CHAPTER I

Why Ethical Hacking?

This book aims to explore the issue of ethical hacking from an unconventional and unique viewpoint, one that draws upon my own vast experience in this area. My background spans seventeen years and has incorporated roles as a law and cyber-security professor, human-rights activist, cyber-policy consultant, technology developer, and cybercrime investigation advisor. It is this experience that I will draw upon to form the pillars of the book, which departs from some of the conventional thinking in this area. This is not a book about Anonymous or about hacking organizations per se, though case studies from various incidences are certainly explored. This book is about various types of activities that are often referred to as "ethical hacking"—hacking for an ethical reason—whereby it will be argued that law and policy ought not to be the same here as for those hacking activities that are purely for economic gain or to cause harm or mischief. As will be seen, I have grouped ethical hacking into five groups:

- online civil disobedience;
- hacktivism;
- penetration testing and security-vulnerability disclosure;
- counterattack/hackback; and
- security activism.

Let us start this journey first by talking briefly about you, about me, and then a lot about ethical hacking.

1.1 You

The book is designed to cater to a broad spectrum of readers, ranging from cyber-security experts and policy-makers to academics. Despite its intended primary audience, the book has also been written in such a manner as to make it accessible not only to university students but the broader general public. The complexity and rate of change seen within areas of technology, cyber security, and ethical hacking make it essential not to assume that you are across all terminology. There are many terms that common media and blogs use incorrectly or interchangeable, such as "computer virus," which turns out to be a "computer worm." Other new methods of malicious-software propagation may emerge that a reader would not necessarily be familiar with. In general, ethical hacking involves many technical terms that require a foundational level of understanding in order to better understand policy and other issues. For example, a denial-of-service attack is potentially lawful if your own device is used to participate in an online political protest. It would not be lawful to use a botnet that connects to unknown or third-party devices to participate in the same protest. The aim is to provide you with digestible material that demonstrates concepts through engaging case studies. These case studies of ethical hacking, spanning the last twenty years, are dissected and catalogued in a manner that identifies the groups and movements, their motivations, and the techniques they used. You will see some of the most notorious of these incidences explored referenced in chapters 4–6, then selected incidences are looked in context and by issues in chapters 7–13.

If you are a policy-maker, chapters 3–7 and 14 are essential reading. Chapter 3 provides the only publicly available quantitative analysis of ethical hacking in the world. The stark numbers contained within this chapter will assist you in demonstrating why the decisions and policies you recommend are fundamentally essential. As a policy-maker, you are all too aware that in a world of cleverly masked sensationalism posing as substantive information it has become difficult to discern what information can be trusted. Chapters 4–6 table legal cases and selected noteworthy incidences from the quantitative analysis. Throughout chapters 7–13 I aim to provide you with

intricate and, at times, intimate looks at the world of ethical hacking, which will assist you in generating well-informed and robust policy. Chapter 14 discusses the required frameworks and changes required as a matter of both policy and law.

If you are a cyber-security expert or consider yourself a hacktivist, there are ethical and legal issues contained within this book that are essential reading. This includes policy and legal lines to be cautious of, which could easily see you cross from that of "ignore action with caution" to one of "prosecute" by authorities. These cautionary tales are drawn from my experience undertaking a large range of roles, as described above.

As I know all too well, the issues surrounding cyber security have garnered interest from a broad demographic of society, and is not limited to just policy-makers, experts, and academics. Even if you do not fit within any of the three later categories, I would still love for you to drop me a line at alanacybersecurity.com and let me know your background. While I keep analytics on how many people visit the site, and the general geographic area of the IP addresses, this will give me an opportunity to engage with you and understand the broader community interests. But please remember that if you are looking at the site or wish to contact me about a private or sensitive matter, this site offers no anonymity to you. So, connect with a VPN, proxy or other anonymizer such as TOR.

www.alanacybersecurity.com

There is also the option of communicating later using encryption and, for journalists, I have and use Signal.

1.2 Me

I have a confession: I am an ethical hacker. *I use technology in a non-violent way in the pursuit of a cause, political or otherwise, which is often legally and morally ambiguous.* I don't intentionally break the law. Many of the actions I take are assumed by politicians, lawmakers, and people around the globe to be legal because there are few to no legal precedents and scant reportage. The law is written broadly, in a way that captures far more than one might expect. Part of my motivation for writing this book is to highlight how desperately new law and policy are required for ethical hackers.

As a human-rights activist I work to educate and protect online civil liberties globally, but more specifically for the jurisdictions in which I have lived and worked, namely Canada, Hong Kong, and Australia. When I lived in Hong Kong I provided research assistance for the OpenNet Initiative (a collaborative partnership between the Citizen Lab at the University of Toronto, the Berkman Center for Internet & Society at Harvard Law School, and the Advanced Network Research Group at the Cambridge Security Programme, Cambridge University) to examine how Chinese authorities filtered the Internet in 2003–2005. The testing of which sites were blocked in the Chinese firewall meant that a host of domestic Chinese laws were violated, even though the object was merely to provide an accurate reflection of what types of sites were blocked, along with where, when, and possibly why these sites were filtered. I continue to be involved in research efforts addressing civil liberties and Internet freedom for the nongovernmental Freedom House, a liberty watchdog. I was the researcher and author of the Australian Internet Freedom portion of the annual Freedom House Report, *Freedom on the Net* (2011–2017). *Freedom on the Net* is the most widely utilized worldwide resource for activists, government officials, journalists, businesses, and international organizations aiming to understand the emerging threats and opportunities in the global Internet landscape, as well as policies and developments in individual countries.

I am a professor and researcher above all else—I currently am the Professor of Cybersecurity and Behaviour at Western Sydney University. I am in the privileged position of leading multidisciplinary research and lecturing teams across a range of cyber-security projects and courses. I work with industry, government, and civil society on a daily basis. But my views about ethical hacking can be traced to a time and place long before I became a professor of cyber security. Here is a bit more about what informs the research, analysis, and opinions represented in this book.

I was a key researcher with the law and policy division of the Data to Decisions Cooperative Research Centre (D2DCRC). The D2DCRC specializes in big data/artificial intelligence for national-security purposes. The centre involved multiple computer scientists and data scientists from universities, industry (e.g., Palantir and SASS) along with governmental departments predominantly in Australia but also in Canada and the United Kingdom. With the D2DCRC, we worked on confidential matters where we helped

groups make informed decisions on how new technologies were being built and how they would function based on proposed new legal and policy frameworks.

From an international perspective, I was fortunate enough to be asked to speak at a United Nations workshop in China on cyber security and human rights, where the majority of attendees were students and professors in the cyber-security division of the People's Liberation Army's National Defence University. The questions asked and views imparted to me were enlightening, and reminded me how much misinformation there is in cyber security and ethical hacking. My research from my honours in law, masters, and PhD degrees—and indeed my current research—has been entirely interdisciplinary, as has my work with government, law firms, and later with universities. For my PhD I worked with underground security-activist groups concerned with botnets, conducted empirical qualitative research, and worked closely with the technical community to deepen the research. I worked with individuals and organizations in Europe, Asia, North America, and Australia. This included dialoguing and consulting with individuals from Internet-service providers, the Australian Communications and Media Authority, computer emergency response teams (in Australia, Canada, and Estonia), cyber-security journalists, Shadowserver, various computer-science researchers, and the National Cyber-Forensic Training Alliance (an FBI and Carnegie Melon cybercrime training and investigative service, located in Pittsburgh). The thesis could best be described as in the field of cyber security, using methods and analysis from criminology, economics, information systems, and the law. This book borrows from my graduate work in botnets, especially in the chapter on security activism.

I am on the board of directors and am the special cyber adviser for the investigation firm IFW Global. IFW is an investigation firm specializing in cybercrime and intelligence. My advisory work has involved performing a variety of tasks, including surveillance advice, developing protocols for sensitive investigations in foreign countries, providing legal information on investigative procedures and contracting with intelligence units, as well as writing memoranda for arbitration disputes involving counterfeit engineering products. Our investigations have involved online fraud and malicious online conduct, which has led us to cooperate with cybercrime and anti-money laundering divisions of the FBI, CIA, Interpol, the

AFP, the New South Wales Police Force, and Thai and Philippines police. Our investigatory work on one cybercrime case led to corruption investigations and charges against certain members of the Queensland police force. IFW is globally renowned for shutting down and recovering funds from sophisticated online organized crime, including payment-diversion fraud and boiler-room and binary-option scams.

Payment-diversion fraud typically involves a situation where a network and/or devices on a network are compromised, a criminal watches the actions of the company over time and is able to divert payment due to a supplier to an unknown third party. This is also known as compromised supply-chain fraud.

A boiler-room scam typically refers to a call centre selling questionable investments over the phone, and nearly almost always with legitimate looking fake websites.

Binary options involve a highly speculative form of trading where you don't trade on a market but you often trade against a binary-option "company" (in market parlance, a bucket shop)—effectively, an illegitimate broker. The binary-option broker has a backdoor into an online trading platform, where the broker can manipulate prices while you, the potential customer, is trading—ensuring that you don't win too often, or win just enough to draw you in to want to invest more. The chances of a payout are remote (one in several million), yet people are lured into investing due to premises of a big payout. Kind of like someone inciting you to invest a large sum of money on a horse race with poor odds. The difference, however, is that the odds are so remote that this type of investment is illegal in many jurisdictions. Additionally, the scammers are actively manipulating prices as you engage and invest, luring you into losing more money. Communication is often done through highly encrypted apps such as Signal, and money is exchanged and funnelled through money-laundering processes and, increasingly, through cryptocurrencies. It is extremely difficult to recover money laundered through encrypted cryptocurrencies, making this type of online fraud a lucrative business.

I provide legal and ethical information to computer-security experts (and almost certainly some hackers) on a wide range of topics, such as deviation of application program interfaces (APIs), data crawling on the Deep Web, sale of vulnerabilities and bugs, copyright issues in proof-of-concept videos, subverting national firewalls,

disclosure of corrupt practices, and hacking targets. I do know that requests for information have come from Russia, Estonia, China, Jordan, Saudi Arabia, Australia, and Canada, but possibly too from anywhere as people tend to use anonymizing technology to contact me to reduce risk of identification. One person goes so far as to only send me hard documents by post.

Lastly, I have done consultancies for government and industry. In fact, this book is largely the product of research/consultancy work on ethical hacking for Public Safety Canada in 2010. Public Safety Canada engages and works with various departments on a range of cybersecurity issues and also houses the Canadian Cyber Incident Response Centre. As you can see, my understanding of cyber-security behaviour and ethical hacking is based on first-hand knowledge as well as research. That's more than enough about me; let's move onto the topic of the book: ethical hacking.

1.3 Ethical Hacking

What is ethical hacking? My definition differs from the computer-science terminology (which only covers penetration/intrusion testing and vulnerability discovery), whereby I include online civil disobedience, hacktivism, penetration/intrusion testing and vulnerability discovery, counterattack/hackback, and security activism.

Ethical hacking is the non-violent use of a technology in pursuit of a cause, political or otherwise, which is often legally and morally ambiguous.

This book examines five types of ethical hacking: online civil disobedience, hacktivism, penetration/intrusion testing and vulnerability discovery, counterattack/hackback, and security activism. I have briefly defined these below. Controversial aspects of my definitions are examined in chapter 2.

Online civil disobedience is the use of any technology that connects to the Internet in pursuit of a political end. Civil disobedience involves a just cause, where specific technology use is often legal.

Hacktivism is a clever use of technology that involves unauthorized access to data or a computer system in pursuit of a cause or political ends.[1]

Penetration/intrusion testing is a type of information-systems security testing on behalf of the system's owners. This is known in the computer-security world as ethical hacking. There is some

argument, however, as to whether penetration testing must be done with permission from a system's owners or whether a benevolent intention suffices in the absence of permission. Whether permission is obtained or not, however, does not change the common cause: improving security.

Vulnerability discovery is the process of finding weaknesses and ways in a network, device, or within the organization themselves that are capable of being exploited by others (sometimes for nefarious reasons). Vulnerability discovery is often done with the authorization of the owner/operator of a network or device, but not always.

Counterattack/hackback is also referred to as strikeback. Counterattack is when an individual or organization that is subject to an attack on their data, network, or computer takes similar measures to attack back at the "hacker/cracker" (see ch. 2 for definitions). For example, when an individual or organization is subject to a denial-of-service attack, that organization might initiate their own denial-of-service attack on the responsible party's website.

Security activism is similar to penetration/intrusion testing in that the cause is to improve security. Security activism goes beyond mere testing of security, however, to gather intelligence on crackers and to launch active attacks to disrupt criminal online enterprises. One example is the taking down of a botnet.

There is no clear line between ethical hacking and vigilantism. Indeed, the water is murky, and what many might characterize as ethical others might see as a form of unwanted vigilantism. Vigilantism is understood to be outside of the state or beyond legal, or extra-state or extra-legal. Vigilantism may involve citizens acting in a manner they believe the state should permit yet currently sanctions. Often a vigilante will break the law, often in response to the state's own violation of laws. There may be a sense that justice under due course will not occur, hence reaction to an action is required. Some might classify this as a valid or even ethical action under the circumstances, while others would paint the same act in a negative fashion, as vigilantism. Cyber vigilantism is similar to traditional forms of vigilantism. Traditional vigilantism might involve the planning of an act, use or threat of force, reaction to a crime or other social act, and the notion of personal and collective security.[2] Cyber vigilantes, as argued by Trottier, are individuals with computer-science skills who respond to cybercrime and cyber security.[3] In this sense they might use an invasive "traceback" search,

shut down a website, issue a distributed denial-of-service protest/attack, and hack into databases to expose corrupt practices. Or perhaps they take down botnets.

But before we delve further into the world of botnets, cryptocurrency, Dark-Net forums, and hackers let's begin with a tale of civil disobedience in 1960, with Martin Luther King Jr. and the civil rights fight for equality and justice for African-American people. From there we look at what some see as Julian Assange's first escapade into hacktivism, with the use of the WANK worm to protest NASA's use of nuclear fuel in rocket ships in the 1980s. You see, hacktivism isn't as new as one might think, but it has and will continue to take new forms and be a prevalent form of protest and activism.

Forcing the Line of Transparency[4]

Civil activists in the 1960s and 1970s had sit-ins and protests for civil rights and against war. Many people thought that civil disobedience would lead to change. Change would lead to rational and critical discussion of citizens with governments in a move toward more open and transparent democratic governance. In the late 1970s and early 1980s, many governments enacted laws around freedom and access to information to better ensure open disclosure and government transparency. Prior to such enactment of freedom and access to information laws, it was difficult to obtain copies of government documents. These laws were devised in an attempt to move the disclosure of information default from private to public. In this sense, a government employee would not ask when something should be made public but, rather, when something should be made private (in other words, transparency by default).

While freedom and access-to-information laws have shifted the line of transparency, they did not achieve transparency by default. Internal guidelines for when information should remain private or public were muddled with bureaucratic wording. The result was that government employees began to self-censor. This took place in two main ways. The first, employees erred on the side of caution when classifying documents, and thus over-classified documents as private/secret and under-classified documents as public/transparent. The second, when access-to-information requests were granted, documents were often so blacked out that it was difficult to ascertain with any certainty what decision or policy was adopted, or why. The "black pen" effect began.

The early twenty-first century will likely be seen as an era when ethical hackers opened governments. The line of transparency is moving by force. The Twitter page for WikiLeaks demonstrates this ethos, through its motto ("We Open Governments") and its location ("Everywhere"). Hacktivism is a form of civil-rights activism in the digital age. In principle, hacktivists believe in two general but spirited principles: respect of human rights and fundamental freedoms, including freedom of expression and personal privacy; and the responsibility of government to be open, transparent, and fully accountable to the public. In practice, however, hacktivists are as diverse in their backgrounds as they are in their agendas.

Ethical hacking is not new. In the late 1980s Australian hacktivists penetrated a NASA network releasing a computer worm known as WANK—Worms Against Nuclear Killers.[5] The worm was written and released as a form of protest against the NASA launch of the Galileo rocket, which was to navigate itself to Jupiter using nuclear energy. The infamous German hacker group Chaos Computer Club (CCC) was also busy in the late 1980s, attacking German government systems to protest the collection and storage of census information; the groups believed that the state should not amass the personal information of its citizens.[6]

Moving forward to the first decade of the twenty-first century, ethical hacking, while not new, had fundamentally changed in one distinct manner—the ability to participate in attacks (denial of service) is no longer limited to an elite group of people with excellent computer skills; the technology is available to the masses in an accessible format for those with limited technical skill. People follow the tweet feeds of Anonymous and Lulz Security (LulzSec), two hacktivist groups, where hacking operations are communicated. One can simply click the download button for open-source LOIC (Low Orbit Ion Canon) software, select the demonstration one wishes to participate in by typing in the URL, then click again. *Fait accompli*. One is now participating in a denial-of-service attack. It must be noted that denial-of-service attacks using LOIC require a critical mass to be effective. This means that many people must participate in the event.

People around the globe are participating in denial-of-service attacks on many types of websites for a variety of causes. Major websites that have been attacked include those of the Australian Parliament, PayPal, MasterCard, paedophilia websites, the New York

Stock Exchange, the Toronto Stock Exchange, *News of the World*, Oakland City Police, the governments of Mexico, Ecuador, and Peru. The list goes on.

One of the most well-known hacktivism groups is Anonymous. The word "group" here is arguably used incorrectly as Anonymous is more like an umbrella name for a decentralized collective of participants and operations. In addition to performing denial-of-service attacks, members of some of the smaller Anonymous groups participate in more sophisticated forms of hacktivism that require a higher range of computer skills. Instances of these more sophisticated attacks include the release of names and details of the Mexican drug cartel Los Zetas, the names and details of consumers of child-pornography sites, and the capturing of secret documents held by governments around the world—some of these documents are then given and released by WikiLeaks.

Hacktivism isn't limited to attacking information systems and retrieving documents. It also extends to finding technical solutions to mobilize people. At the height of the Egyptian e-revolution the major Internet-service providers and mobile-phone companies shut down Internet traffic, preventing people from using the Internet and mobile phones. This, in turn, affected people's ability to mobilize. Anonymous worked around the clock to ensure that images from the revolution were still being sent to the international press. Hacktivists have worked to penetrate the Iranian government's firewall to tunnel passages allowing Iranian citizens to view blocked sites. I was involved with a similar firewall penetration when I organized some of the internal testing of the Chinese firewall for the OpenNet Initiative.[7] There are similar initiatives for Saudi Arabia and other parts of the world with strong censorship. Keeping secrets and preventing citizens from accessing information may no longer be an achievable goal. The question becomes, should governments adopt heavy-handed policies and laws to investigate and prosecute ethical hackers, to deter such activity and keep the status quo? Or should governments enact an appropriate legislative response that reflects the reality of this new era—the forced line of transparency?

Other forms of ethical hacking are rooted in ensuring the security of networks. This has taken shape in four main ways. The first is through intrusion or penetration testing, where experts are invited to expose the security vulnerabilities of an organization's network. The second is somewhat more controversial as it involves

hackers who, without authorization, illegally access a network, software, or hardware to expose security vulnerabilities. Sometimes these hackers will go so far as to fix the vulnerability or to report it to the system's owner. Third, there is a growing concern that many organizations, including corporations and governments, are engaging in counterattack efforts to deter attacks to their systems. This is known as hackback or counterattack. Increasingly, attacks have moved into the corporate world, where organizations are moving from defensive protection against cyber threat to responding with similar measures. There is growing momentum in some jurisdictions to legalize hackback, including a recent United States bill for its legalization (see ch. 10). Last, many security experts are forming self-organized security communities to actively engage in intelligence gathering and counterattacks—here called security activism.

How courts and governments will deal with hacking attempts that operate in grey areas of the law, and where different ethical views collide, remains to be seen. There are no exceptions to the cybercrime/computer-crime provisions for security research or for the public interest in most jurisdictions. The US bill on hackback remains controversial. Equally difficult is how civil rights apply to hacktivism. This question is shrouded with uncertainty. How will governments and courts manoeuvre in this new era of digital activism within the boundaries of protected civil liberties?

As will be seen throughout this book, online protests are and will continue to increase, and the type and size of such attacks will escalate in order to, in part, capture the interest of the media.

There is a growing movement in some online communities (hackers) to ensure that "back doors" (ways to exploit a program) are inserted into computer programs and then kept quiet as a means of ensuring access to future information (especially government websites). These types of "attacks" are not done for media attention.

Technologies such as LOIC will evolve to allow for encryption and anonymity. This will parallel similar developments that took place with peer-to-peer file-sharing networks. We are already seeing groups of hackers come together in countries without extradition treaties with the United States, or to protect vulnerable investigative journalists and whistle-blowers. These groups are at the forefront of encryption expertise and data and identity protection.

As will be seen in the data-analysis chapter (ch. 3), the most popular discussion threads in hacking forums are "beginner hacking"

and "hacking tools and programs," indicating the likelihood of increased hacking, both ethical and for criminal purposes. United Nations–sponsored research on hackers demonstrated that legal deterrence only works with beginners and with young hackers (under aged twenty-five).[8] These individuals will generally quit illegal hacking after a first conviction. The law does not have a deterrent effect for highly skilled and often older hackers (over twenty-five). This United Nations Commission on International Trade Law study, however, did not address hacktivism, nor motivation or deterrence, as hacktivism didn't become popular until 2011, with the UN quantitative and qualitative study being performed in the early 2000s. More recent studies on hacktivism are qualitative, not quantitative.

This book looks at qualitative studies, but it is also the first and only study of its kind to have performed quantitative analysis of emerging ethical-hacking events. While there are many academics writing on this topic, no one to my knowledge is performing metrics. There are, therefore, no current reliable open metrics for government to make decisions (it is an assumption only that intelligence is more knowledgeable on point). Many law-enforcement agencies, for example, are not authorized to run analytics on the dark Web (see ch. 2) as their work must be tied to a specific investigation or operation. While a law-enforcement agency can seek authorization to go onto Dark-Net forums, what they can do once there is limited to their enabling statute coupled with privacy restrictions. The importance of the study of ethical hacking on the dark Web is intuitive—evidence-based policy relies on evidence. If evidence is limited to media reports and police investigations, policy-makers and experts may be able to apply a corollary to a specific incidence, but they will not be aware of the extent to which citizens are increasingly taking to ethical hacking as a means of political and social discourse, or as a means of vigilantism. This book, therefore, has a distinct benefit in using three different measurements to look at ethical hacking from 1999 to 2018.

My team of researchers has been cataloguing the most interesting case law and ethical-hacking incidences for the past twenty years. The case law spans multiple jurisdictions and is included in grouped table format in chapter 4. Over 200 ethical-hacking incidences from around the world are presented, classified first by organization (e.g., Anonymous, CCC, etc.), in chapters 5 and 6. Chapters 7 through 13 then take a sample of incidences and cases and probe

the incidences in detail, dissecting policy, motivation, ethical, and other considerations.

As will be seen in the case studies, some individuals involved in hacking are considered as having an addiction similar to gambling, video games, drugs, or alcohol. The role of hacking addiction in sentencing has been mentioned in a few key legal decisions, but there has been no detailed analysis of how a proper framework might be established to address technology addiction.

As will also be seen through an examination of emerging events, a significant portion of corporations and organizations are engaged in some form of counterattack/hackback, though this is not widely known and rarely spoken of publicly. On a computer network, intrusion-detection software not only detects denial-of-service attacks but also automatically initiates counter-denial-of-service attacks. There are no legal exemptions for these types of counterattacks. The problem of corporate hackback, while still controversial, is increasingly being recognized as an issue that requires new law and policy. Both governments and corporations are moving from a defensive cyber-threat posture to one of mitigation of threat, and often moving to the offensive or active cyber-security posture.

Other ethical-hacking incidents are closely tied with the objective of protecting human rights and promoting an open, transparent democracy. Many ethical hackers view their work as acts of civil disobedience, and align their actions with traditional civil disobedience as espoused by Ghandi, King, and Henry David Thoreau. Other hackers identify with an ethos of hacking that developed in the 1980s, and look to technical gurus and to the writings of "Hacktivismo Declaration" by the Cult of the Dead Cow, "The Hacker Manifesto," "The Anonymous-Anonops," the Electrohippies collective's "Client-Side Distributed Denial-of-Service," and the "Gospel According to Tux." Other groups are less ideal in their philosophy, citing motivation as "for the laughs." However, further probing of such hackers reveals that their hacking is done out of "a sense of wrongdoing," without always being able to clearly articulate what that wrongdoing is.

Denial-of-service attacks by movements such as Anonymous require critical mass for success. As will be seen, there is often a correlation between the number of participants in a denial-of-service attack and the worthiness/morality of the cause. Which causes will acquire critical mass is unpredictable, though it may be possible in

future research to use a machine-learning approach across social media and Dark-Net forums to predict which causes are likely to acquire critical mass.

Explored in depth throughout the book is the concept of assumptions as dangerous. For example, it would be incorrect for governments or organizations to assume that members of ethical-hacking groups come from one type of community, race, or age demographic. Many ethical hackers are not aware that their activities are illegal, especially those participating in politically motivated denial-of-service attacks. The analytics performed in our qualitative and quantitative analysis demonstrates that this is a global trend, and not one limited to those with technical skills and prowess; the ease and affordability of hiring someone to perform acts makes ethical hacking appealing. Further, the risk of "getting caught" for many of these activities is extremely low for some acts (e.g., corporate hackback) but is quite high for other activities, especially where hacktivism targets an entity with deep pockets or where there is a strong desire to use the law as a deterrence. This has been the case with some politically sensitive acts of Anonymous. While most instances of ethical hacking are illegal, it is interesting to note that some methods used by law enforcement and by security firms contracted to perform criminal-intelligence gathering may also be illegal, or at best highly controversial. The legal framework is a blunt object that is rarely applied to certain acts, but it remains deliberately broad to allow the prosecution of an individual when political appetite changes. This, as will be seen throughout the book, makes working in cyber security—expert or not—an ever-changing field of play in which what is low risk one day is high risk the next.

This book concludes by providing a series of detailed recommendations to:

- Develop and publicize guidelines and public policy for online civil disobedience and hacktivism. In the United States, recent Department of Justice guidelines related to vulnerability and "bug bounty" programs such as HackerOne is an excellent example of government-led policy that clarify exemptions to criminal and civil law when security activities are performed within certain parameters. The guidelines promote online bug-bounty programs wherein companies pay individuals—hackers—for revealing software

defects/bugs in their networks or products. The guidelines not only encourage these types of programs but recommend legal immunity in such matters. This means that a hacker who discovered a bug would be shielded from criminal and civil-law sanctions. This could be a model explored for some forms of ethical hacking.

- Run an education campaign once these guidelines are finalized.
- Allow and encourage a legitimate "space" for virtual protests.
- Implement a security-research exemption for computer offences.
- Further consider the idea of a public-interest exemption for hacking offenses. This could be done in a multi-party working group for both security-research and public-interest exemptions.
- Develop a code of conduct for counterattack and have a legislative review of how principles of self-defence might apply to a counterattack situation.
- Treat any governmental engagement with ethical hacking as legal and transparent. These activities should not be contracted out to security firms unless they are closely scrutinized and held accountable in some form of safeguard or compliance mechanism.
- Review the insecure practices of corporations and organizations that hold sensitive personal data, and consider implementing more effective legislation, such as data-breach notification—but significantly more important is the obligation to encrypt all personal information held by such entities and to encourage data minimization.
- Ensure that data owned or generated by Canadians is protected and that such data, if collected and stored, is deleted after a reasonable period when using foreign services such as Google, Facebook, and Twitter (US-based). Currently, any person who uses Google, Facebook, Twitter and similar services is subject to US Internet monitoring by governments and law enforcement, and potentially is exposed to subpoenas to release personal information even in the *absence* of a criminal investigation.

Each of these recommendations are explored in further detail in the final chapter: Toward an Ethical Hacking Framework.

On a final note: this book was conceived with web viewing in mind. As a result, many of the illustrations are less conducive to the printed format. However, since they are key to understanding the material, we have decided to include all figures and illustrations in both the print and the digital versions.

Notes

1. Samuel 2004.
2. Johnston 1996.
3. Trottier 2016.
4. The introduction is taken with permission from Maurushat 2012 ("Forced Transparency: Should We Keep Secrets in Times of Weak Law, and Should the Law do More?," *Media & Arts Law Review* 17.2).
5. Dreyfus and Assange 2011.
6. Dreyfus and Assange 2011.
7. OpenNet Initiative.
8. Chiesa, Ducci, and Ciappi 2009.

Page left blank intentionally