THE REGIONALIST
INSTITUTE FOR REGIONAL SECURITY

CYBER WEAPONS: AUSTRALIA'S NEXT SECURITY CHALLENGE

Bowany Pugh

SYNOPSIS

Australia has made a late start in managing cyberspaces' blowback effects – which are the negative side effects of technology advancing at a rate faster than the population's ability to understand the changes occurring. Policy-makers now need to better focus on ensuring Australia is resilient to cyber events. Cyber resilience is the ability to prepare for, respond to and recover from a cyber-attack. By building up strong resilience, organisations can continue to operate during a cyber event and have the capacity to recover from or adapt to such events. Cyberspace will become more important in inter-state conflicts and states are likely to push the boundaries of acceptable cyber behaviour if international norms and rules of engagement for cyber-attacks are not developed or enforced.

The government has begun to give cyber challenges the attention they deserve. However, Australian companies still need to be better supported in dealing with these challenges. To achieve this goal, cyber resilience needs to be built at the national level. The Australian government must invest now to develop indigenous cyber industries so that Australia's cyber technology, capabilities and workforce are strengthened. There needs to be greater partnership between industry and government, and collaboration between government agencies and with academia and international partners. And Australia needs to develop the technical capabilities, coherent national response and international cooperation needed to deal with the cyber-security challenges of the future.

THE DIFFICULTIES OF MANAGING CYBER ATTACKS

The impact of cyber threats extends beyond the commercial sector. Cyber technology has become an important tool of warfare and most conflicts today contain a cyber element – whether that be in the form of intercepting communications, providing tactical support or hacking power grids. At an estimated cost of US$450bn on the global economy, according to the CNBC, cyber attacks can have an enormous economic impact, and are a threat to intellectual property, privacy and state secrets. Cyber attacks are used for purposes of state sponsored espionage, sabotage, covert cyber influence and organised crime. Cyber attacks on Australian government agencies are now routine and most of them are sponsored by foreign state actors. The Australian Signals Directorate detected more than 1200 cyber attacks against Australian interests in 2015. The number is likely to be greater given that most cyberattacks go unreported or under-reported, and information concerning breaches is often kept classified. However, it is the ability for cyber attacks to cause physical damage, and the notion of the cyber weapon, that should be particularly concerning to policy-makers around the world. Warfare generally involves attacks through land, sea, air and even space. But, recognition of cyberspace as the fifth operational domain of warfare is spreading amongst experts worldwide. The recognition of cyberspace as an operational domain of warfare reflects a preparedness to respond to severe cyberattacks with the use of conventional weapons. For instance, NATO's Article 5 principle of self defence might now be triggered in the event of a digital attack rather than being limited to attacks by sea, air or land.

Applying existing frameworks of international law to the unique characteristics of state conflict through cyberspace would be a difficult task. In cyberspace, attacking is easier than defending. Finding the origin computer of the attack is difficult, and where the origin is found it is then hard to tell whether the computer used was the true source of the attack, or whether it was itself hacked. On top of this issue, analysts will struggle to distinguish between attacks which are carried out by individuals and those conducted by a state's military. Unlike conventional forms of attack, cyber investigations do not easily identify the culprit and so it is hard to attribute cyber attacks. Governments almost never admit to hacking each other's computers, leaving those affected to infer the origin by the target list or the complexity of the attack. Tracing an attack is technically difficult, but it is further complicated because connection pathways can cross national borders and network domain boundaries, which may require cooperation from foreign law enforcement agencies, security agencies and network administrators. There are positive international efforts to cooperate on cybercrime investigations, such as by Europe's Joint Cybercrime Action Taskforce (J-CAT). However, the bodies in charge of leading or coordinating cyber-security policy in a country vary from cabinet offices to national security directorates and the power and reach of these bodies are likewise inconsistent across jurisdictions. This uneven approach means that cooperation can be uncoordinated

or reactive, and information-sharing between the public and private sectors can vary. Consequently, vital information is often missed by those investigating an attack and goes unnoticed by those developing cyber resilient capabilities. Cyber authorities may not be able prove the attack was state-sponsored even if they determined the cyber attack's country of origin. Governments must make attribution with high confidence before they can retaliate. If attribution is indeed achieved with some degree of certainty, the process taken to reach that certainty is often time-consuming, further delaying retaliatory actions. Disclosing information related to the cyber attack could also expose vulnerabilities or provoke further probing attacks.

AUSTRALIA'S INCREASING VULNERABILITY

Cyber attacks are evolving in the manner that they are occurring. Traditional espionage is one government's efforts to acquire classified or protected information from another government. In the pre-internet era of the Cold War, electronic methods of espionage largely consisted of specifically targeting communication circuits. For example, from the early 1970s, the US conducted *Operation Ivy Bells,* which placed wiretaps on Soviet underwater cables. These types of operations were usually linked with political and military intelligence. Contemporary cyber espionage is likely to involve breaking into a computer network to install malicious software that will extract data. Instead of passively intercepting communications, it is now easier for a state's adversary to actively hack, search and extract from computer networks. For example, in 2014, North Korea breached Sony Pictures Entertainment servers, stealing sensitive documents, destroying computer systems and downloading unreleased movies.

States sponsor cyber espionage for a number of reasons. China uses cyber espionage as a tactic to enhance military modernisation and steal intellectual property, trade secrets, and other information which could make China more economically competitive. Iran uses cyber espionage to damage opponents. State or non-state actors can also spread misinformation or influence public opinion through the internet and social media platforms. In 2016 Russia attempted to influence US political debates through covert cyber influence activities, including hacking the Democratic National Committee to obtain and distribute information that was harmful to the Clinton campaign.

ATTACKS THAT CAUSE PHYSICAL DAMAGE

States are increasingly using cyber attacks to cause physical damage, and what should be of particular concern to policy-makers around the world are vulnerabilities associated with critical infrastructure. The 2009 Stuxnet attack is an important development in this area. According to the New York Times,

the Stuxnet virus damaged one-fifth of Iranian centrifuges at the Natanz nuclear facility. The centrifuges used to enrich uranium gas began to fail at an unprecedented rate and a series of computers were crashing and rebooting repeatedly, causing significant physical damage to the Natanz nuclear facility. A virus related to Stuxnet was also used in tandem against North Korea. According to some legal experts, this level of damage is significant enough to constitute an armed attack under international law. In line with this argument, the virus can be defined as the world's first cyber weapon. As reported by Reuters, due to the sophistication and complexity of the Stuxnet attack, it is widely believed that it originated from a joint program by the US and Israel.

The theoretical possibilities of gaining military advantage by subverting computer networks to render them useless was explored by the Defense Science Board as early as 1970. Decades later, the notion of the cyber weapon began to come into fruition. Offensive cyber operations were first added to the Pentagon's network defence task force's mission in 2000, and focus by the US on offensive operations have been rising ever since. In 2011, the US used cyber to prevent Libya's early warning systems from detecting the arrival of NATO warplanes. According to the documents leaked by Edward Snowden, there were more than 200 offensive cyber operations mounted by the NSA against other countries in that same year. These offensive operations are typically conducted in support of the military, or to steal or distort data. Stuxnet is fundamentally different in that it involved a digital attack as a substitution for conventional weapons.

CLOSING LOOPHOLES IN INTERNATIONAL LAW

States are reluctant to develop international laws and norms to govern cyberspace. It is not yet clear to what degree a cyberattack may be classified as an act of war, but how we are to govern war waged in the cyber domain is already being considered by participants of the 'Five Eyes' treaty group and others. The notion of cyberwar has called into question whether international law for armed attack should also apply to cyberspace. The Tallinn Manual, drafted by NATO, is a non-binding guide to the application of international law to cyber conflicts. This guide is not yet universally accepted, but it does represent one possible approach to governing cyber attacks at the international level.

If cyber war is integrating into conventional warfare, then, under the 1949 Geneva Conventions on the Law of Armed Conflict, retaliatory action would need to be comparable to the initial attack and not amount to an escalation. This proportionality principle, as understood under existing international law frameworks, also affords greater protection to civilians who are often the source in a cyber attack. One possible solution is the notion of state responsibility for attacks by non-state actors. This notion is based on the idea of due diligence: the state should be obliged to take measures to ensure their territories are not used to the detriment of other states. In the case of cyber, that responsibility

would include ensuring that their territories do not become launching pads for cyber attacks. Experts exploring the idea of extending the sovereignty of the state to the cyber activities originating from within their territory have been met with some reluctance. If states are held accountable for cyber attacks under the notion of due diligence, responsibility may also be attributable to the state when a non-state actor operating from outside the state's territory takes control of cyber infrastructure to attack another state. There are obvious complications associated with a state implementing due diligence in the cyber domain practically, particularly for those states that are more intricately connected and so have more vulnerabilities which may be exploited. It might be argued that traditional laws of war may not actually be applicable or adaptable to cyber warfare. A more appropriate response may be to develop specialised international rules and norms about the consequences for cyber attacks, that is, to adapt the notion of state responsibility for the conduct of cyber attacks from a nation's territory.

ADJUSTING OUR APPROACH TO CYBERSECURITY

State-sponsored cyber attacks are occurring more regularly during times of peace, and offensive cyber operations are more likely to be paired with conventional methods of warfare during conflict. Australia needs to develop strong cyber resilience in response to the increasing threat to industry and government from cyberspace, and in anticipation of the threats that are yet to emerge. Australia has gone on the offensive with relation to cybercriminals and there have been calls from Cyber Security experts for a cyber militia to protect Australian corporations and critical infrastructure. A more coherent national response needs to be developed, and that will be achieved by building a more resilient cyber security policy apparatus. Promising steps, such as the establishment of the Australian Cyber Security Centre, have been made. We have also begun to focus on a global response through the appointment of a Cyber Ambassador, who will lead Australia's efforts in cyber affairs and develop international cyber engagement. Despite these developments, Australian companies do not yet have the confidence they need and the government is not yet adequately equipped to handle the threats we face.

The secrecy that frequently surrounds cyber attacks impedes our ability to effectively detect and defend against current threats. Cyber threats are constantly evolving, with adversaries rapidly improving their tradecraft and exposing new vulnerabilities. In a TED Talk filmed in late-2016, IBM's security expert, Caleb Barlow, likens cyber attacks to health epidemics such as Ebola. If governments, security companies and private institutions respond openly and collectively, Caleb argues, it may be possible to stop the 'disease' in its tracks. The information about one attack could then be utilised by another potential target to defend against similar attacks. If Australia and its allies achieve this

collective action at speed, we may keep pace with our adversaries. If industry, government and academia work together and develop a system where information is shared quickly and efficiently, we may be able to defend against known and future threats in the cyber domain. This system would entail greater collaboration between all bodies involved in cyber security, internationally standardised approaches, and transparency and information sharing throughout the public and private sectors.

Cyber security is a reactionary process, whereby security is developed around existing detected threats. This process means that if the information about an attack is not shared quickly and comprehensively, the chance to defend against similar attacks is weakened. Attackers will be likely to remain one step ahead. Australia will not eliminate the cyber threat, but a strong cyber resilience will limit the impact of cyber attacks and prepare Australia for the next security challenge – cyber weapons.