CHAPTER XIV

Toward an Ethical-Hacking Framework

14.1 Ethical Hacking in Context

Ethical hacking is a complex area. This book broke down ethical hacking into online civil disobedience, hacktivism, counterattack/hackback, penetration/intrusion testing and vulnerabilities, and security activism. We used a mixed-methods approach in chapter 3 to capture emerging ethical-hacking incidences as found in the media, blogs, law databases, and forums on the Dark Net. Chapters 4 through 6 looked at over 200 of the most interesting legal cases and incidences of ethical hacking across the globe. Chapters 7 through 11 used case studies to provide a deeper understanding around motivation, techniques, ethical issues, and other considerations.

The online civil-disobedience chapter compared online versus off-line protests, and argued that the characterization of online civil disobedience as criminal versus off-line protests as legitimate was inappropriate in the digital age. Likewise, the penalties for online civil disobedience were disproportionate with the form of protest. We saw that some people who participated in acts of online civil disobedience believed that their actions were lawful forms of protest. There were no legal exemptions for acts of online civil disobedience under most criminal-law frameworks.

Hacktivism was more controversial in that it was evident that drawing the line between lawful protest and criminal act was not

as clear cut as in the case of online civil disobedience. Here some acts showed elements of vigilantism; specifically, acts that were extra-legal and, in some instances, extra-state. Here individuals had become so fed up with political or social processes that they no longer had faith in the government to deal with a problem in an ethical or just fashion. There are no legal exemptions for hacktivist actions under criminal-law frameworks. That said, the connection between protected human rights and supposed unlawful acts is a territory that courts will have to grapple with in the years to come.

Even security researchers encounter ethical and legal issues when performing penetration testing and vulnerability discovery. Again, the law does not provide security research or public-interest exemptions from the criminal framework. While copyright law in some jurisdictions provides a "fair dealing" framework, allowing security research and encryption research, these exemptions require several conditions to be met. These exemptions, however, only provide assurance from being prosecuted for copyright offences, they do not provide exemptions from being prosecuted for an offence in a criminal code or act.

As will was seen in the counterattack/hackback case studies, some organizations are engaged in some forms of counterattack/hackback, though this is not widely known and rarely spoken of publicly. Some intrusion-detection software for computer networks 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, even further, to the offensive or active cyber-security posture.

Security activism is likewise an area where professional security experts and researchers are faced with an abundance of ethical and legal issues. Many incidences were noted where security experts sat quietly in systems, performing actions to clean up cyber issues or fixing security vulnerabilities. Some may find this similar to a neighbour shovelling the snow from your driveway before you wake in the morning or cutting your grass—acts of kindness. The difference with security activism is that often the end user or organization is unaware that the random act of kindness has occurred. Again, there

are no legal exemptions from relevant criminal-law frameworks for these actions. As with all instances of ethical hacking, there is only the discrepancy to prosecute or not to prosecute. Prosecution guidelines are rarely made public.

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. Yet the legal framework is a blunt object which is rarely applied to certain acts, but remains deliberately broad to allow the prosecution of an individual when political appetites change. This, as has been seen throughout the book, makes working in cyber security—expert or not—an ever-changing field of play, where low risk today is high risk tomorrow

As was seen in the case studies, some individuals involved in hacking were considered to have an addiction in the same way that an individual may become addicted 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 framework should be established to properly deal with technology addiction. Likewise, autism has featured in some of the ethical-hacking incidences, with some jurisdictions such as the United States not factoring this into sentencing young hackers. Whereas we have seen that, in Australia and New Zealand, having Asperger's has led courts to show leniency, to render suspended sentences on condition of community work, which, in one case, led a hacker to lawful employment in the cyber-security field.

There are no simple solutions to the issues that arise with ethical hacking. Below contains some recommendations which should be explored further through multi-party stakeholder processes, where stakeholders could include organizations, internet and cyber-security associations, human-rights groups, relevant CERTs, and government policy-makers, with input from hackers, psychologists, and autism groups.

14.2 Encourage Legitimate Space for Virtual Protests

What might a legitimate space for virtual protests look like? Many would argue that there are already legitimate spaces for virtual protests. These are online petitions, expressing opinions on social media, supporting online political advertisements and awareness campaigns,

and sending communications, by paper or online, to legislative representatives. Yet none of these allows for the same online effect that a physical protest might have outside of a parliament.

Off-line protests are allowed if certain conditions are met. Depending on the jurisdiction that you are in, you may need a license for the protest. You may need to make certain that you do not block access to essential services. And you need to ensure that you do not damage property or cause violence, otherwise you clearly cross the line of potentially legal to illegal. DDoS is the closest thing at the moment to the equivalent in an online world. But what if there was a way to perform DDoS or achieve the same effect with similar off-line restrictions? In theory this could be done by allowing people the right to protest where posters and other could be displayed on visible parts of the website. This is not a DDoS, but the protest message is clearly visible on the landing page of the website. There is no physical damage to property, no one is injured, and essential online services are not blocked. This is merely one example of how a legitimate space might work for online civil protest. A multi-stakeholder group could develop other methods and policies.

14.3 Guidelines and Policy

The government should provide publicly available policies and guidelines for the different types of ethical hacking. These policies and guidelines will play two important roles. The first, is that people will know what is and is not legal, but, more importantly, make prosecution guidelines transparent. Such guidelines operate to say that, while an action may be caught within the broad scope of the criminal law, prosecution should only occur when certain conditions are met. These guidelines could further look at appropriate sentences for acts of ethical hacking.

The Netherlands was the first country to issue guidelines for responsible disclosure, in 2013.[1] Afterward, the US Department of Justice developed guidelines and policies for responsible vulnerability disclosure and bug-bounty programs. This is an excellent example of a government initiative to assist in clarifying exemptions to criminal and civil law when security activities are performed in ways deemed to be within an acceptable range. The cyber-security unit within the Computer Crime and Intellectual Property Section of the Criminal Division of the US Department of Justice issued

"A Framework for a Vulnerability Disclosure Program for Online Systems" in 2017.[2] The framework is a public document that clearly discusses acceptable and lawful methods of security-vulnerability disclosure. But it also does more than this; the framework sends a clear message that organizations should be viewing responsible disclosure as something positive. The framework likely would not work on its own without the complementary bug-bounty programs and platforms (such as HackerOne and Bugcrowd) that have emerged as third-party organizations that coordinate lawful security-vulnerability disclosure and payment for services between "hacker" and organization. These platforms also strongly encourage ethical conduct among their cyber-security researchers, as will be seen below.

14.4 Code of Conduct for Hackback

Codes of conducts and similar documents are emerging in the security-vulnerability space. For example, HackerOne has on its website landing page "Vulnerability Disclosure Philosophy,"[3] which outlines principles that should be respected, including:

Finders should...

- **Respect the rules.** Operate within the rules set forth by the Security Team, or speak up if in strong disagreement with the rules.
- **Respect privacy.** Make a good faith effort not to access or destroy another user's data.
- **Be patient.** Make a good faith effort to clarify and support their reports upon request.
- **Do no harm.** Act for the common good through the prompt reporting of all found vulnerabilities. Never wilfully exploit others without their permission.

Security Teams should...

- **Prioritize security.** Make a good faith effort to resolve reported security issues in a prompt and transparent manner.
- **Respect Finders.** Give finders public recognition for their contributions.
- **Reward research.** Financially incentivize security research when appropriate.

- **Do no harm.** Not take unreasonable punitive actions against finders, like making legal threats or referring matters to law enforcement.

This approach is interesting in that it does not refer to absolutes found in criminal law, such as authorized or unauthorized access. Here, one is expected to make "good faith" efforts to not perform certain acts. While this is not a binding legal document, having the guidelines up front allows some form of transparency in processes.

The question becomes whether there should be transparent guidelines and policies for hacktivism or hackback in the same way as there are for vulnerability finding and disclosure? There are clearly different ethical considerations and policy goals in hacktivism than there are for security-vulnerability disclosure. The latter has the benefit of incentivizing the finding and disclosure of security vulnerabilities. Whereas, hacktivists are incentivized by righting a wrong; disclosure of what they see as wrongful or unjust acts; or promoting a political cause or party. As with unlawful protests, participants accept that they may be arrested and detained for peaceful protest. Where an act of hacktivism is also peaceful, participants should also accept that they may be arrested and detained. There is a body of case law, however, for unlawful peaceful protest including a common understanding of when it might be appropriate to prosecute, what offences to use, and what sentences may or may not be appropriate. There is no equivalent for hacktivists. A white paper on hacktivism is highly desirable in order to start conversations around the limits of acceptable hacktivism and appropriate responses.

Hackback is both similar and different from hacktivism. Where hackback takes the form of retaliation for a prior act of hacktivism it is more readily associated with retribution and/or vigilantism. As seen in the WikiLeaks, MasterCard, and Stratfor debacle, where the initial hacktivist act quickly spiralled into an out-of-control retaliatory conflict involving all parties. Here, guidelines would be useful for not only hacktivists, but also considering guidelines for governments and law-enforcements agencies (or their hired third-party agents) on appropriate conduct. Where hackback moves into the area of protecting corporations and shielding assets, it begins to look more like self-defence. As was discussed, the United States is looking at legitimizing hackback. Again, there are many restrictions imposed and the Hackback Bill faces fierce opposition. However, the

bill initiates a discussion on whether hackback might be appropriate under certain conditions. More work is needed at the global level to discuss possible rules around hackback and, in particular, what would constitute sufficient evidence of attribution.

14.5 Transparency of Government Engagement with Hackback

As previously mentioned, there needs to be more transparency when law enforcement, government agencies, and third-party contractors engage with hackback techniques. While there are clear rules for law-enforcement use of hackback, the use of third-party contractors for investigations and hackback functions is not readily discussed in the media, at conferences, or other forums. This activity deliberately remains in the shadows so that the actions of the third party remain at arm's length from law enforcement, intelligence agencies, and such. This is not well-documented in the area of cyber security outside the discussion of cyberwar. Cyberwar involves state-to-state measures, or state-to-state sponsored measures. Hackback, as discussed in this book, referred to at least one non-state party or non-state-sponsored party—there is little to no literature for corporate hackback. There needs to be more open discussion around corporate hackback.

14.6 Security Research Exemption and Public-Interest Consideration

Exemption from liability and criminal prosecution has been argued for application to security researchers. A resounding question underlies the debate: do the ends justify the means? Some examples might include the recording industry's proposal to hack into users' computers to find copyright-infringing material and cyber-activists placing Trojans on child pornography to track and record the contents of offenders hard drives for evidential purposes. These examples go to the question of intent as well as whether an act may be justified as a social utility, for the good of the public, similar to how public-interest exemptions work for the admissibility of evidence in court.

It is indeed curious that, in some jurisdictions, there are both security-vulnerability and encryption-research exemptions found in copyright legislation, but these exemptions are not defences to hacking offences in criminal codes and acts. If security research is

considered a public benefit (and it is difficult to see how it is not), then a security- and encryption-research defence should be considered a vital requirement to any criminal code or act. That is not to say that the exemption should be automatic; indeed, there will need to be detailed regulations and guidelines in terms of who, how, and what would satisfy the requirements for a security-research exemption. But it is ludicrous that professional cyber-security researchers perform their work under the duress of the possibility of criminal charges and civil lawsuits.

14.7 Concluding Remarks

There is no shortage of work to be done in the field of cyber security and, within that field, ethical hacking. Working with cyber-security professionals and all shades of hackers over the past seventeen years has taught me that while many *claim* to understand the frameworks and limits of the law, I have yet to meet a hacker—ethical or otherwise—who *clearly* understood those laws and frameworks. Much work remains to be done on finding appropriate ways of responding to ethical hacking that protect civil liberties while providing proficient deterrence to some forms of hacking.

It is my firm opinion that the broad wording of computer offences, both within the Convention of Cybercrime and in domestic criminal law, desperately needs to be revisited. At the moment the legal framework is the same for any act, regardless of the motivation, lack of damage, or whether it was a form of ethical hacking. There is only prosecutorial discretion. Can you imagine if we charged someone with stealing a bag of chips to give to someone in need? If we did, the act would clearly be a misdemeanour. There are no misdemeanour equivalents in these computer offences. And to make matters worse, often those called upon to make prosecutorial decisions are not versed with a deep understanding of the technologies and techniques involved, and some could be described as cyber-illiterate. I will leave you with a recent news story that perhaps best sums up why revision is required to all cyber-security frameworks, law, and policies, and, within those, revisions to ethical hacking. Japan's newly appointed deputy minister responsible for cyber security openly admitted in parliament that he has not used a computer in forty-three years, and that he did not know what a USB stick was.[4] On the plus side, as one commentator ironically stated, "If a hacker targets this

Minister Sakurada, they wouldn't be able to steal any information. Indeed it might be the strongest kind of security!"

Notes

1. National Cyber Security Centrum 2013.
2. United States Department of Justice, "A Framework for a Vulnerability Disclosure Program for Online Systems."
3. HackerOne 2018.
4. Currie 2018.

Page left blank intentionally