The Hack Back: The Legality of Retaliatory Hacking

Valeska Bloch, Sophie Peach and Lachlan Peake consider whether organisations in Australia and abroad have a right to 'hack back' in response to a cyber attack.

Today, the cyber battlefield is just as important as the physical one. However, in circumstances where government departments and law enforcement agencies are unable or unwilling to effectively respond to cybercrime, organisations are increasingly questioning whether or not they have (or ought to have) a right to 'hack back' as an offensive retaliatory measure. This article looks at how this debate is evolving at home and abroad.

What does it mean to 'hack back'?

Hacking back generally refers to the proactive steps taken by the victim of a cyberattack to turn the tables on its assailant in order to:[6]

- identify the source of an attack, including by probing a cybercriminal's infrastructure for weaknesses or snippets of information that could reveal who is behind an attack;
- thwart or stop the crime, including by disabling the hacker's malware, or launching distributed-denial-of-service (DDoS) attacks;[7] or
- destroy or steal back what was taken, including by remotely breaking into a target's servers and wiping any data including stolen information or intellectual property.[8]

Developments in Australia

The legal position

The Cybercrime Act prohibits the unauthorised access to, or modification or impairment of, data held on a computer.[9] Although these laws do not draw a distinction between hacking and hacking back, 'depending how it is done, [hacking back] may not be illegal.'[10] One possible legal argument is that 'computerised counter attack' is an example of self-defence.[11] Some academics believe self-defence should permit hacking back in particular circumstances. The law recognises a right to engage in active 'self-help' in certain circumstances, for example, 'the right of restraint and self-help eviction remedies in landlord-tenant relations' and the right of self-defence in criminal law to protect personal safety or property.[12] This is the basis on which some argue that, in principle, the law could similarly allow active self-help against cybercrime, subject to certain limitations such as necessity and proportionality.[13]

Dr Alana Maurushat advocates for legislation that permits hacking back provided it meets certain conditions – in particular, that a party can sufficiently attribute the source of the hacking to minimise the likelihood of retaliatory measures being taken against the wrong target, and that the counter-hacking is reasonable, proportionate and necessary when considered against the harm sustained by the victim.[14]

While the position in Australia might seem slightly more opaque than elsewhere, it is likely that hacking back is an offence under Commonwealth law. Speaking to the Australian Strategic Policy Institute on 29 October 2018, ASD Chief Mike Burgess issued a strong warning to Australian businesses contemplating 'hacking back'.[15] Burgess unequivocally stated hacking back is illegal in Australia and should not form part of any organisation's cyber strategy.[16] He expressed particular concern that cyber attacks launched by Australian businesses, or at their behest, 'risk misattribution and an escalation in malicious activity'.[17] Further, privately initiated attacks risk that attack being misinterpreted as a state sanctioned attack, which could have significant negative consequences.[18]

1 Nicholas Schmidle, *The digital vigilantes who hack back, The New Yorker* (7 May 2018).
2 Ibid.
3 Melissa Riofrio, *Hacking back: digital revenge is sweet but risky, PC World* (9 May 2013).
4 Tom Kulik, *Why the Active Defense Certainty Act is a bad idea,* Above the Law (29 January 2018).
5 TimeBase, *The legality of defensive hacking* (30 September 2013).
6 Dan Lohrmann, Can 'hacking back' be an effective cyber answer? *Government Technology* (13 February 2016).
7 Joseph Cox, *Revenge hacking is hitting the big time, Daily Beast* (19 September 2017).
8 Liam Tung, Is hacking in self-defence legal? *Sydney Morning Herald* (27 September 2013).
9 *Cybercrime Act 2001* (Cth) ss 477.1 – 477.
10 Alana Maurushat, senior lecturer at UNSW Faculty of Law (see Liam Tung, *Is hacking in self-defence legal? Sydney Morning Herald* (27 September 2013)).
11 Ibid.
12 Jay P Kesan and Ruperto P Majuca, 'Hacking Back: Optimal Use of Self-Defense in Cyberspace', Oxford Research Paper, p1.
13 Ibid pp 20–24.
14 Alana Maurushat, senior lecturer at UNSW Faculty of Law (see Liam Tung, *Is hacking in self-defence legal? Sydney Morning Herald* (27 September 2013)).
15 Mike Burgess, Director-General ASD, *Speech to ASPI National Security Dinner* (29 October 2018).
16 Ibid.
17 Julian Bajkowski, *Australia's cyber spy chief slams corporates contemplating 'hacking back', IT News* (30 October 2018).
18 Ibid.

The industry position

A 2017 Commbank Report found that Australian industry is split on active defence and referred to a survey by the Australian Strategic Policy Institute which said only 10% of respondents were in favour of a right to hack back. In Australia, more than 70% of data breaches are detected by law enforcement agencies or third parties and less than 20% by companies' internal security teams.[19] This may be one reason why the preference among the business and broader community appears to be for increased law enforcement competencies (both legal and technical) to respond to identified cyber intrusions, rather than legal permission for victims to hack back themselves. Nevertheless, hacking back is 'reasonably common' in Australia,[20] suggesting there is some degree of frustration among the business community at perceived ineffectiveness of formal legal responses to hacking.

The Government's approach

In July 2017, the Australian Government established the Information Warfare Division (***IWD***) within the Department of Defence, headed by the Deputy Chief (Information Warfare), Major-General Marcus Thompson. This unit is tasked with 'defending the country's critical infrastructure against cyberattacks and launching offensive cyber strikes on foreign actors.'[21] The former Minister for Cybersecurity, Dan Tehan, explained that the focus of this unit is on 'military cyber operations, military intelligence, joint electronic warfare, information operations and [the] military's space operations.'[22] Thus, the Division is mostly concerned with the defence implications of state-to-state cyber warfare.

At the same time that the IWD was established, former Prime Minister Malcolm Turnbull also unveiled plans for the ASD to be given increased powers to respond to overseas cyber criminals, stating that '[o]ur response to criminal cyber threats should not just be defensive. We must take the fight to the criminals.'[23] At the time, Opposition Leader Bill Shorten remarked that the protective focus should not be limited to the 'military establishment' and 'big banks' but also smaller and medium-sized businesses, other organisations, and the health system.[24] If the ASD's new competencies are focused mainly on protecting government departments and the largest private organisations, then many sectors of the Australian economy could continue to exist in a kind of regulatory gap, where active defence against cybercriminals will either be self-initiated, or not occur at all.

Global Developments

The US's Active Cyber Defense Certainty Bill

As in Australia, the criminal prohibition in the US[25] does not draw a distinction between hacking and counter-hacking, but simply provides that using a computer to intrude upon or steal something from another computer is illegal.

The Active Cyber Defense Certainty (***ACDC***) Bill[26], introduced in 2017, would lift the restriction on hacking back. The long title of the Bill states its purpose is 'to provide a defense to prosecution for fraud and related activity in connection with computers for persons defending against unauthorized intrusions into their computers'. Interestingly, the Bill expressly recognises that the nature of cybercrime makes it 'very difficult for law enforcement to respond to and prosecute [it] in a timely manner'.[27]

To give effect to its purpose, the ACDC Bill would make limited hacking back legal by allowing organisations defending their networks to:

- destroy any stolen data;[28] and
- go outside those networks to access the servers being used to conduct the attacks to gather information in order to:
    - deploy technology to identify the physical locations of the hackers;
    - disrupt those servers to interrupt the attack; and
    - monitor the behaviour of an attacker to assist in preventing future attacks.[29]

The Bill also imposes the following safeguards:

- The Bill provides that hacking back, or 'active defense', be restricted to computers in the US. The difficulty with this, however, is that domestic hacking can be routed via overseas servers, thus circumventing the application of the ACDC Bill. As cybercrime is truly borderless, a geographic limitation on hacking is of limited utility.
- The Bill contains a liability provision making organisations financially responsible for any damage caused to innocent computer users.

19 Commonwealth Bank, *Signals: quarterly security assessment* (Q1 2017).

20 TimeBase, *The legality of defensive hacking* (30 September 2013); and Liam Tung, *Is hacking in self-defence legal? Sydney Morning Herald* (27 September 2013).

21 Australian Government Department of Defence, *Information Warfare Division.*

22 James Elton-Pym, *'New Australian military unit will specialise in cyber warfare', SBS News* (30 June 2017).

23 Ibid.

24 Ibid.

25 Computer Fraud and Abuse Act (1984) Title 18, Sec. 1030.

26 ACDC Bill 2017.

27 ACDC Bill 2017 s2(2).

28 ACDC Bill 2017 s3.

29 ACDC Bill 2017 s4.

Key Takeaways

- As the frequency and severity of cybercrime continues to increase, a debate has emerged as to whether or not companies should be allowed to exercise a kind of 'digital vigilantism'[1] by taking active steps to prevent or respond to cyber incidents. There tends to be two key schools of thought:
    - Those that reject hacking-back note that the risks associated with hacking back are significant and that hacking back can have unintended consequences. First, there is considerable difficulty associated with identifying the perpetrator and, even if the hack works, a victim may simply have invited further retaliation.[2] Second, counter-attacks can also damage hijacked computers belonging to innocent third parties.[3] Third, most companies don't have the skillset internally to effectively take affirmative countermeasures against cyber criminals. Companies are finding it hard enough to implement defence mechanisms to prevent attacks in the first place – arming staff with the skillset to effectively 'hack back' takes this to an unprecedented level.[4] Nevertheless, or perhaps precisely for that reason, a 'new breed of security company' has emerged which offers to aid companies in implementing active defence measures.[5]
    - Hacking back proponents tend to argue that provided that the cybercrime can be accurately attributed and that any response is reasonable and proportionate, in the absence of greater government involvement, hacking back is the only realistic solution.
- In Australia, computer intrusion and unauthorised access to or modification of data (including data destruction) are offences under the *Cybercrime Act 2001* (Cth) (the ***Cybercrime Act***). Hacking the hacker outside your network therefore runs the risk of committing a criminal offence.
- We are seeing a fascinating development in the US: on the one hand, legislative moves to sanction private entities to engage in active defence, a kind of 'cyber vigilantism'; and on the other, pressure from security and defence agencies for an increased political appetite to operate aggressively in response to foreign hacking.
- The approach taken by German legislators has been to expand the powers and responsibilities of state agencies. This culminated in the creation of a new army command responsible for responding to malicious attacks.

- The Bill would require counter-hackers to give prior notice to the FBI's National Cyber Investigative Joint Task Force so that it can check for any extra-territorial impact and interference with national security operations.
- The legislation will have a sunset date of two years after passage and the US Justice Department is obliged to report to Congress once a year on activity carried out under the ACDC regime.

The question becomes: is a measure such as that introduced by the ACDC Bill 'a necessary tool for companies to protect their valuable information assets' or is it 'cyber-vigilantism'?[30] While members of the internet security industry in the US have suggested that many companies and large organisations already have in place measures for defending against cyber-intrusion that may amount to hacking back,[31] it appears that 'most companies and cybersecurity experts' in the US are *against* legally permitting counter-hacking by non-state victims of cyberattacks.[32]

To the extent that there is support for the reform in the US, it would seem to be founded on the same justification expressly identified by the ACDC Bill[33] – that is, although it would be preferable that law enforcement and government agencies had the sole remit and responsibility for responding to cybercrime, the logistical enormity of that task, coupled with the vital importance of cybersecurity in the modern world, may justify an exception to the general principle against justice being meted out by victims.

The ACDC Bill was referred to the Congressional Subcommittee on Crime, Terrorism, Homeland Security, and Investigations on 1 November 2017. It can be expected the debate will continue whatever view the Committee forms on the measure.

Germany

Unsurprisingly, this issue is also occupying the attention of policymakers in Europe. In Germany, intelligence officials are advocating for greater legal authority to hack back in the event of cyberattacks from foreign powers and overseas criminals.[34] The legal complication there is centred on which of Germany's 'more than three dozen security agencies' will be responsible for hacking back, and what the scope of their powers would be.[35] Front of mind for German legislators when considering this issue is the weeks-long intrusion by foreign-based hackers into the networks of

30 Tom Kulik, '*Why the Active Defense Certainty Act is a bad idea,' Above the Law* (29 January 2018).
31 Nicholas Schmidle, *'The digital vigilantes who hack back,' The New Yorker* (7 May 2018).
32 Josephine Wolff, 'When companies get hacked, should they be allowed to hack back?' *The Atlantic* (14 July 2017).
33 ACDC Bill 2017 s2.
34 Andrea Shalal, 'German spy agencies want right to destroy stolen data and 'hack back',' *Thompson Reuters* (6 October 2017).
35 Janosch Delcker, 'A hacked-off Germany hacks back,' *Politico* (28 January 2018).

the Bundestag, Germany's Lower House, in 2015. This precipitated the creation of a new German army command comprising 13,500 'cyber soldiers' and contractors in 2017, before prompting this most recent agitation for increased security powers. The new army command 'protects military intelligence, communications, and geographic-information systems' and 'currently consists largely of military personnel with backgrounds in IT.'[36] The incorporation of this new capacity within traditional defence structures was metaphorically described by the unit's head, Lieutenant Colonel Marco Krempel, as 'tuning a driving car.'[37]

This state-oriented approach, focusing on augmenting the powers and diversifying the capacities of traditional security and law enforcement agencies, provides an interesting contrast to the ACDC Bill in the US. The sponsors of the proposed German legislation clearly do not share the view of their American counterparts that it is overly difficult to guarantee timely and effective responses by a nation's agencies to the dynamic and fast moving problem of malicious hacking.

The US Military View

Nevertheless, the view that defence and intelligence capabilities must be reorganised and augmented to deal with the threat of cyberwarfare is stirring in the US. In testimony before the Senate Armed Services Committee, outgoing head of US Cyber Command (***USCYBERCOM***) and the NSA, Admiral Michael Rogers, identified his 'greatest concern' to be 'state-sponsored malicious cyber actors and the states behind them', as 'many states now seek to integrate cyberspace operations with … their traditional military capabilities.'[38] Indeed, several have mounted sustained campaigns to scout and access [the US's] key enabling technologies, capabilities, platforms and systems'.[39] Admiral Rogers explained that the problem in defending against cyberattacks on US infrastructure and systems from state, state-sponsored and non-state actors alike, is that these attacks occur at a level that is 'below the threshold of the use of force and outside of the context of armed conflict, but cumulatively accrue[s] strategic gains to our adversaries'.[40]

One implication from the Admiral's comments is that a sophisticated response from defence, security and intelligence agencies will need to occur at the same level – something above intelligence gathering and espionage, but below the use of force. The intention behind such a strategic shift will be to prompt rethinking by perpetrators: a key challenge which USCYBERCOM has faced in responding to network intrusions by 'Russian actors' is that nothing has been done by the US to force perpetrators to 'change their calculus.'[41] However, Admiral Rogers was guarded and, under questioning from Senators, quickly pointed out that such a shift is a shift in policy, stating: 'I'm not going to tell the president what he should do or not do … I'm an operational commander, not a policymaker.'[42]

Valeska Bloch is a Partner in the Technology, Media and Telecommunications Practice Group at Allens and **Sophie Peach** and **Lachlan Peake** are Head Paralegals at Allens in Sydney. This article represents the personal view of the authors and is not necessarily the views of the firm.

36 Ibid.

37 Sumi Somaskanda, 'Cyberattacks are "ticking time bombs" for Germany', *The Atlantic* (4 June 2018).

38 Admiral Michael S Rogers, Commander: United States Cyber Command, Statement before the Senate Committee on Armed Services (27 February 2018) p4.

39 Ibid.

40 Ibid p 12

41 Sean Gallagher, 'Why US "cyber-warriors" can't do anything about Russian "cyber-meddling"', *ars Technica*, 1 March 2018.

42 Ibid.