22. See http://twitter.com/#!/search?q=%23CabinCr3w. This link has been removed from Twitter. The video of the beating can now be found on news websites such as https://www.youtube.com/watch?v=Doh_gGIzuHQ (February, 2011).
23. Shane and Burns 2011.
24. Thomas 2001.

CHAPTER X

Counterattack/Hackback

Many 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 any 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, more likely, will report it to the system's owner. Third, many security experts are forming self-organized security communities to actively engage in intelligence gathering and counterattacks, here called security activism. Last, 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.

As will also be seen through an examination of emerging events, many corporations and organizations are engaged in some form of counterattack/hackback. 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. The legal ambiguity arises when these security experts find security vulnerabilities, then actively investigate further without permission or authorization from the system's owner, and then go on to disclose the vulnerability. Or, security researchers may sell the vulnerability to be used to hackback as a method of offensive cyber security.

This chapter has the modest aim at looking at hackback, drawing from recent case studies, including deliberate corporate hackback with plausible deniability, the use of hackback by third-party providers contracted by intelligence units (also with plausible deniability), and automated methods to counter denial of service. The chapter then examines recently proposed legislation in the United States to legalize hackback. The conclusion looks at appropriate legal and policy frameworks relative to emerging issues in ethical hackback.

10.1 Counterattack/Hackback in Context

As noted, counterattack is also referred to as hackback or strikeback. Counterattack is when an individual or organization which is subject to an attack of their data, network, or computer takes similar measures to attack back at the hacker/cracker.

Counterattack also refers to a self-help measure used in response to a computer offence. In criminal law, this is expressed as self-defence. In most instances, computer offences refers to an act that is or has already occurred, such as a cyber attack (e.g., deliberate actions to alter, disrupt, or destroy computer systems; unauthorized access or modification to data or computer system, e.g., this may merely mean accessing a computer system), installing malware onto a computer system, or launching a denial-of-service attack.

Consider the example of a denial-of-service attack launched against a corporation's website. A botnet has been used to launch the attack. The corporation would have several options to pursue:

- Implement passive measures to strengthen its defensive posture (e.g., upgrade security software, firewalls, and training to staff).

- Report the cyber attack to law-enforcement authorities and leave it to them to take appropriate action. If the denial-of-service attack has been done for blackmailing purposes, the corporation may elect to pay the sum.
- Do nothing and wait for the attack to be over. Purchase insurance against cyber attack to mitigate against future attacks.
- Contact a third party specializing in cyber attacks to assist in the matter (e.g., AusCERT, SANS Institute, National Cyber-Forensics and Training Alliance).
- Take self-help measures to gather information and investigate the source of the attack toward mitigation of damage and traceback to the source.
- Take actions to actively neutralize the incoming attack through forms of counter-strike, such as a counter of denial-of-service attack

Often an organization will use a combination of options in dealing with the matter. Mitigation of damages is the key priority of most corporations under cyber attack.[1] The most important component in mitigating against damage is protecting assets not already compromised. This could mean protecting data that has not yet been stolen. It could also mean stopping the denial-of-service attack as soon as possible through various means—technical measures, paying a ransom, or launching a counter-denial-of-service attack. Damage control may also mean limiting media attention to the matter in order to keep stock prices from falling, say. Corporations and organizations are taking self-help measures such as counterattack.

Hackback is controversial. There are no shortage of academics and experts writing on the topic. Indeed, many academics—such as Messerschmidt,[2] Rosenzweig,[3] Kallberg,[4] Kesan,[5] and Halberstam,[6] generally take a negative view of hackback where it is unlawful, but additionally have grave concerns about the legalization of hackback as well. These authors look at a wide range of hackback, listed in table 2.

Table 2. Parties and Lawfulness of Hackback

Parties involved in Hackback	Lawfulness of Action
State-to-state counterattack	The Tallinn Manual 2.0 is a NATO initiative to address possible rules around cyberwarfare. Generally, the policy document outlines that states may engage in cyber attacks during times of war and armed conflict. In theory, international laws govern this area, but in practice there is no international agreement by states. China and Russia, for example, take a guarded view of the manual, and of many other international laws. They have been vocally opposed to many of the Tallinn provisions.
State sponsored (hire a private entity) for counterattack of private organization	Not lawful under international law or Tallinn. State-sponsored attacks by private entities are considered state-to-state attacks.
Law-enforcement counterattack on a private entity	Lawful in some countries, but under very strict frameworks. The Computer Crimes Act in the Netherlands, for example, gives law-enforcement investigators the right to hack into private computers and install spyware, or to disable access to files. Law-enforcement investigators are permitted to do so if there is a serious offence and a special warrant. There are several other technical restrictions.
Law-enforcement or government entity hiring or working with a private entity to engage in counterattack of a private entity	Unlawful. But there seems to be some toleration for this type of activity, as will be explored in this paper. This scenario is not contemplated by most authors writing on hackback as these incidents are kept secret and rarely make the news. They are generally dealt with in a way so as to have plausible deniability. These scenarios typically only come to light through whistle-blowers and on websites such as WikiLeaks or on the Dark Net.

Parties involved in Hackback	Lawfulness of Action
	Or in the case where cryptocurrency is involved, the only way to recover these funds typically involves a form of hacking though not necessarily hackback. Cryptocurrency hacks typically involve the theft of "coins." These types of cryptocurrency recovery instances typically involve private organization counter-hack to recover the coins. One cannot use traditional legal frameworks for recovery of stolen assets or money-laundering leaving counterattack as the only means possible of recovering stolen goods and money.
Hiring a private entity to perform counterattack on a private entity	Unlawful in most jurisdictions as the notion of "self-defence" is currently unrecognized in the cyber context. There is a bill in the United States (the so-called Hackback Bill), however, that could make hackback legal under certain conditions. More precisely, the bill—the Active Cyber Defense Certainty Act (amended Computer Fraud and Abuse Act 1986)—would provide a defence to persons who are prosecuted for performing hackback if it was to defend themselves or property. There are many other proposed restrictions.
Private organization counterattack of another private entity	Unlawful in most jurisdictions as "self-defence" is currently unrecognized in the cyber context. The proposed Active Cyber Defense Certainty Act (the Hackback Bill) may have an effect, as noted above.
Private entity counterattack of a law-enforcement or state entity (or private entities engaged by a state or law enforcement)	Unlawful

10.2 Case Studies

There are some interesting hackback scenarios that what could only be described as potential movie material. One such incident is the hack and hackback exchange between LulzSec, MasterCard, PayPal, and Aaron Barr, CEO of the computer-security firm HBGary Federal. Other incidences, however, involve everyday corporate network activities as will be seen below.

10.2.1 LulzSec, MasterCard and PayPal, and Barr

WikiLeaks founder Julian Assange was arrested in London on charges of sexual crimes under Swedish law. Many viewed this as a false arrest and an indirect way of incarcerating Assange for the release of secret US cables to WikiLeaks. A legal defence fund was quickly established wherein people could make donations via MasterCard or PayPal. But MasterCard and PayPal soon disallowed payments to be made to the Assange defence fund, causing an international uproar, particularly within hacktivism communities. Members of LulzSec launched a denial-of-service attack against MasterCard and PayPal, which took down their capabilities in December 2010, and then again in June 2011.

The LulzSec DDoS attacks against MasterCard and PayPal were motivated by the treatment of the companies' refusals to accept online donations for the WikiLeaks situation. Someone (perhaps members of the MasterCard and PayPal team, or perhaps other security researchers upset with WikiLeaks) launched a counter-denial-of-service attack against the LulzSec website. One DDoS attack was met with a counterattack.

Additionally, law enforcement was on the hunt for the members of LulzSec who had launched the attacks against MasterCard and PayPal. During this time, HBGary Federal CEO Aaron Barr was investigating the matter and claimed that he had identified the members who had performed the attacks, claiming he had proof. Barr's emails on the matter were leaked to the Internet and may be found on a number of websites.[7] According to the leaked emails, Barr used IRC to obtain the handle names of those members involved in the attack. He then used social media, such as Facebook and LinkedIn, to allegedly look at friends and family of the hacker group. He then made inferences to the point where he claimed he had identified members who launched the attack. Members of LulzSec retaliated, claiming he had put many innocent individuals in danger. If Barr had indeed used social media to retrieve this information, his methodology remains unclear. Most people are unable to view one's Facebook account unless they befriend them. There are, however, methods to hack into a Facebook account without authorization.[8] It is likely that Barr had indeed accessed this information without authorization. Members of LulzSec responded to Barr's claims by allegedly copying 40,000 emails from HBGary Federal and making it available on the Pirate Bay file-sharing site, launching a denial-of-service attack

to his company's website, and posting: "now the Anonymous hand is bitch-slapping you in the face."

According to the *Guardian*, the exposed emails from HBGary revealed that they, along with security firms Palantir and Berico, "were discovered to have conspired to hire out their information war capabilities to corporations which hoped to strike back at perceived enemies, including US activist groups, WikiLeaks and journalist Glenn Greenwald."[9] My interview with Dreyfus (December 2010, Sydney, Australia) revealed a similar theme of corporations and governments engaging "cowboy security firms" to perform attacks either directly on hacktivism websites and other targets. Dreyfus also revealed that there were several recent attacks performed by cowboy security firms who had made it look as though such attacks came from Anonymous. This, of course, cannot be verified as having occurred for certain. The contracting out of intelligence services, "for hire cyber-attack services" by governments to security firms was also exposed in the Canadian television program *The Agenda*.[10] Identifying attack sources is a difficult proposition.

There are ongoing investigations and arrests had been made against two members of LulzSec for participation in the MasterCard and PayPal attacks. There has been no public investigation or charges laid against those responsible for the counter-DDoS attack against the LulzSec website. Furthermore, there has not been a public investigation made or charges laid in relation to how Barr obtained his supposed information of members of LulzSec through social media. There have not been any arrests made for those members of LulzSec/Anonymous responsible for releasing Barr's personal email and for the DDoS attack of his website. It would appear that investigations and charges are highly, and perhaps unfairly, discretionary.

10.2.2 Illegal Streaming Link Sites

Watching professional sporting events is expensive in many parts of the world. Sometimes coverage of the sport is only offered through one service provider, and a subscription can be beyond the means of most people. The only legal way to view the big match is to purchase a ticket to be physically present in the stadium, pay the price for the subscription to the provider carrying the event, or go to a bar or venue showing the event. This means that many devoted fans are not able to legally watch sporting events from the comfort of their homes. Whether it is soccer/football, cricket, rugby, badminton,

tennis, football, or ice skating, fans will always find ways to watch, whether it is by legal or illegal means. Some popular methods are to watch through illegal streaming sites or through P2P channels. Google can be used to find a single site streaming the event, but more often than not, a sports fan will use a torrent index site to see where and how the big game can be watched. These indexing sites do not host the content, nor do they stream the content; they merely provide an index to sites and torrents that will show the content.

Some of these linking indexes include Wiziwig, FirstRowSports, MyP2P.eu, and Rojadirecta. These indexing sites have been treated differently in courts around the world. In 2009, for example, a Spanish district court declared Rojadirecta did not violate copyright law as they only provided links to the materials in question.[11] Such indexes are lawful in many parts of the world. Even in jurisdictions where the indexes do violate copyright law, and are therefore unlawful, there is little that a company can do to take down the foreign-based infringing indexes. A website simply has to register in a jurisdiction with copyright-friendly laws and it becomes out of legal reach.

Since 2013, sporting index sites have suffered ongoing denial-of-service attacks which temporarily take down the sites.[12] This is particularly common right before or during a high-profile sporting event. While no one has openly claimed responsibility for these attacks, there are two prevalent theories. The first is that a competing sporting index is DDoS-ing the competition. In fact, they could be routinely DDoS-ing one another. The second, and more likely, is that the entities with exclusive rights to a sporting event have engaged a private entity to DDoS these indexing sites. Of course, neither of these activities is lawful in a jurisdiction with hacking provisions. They both clearly violate the hacking provisions in most countries in the world, but not in all countries. The DDoS could have been performed in a country with no cybercrime law, or in a country where enforcement is unlikely and there are no extradition treaties between that country and the United States or Europe Union, or, lastly, the DDoS could have been performed on a vessel strategically located in "non-jurisdiction" international waters.

10.2.3 Automated Counter-DDoS

The ironic reality is that hackback occurs hundreds of thousands of times per day around the globe without anyone deliberately setting

out to perform a counterattack. This is because many cyber-security software and systems have several technical features to minimize the damage caused from a DDoS attack and to thwart a DDoS altogether. Many of these systems automatically perform counter-DDoS as a means of reducing and blocking the threat. There is an assumption that these systems are perfectly legal, when of course, they are not; the law does not allow for unauthorized access or modification of any system. There are no exemptions to these "hacking" provisions.

10.3 The Legalization of Hackback

The legalization of hackback has been gaining momentum in the United States. It is important to recognize that hackback involving state actors is governed under international law and is not considered within the scope of ethical hacking in this book. For example, the International Court of Justice upholds state-to-state counterattacks where four criteria are met.[13] First, the counterattack must have been directed at whomever performed the original cyber attack. Second, the attacker must have been asked to cease the attack. Third, the counterattack must be proportionate to the original act and reversible. Fourth, the counterattack must induce the attacker to comply with international standards.

Law enforcement's use of hackback has become legal in some jurisdictions. The Netherlands permits law-enforcement agencies to perform counterattack. Under the country's Computer Crime Act, investigative officers have the right to hack into private computers to install spyware (this allows attribution) and to destroy or disable access to files. Law enforcement must first obtain permission from prosecutorial services, after which it may proceed in court to obtain written authorization. The authorization is limited to a serious offence and must meet many technical requirements.

The United States is considering the legalization of hackback outside of law-enforcement and state-to-state contexts, specifically corporate hackback. The Active Cyber Defense Certainty Act, a bill proposed by US Senator Tom Graves in 2017, addresses "active cyber defence," which is a disputed term. Task force and cyber-security expert Bob Chesney describes the term as:

> "Active defense" is a phrase of contested scope, but the general idea is that when someone has hacked into your system, there

> are steps the victim might take (or might hire someone to take) that help identify or even disrupt that unauthorized access (including, perhaps, steps that take place outside your system, giving rise to the phrase "hacking back").[14]

Under the proposed bill—dubbed the Hackback Bill in the press—a person prosecuted under computer-crime provisions may raise active defences in response to a cyber intrusion. The general framework of self-defence is fraught with ambiguities and uncertainty as to how it would be applied to "cyber." The point of the bill is to recognize a range of activities that are permissible in response to a cyber intrusion. An organization may engage a third party to perform work outside of their own network to disrupt, monitor, and react to a cyber intrusion on their network system.

The two glaringly obvious problems with any form of hackback are attribution and damage to innocent third-party systems. The Hackback Bill provides many limitations. The first is the limited definition of "victim" to only include an entity that has suffered from a *persistent* unauthorized *intrusion* of the entity's computer or network. Figure 19 below looks at a typical life cycle of a cyber intrusion.

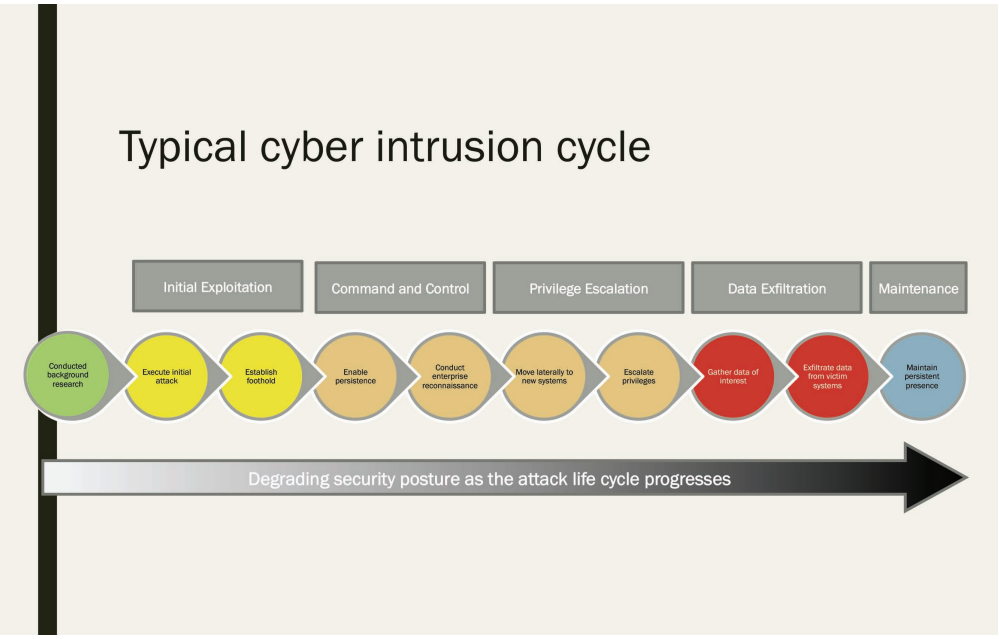

Figure 19. Life cycle of a Cyber Intrusion.[15]

In the above instance, there is an escalation of the initial exploitation, leading to privileged escalation and later data exfiltration. The Hackback Bill only requires that there is an intrusion that is done more than once and does not suddenly stop—it must be continuous. Intrusion in this life cycle and proposed in the bill is something more significant than a denial-of-service attack.

As the bill would require that the attack be persistent and intrusive, this precludes denial-of-service attacks. By not including denial-of-service threats, it stands to reason that the act also would not legalize a counter-denial-of-service attack.

Other requirements under the proposed act include the duty of the entity performing active defence to notify the FBI National Cyber Investigative Joint Task Force prior to engaging in activity. The counterattack must be proportionate. Active defence measures are described as:

- undertaken by, or at the direction of, a victim; and
- consisting of accessing without authorization the computer of the attacker to the victim's own network to gather information in order to establish attribution of criminal activity; to share with law enforcement or to disrupt continued unauthorized activity against the victim's own network.

There are a few parts to the permissible activities above that require further speculation. The first is that attribution is assumed possible. Second is that attribution intelligence when shared with the FBI will lead to establishing that the attribution is in fact correct. Third, and more important, is that the active measures will disrupt the attack.[16] While all the above is noble in theory, it assumes that attribution is possible, and that an active measure would be directly against the person/entity responsible for the initial attack. A distinct problem with this line of reasoning is that attackers hardly ever use one system, let alone their own, to perform an attack. Third-party devices are nearly almost always used to perform cyber intrusion. These third-party devices are rarely, if ever, aware that they are part of the attack. They are obfuscated.

Because attribution is inherently difficult and attackers nearly always use multiple third-party devices, innocent parties will most likely be affected by any active defence mechanism. It is one thing to say that the active defence may be liable for damages, but the reality

is that the innocent parties will never know if they have been used to commit an attack, or why active defence measures are being taken against their systems. The incoming data traffic will only read as an attack. Also, there is no obligation under the bill to notify third-party systems of active defence measures. In other words, if damage is caused by the active defence measures, they would not know who to sue for damages. Even more problematic is that innocent third-party devices are likely scattered across the globe—jurisdiction for any of this mess would be a nightmare for legal recourse.

The Hackback Bill states that the defence is no longer valid if the measure destroys information on the other system, there is physical injury, or a threat to public safety or health.

If the active defence is later found to be excessive, the entity who performed active defence can be liable for damage caused, and the defence will no longer apply. This means that the entity could be charged with a computer-crime offence. The reality is that Senator Graves' proposal is likely to remain just that for now, a proposal that will not lead to legislation. However, the questions the bill raises remain essential. Appropriate responses to cyber-security threats are few and far between. Finding a way forward in this discussion is a nearly insurmountable task.

10.4 Observations

Counterattacks are launched as a form of self-defence or as a means of retribution. The LulzSec and PayPal examples certainly highlight the retribution motive. However, most organizations perform acts of counterattack as a form of self-defence. In 2001, researchers surveyed 528 IT managers in Western Australia and Victoria to obtain their views on counterattack. Those surveyed were asked a variety of questions, including whether strikeback should be allowed if their organization was subject to an attack (65 per cent replied "yes," 30 per cent "no," and 5 per cent were undecided).[17] This question was then broken down into specific types of attacks, such as attempt at network access and attempt to destroy or alter data, which resulted in increased "yes" response rates to ranges between 70 per cent and 93 per cent. The survey was done in 2001. The author is unaware of any more current surveys on hackback.

The main targets are the IP addresses (often of websites or computers) that initialize the attack. Information may also be gathered

and collected, where possible, of those individuals who perform the attack, though this can be difficult to trace.

Again, the motivation is either to defend or retaliate against the origin of the attack. The target is normally a website and does not typically involve the individual per se behind the attack (because identification is often difficult).

There are a variety of ethical and moral issues at play with counterattack. One principle could be seen as defending one's property against attack. The other main principle is retribution. There appears to be an additional principle of hacking to discredit an organization, typically by deliberately launching an attack to make it look as though it has come from another organization. Plausible deniability is endless with hacking and hackback.

There is no consensus as to whether corporations and organizations engaged in counterattack are aware of the illegality of their activity. Some security software will automatically initialize a counterattack, whereby the organization may or may not be aware. It may be the case that those individuals running the security of the organization are aware of the illegality of the action, but that the board of directors are kept in the dark. There is also evidence that many organizations employ former black-hat hackers under strict control and surveillance, yet this type of arrangement is rarely publicized.[18]

Self-defence may apply to some forms of counterattack. There are no cases that deal with defending oneself against an online attack. There is likewise little literature on the topic in most jurisdictions other than the United States, where there is an emerging discussion but no advancement in terms of a clear policy or legislative reform. Indeed, the Hackback Bill has no sufficient support from Congress or the Senate. Curiously, Australia's Model Criminal Code (MCC) provides guidance as to the scope of self-defence in such situations. The MCC discussed at length the growing trend in the United States for corporations' use of computer software with counter-strike abilities. The MCC committee stated that:

> It is possible that the defence of self-defence in chapter 2, s.10.4 of the Model Criminal Code might extend to some instances of computerised counterattack against cybernet intruders. Self-defence includes conduct which is undertaken "to protect property from unlawful appropriation, destruction, damage or interference". It is possible that a strikeback response to the

> hacker's attack could be characterised in this way. In practice, counterattack involves serious risk since hackers are likely to adopt precautions which divert the counterattack to innocent third parties. It is apparent that principles of self-defence of persons, which extend without undue strain to include protection of tangible property, are inadequate for the purpose of regulating computerised counterattack against hackers. The familiar concepts of necessity and reasonable response, which excuse or justify counterattack against physical threats, are next to useless as guides in this field.[19]

The MCC committee concluded that "legislative intervention would be 'premature.'" They further noted that corporations who resorted to self-help/hackback "would be left to the uncertain promise of a merciful exercise of prosecutorial discretion."[20] The concluding sentence provides even more ambiguity to the MCC, where it is stated:

> The familiar criteria of necessity and proportionality which govern self-defence in other applications have no obvious application here. Reliance on a test of what is or is not reasonable in the way of counterattack against hackers would place an inappropriate legislative burden on courts to determine issues of telecommunications policy.[21]

The conclusion seems to echo a recurring theme of "This is a tough one so let's wait and see." The MCC committee declared that legislation was premature and that courts should not be the ones to determine issues of telecommunications policy. So who should make these determinations? The reality is that individuals and corporations are making these determinations as a matter of internal policy. The actions and reactions of corporations are simply non-transparent at the moment. In the United States, however, Senator Graves's bill recognizes that corporate hackback is occurring and that appropriate measures need to be taken to form not only sound policy, but a certain legislative framework.

There has been much criticism of hackback as it is seen by many as a form of cyber vigilantism. Common concerns include the risk of launching a counterattack on an innocent third party. There are many obfuscation methods used in hacking, such as routing traffic

through third-party devices and networks.[22] A counterattack would almost definitely affect these third-party systems. Even if an organization believes that it will not affect innocent third-party systems, the risk of misidentifying the source/person responsible is inherently challenging. Attribution remains a significant hurdle. Others question whether hackback would have a deterrent effect or whether it would merely provoke an escalation of hacking and counter-hacking. The notion of what is proportionate as a response to a hack is also a challenging area. It is further contended that legalizing hackback with insufficient oversight by a public body could result in deteriorating trust in the international system and could even go so far as to undermine cyber norms.

Is there a way forward? Perhaps. There used to be a time where security-vulnerability disclosure was highly contentious and fraught with legal uncertainties with constant legal threats to researchers who exposed significant vulnerabilities in corporate and government systems. The US Department of Justice worked to develop policy around vulnerability disclosure, authorized vulnerability, and bug-bounty platforms, such as HackerOne and Bugcrowd, and has openly discouraged legal action against cyber-security researchers. The result is that many corporations are openly publishing vulnerability and bug-bounty programs that limit legal recourse and pay researchers for finding vulnerabilities and bugs in the code, albeit the money paid out being a small amount in comparison with the time, effort, and number of coders working to find such.

Hackback is clearly different from cyber-security vulnerabilities and bug bounties, but the aims are similar: to discourage and disrupt cyber-security threats through soft policy and change in corporate attitudes toward novel programs. Hackback requires soft policy that has been negotiated between government, relevant authorities such as CERTs, and with private corporations. This could start with a pilot project in one jurisdiction to see how this would work in practice. Perhaps attribution and third-party damage is more problematic than anticipated, or perhaps it is not. This would make for an interesting case study that could lead to policy at the national level, and, later, at the international level, if the pilot projects are successful.

Of course, diplomacy in parts of the world where cyber threats are clearly attributed is also an option, especially when coupled with an international agreement. Intellectual property and counterfeit goods by way of example have been the subject of intense

international negotiations, trade retaliation, and soft measures. This has led to some effective programs in jurisdictions with known IP issues, such as China. While not a perfect solution, there has been progress. However, corporate hackback is only at the beginning phase as a topic of limited conversation, one lacking a global audience.

Notes

1. Email correspondence with Ron Plescoe, director of the National Cyber-Forensics and Training Alliance (NCFTA) 2009 as part of PhD Thesis MAURUSHAT, A. 2011. Notes from the interview have been kept on file by the author.
2. Messerschmidt 2013.
3. Rosenzweig 2013.
4. Kallberg 2015.
5. Kesan and Hayes 2012.
6. Halberstam 2013.
7. For a link to the emails, see *The Old Computer* in references.
8. AusCERT 2011 presentation by Christian Heindrick.
9. B. Brown 2013.
10. *The Agenda*, "Attack of the Hacktivists."
11. Ernesto, 2010.
12. Andy, 2013.
13. Chesney 2017.
14. Chesney 2017.
15. Figure provided with permission by cyber-security firm Gridware.
16. Centre for Homeland Security, George Washington University 2016.
17. Hutchinson and Warren 2001.
18. For example, former botnet master Owen Walker is now employed by Telstra; see Maurushat 2011.
19. Model Criminal Code, p. 108.
20. Model Criminal Code, p. 109.
21. Model Criminal Code, p. 109.
22. Dupont 2017.