ness, J. (2007). *Gray hat hacking*. McGraw-Hill, Inc.

Hartley, R. D. (2015). Ethical hacking pedagogy: An analysis and overview of teaching students to hack. *Journal of International Technology and Information Management, 24*(4), 6.

Herley, C., & Van Oorschot, P. C. (2017, May). Sok: Science, security and the elusive goal of security as a scientific pursuit. In 2017 IEEE Symposium on Security and Privacy (SP) (pp. 99-120). IEEE.

Herley, C., & Van Oorschot, P. C. (2018). Science of security: Combining theory and measurement to reflect the observable. *IEEE Security & Privacy, 16*(1), 12-22.

Herzog, P. (2010). OSSTMM 3–The open source security testing methodology manual. Barcelona, España: ISECOM.

Hilder, T. (1995). The viable system model. Retrieved June, 28, 2005.

Hofstede, Geert. (1980). Culture's consequences, international differences in work-related values. Beverly Hills, Calif: Sage Publications.

Hofstede, G. (2001). Culture's consequences: Comparing values, behaviors, institutions, and organizations across nations. Thousand Oaks, Calif: Sage Publications.

Hume, D. (1748/1902). An Enquiry Concerning Human Understanding, in Enquiries Concerning the Human Understanding and Concerning the Principles of Morals, 2nd edition, L.A. Selby-Bigge (ed.), Oxford University Press, Oxford, UK.

INFOSEC Evaluation Methodology (IEM). Retrieved January 21, 2020, from http://www.iatrp.com/

Information Security Forum (ISF). (2018). Threat Horizon 2020: Foundations Start To Shake. Retrieved from September 11, 2019, from https://www.securityforum.org/research/threat-horizon-2s-start-to-shake/

ISACA. (2008). Glossary of terms, 2008. Retrieved January 21, 2020, from http://www.isaca.org/Knowledge-Center/Documents/Glossary/glossary.pdf

ISSAF (Information Systems Security Assessment Framework). Retrieved January 21, 2020, from http://www.oissg.org/information-systems-security-assessment-framework-issaf.html

Jackson, W., Gillis, A., & Verberg, N. (2011). Qualitative Research Methods. In Eid, 2011, *Research Methods in Communication*.

Jesson, J., Matheson, L., & Lacey, F. M. (2011). *Doing your literature review: Traditional and systematic techniques*. Thousand Oaks: Sage.

Kallberg, J., & Thuraisingham, B. (2012). Towards cyber operations-The new role of academic cyber security research and education. In 2012 IEEE International Conference on Intelligence and Security Informatics (pp. 132-134). IEEE.

Kool, L., Timmer, J., Royakkers, L. M. M., & van Est, Q. C. (2017). Urgent upgrade: Protect public values in our digitized society. The Hague, Rathenau Instituut.

Koops, B.J. (2013). Police investigations in Internet open sources: Procedural-law issues. *Computer Law & Security Review 29* (2013) 654-665.

Kuhn, T. S. (2012). *The structure of scientific revolutions*. University of Chicago press.

Landoll, D. J., & Landoll, D. (2005). *The security risk assessment handbook: A complete guide for performing security risk assessments.* CRC Press.

Latour, B. (2012). *We have never been modern*. Harvard university press.

Levy, S. (1984). Hackers, Heroes of the Computer Revolution. Publisher: Anchor Press / Doubleday, New York. ISBN: 0-385-19195-2.

Lin, X., & Luppicini, R. (2013). Socio-technical influences of cyber espionage: A case study of the GhostNet system. *International Journal of Technoethics (IJT), 2*(2), 65-77.

Logan, P. Y., & Clarkson, A. (2005, February). Teaching students to hack: curriculum issues in information security. In ACM SIGCSE Bulletin (Vol. 37, No. 1, pp. 157-161). ACM.

Luppicini, R. (2005). A systems definition of educational technology in society. *Educational Technology & Society, 8*(3), 103-109.

Luppicini, R. (2009). Technoethical inquiry: From technological systems to society. *Global Media Journal -- Canadian Edition, 2 (*1), 5-21

Luppicini, R. (2010). *Technoethics and the evolving knowledge society: Ethical issues in technological design, research, development, and innovation*, Information Science Reference, Hershey, PA.

Luppicini, R. (2014). Illuminating the Dark Side of the Internet with Actor-Network Theory: An Integrative Review of Current Cybercrime Research. *Global Media Journal: Canadian Edition, 7(*1).

Luppicini, R. (2017). Technoethics and Digital Democracy for Future Citizens. In R. Luppicini, & R. Baarda (Eds.), *Digital Media Integration for Participatory Democracy* (pp. 1-21). Hershey, PA: IGI Global. doi:10.4018/978-1-5225-2463-2.ch001

Luppicini, R., & So, A. (2016). A technoethical review of commercial drone use in the context of governance, ethics, and privacy. *Technology in Society 46* (2016) 109-119.

Luppicini, R. (2020). Digital Transformation and Innovation Explained: A Scoping Review of an Evolving Interdisciplinary Field. In Interdisciplinary Approaches to Digital Transformation and Innovation (pp. 1-21). IGI Global.

Marsh, S. P. (1994). Formalising trust as a computational concept. University of Stirling PhD thesis.

Mautner, T. (2005), 2nd ed. The Penguin Dictionary of Philosophy ["open society" entry], p. 443.

May, S. (2012). *Case studies in organizational communication: Ethical perspectives and practices*. Sage.

McClure, S., Scambray, J., Kurtz, G., & Kurtz. (2009). *Hacking exposed: network security secrets and solutions*. McGraw-Hill Professional.

McConchie, A. (2015). Hacker cartography: Crowdsourced geography, openstreetmap, and the hacker political imaginary. *ACME, 14*(3), 874-898. Retrieved from www.scopus.com

McLaughlin, Michael W. (2012). Using open source intelligence software for cybersecurity intelligence. Retrieved August 24, 2019, from https://www.computerweekly.com/tip/Using-open-source-intelligence-software-for-cybersecurity-intelligence

Mearsheimer, J. J. (2001). The tragedy of great power politics. WW Norton & Company.

Miller, K. (2009). *Organizational communication: Approaches and processes*. Wadsworth Publishing Company.

Minei, Elizabeth & Matusitz, Jonathan. (2011). Cyberterrorist messages and their effects on targets: A qualitative analysis. *Journal of Human Behavior in the Social Environment, 21*, 995-1019.

Mitcham, C., & Cutcliffe, S. H. (Eds.). (2001). *Visions of STS: Counterpoints in science, technology, and society Studies*. State University of New York Press.

Morgan, S. (Dec. 7, 2018). Cybercrime Damages $6 Trillion By 2021. Retrieved July 7, 2019, from https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/

Mumford, L. (1967). The myth of the machine: Technics and human development (Vol. 1). Harcourt Brace Jovanovich.

NCC (National Computing Centre). (2005). IT Governance: Developing a Successful Governance Strategy (published by ISACA). Retrieved August 20, 2019, from http://m.isaca.org/Certification/CGEIT-Certified-in-the-Governance-of-Enterprise-IT/Prepare-for-the-Exam/Study-Materials/Documents/Developing-a-Successful-Governance-Strategy.pdf

Neuman, W. L. (2011). Social research methods: Qualitative and quantitative approaches. In M. Eid (Ed.), *Research methods in communication (*341-377). Boston, MA: Pearson.

NIST Special Publication 800-115: Technical Guide to Information Security Testing and Assessment (NIST 800-115). Retrieved January 21, 2020, from http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf

NSA. (n.d.). Signals Intelligence. Retrieved January 17, 2020, from https://www.nsa.gov/what-we-do/signals-intelligence/

OECD. (2019). Comparative analysis of national cybersecurity strategies. Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies. Retrieved June 2, 2019, from https://www.oecd.org/sti/ieconomy/comparativeanalysisofnationalcybersecuritystrategies.htm

Okoli, C., & Schabram, K. (2010). A guide to conducting a systematic literature review of information systems research. Available at SSRN 1954824.

Orol, R. (May 14, 2019). In cyberspace, all banks are vulnerable. Centre for International Governance Innovation. Retrieved July 30, 2019, from https://www.cigionline.org/articles/cyberspace-all-banks-are-vulnerable

OWASP (The Open Web Application Security Project). Testing guide v4. OWASP Foundation. Retrieved January 21, 2020, from https://www.owasp.org/images/1/19/OTGv4.pdf

Paganini, P. (February 18, 2018). Germany's defense minister: Cyber security is going to be the main focus of this decade. Retrieved September 11, 2019, from https://securityaffairs.co/wordpress/69221/security/germanys-defense-minister.html

Palmer, C. C. (2001). Ethical hacking. *IBM Systems Journal, 40*(3), 769-780.

Pashel, B. A. (2006). Teaching students to hack: Ethical implications in teaching students to hack at the university level. Proceedings of the 2006 Information Security Curriculum Development Conference, InfoSecCD '06, September 22, 2006 - September 23, 2006, 197–200. Association for Computing Machinery. doi:10.1145/1231047.1231088

PCI-DSS v.1 2015 Penetration Testing Guide. Retrieved January 21, 2020, from https://www.pcisecuritystandards.org/documents/Penetration_Testing_Guidance_March_2015.pdf

Pike, R. E. (2013). The "ethics" of teaching ethical hacking. *Journal of International Technology and Information Management, 22*(4), 4.

Popper, K. R. (1957). *The poverty of historicism*. na.

Popper, K. R. (1966). *The Open Society and Its Enemies* (Revised.). Routledge & Kegan Paul.

Popper, K. R. (Jan 31st 2016). From the archives: The open society and its enemies revisited. Retrieved on 29 July 2019 from https://www.economist.com/democracy-in-america/2016/01/31/from-the-archives-the-open-society-and-its-enemies-revisited

Popper, Karl (2002) [1959]. *The Logic of Scientific Discovery* (2nd English ed.). New York, NY: Routledge Classics. ISBN 0-415-27844-9. OCLC 59377149.

Popper, K. R. (2003). *Conjectures and Refutations: The Growth of Scientific Knowledge*, Routledge. ISBN 0-415-28594-1

Popper, K. (2005). *Unended Quest: An Intellectual Autobiography*, Routledge.

Popper, K. (2014). *The Myth of the Framework: In Defence of Science and Rationality*, Routledge.

PTES (The Penetration Testing Execution Standard). Retrieved January 21, 2020, from http://www.pentest-standard.org/index.php/Main_Page

Public Safety Canada. (2013A). Canada's Cyber Security Strategy. Retrieved December 19, 2013, from http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/index-eng.aspx

Public Safety Canada. (2013B). An Open Letter to Canadians on Cyber Security Awareness. Retrieved December 19, 2013, from http://www.publicsafety.gc.ca/cnt/nws/nws-rlss/2013/20131003-eng.aspx

Public Safety Canada. (2013C). Harper Government announces action plan for cyber security. Retrieved December 19, 2013, from http://www.publicsafety.gc.ca/cnt/nws/nws-rlss/2013/20130418-eng.aspx

Public Safety Canada. (2019). National Cyber Security Strategy (2018): Canada's Vision for Security and Prosperity in the Digital Age. Retrieved January 17, 2020, from https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/index-en.aspx

Quan-Haase, A. (2016). *Technology and society: Social networks, power, and inequality*. Don Mills, Ontario: Oxford University Press.

Radziwill, N., Romano, J., Shorter, D., & Benton, M. (2015). The ethics of hacking: Should it be taught? Retrieved November 16, 2019, from https://arxiv.org/abs/1512.02707

Rasskazov, V. (2013). Analysing vulnerability scanning reports. *PenTest Magazine, 3*(7), pp. 51-60.

Reynolds, G. W. (2012). *Ethics in information technology*. Boston, MA: Cengage Learning.

Rid, Thomas. (2012). Cyber war will not take place. *The Journal of Strategic Studies, 35*, 5-32.

Riley, S. (2014A). "Cyber Terrain": A Model for Increased Understanding of Cyber Activity. Retrieved August 2, 2019, from https://cyber-analysis.blogspot.com/2014/

Riley, S. (2014B). Science of Security: Does Your Cyber Security Team Include Cyber Security Scientists? Retrieved August 2, 2019, from https://cyber-analysis.blogspot.com/2014/

Rodger, J. (2013). Anatomy of vulnerability scans before a penetration test. *PenTest Magazine, 3(*7), pp. 41-50.

Rosenbach, E., Peritz, A. J., & LeBeau, H. (2009). *Confrontation or collaboration? Congress and the intelligence community*. Harvard Kennedy School, Belfer Center for Science and International Affairs.

Rosenthal, S. B., & Buchholz, R. A. (2000A). *Rethinking business ethics: A pragmatic approach*. New York: Oxford University Press.

Rosenthal, S. B., & Buchholz, R. A. (2000B). *The empirical-normative split in business ethics: A pragmatic alternative*. Business Ethics Quarterly, 399-408.

Rossman, G. B., & Rallis, S. F. (1998). *Learning in the field: An introduction to qualitative research*. Sage.

Sabillon, R., Serra-Ruiz, J., & Cavaller, V. (2019). An effective cybersecurity training model to support an organizational awareness program: The Cybersecurity Awareness TRAining Model (CATRAM). A Case Study in Canada. *Journal of Cases on Information Technology (JCIT), 21*(3), 26-39.

Saltzer, Jerry H. & Schroeder, Mike D. (September 1975). The protection of information in computer systems. Proceedings of the IEEE. 63 (9): 1278–1308. CiteSeerX 10.1.1.126.9257. doi:10.1109/PROC.1975.9939.

Samonas, S. & Coss, D. (2014). The CIA Strikes Back: Redefining Confidentiality, Integrity and Availability in Security. *Journal of Information System Security. 10* (3): 21–45.

Saner, M. (2004). Ethics Codes Revisited: A New Focus on Outcomes. Institute on Governance Policy Brief, (20).

Saner, Marc A. & Marchant, Gary E. (2015). Proactive International Regulatory Cooperation for Governance of Emerging Technologies, *55 Jurimetrics 147* (2015).

Schneier, B. (2015). *Data and Goliath*. New York, NY: W.W. Norton & Company, Inc.

Schultz, E. E. (2002, October). Taking a stand on hackers. Computers & Security.

Schwab, K. (May 25, 2018). The Fourth Industrial Revolution. Encyclopædia Britannica, inc. Retrieved December 07, 2019, from https://www.britannica.com/topic/The-Fourth-Industrial-Revolution-2119734

Shah, S., & Mehtre, B. M. (2015). An overview of vulnerability assessment and penetration testing techniques. *Journal of Computer Virology and Hacking Techniques, 11*(1), 27-49. doi:10.1007/s11416-014-0231-x

Sharma, S. K., & Sefchek, J. (2007). Teaching information systems security courses: A hands-on approach. *Computers & Security, 26(*4), 290-299.

Shields, P. & Rangarjan, N. (2013). *A Playbook for research methods: Integrating conceptual frameworks and project management*. Stillwater, OK: New Forums Press.

Shoker, S. (May 9, 2019). How artificial intelligence is reshaping global power and Canadian foreign policy. Retrieved 21 August 21, 2019, from https://www.cigionline.org/articles/how-artificial-intelligence-reshaping-global-power-and-canadian-foreign-policy

Shull, A. (2019). Governing Cyberspace during a Crisis in Trust. Centre for International Governance Innovation. Retrieved December 20, 2019, from https://www.cigionline.org/articles/governing-cyberspace-during-crisis-trust

Silverman, D. (2011). *Interpreting Qualitative Data* (4th ed.). SAGE Publications.

Snedaker, S., & McCrie, R. (2011). *The Best Damn IT Security Management Book Period*. Syngress.

Social Sciences and Humanities Research Council (SSHRC). (2019). Definitions of Terms. Retrieved January 21, 2019, from https://www.sshrc-crsh.gc.ca/funding-financement/programs-programmes/definitions-eng.aspx?wbdisable=true

Springer-Verlag Berlin Heidelberg (21 November 2008). Topic Overview: Business Intelligence. doi:10.1007/978-3-540-48716-6. ISBN 978-3-540-48715-9.

Stallman, R. M. (2001). Free software: Freedom and cooperation.

Stamp, M. (2011). *Introduction in information security: Principles and practice*, Second Edition, John Wiley & Sons, Inc., Hoboken, NJ, USA.

Stake, R. E. (1995). *The art of case study design*. Sage Publications.

Stebbins, R. A. (2001). *Exploratory research in the social sciences* (Vol. 48). Sage.

Stehr, N. (2002). *Knowledge and economic conduct*. Toronto: University of Toronto Press.

Sterling, B. (1993). "Part 2(d)". *The hacker crackdown*. McLean, Virginia: IndyPublish.com

Stewart, J. (2012). CISSP Certified Information Systems Security Professional Study Guide Sixth Edition. Canada: John Wiley & Sons, Inc. pp. 255–257. ISBN 978-1-118-31417-3.

Sweet, M., & Moynihan, R. (2007). R: Improving population health: The uses of systematic reviews.

Thomas, G., Burmeister, O., & Low, G. (2018). Issues of Implied Trust in Ethical Hacking. *ORBIT Journal, 2*(1).

Thomas, J. (2005). The moral ambiguity of social control in cyberspace: A retro-assessment of the 'golden age' of hacking. *New Media and Society, 7*(5), 599-624.

Thompson, D. (May 9, 2019). Why surveillance is the climate change of the Internet. Retrieved June 1, 2019 from https://www.theatlantic.com/ideas/archive/2019/05/crazygenius-season-three-privacy-internet/589078/

Thompson, L. & Cupples, J. (2008). Seen and not heard? Text messaging and digital sociality. *Social & Cultural Geography, 9*(1), 95-108.

Tillich, P. (2001). *Dynamics of faith*. Zondervan.

Treurniet, J. (2004). An Overview of Passive Information Gathering Techniques for Network Security. Defence R&D Canada, Technical Memorandum DRDC TM 2004-073. Retrieved August 20, 2019, from http://cradpdf.drdc-rddc.gc.ca/PDFS/unc30/p521745.pdf

United Nations Educational, Scientific and Cultural Organization (UNESCO). (2005). Toward knowledge societies. UNESCO World Report. Conde-sur-Noireau, France: Imprimerie Corlet.

Universal Declaration of Human Rights. (1948). UN General Assembly Resolution 217A (III) of 10 December 1948. Retrieved April, 7, 2020, from https://www.un.org/chinese/center/chbus/events/hurights/english.htm

U.S. Department of Education (n.d.). Protecting Student Privacy. Retrieved December 20, 2019, from https://studentprivacy.ed.gov/Security

Valvis, G., & Polemi, D. (2005). An XML-based data model for vulnerability assessment reports. In *Challenges of Expanding Internet: E-Commerce, E-Business, and E-Government* (pp. 513-526). Springer, Boston, MA.

Van Oorschot, P. C. (2017, October). Science, security and academic literature: Can we learn from history? *In MTD@ CCS* (pp. 1-2).

Velu, V. (2013). 200 OK on Audience. *PenTest Magazine, 3*(7), pp. 7-16.

Venter, H. S., & Eloff, J. H. (2003). A taxonomy for information security technologies. *Computers & Security, 22(*4), 299-307.

Walker, M. (2017). CEH Certified Ethical Hacker All-in-One Exam Guide, Second Edition. New York, NY: McGraw-Hill Education.

Weick, K. (1969). *The Social Psychology of Organizing*. Reading, Massachusetts: Addison-Wesley.

Weick, K. (1979). *The social psychology of organizing*. Reading, Massachusetts: Addison-Wesley.

Weick, K. E. (1995). *Sensemaking in organizations*. SAGE Publications, Inc.

Weick, K. E., Sutcliffe, K. M., & Obstfeld, D. (2005). Organizing and the process of sensemaking. Organization Science, 16(4), 409-421. Retrieved from http://search.proquest.com/docview/213832611?accountid=14701

Weill, P., & Ross, J. W. (2004). IT governance: How top performers manage IT decision rights for superior results. Harvard Business Press.

Weingarten, Harvey P. & Hicks, M. (November 23, 2018). On Test Skills, Summary of Findings from HEQCO's Skills Assessment Pilot Studies. Higher Education Quality Council of Ontario. Retrieved December 20, 2019, from http://www.heqco.ca/en-ca/Research/ResPub/Pages/On-Test-Skills-Summary-of-Findings-from-HEQCO%E2%80%99s-Skills-Assessment-Pilot-Studies.aspx

Wettersten, John R. (n.d.). Karl Popper: Critical rationalism. Retrieved August 1, 2019, from https://www.iep.utm.edu/cr-ratio/

Winch, P. (1990). *The idea of a social science and its relation to philosophy*, London: Routledge.

Winick, E. (Oct 18, 2018). A cyber-skills shortage means students are being recruited to fight off hackers. Retrieved July 12, 2019, from https://www.technologyreview.com/s/612309/a-cyber-skills-shortage-means-students-are-being-recruited-to-fight-off-hackers/

Xu, Z., Hu, Q., & Zhang, C. (2013). Why computer talents become computer hackers. *Communications of the ACM, 56*(4), 64-74.

Yin, R. K.(1994). *Case study research: Design and methods*. Thousand Oaks: SAGE Publications.

Yin, R. K., (2003). *Case study research: Design and methods*. Third Edition. Thousand Oaks: Sage Publications.

Young, R., Lixuan, Z., & Prybutok, V. R. (2007). Hacking into the Minds of Hackers. *Information Systems Management, 24*(4), 281-287.

ZHENGCHUAN, X., QING, H., & CHENGHONG, Z. (2013). Why Computer Talents Become Computer Hackers. *Communications of The ACM, 56*(4), 64-74.

Appendices

Figures

Figure 1: The 15 Layer Cyber Terrain Model (Riley, 2014A)

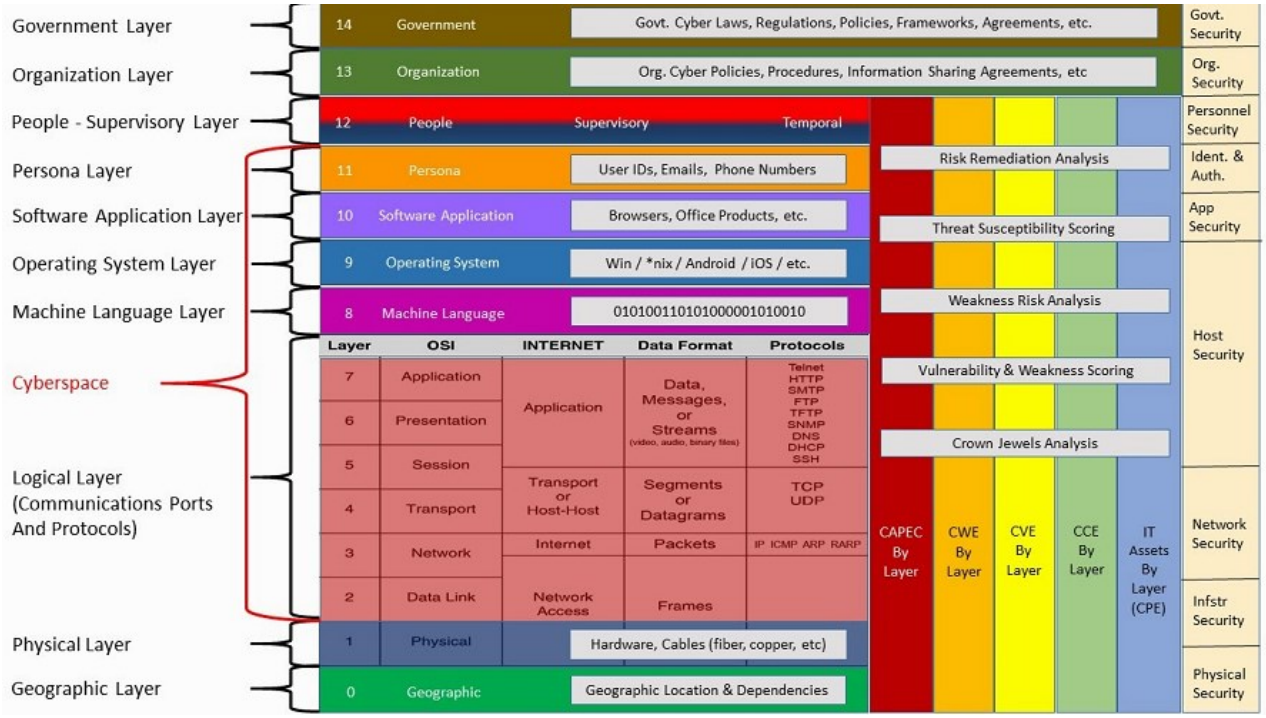
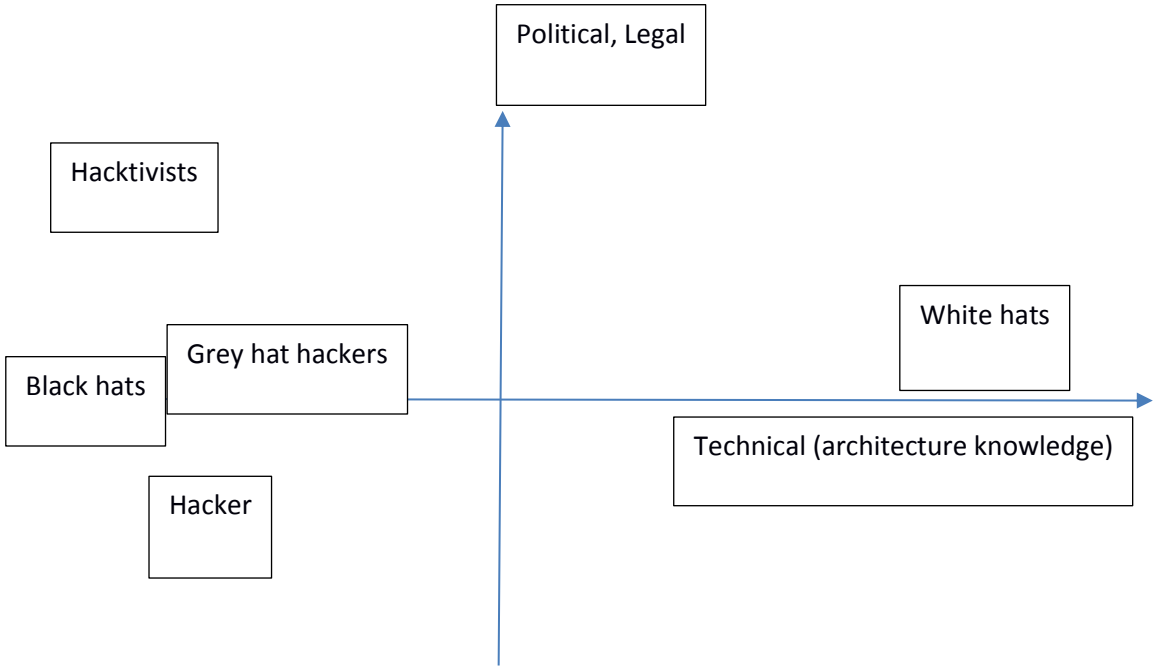


Figure 2: Profiles of Hackers Graph



Tables

Table 6: The Meaning of 'What constitutes ethical hacking teaching practices?'

Present Thesis (RQ2)	Present Thesis (RQ1)	Present Thesis (RQ1)
RQ2 What constitutes hacking skills?	Ethical hacking technology comprehensive systems definition	Teaching ethical hacking as a body of knowledge or a set of skills
Synthesis/data collection: • interviews of university experts • open/open source technologies/methodologies -literature/scholarship claims of "hacking" or "ethical hacking" skills Key high-level ethical hacking concepts focused on network penetration testing and network surveillance using AI (knowledge-making/hacking technology).	Ethical hacking systems definition Synthesis/data collection: SLRs Interviews Organizational documentation (context)	Hacking: penetration testing (information security testing) Focus: cybercrime and surveillance Synthesis/data collection: Teaching: • interviews of university experts (what constitutes ethical hacking teaching practices) • literature review: What "ethical hacking" courses/content is taught in CS/CE programs What is taught as "information security testing" or "security" or "testing" in CS/CE progs Practice/industry: • interviews of industry practitioners • leading industry certifications: OSCP, CEH • job listings

Present Thesis (RQ3)	Future Research
Ethical teaching of hacking skills	Teaching of ethical hacking skills
Hacking: penetration testing (information security testing) Focus: cybercrime and surveillance Ethical: normative pragmatic (STEI-DMG) Use STEI-DMG for comprehensive ethical analysis/decision making regarding hacking technology use in ethical hacking teaching practices and in society Use STEI-KW for the case studies to assess teaching practices (instruction and content) as communication practices (sensemaking) Use STEI-KW to derive EDP to guide ethical hacking teaching practices and ethical governance of technology use "Dissolving the problem"--i.e., answering RQ1 What constitutes ethical hacking teaching practices) via applying EDP-STEI-KW to arrive at OSINT Analyst role/BoK foundation as an interdisciplinary research area.	Hacking: OSINT gathering/surveillance/countersurveillance as knowledge making (broadly, penetration testing as knowledge making) AI applications in countersurveillance as counterhegemony Focus: Surveillance STEI-KW can guide ethical AI knowledge making process design Ethical: process based (knowledge making process against STEI-KW) The nexus of the dialectics of empowerment and exploitation of technology use is located in the synthesized knowledge making epistemology (STEI-KW).

Table 9: Hacking Skills Coding Table (Network Penetration Testing)

Constructs/ Competency Areas	Key Themes	Network exploitation analyst (CSIS)	Network Security Analyst (CSE)	Practice: Business /industry	Industry practitioners	Teaching Carleton University	Teaching University of Ottawa	Literature
Technical	Skills/knowledge	Experience in scripting/ automating	Strong understanding of Operati	OSCP certification: A solid understandin	"Things like C language,	"You need to know C, even if you	CSI 4118 Computer Networ	Ethical hacking skills:

	Programming and computer networking skills; and have published in peer reviewed journals Programming languages (C++, Java, C#, C) Scripting languages (PHP, JavaScript); Python scripting Network services and protocols (TCP/IP)	processing (e.g. Python, PHP, shell) or software development (C/C++) Experience in IT Security appliances (e.g. VPN, Firewall, IDS, etc.) Experience with network communication protocols (e.g. DNS, TCP, etc.) Experience with IT Infrastructure (LAN/WAN, networking)	ng Systems principles and technologies (Windows or UNIX). Strong understanding of Internet and networking protocols, including packet capture analysis. Applying analysis and innovative thinking to solve challenging technological problems. Experience in administration of	g of TCP/IP and various network services (OSCP) Using multiple information gathering techniques to identify and enumerate targets running various operating systems and services (OSCP) Identify existing vulnerabilities and execute organized attacks in a controlled and focused manner (OSCP) Deploy tunneling techniques to bypass firewalls. write simple Bash or Python scripts (OSCP) --	C++, python, but most importantly, and it's not much known actually, called Assembly language … this is where what a hacker is trying to exploit what's, for example, what's called the buffer overflow" (PPT 9). "You're	don't think C should be used in programming new systems. There is a large legacy base of C and C++ code that continues to be exploited. You need to learn JavaScript. A lot of web security exploits boil down to exploiting JavaScript" (PPT14). Computer Science Network Computing	ks Protocols: Communication services, protocols and software. Details of layered protocol hierarchies. The transport, session, presentation and application layers. Fundamental concepts of computer network design. Computer network and communication protoco	Ethical hackers typically have "very strong programming and computer networking skills and have been in the computer and networking business for several years" (Palmer, 2001, p. 771); further, the "best ethical hacker candidates will have successfully

	IDS/IPS evasion OSINT (DNS footprinting) Vulnerability assessment (scanning) Bypassing firewalls		remote network endpoints where there is little to no assistance at the remote end. Experience in troubleshooting and debugging network communications. Strong knowledge of computer of network and host-based vulnerabilities, intrusion techniques and practices. Strong knowledge of one or	CEH certification: Network/host-based intrusion Network/wireless sniffers (Wireshark, AirSnort and so on) Access control mechanisms (smartcards and similar) Cryptography techniques (IPsec, SSL, PGP) Programming languages (C++, Java, C#, C) Scripting languages (PHP, JavaScript) Boundary protection appliances Network topologies Subnetting Port scanning (Nmap) Domain Name System (DNS) Routers/modems/switches Vulnerability scanners	going to need to be able to either edit or write shell scripts like something a system admin would do. With other skills in terms of low level skills like assembly language skills are very important. That depends on the depth	Stream COMP 3203: Protocol Architectures and Internetworking, Types of Networks, Communication Protocols, End-System and Network Traffic Management, Structure of Routing and Congestion Control. Wireless Networks and Security COMP 4203: Fundamentals of	l architectures. CSI 5105 Network Security and Cryptography: Advanced methodologies selected from symmetric and public key cryptography, network security protocols and infrastructure, identification, anonymity, privacy technologies, secret-sharing, intrusion detection, firewall	published research papers or released popular open-source security software" (p. 772). Ethical hackers "are also adept at installing and maintaining systems that use the more popular operating systems (e.g., UNIX or Windows NT) used on

			more of the following: Penetration testing Security event monitoring Forensics Basic knowledge of networking (Firewalls, Intrusion Prevention Systems, Intrusion Detection Systems, network architecture) Familiarity with virtualized network environments.	(Nessus, Retina and so on) Vulnerability management and protection systems (such as Foundstone and Ecora) Operating environments (Windows, Linux, Mac) Antivirus systems and programs Log analysis tools Security models Exploitation tools Database structures	of the ethical hacking exercise you want to go, so if you want to go really deep into it, you're going to want probably grab some binary files and do a reverse engineering on them to try to find" (PPT 12).	mobile LANs, ad hoc, sensor networks, secure routing, searching, clustering, multicasting, localization, mobile IP/TCP, confidentiality, key establishment, authentication, broadcasting, RFIDs, and rogue attacks.	s, access control technologies, and defending network attacks. This course is equivalent to COMP 5406 at Carleton University.	target systems. These base skills are augmented with detailed knowledge of the hardware and software provided by the more popular computer and networking hardware vendors" (p. 772). Bypassing Firewalls Router testing IPS/IDS

			Familiarity with various IT security solutions at the network and host level. Competencies					evasion DNS footprinting Open port scanning and testing SSH attacks Proxy Servers Network vulnerabilities Application penetration testing (Rodriguez, 2019).

Table 10: Professional Ethical Hackers Coding Table

Constructs/ Competency Areas	Key Themes	Government	Practice: Business /industry	Literature
Communication	Meanings Ethical hacking is a test that involves exploiting discovered vulnerabilities (OSSTMM 3.0; NIST 800-	Ethical hacking is an IA process "A method for gaining assurance in the security of an IT system by	Exploiting a vulnerability in a test, the "magic" (Walker 2017). submit a comprehensive OSINT assessment test report (OSCP)	Ethical hacking is a test that involves exploiting discovered vulnerabilities. A penetration test is "a proactive and authorized attempt to evaluate the security of an IT infrastructure by safely attempting to

	115; CSE/RCMP, 2007; Rodger, 2013; Harper et al.). Ethical hacking is a process of risk assessment (OSSTMM 3.0; NIST 800-115; CSE/RCMP, 2007; Harper et al.). Ethical hacking is a legal process (Graves, 2010; Palmer, 2001).	attempting to breach some or all of that system's security, using the same tools and techniques as an adversary might" (NCSC)	An Ethical Hacker is "a skilled professional who understands and knows how to look for weaknesses and vulnerabilities in target systems and uses the same knowledge and tools as a malicious hacker, but in a lawful and legitimate manner to assess the security posture of the target system(s)." ethical hacking definition: *** "An ethical hacker is someone who employs the same tools and techniques a criminal might use, with the customer's full support and approval, to help secure a network or system." (Walker, 2017)	exploit system vulnerabilities" (Rodger, 2013, p. 41). Ethical hacking is a process of risk assessment. The goal of risk assessment is "to identify which investments of time and resources will best protect the organization from its most likely and serious threats" (Reynolds, 2012, p. 103). Ethical hacking is a legal process (Ethical is legal). The practices of professional ethical hackers are governed by a legal framework (Graves, 2010; Palmer, 2001). Ethical hacking "includes the application of computer skills to find vulnerable systems, penetrate systems, and to remove evidence of access to a system" (Logan & Clarkson, 2005 p. 157).
Ethics-legal	Ethics Ethical hackers protect society		The three attributes of trust, honouring the integrity of the client's	Ethical hacking is legal hacking Logan and Clarkson (2005), Pashel (2006),

	and act honorably Ethical hacking is legal hacking		system, and on seeking prior permission from the client, constitute ethical hacking as a set of professional ethics (EC-Council). The Code of Ethics Canons of The International Information Systems Security Certification Consortium (ISC)2 on what constitutes ethical behaviour. The provisions call on information security professionals to 1) Protect society, the commonwealth, and the infrastructure; 2) Act honorably, honestly, justly, responsibly, and legally; 3) Provide diligent and competent service to principals; and 4) Advance and protect the profession (Schultz, 2002).	Sharma and Sefchek (2007), Xu, Hu, and Zhang (2013), and Young, Zhang, and Prybutok (2007) all more or less echo Pike's definition--essentially placing hacking and hackers at either side of the law. An ethical hacker reports the findings (vulnerabilities) of the security assessment process back to the owner with remediation options. An ethical hacker will not damage or harm the test network infrastructure or information assets and will report on and remediate any accidental damage (Graves, 2010).
Political	Values		An ethical hacker is	Ethical hackers are trustworthy.

	Ethical hackers are trustworthy		someone who employs the same tools and techniques a criminal might use, with the customer's full support and approval, to help secure a network or system (Walker, 2017). According to the International Council of Electronic Commerce Consultants (EC-Council), an Ethical Hacker is, "very similar to a Penetration Tester. The Ethical Hacker is an individual who is usually employed with the organization and who can be trusted to undertake an attempt to penetrate networks and/or computer systems using the same methods and techniques as a Hacker."	Ethical hackers are grey hat hackers by necessity: "as soon as you … tell the CEO that his password is "IAmWearingPanties," they will all want to learn more about the importance of a firewall and other countermeasures that should be put into place. (p. 11) Graves (2010) and Palmer (2001) agree on the three attributes of trust, honouring the integrity of the client's system, and on seeking prior permission from the client, as characteristic of ethical hackers. Graves refers to these traits as professional. Palmer adds that ethical hackers have drive and patience. First, ethical hackers should gain the trust of clients. Second, they should take "all precautions to do no harm to their systems during a pen test" (para. 1). A third key component of professional ethical hacking ethics is the imperative to obtain permission before attempting to access the computer network.

				First and foremost, writes Palmer (2001), ethical hackers "must be completely trustworthy" (p. 771). During an evaluation, "the ethical hacker often holds the 'keys to the company,' and therefore must be trusted to exercise tight control over any information about a target that could be misused" (p. 771). Second, ethical hackers "neither damage the target systems nor steal information. Instead, they would evaluate the target systems' security and report back to the owners with the vulnerabilities they found and instructions for how to remedy them" (p. 770).
Management	Roles & responsibilities		Pentesters Security Professionals Network Administrators (OSCP) The purpose of penetration testing activities includes: 1) compliance with government legislation (e.g., Privacy Act, 1983; PIPEDA,	Ethical hackers should address both systemic vulnerabilities as well as preventive measures (Harris, 2007; Palmer, 2001).

			2000), and industry regulations (e.g., PCI DSS, ISO/NIST); 2) validation of existing security controls; 3) identification of unknown security gaps; and 4) Prioritizing existing security initiatives. 5) verify VA results Compile and track vulnerabilities over time for metrics purposes Track and disclose vulnerabilities to national repositories (e.g., the National Vulnerability Databases).	
Technical	Practices		• Vulnerability scanning • Vulnerability assessments • Threat modeling • Risk assessments (Rodger, 2013)	

Table 12: Applying KW and VSM in Communication Analysis

	VSM (viable system model)	KW (sensemaking)
Data collection	Content of hacking skills curricula and instruction	Content of hacking skills curricula and instruction
Analytical focus	How information flows within a teaching/educational system. How communication happens: what "muscles and organs" are used, i.e., what technologies are used in instruction.	Knowledge making/management through interaction and iteration (how participants interact to construct common knowledge). How communication happens: through behavior cycles or assembly rules.
Interpretation	Regulation of information variety through a power gradient from high variety to lower to reduce equivocality.	Making tacit knowledge explicit and engage in more communication opportunities to reduce equivocality.
Recommendation	Emphasis on design of information system Prescribes how information should be managed	Emphasis on design of communication interaction Explains/descriptive how information is managed

Table 13: Search Record for RQ1 (What Constitutes Ethical Hacking Teaching Practices?)

Data source: SCOPUS	Date of search	Search strings/Query ("AND" "OR" "NOT")	Search limiters
Search	August 12, 2019	ABS("offensive security" OR "security course" OR "security training" OR "security curriculum" OR "security education" OR "hacking course" OR "hacking training" OR "hacking curriculum" OR "hacking education" OR "offensive cyber security" OR "offensive cyber-security" OR "offensive cybersecurity" OR "offensive information security" OR "offensive hacking" OR "offensive hacking	Results: 99 Search field: Abstracts Publication years: 2007 to 2019 Search mode:

		skills" OR "information security course" OR "information security curriculum" OR "cyber security course" OR "cyber security curriculum" OR "information security training" OR "computer security" AND "higher education" OR "post-secondary education" OR "third level education" OR universities OR colleges OR "post-secondary institutions" OR "institutions of higher education")	Boolean/Phrase Document type: All Subject Areas: All checked Source Type: Journals and Conferences

Table 14: Profiles of Hackers

	Black hat hacker	Hacker	Hacktivist/FOSS	Grey hat hacker	White hat hacker (professional ethical hackers)
Software vulnerability disclosure policy	N/A	Full disclosure "To illustrate further, it has become very prevalent to announce discoveries and claim that by making the vulnerability details public catastrophic consequences would ensue, as we'll see in the example below. Most of the hacking community	Full disclosure	Responsible disclosure	No disclosure (e.g., pentesters at Microsoft)

		are quick to criticize this behavior, often ostracizing the person making the claim, and in a few cases hacking them in an attempt to publicly expose them." (Phrack)			
Ethics Coleman and Golub (2008) take an anthropological focus on practices and idioms of hackers.	Amoral/instrumental Or Professional ethics	Hacker ethic A hacker commitment to information freedom and meritocracy as well as mistrust of authority, and firm belief that computers can be the basis for beauty and a better world (Levy, 1984: 39–46). "In the hacking scene doing great work is often recognized and	Hacker ethic A hacker commitment to information freedom and meritocracy as well as mistrust of authority, and firm belief that computers can be the basis for beauty and a better world (Levy, 1984: 39–46).	Security researcher ethic Or Academic researcher ethic	Professional ethics (e.g., certified ethical hackers ethics in CEH by EC-Council)

		admired. Those hackers that are able to write that exploit thought to be impossible, or find that unbelievably complex vulnerability, are recognized and praised by the community. ” (Phrack) Those outside of the hacker community are “more ignorant” and “have a different set of criteria to judge work quality.” (Phrack)			
Software code openness	N/A	Open code transparent practices Hackers develop software tools and release them to the open source community.	Open code transparent practices Free software is defined by four basic freedoms or ethical imperatives (The openSUSE,	Provisional/contingent	Proprietary code The EC-Council’s definition: A Certified Ethical Hacker is a skilled professional who

		“Also, many hackers tend to develop great tools which are often released as open source. The open source community shares a lot of properties with the hacking community. ” (Phrack)	2016): 1) The freedom to run the program for any purpose (freedom 0); 2) The freedom to study how the program works, and adapt it according to needs (freedom 1). Access to the source code is a precondition for this; 3) The freedom to redistribute copies (freedom 2); and 4) The freedom to improve the program and release the improvements to the public so that the whole community benefits (freedom 3).		understands and knows how to look for weaknesses and vulnerabilities in target systems and uses the same knowledge and tools as a malicious hacker, but in a lawful and legitimate manner to assess the security posture of a target system(s). The CEH credential certifies individuals in the specific network security discipline of Ethical Hacking from a vendor-neutral perspective. There are a number

					of roles that would benefit from this qualification, or for which being a certified Ethical Hacker is a requirement. These include: Penetration tester Security Auditor Network Security Administrator Security professionals (including incident response roles)
Culture Coleman and Golub (2008) compare three modes of hacker practice/liberal moral expressions (cultural sensibilities or hacker ethics) of	Counterculture Or dominant culture The hacker underground espouse moral conventions and practices bespeaking "a Nietzschian notion of power and pleasure, and especially a critique of	Counterculture Cryptofreedom: in 1991 Phil Zimmerman, an amateur cryptographer, 'freed' encryption by developing a method that could be used on	Subculture The free and open source software movement. Richard Stallman is the founder of the Free Software movement, the GNU project, and the Free	Dominant culture	Dominant culture While a white-hat hacker can be defined as a hacker "who is committed to full compliance with legal and regulatory

hacking revealed variably in the context of computer hacking: cryptofreedom, free and open source software, and the hacker underground.	liberalism" (p. 263). Quite distinct from the politics of inversion evident in free software legal techniques, the hacker underground enacts its political critique primarily through transgression. (p. 263) The under-ground seeks to remind those in power that there are individuals in an unknown, cavernous 'out-there' who can and always will unsettle, even if only temporarily, the purported absolute power of 'the establishment'. (p. 264)	personal computers. The result was not only a robust piece of technology but a risky act of civil dissent, Pretty Good Privacy (PGP), a project whose widespread adoption was, at the time, uncertain at best. As Zimmerman was putting the final touches on PGP, he heard about a pending bill in the Senate to ban cryptography and quickly released his program to the world, with the hope that its popularity would keep the state from outlawing	Software Foundation. Stallman was a hacker who "realized his liberal ideals in a technological idiom and he linked his political goals to one of the most popular operating systems among the technical community, UNIX" (p. 263). /While Zimmerman engaged in an act of civil disobedience and violated the law by writing PGP, Stallman stayed within the law and used it to his own ends. (p. 261)		statutes as well as published ethical frameworks that apply to the task at hand," a black-hat hacker is a hacker "who either ignores or intentionally defies legal or regulatory statutes with presumably little interest in ethical frameworks" (Pike, 2013, p. 67). Logan and Clarkson (2005), Pashel (2006), Sharma and Sefchek (2007), Xu, Hu, and Zhang (2013), and Young, Zhang, and Prybutok

		cryptography. (p. 259) Hackers have a different set of rules on what is better security (Phrack). “It is because of this, that once a hacker joins the security industry they eventually discover that doing great work no longer means becoming a better security professional. They quickly start discovering a whole new set of rules to achieve what is considered to be the 'optimal', such as getting various industry certifications (CISSP, etc), over-hyping their			(2007) all more or less echo Pike’s definition--essentially placing hacking and hackers at either side of the law.

		research and its impact to generate press coverage, and often having to compromise their ideals in order to protect their source of income (for example the “no more free bugs,” “no more free techniques" movements) .			
Motivation	Fame/notoriety or professional growth Or Crime	The “desire to tinker, learn and create technical beauty above all other goals” (Levy, 1984, cited in Coleman & Golub, 2008, p. 255). Happiness and peer group recognition/ self-actualizatio n. Gaming mentality:	Political reform The “desire to tinker, learn and create technical beauty above all other goals” (Levy, 1984, cited in Coleman & Golub, 2008, p. 255). Free and open-source software (FOSS) is software that can be classified as	Academic/profes sional development and success	Profession al developme nt and success

		focused on winning a technical competency challenge. The "idea of making the code and the underlying designs widely available gives participants a feeling of fulfillment as they are not doing this for profit but to contribute to a better world" (Phrack). It is not hard to see why people enjoy developing open source projects so much. Most open source projects are community organizations lead by meritocracy; where the best programmers	both free software and open-source software. Anyone is freely licensed to use, copy, study, and change the software in any way, and the source code is openly shared so that people are encouraged to voluntarily improve the design of the software.		

		can quickly escalate the ranks by writing great code. (Phrack)			
Political orientation	Provisional/contingent Or N/A	Information should be free, and access to computers should be unrestricted (Levy, 1984). These ideals have also been an integral part of the hacking community where one of its mottos is, "Knowledge should be free, information should be free." (Phrack)	Information should be free, and access to computers should be unrestricted (Levy, 1984).	Provisional/contingent	Non-political

Table 15: Vulnerability Scan and Penetration Test Comparison (Rodger, 2013, p. 49)

	Vulnerability Scan	Penetration Test
How often to run	Continuously, especially after new equipment is loaded	Once a year
Reports	Comprehensive baseline of what vulnerabilities exist and changes from the last report	Short and to the point, identifies what data was actually compromised
Metrics	Lists known software vulnerabilities that may be exploited	Discovers unknown and exploitable exposures to normal business processes
Performed by	In house staff, increases expertise and knowledge of normal security profile	Independent outside service
Required in regulations	FFIEC; GLBA; PCI DSS	FFIEC; GLBA; PCI DSS
Expense	Low to moderate: about $1200 / yr + staff time	High: about $10,000 per year outside consultancy
Value	Detective control, used to detect when equipment is/could be compromised	Preventative control used to reduce exposure

Table 16: Search Record for RQ2 (What Constitutes Hacking Skills?)

Data source	Date of search	Search strings/Query ("AND" "OR" "NOT")	Search limiters	Relevant results (using the search strings)
SCOPUS	July 22, 2019	"open" OR "open source" AND "hacking" OR "hacking skills" OR "ethical hacking" OR "ethical hacking skills" OR "security testing" OR "penetration testing" OR "pen testing" OR pentesting OR pentest OR "testing method" OR "test" OR "testing methodology" OR "vulnerability analysis" OR "vulnerability assessment" OR "vulnerability testing" AND resources OR software OR tools OR "security resources" OR "security software" OR "security tools" OR "software tools"	Publication years: 2007 to 2019 Document type: All Subject Areas: All checked Advanced Search:	Results: 50 Peer-reviewed Articles Conference Proceedings

			Only Abstract	

Table 17: Five Phases of Reconnaissance (Faircloth, 2011, p. 33)

Phase	Objectives	Output	Tools
Intelligence Gathering	To learn as much about the target, its business, its organizational structure, and its business partners as possible.	The output of this phase is a list of company names, partner organization names, and DNS names which reflect the entire target organization including all of its brands, divisions, and local representations.	# Search engines # Financial databases # Business reports # WHOIS # RWHOIS # Domain name registries and registrars # Web archives # Data mining tools
Footprinting	To mine as many DNS host names as possible from the domains or company names collected and translate those into IP addresses or IP address ranges.	The output of this phase is a list of DNS host names, IP addresses, and IP address ranges.	# DNS # WHOIS # DIG # SMTP # Data mining tools
Human Recon	To analyze the human perspective of the target and gain as much intelligence as possible about the people associated with the organization.	The output of this phase is a list of names, job titles, contact information, and other personal details about the people associated with the organization.	# Search engines # Email lists and web site posts # Social networking services # Publicly available records
Verification	To confirm the validity of information collected in the prior phases.	This phase rarely produces new output, but can clean up existing output by removing invalid data. Some additional information can	# DNS # WHOIS # DIG

		sometimes be gathered as a side-product of the verification.	
Vitality	To confirm the reachability of the IP addresses identified in prior phases. This is a phase which spreads between reconnaissance and enumeration.	The output of this phase is a list of IP addresses from prior phases which have been confirmed as reachable.	# PING # Port scanners # Mapping tools

Table 18: Pen Source/Free Tools—for Network Penetration Testing (Shah & Mehtre, 2015, p. 45)

Name of tool	Purpose	Operating system	Source
Nmap	Network Scanning Port Scanning OS Detection	Linux, Unix, Mac OS X, Windows	http://www.nmap.org/
Hping	Port Scanning Remote OS Fingerprinting	Linux, Unix, Mac OS X, Windows	http://www.hping.org/
SuperScan	Detect open TCP/UDP Ports Detect Services Running on Open Ports Run WHOIS, PING and LOOKUP Queries.	Windows	http://www.mcafee.com/us/downloads/free-tools/superscan.aspx/
Xprobe2	Remote active OS Fingerprinting TCP Fingerprinting Port Scanning	Linux/Unix	http://www.net-security.org/software.php?id=231
P0f	OS Fingerprinting Firewall Detection	Linux, Unix, Mac OS X, Windows	http://www.net-security.org/software.php?id=164
Httprint	Web Server Fingerprinting Detect Web enabled devices which do not have a server banner string. SSL Detection.	Linux, Unix, Mac OS X, Windows	http://net-square.com/httprint/
Nessus (Personal Edition)	Detect vulnerabilities that allow remote cracker to control or access sensitive data. Detect Misconfigurations, Default Passwords and the Denial of Services.	Linux, Unix, Mac OS X, Windows	http://www.tenable.com/products/nessus/
Brutus	TELNET, FTP and HTTP password cracker.	Windows	http://download.cnet.com/Brutus/3000-2344_4-10455770.html/
Metasploit (Community Edition)	Develop and Execute Exploit Code against a remote target Test the Vulnerabilities of Computer Systems	Linux, Unix, Mac OS X, Windows	http://www.rapid7.com/products/metasploit/download.jsp

Table 19: Properties of a Network and Whether they Can Be Discovered Passively (Treurniet, 2004, p. 2)

Property	Passive Discovery Method	
Device IP address	√	Existence
Device MAC address	√	ARP, DHCP, if sniffer inside
Device Hostname	~ √	DNS, application headers, if sniffer outside NetBIOS, ARP, DHCP, if sniffer inside
Device OS and version	√	Fingerprinting, application headers
Device OS patch level	×	
Applications running	√	Application headers
Usernames	~	Application content
Passwords	~	Application content
Device type (*e.g.* client, server,...)	√	Port and protocol usage, ICMP
Services running	√	Port and protocol usage
Device operational status	~	Activity levels and ICMP
Device system utilization (CPU, memory, disk)	×	
Application status	~	Outgoing activity level of device on application port
Link operational status	~	Activity levels and ICMP
Link utilization	~	Activity levels
Device physical location	×	
Device logical location	~	Hop depth based on TTL

Table 20: Information Security Assessment Methodologies

OSSTMM 3.0	NIST 800-115	TRA-1 (CSE/RCMP, 2007)
Background: This current version is published on Saturday, August 2, 2008. The OSSTMM is for free dissemination under the Open Methodology License (OML) 3.0 and CC Creative Commons 2.5 Attribution-NoDerivs. OSSTMM 3.0 "is maintained by the Institute for Security and	Background: Federal (US) sponsorship September 2008 Section 2 Security Testing and Examination Overview presents an overview of information security assessments, including policies, roles and responsibilities, methodologies, and	Background: At the highest level, the Government Security Policy (GSP) prescribes two complementary approaches to security risk management. The first is "the application of baseline security requirements, or minimum security standards, specified in the policy itself and other supporting documentation, specifically the operational security

Open Methodologies (ISECOM), developed in an open community, and subjected to peer and cross-disciplinary review." "Financing for all ISECOM projects is provided through partnerships, subscriptions, certifications, licensing, and case-study-based research. ISECOM is registered in Catalonia, Spain as a Non-Profit Organization and maintains a business office in New York, USA. p.1	techniques. Section 3 Review Techniques provides a detailed description of several technical examination techniques, including documentation review, log review, network sniffing, and file integrity checking.	standards and technical documentation described in section 9 of the GSP." The second approach is to "address these issues, the GSP provides for continuous risk management in the form of a threat and risk assessment (TRA) as an effective supplement" (p. MS-1). The Harmonized TRA Methodology presents the TRA as a project conducted in five distinct phases (TRA phases). 1) Preparation: Obtain Management Commitment, Establish Project Mandate, Determine Scope of Assessment 2) Asset Identification: Identify Assets, Assess Injuries, Assign Asset Values
11.2 Logistics: This is the preparation of the channel test environment needed to prevent false positives and false negatives which lead to inaccurate test results. Framework and Network Quality. Framework: activities similar to recon information gathering, e.g., (a) Verify the scope and the owner of the targets outlined for the audit. (b) Determine the property location and the owner of the property housing the targets. (c) Verify the owner of the targets from network registration.	Section 4 Target Identification and Analysis Techniques describes several techniques for identifying targets and analyzing them for potential vulnerabilities. Examples of these techniques include network discovery and vulnerability scanning.	3) Threat Assessment: Identify Threats, Assess Threat Likelihood, Assess Threat Gravity, Assign Threat Levels 4) Risk Assessment: Identify Existing Safeguards, Assess Safeguard Effectiveness, Determine Vulnerabilities, Assess Vulnerability Impact, Assign Vulnerability Values

11.3 Active Detection Verification 11.3.1 Filtering 11.3.2 Active Detection		
11.4 Visibility Audit Enumeration and indexing of the targets in the scope through direct and indirect interaction with or between live systems. 11.4.1 Network Surveying -- activities similar to recon footprinting e.g., (a) Identify the perimeter of the network segment. 11.4.2 Enumeration - activities similar to scanning and enumeration (Faircloth 2011 e.g., Examine target web-based application source code and scripts to determine the existence of additional targets in the network.		
11.5 Access Verification Tests for the enumeration of access points leading within the scope. - activities similar to port scanning (Faircloth 2011 11.5.1 Access Process (a) Request known, common services which utilize UDP for connections from all addresses. (b) Request known, common VPN services including those which utilize IPSEC and IKE for connections from all addresses. 11.5.2 Services (a) Request all discovered TCP ports for service banners (flags).	Section 6 Security Assessment Planning presents an approach and process for planning a security assessment.	

11.5.3 Authentication		
11.6 Trust Verification Tests for trusts between systems within the scope where trust refers to access to information or physical property without the need for identification or authentication. 11.6.1 Spoofing 11.6.2 Phishing	Section 5 Target Vulnerability Validation Techniques explains techniques commonly used to validate the existence of vulnerabilities, such as password cracking and penetration testing.	
11.7 Controls Verification Tests to enumerate and verify the operational functionality of safety measures for assets and services.		
11.8 Process Verification 11.9 Configuration Verification 11.10 Property Validation 11.11 Segregation Review 11.12 Exposure Verification 11.13 Competitive Intelligence Scouting 11.14 Quarantine Verification 11.15 Privileges Audit 11.16 Survivability Validation 11.17 Alert and Log Review	Section 7 Security Assessment Execution discusses factors that are key to the execution of security assessments, including coordination, the assessment itself, analysis, and data handling. □ Section 8 Post-Testing Activities presents an approach for reporting assessment findings, and provides an overview of remediation activities.	5) Recommendations: Identify Unacceptable Risks, Select Potential Safeguards, Identify Safeguard Costs, Assess Projected Risk

Université d'Ottawa | University of Ottawa

Département de communication | Department of Communication

55 Laurier E. (DMS 11125)
Ottawa ON Canada K1N6N5
Tél. : 613-562-5800 X8971
Téléc. : 613-562-5240

55 Laurier E. (DMS 11125)
Ottawa ON Canada K1N 6N5
Tel.: 613-562-5800 X8971
Fax : 613-562-5240

Tel.: 613-562-5238
Ottawa ON Canada K1N 6N5

Recruitment Invitation for a PhD Thesis Study

August 1, 2018

Baha Abu-Shaqra
PhD in E-Business
Faculty of Engineering
University of Ottawa

Rocci Luppicini
Department of Communication
Faculty of Arts
University of Ottawa

Thesis Title: Technoethics and Viable Systems: Exploring a Networked Centre of Excellence of Ethical Hacking Communities of Practice Within a Canadian University

Hello,

You are cordially invited to participate in a PhD thesis about effective ethical hacking teaching practices in higher education. The thesis explores a networked centre of excellence of ethical

hacking communities of practice focused on effective ethical hacking teaching practices in higher education. Benefits for the participants may be self-reward for their contributions to academic research. The main benefit to society will be a contribution toward a scholarly understanding of effective ethical hacking teaching practices in higher education in Canada. Participants will be invited to respond to interview questions for a session of about 45 to 60 minutes in duration. Interviews will take place on the university campus or over the phone during normal working hours or at times more suitable for the participants.

The interview period is proposed for November 26 to December 14, 2018. Please feel free to indicate an interview time and place suitable for you in the appended Consent Form.

Before interviews are conducted, participants are invited to sign a consent form highlighting their rights—such as the right to withdraw from the study at any time without suffering any negative consequences—and other pertinent information related to the nature of the study and the ethical conduct of the study, including information about participant identification and research site identification in the thesis, potential study risks, and information confidentiality.

Thank you for your time and consideration.

I look forward to hearing from you.

Sincerely,

Baha Abu-Shaqra

Ethics Approval Certificate

Université d'Ottawa

11/09/2018

Bureau d'éthique et d'intégrité de la recherche

University of Ottawa

CERTIFICAT D'APPROBATION ÉTHIQUE | CERTIFICATE OF ETHICS APPROVAL

Numéro du dossier / Ethics File Number

Titre du projet / Project Title Technoethics and Viable Systems: Exploring a Networked Centre of Excellence of Ethical Hacking Communities of Practice Within a Canadian University

Type de projet / Project Type Thèse de doctorat / Doctoral thesis

Statut du projet / Project Status Approuvé / Approved

Date d'approbation (jj/mm/aaaa) / Approval Date (dd/mm/yyyy) 11/09/2018

Date d'expiration (jj/mm/aaaa) / Expiry Date (dd/mm/yyyy) 10/09/2019

Équipe de recherche / Research Team

Chercheur / Researcher	Affiliation	Role

Baha ABU-SHAQRA	Département de communication / Department of Communication	Chercheur Principal / Principal Investigator
Rocci LUPPICINI	Département de communication / Department of Communication	Superviseur / Supervisor

Conditions spéciales ou commentaires / Special conditions or comments

(CÉR) de l'Université d'Ottawa, opérant conformément à l'*Énoncé de politique des Trois conseils* (2014) et toutes autres lois et tous règlements applicables, a examiné et approuvé la demande d'éthique du projet de recherche ci-nommé.

L'approbation est valide pour la durée indiquée plus haut et est sujette aux conditions énumérées dans la section intitulée "Conditions Spéciales ou Commentaires". Le formulaire « Renouvellement ou Fermeture de Projet » doit être complété quatre semaines avant la

Le Comité d'éthique de la recherche

date d'échéance indiquée ci-haut afin de demander un renouvellement de cette approbation éthique ou afin de fermer le dossier.

Toutes modifications apportées au projet doivent être approuvées par le CÉR avant leur mise en place, sauf si le participant doit être retiré en raison d'un danger immédiat ou s'il s'agit d'un changement ayant trait à des éléments administratifs ou logistiques du projet. Les chercheurs doivent aviser le CÉR dans les plus brefs délais de tout changement pouvant augmenter le niveau de risque aux participants ou pouvant affecter considérablement le déroulement du projet, rapporter tout évènement imprévu ou indésirable et soumettre toute nouvelle information pouvant nuire à la conduite du projet ou à la sécurité des participants.

The University of Ottawa Research Ethics Board, which operates in accordance with the *Tri-Council Policy Statement* (2014) and other applicable laws and regulations, has examined and approved the ethics application for the above-named research project.

Ethics approval is valid for the period indicated above and is subject to the conditions listed in the section entitled "Special Conditions or Comments". The "Renewal/Project Closure" form must be completedfour weeks before the above-referenced expiry date to request a renewal of this ethics approval or closure of the file.

Any changes made to the project must be approved by the REB before being implemented, except when necessary to remove participants from immediate endangerment or when the

modification(s) only pertain to administrative or logistical components of the project. Investigators must also promptly alert the REB of any changes that increase the risk to participant(s), any changes that considerably affect the conduct of the project, all unanticipated and harmful events that occur, and new information that may negatively affect the conduct of the project or the safety of the participant(s).

Responsable d'éthique en recherche / Protocol Officer

Pour/For ----- ----- Président(e) du/ Chair of the Comité d'éthique de la recherche en sciences sociales et humanités / Social Sciences and Humanities Research Ethics Board