SPECIAL REPORT

ASPI

April 2012 — Issue 46

ANZUS 2.0

Cybersecurity and Australia–US relations

Papers by Andrew Davies, James Lewis, Jessica Herrera-Flanigan and James Mulvenon. Lydia Khalil, Visiting Fellow in ASPI's National Security Program prepared the introduction and conclusion.

Introduction

At the 15 September 2011 AUSMIN talks in San Francisco, Australian and US officials took advantage of the 60th anniversary of the signing of the ANZUS Treaty to announce the alliance would now extend into cyberspace. It was the first time, outside of NATO, that two allies had formalised their joint cooperation in cyberspace.

The then Foreign Minister Kevin Rudd, Defence Minister Stephen Smith and their US counterparts, Secretary of State Hillary Clinton and Secretary of Defense Leon Panetta, issued a joint statement outlining this transformation of the alliance:

> Mindful of our longstanding defense relationship and the 1951 Security Treaty between Australia, New Zealand, and the United States of America (ANZUS Treaty), our Governments share the view that, in the event of a cyber attack that threatens the territorial integrity, political independence or security of either of our nations, Australia and the United States would consult together and determine appropriate options to address the threat.

This is a critically important evolution of the ANZUS alliance. As more and more of our lives are carried out on computer networks, it makes sense that the potential for future conflict and maintenance of national security would also be within the cyber domain and that the ANZUS treaty could be invoked in that context.

Yet the joint statement raised more questions than it answered. What exactly are 'mutual threats and challenges' in cyberspace? What type of cyberattack would qualify as one that would 'threaten the territorial integrity, political independence or security' of either nation? Do Australia and the US view these threats differently? What type of collaborative military response would be appropriate, given the difficulties of attribution in the cyber domain? How do the respective governments define a cyberattack? What are the international cyber-norms that both countries will promote?

In an effort to explore some of these issues, ASPI convened a conference of Australian and American experts on 9 December 2011 in Washington DC. We brought together a panel of experts from the defence, academic and scientific fields to discuss what this means for the future of conflict and defence in cyberspace and how allies perceive and respond to mutual threats.

In this *Special Report* we've compiled papers from Dr Andrew Davies, Director of ASPI's Operations and Capability Program; Dr James Lewis, Director and Senior Fellow, Technology

and Public Policy Program at the Center for Strategic and International Studies; Jessica Herrera-Flanigan, a former federal prosecutor and congressional adviser now working for the Monument Policy Group; and Dr James Mulvenon, a specialist on the Chinese military and cyberwarfare who is the Vice-President of Defense Group Inc.

Two papers in the report deal with the Australian and US perceptions of the cyberthreat, written by Andrew Davies and James Lewis. Two others deal with legal and military responses. Jessica Herrera-Flanigan writes of the legal and normative issues both countries must pay attention to and promote in cyberspace. James Mulvenon articulates how Australia and the US can respond as allies.

In assessing the US and Australian perceptions of the cyberthreat, it's useful to highlight some of the similarities and differences. Both countries see threats emanating from a wide variety of actors, from nation-states to hackers, and in many forms, from cyberespionage to potential attacks on critical infrastructure. Both countries struggle with how to define such threats and order their severity, but cyberwarfare or cyberattack in pursuit of or within the confines of traditional war is seen as the highest order threat, more so than cyberespionage and cybercrime. This is despite the fact that the latter two types of activity are currently the largest breaches in cybersecurity. Lewis makes the point that cyberespionage, particularly by China, is the most immediate current threat facing the US. However, it's unlikely that even high order cyberespionage would be enough to trigger the ANZUS alliance.

Davies's conclusion, that 'it's hard to come up with credible scenarios that put cyberattacks into the same league as threats to territory or national security as it's traditionally been understood', stands in some contrast to Lewis's assertion that many nations have adapted cybercapabilities into their military and intelligence portfolios and that cyberactions must be reviewed within the framework of an 'escalation matrix'.

But there's also agreement that very few states are currently capable of creating physical damage or serious disruption through cyberattack. Many of those nations are deterred from launching frivolous cyberattacks and are unlikely to use cyberattack techniques outside of a 'regular' armed conflict.

In responding to cyberthreats, it's equally important to acknowledge the legal and normative issues permeating cyberspace. Differences in domestic legal systems can hinder cooperative responses, and an agreement on international norms needs to be negotiated so that both countries can promote common interests effectively within the international system.

It's equally important to note, as Herrera-Flanigan points to in her paper, that the effort of the US and its allies to define cybersecurity and norms in cyberspace stands in contrast to the efforts of China and Russia to put forward their own competing paradigm. As she states, 'underlying any global effort to put together legal norms for cybersecurity is an inherent conflict between promoting internet liberty and assuring internet sovereignty.' Although the US seeks to promote an internet freedom agenda, capacity building and security in economic transactions, Russia and China define cybersecurity as the control of content, communication and interaction in cyberspace so that they don't undermine domestic governance and political stability.

This makes it even more critical for those countries with shared values and perceptions of cybersecurity threats to develop common strategies and policies for addressing those

threats. That's why, as Mulvenon points out, 'we should first align and normalise cybercooperation among ourselves before pursuing the more difficult challenge of cyberdialogue with adversary states.'

It is hoped that this compilation will contribute to what will be a continuing dialogue between allies as they navigate the difficulties and opportunities of operating in cyberspace.

An Australian perspective on ANZUS and cyberthreats

Andrew Davies

Last year produced one of the more intriguing announcements to have come from an Australia–US ministerial meeting. Along with the usual restatements of the importance of ANZUS, the security treaty between Australia, New Zealand and the US, and the enduring alignment of both countries' interests, there was—for the first time—a joint statement on cyberspace.

Some of it was entirely uncontroversial—that Australia and the US seek a 'secure, resilient and trusted cyber space that ensures reliable access for all nations' isn't exactly a surprise. But the statement continued with an agreement on cybersecurity that linked it explicitly (if not formally) to the ANZUS Treaty:

> Mindful of our longstanding defense relationship and the 1951 Security Treaty between Australia, New Zealand, and the United States of America (ANZUS Treaty), our Governments share the view that, in the event of a cyber attack that threatens the territorial integrity, political independence or security of either of our nations, Australia and the United States would consult together and determine appropriate options to address the threat.[1]

Although the communiqué stopped short of formally tying cybersecurity to ANZUS, Australian Defence Minister Stephen Smith did so when he said that a substantial cyberattack on Australia or the US could cause the ANZUS Treaty to be triggered.[2]

These statements extend the notion of attack into cyberspace, but the practical implications aren't clear. The aim of this paper is to examine the issues that will come up when governments try to establish realistic policy settings to operationalise the joint statement.

ANZUS

The ANZUS Treaty was formulated in 1951 with the aim of securing the Pacific region, at a time when the events of World War II were uppermost in strategic thinking. Australia was especially concerned about the possibility of a resurgent Japan and was seeking reassurance that the US would again come to its assistance should that occur.[3] In that context, the treaty is understood as a device intended to deal with state-on-state conflict.

For the purpose of scrutinising the joint statement on cybersecurity, the most important clauses of the ANZUS Treaty are Articles III, IV and V:[4]

> Article III: The Parties will consult together whenever in the opinion of any of them the territorial integrity, political independence or security of any of the Parties is threatened in the Pacific.
>
> Article IV: Each Party recognizes that an armed attack in the Pacific Area on any of the Parties would be dangerous to its own peace and safety and declares that it would act to meet the common danger in accordance with its constitutional processes ...
>
> Article V: For the purpose of Article IV, an armed attack on any of the Parties is deemed to include an armed attack on

> the metropolitan territory of any of the Parties, or on the island territories under its jurisdiction in the Pacific or on its armed forces, public vessels or aircraft in the Pacific.

The treaty clearly distinguishes between threats to security and armed attack. The onus on the signatories is to consult when faced with a threat and to 'act to meet the common danger' in the event of an attack. Interestingly, the language used to draft the joint statement echoes Article III (threats to security) rather than Articles IV and V (armed attack). The possible reasons for that distinction are explored below.

Who, where, what?

One difficulty in applying the ANZUS formulation to the cyberworld is that there's a much finer continuum of activities that could be construed as an attack in cyberspace than there is in the realm of armed conflict. The first task is to decide what constitutes an attack. Even that isn't straightforward. 'Cyberattack' is a compact phrase, but it actually contains a multitude of possibilities. In fact, one of the problems with the broad topic of cybersecurity is that there isn't a shared understanding of the various terms that are used.

Lumping everything under the single heading of 'cybersecurity' makes the domain simultaneously seem more homogeneous than it actually is and intractably large. Ideas that are in practice quite disparate are conflated and, as a result, policy prescriptions are too general to be useful. In this environment, it's not surprising that the joint statement is a little vague. But when cyberattacks are elevated to the level of ANZUS, it's especially important to understand precisely what's meant.

Both the potential targets and the possible perpetrators of cyberattacks constitute broad spectrums. Figure 1 shows the possible range of targets of illicit cyberactivity, arranged in increasing order of centrality to the nation-state. At the left there are end users and service providers in the community and general business sectors. At the other extreme there are systems that form part of the state's national security apparatus.

As well, cyberattacks can vary enormously in impact. At the lower end (in terms of national security) there's nuisance or criminal activity against individuals or businesses, perpetrated by other individuals or criminals. At the higher end, there are state-backed activities against government systems. Even within those categories there are important distinctions to be made. For example, espionage in the form of efforts to obtain sensitive or classified information falls into a different category from attacks on military systems designed to degrade or disable them.

Defence Minister Smith explained that the thinking behind the recent announcement was very much focused on the latter:

> ...we're talking here at a level which is much higher than for example people using the internet, using cyberspace to steal commercial or state secrets. We're talking about a significant attack upon the communications fabric of a nation ... In particular, to thwart the communications system of the military—the national security apparatus, the national security arrangements of a country.

That's a helpful clarification, but some questions remain—for example, does this formulation apply when the perpetrators are non-state actors? Or would a state-sponsored attack on civilian infrastructure—electricity supplies or air traffic control, for example—fall outside the new ANZUS rubric?

Figure 1: The potential targets of cyberattack

It's also not entirely clear how the severity of an attack would be measured. For example, would a half-hour outage of a national air defence system caused by an external actor constitute a 'significant attack', or would it need to be accompanied by other hostile activity? In practice, it would depend on the details of the attack and the broader context in which they arise—loss of life, or threats to lives, would likely be an important factor.

Non-state cyber actors

The post-9/11 'global war on terror' provided a precedent for non-state actors becoming the subject of a response under the ANZUS framework when Prime Minister Howard invoked the treaty immediately after the attacks in New York and Washington. That invocation recognised the application of ANZUS beyond the Pacific region in the case of an armed attack on the metropolitan territory of either party. Cyberattacks are perhaps less clear cut. For example, American military networks can have nodes anywhere US forces are deployed, and the attacks can be routed through terrestrial, undersea or space-based communications systems. It's possible that for ANZUS purposes the consideration would be the location of the most dramatic effects of the attack—although even that could be widely dispersed.

The 9/11 precedent was evoked by the Defence Minister at the time of the announcement of the new arrangements:

> ... a substantial cyber attack can open up the prospect of invoking or triggering the ANZUS Alliance ... just as we did for example in the triggering of the ANZUS Alliance after September 11 ...

There are practical difficulties here. In the case of state-on-state activity, in which military or government systems are used to launch a cyberattack on the systems of another military or government, it's fairly straightforward—a response, either 'in kind' or by some other means, could be appropriate. But if the attack comes from a non-state source or is vectored through the systems of an actor not directly involved, probably involving civilian communications infrastructure, the appropriate response isn't so clear-cut. As with conventional armed force, both the potential for collateral damage and the rules of armed conflict would need to be considered carefully.

The public discussion of the Pentagon's first cyberstrategy began in May 2011. That document includes the statement that 'certain aggressive acts in cyberspace' coming from another country might justify the invocation of the right to self-defence under the UN Charter—a view that would allow a traditional military response if the US judged it to be 'equivalent' to a traditional military attack. Of course, that's entirely consistent with the inclusion of cyberattacks within the ANZUS framework, but it's not very clear how 'equivalence' is defined. A cyberattack would probably have to cause death or destruction to be used as justification for a 'kinetic' response with high explosives or other weapons.

And there's a question about what constitutes 'war' when one of the parties is not a state. Because the threshold for entry into cyberactivity is much lower than for other 'traditional' military capabilities, civilians with nationalist or other motives, either alone or collectively, could participate in cyberattacks against national security systems. Adversary states could take advantage of the 'greyness' of cyberspace and could establish 'cyber Hezbollahs'—groups that are state sponsored but which operate outside of traditional military or government structures. Figure 2 shows the spectrum of potential players in cyberspace, arranged by degrees of organisation or state control.

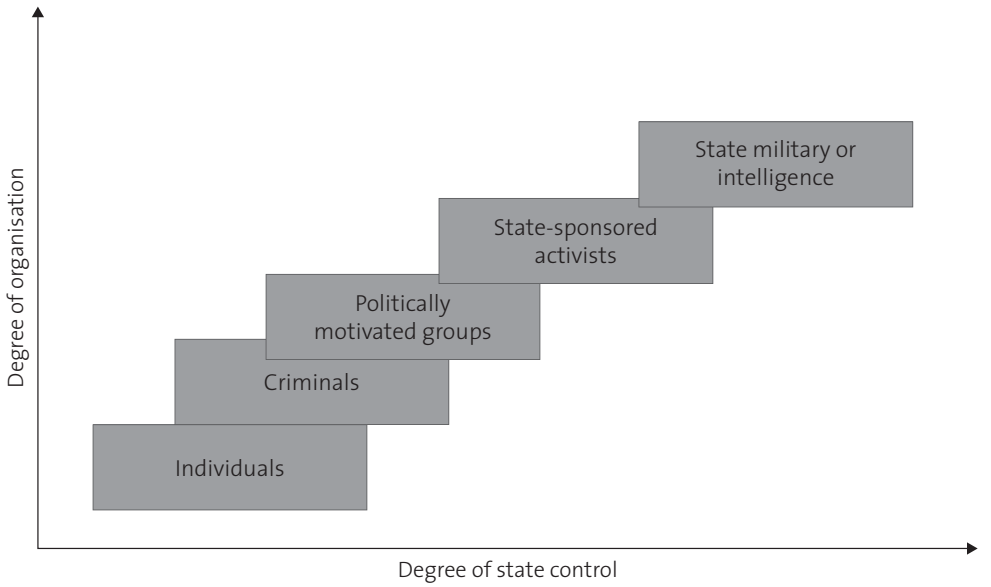
Cyberspace and war

States use cyberspace for a variety of purposes, including communications, conducting espionage or as a command and control channel for their military forces. In that sense, it's like the electromagnetic spectrum—a medium that's used to enable other activities. In that respect, cyberwarfare might prove to be primarily a 21st century extension of electronic warfare.

Electronic warfare is a technical discipline used to attack electronic systems to disrupt the ability of an adversary to accurately gather information, target its weapon systems or communicate. It isn't an end in itself and is typically used as an adjunct to operations that deliver kinetic effects. By reducing the effectiveness of an adversary's systems, it allows military and civilian targets to be attacked with greater effectiveness and lower risk.

There's already some evidence that yesterday's electronic warfare is morphing into today's cyberwarfare. There are striking similarities between the operational approaches of the Soviet forces that intervened in Czechoslovakia's 'Prague spring' uprising in 1968 and those used in the 2008 Russian intervention in South Ossetia, Georgia. A US Defense Intelligence Agency study into the former noted 'the Soviet Army's extensive use of electronic warfare

Figure 2: The potential originators of illicit cyberactivity



and jamming during the invasion',[5] which was used to degrade the Czechs' capability to coordinate their response or to communicate what was happening to the wider population.

The 2008 conflict in South Ossetia has been described as being 'among the first cases in which an international political and military conflict was accompanied, or even preceded, by a coordinated cyber offensive'.[6] The Russians used cyberattacks to disrupt Georgian command and control networks (as well as the general civil internet infrastructure) while bringing their conventional forces to bear. And—reinforcing the point made in the previous section—Russian civilians were simultaneously active against Georgian government and media systems.

In both instances, the efforts to interrupt communications and disrupt sensors were coordinated with a physical invasion. Synchronising operations on the ground with electronic warfare or cyberoperations is important because dominance in either domain is likely to be temporary. In fact, that may be truer of cyberwar than electronic warfare. Even a successful attack on a computer system is likely to have its effectiveness measured in hours. If the underlying infrastructure is intact, machines can be rebooted or communications rerouted. Redundancies abound in military systems, and workarounds would almost certainly return a level of functionality sooner rather than later.

A concerted attack on core military and government command and control systems would necessarily demonstrate the attacker's methods and access points, which are both perishable commodities in a rapidly moving field. The attacker would only give up the 'crown jewels' if there were larger stakes than just making a point in cyberspace. There are symbolic and much less revealing ways of doing that—defacing a defence department or other government website, for example.

Used as an enabler, however, a cyberattack could cause the temporary degradation of other capabilities that rely on the target computers, temporarily reducing the situational knowledge and effectiveness of a military force and rendering it more vulnerable to attack. Of course, taking down a computer network for an extended period is possible if the underlying infrastructure is itself subject to physical attack—the cyberequivalent of physically attacking a radar system rather than temporarily disabling it by electronic warfare means.[7]

But in these instances, where a cyberattack on military infrastructure is part of a wider action, whether or not the ANZUS Treaty applies to the cyberattack is largely moot. The other component(s) of the attack would cause ANZUS to be invoked in any case, either under Article III (threat to security) or Articles IV and V (armed attack).

Politics by other means

However, no military action is an end in itself—as Clausewitz observed, it's just a tool to secure a political goal. The most dramatic example of a cyberattack against a sovereign state (which wasn't accompanied by physical activity) was the assault on Estonian systems in 2007, which is believed to have been a Russian state-sanctioned attack. At the time, Russia was engaged in a series of disputes with Estonia over trade and security issues and the status of a large enclave of Russian speakers in Estonia—hence the cyberassault fits Clausewitz's definition. Over the course of several weeks, Estonian systems were seriously disrupted. Eventually, ways to blunt the effectiveness of the attacks were found and the 'e-siege' was lifted, but the disruption to Estonian society and the country's economy was significant.

This was an extension into cyberspace of coercion that stops short of armed attack. In the physical world, methods such as blockades, embargoes and sanctions—or the threat of any of those—can be used in an attempt to secure a political goal. Threats to a nation's economic wellbeing can be used as leverage without threatening territorial sovereignty. Given the importance of computer systems to commerce and finance today, it's a natural evolution for cyberattacks to be used in this way.[8]

However, it's not so easy to do in practice. Timescales work against cyberattack used this way. Blockades, sanctions and embargoes need to have a cumulative effect, and take time to grind down the will of the targeted party. But, for all of the reasons discussed in the previous section, cyberdominance would tend to be ephemeral. Even Estonia, a country of just 1.4 million people, managed to thwart Russian efforts in the space of a few weeks.

Interfering with the operation of the financial markets in a major economy that's better resourced than Estonia could cause significant disruption, and could leave 'ripples' of lost confidence for some time afterwards. But system redundancy and the measures in place to back up data, and the identification and mitigation of the techniques used, would probably reduce the ability of cyberattack to extract significant political concessions. The 9/11 attacks—about as dramatic an impact as possible—shut down the New York Stock Exchange for only four trading days.

The bit made flesh

One other possibility is that a cyberattack could be used to trigger an event in the physical world. Again, there's a precedent for this. The *Stuxnet* computer worm that was used to attack Iranian nuclear facilities targeted the software that controlled the banks of centrifuges used to separate uranium, throwing them into a state that caused widespread mechanical failure.

The development of *Stuxnet* was almost certainly a state-sponsored activity and probably had years of sophisticated software engineering effort behind it, but the program code is now available on the internet, and modifications of the basic idea are starting to appear. Since similar controllers are used in many other industrial applications, including the control of civilian infrastructure, the possibility of a *Stuxnet*-type attack on other targets in the future seems plausible.

During the media discussion of the shift in American thinking on cyberwarfare, an unnamed US official was reported to have said rather colourfully, 'if you shut down our power grid, maybe we will put a missile down one of your smokestacks.' In fact, that example shows how hard it will be to make a case for a military response that doesn't seem disproportionate. There's no doubt that when the power grid goes down in a major city, it's a significant disruption and hazard—the city grinds to a gridlocked halt, airports stop operating, accidents occur and people can be injured or even killed—but it doesn't take a cyberattack to do that. For example, a 40°C day is quite capable of bringing down the power grid in Washington DC, as has been proved in at least the last three summers. New York City and large areas of California have also experienced well-publicised partial or complete blackouts due to failures of the system to cope with loads.

However, civilian infrastructure is generally pretty resilient. Most cities have contingency plans in place to handle power outages, and vital services typically have backup power supplies. Other utilities, such as water suppliers (another target sometimes cited in warnings about the dangers of cyberattack), have override systems that would render any online attack temporary.

For all of those reasons, it's hard to see why such an attack would hold much appeal for a would-be attacker unless it were part of some wider operation.

The Czechoslovakia and South Ossetia experiences again suggest what might be done. Bringing power grids down or causing some other major disruption to civil or military infrastructure at the same time as other operations would make the job of military, domestic security and civil response agencies much harder, and it might amplify the psychological effect on the general populace.

In the case of the US or Australia, a plausible scenario is an attack on domestic infrastructure that's coincident with a terrorist attack (or military operations elsewhere), with the aim of complicating the government's response. But in either case, the response of the ANZUS allies would necessarily be to the attack in its entirety, not just the cyberattack. And the type of response would be tailored to the overall situation—a missile down a smokestack might be a response to an attack that involves a cyber component, rather than to an isolated cyber incident.

Conclusion

The practical significance of the AUSMIN joint statement on cyberattacks isn't entirely clear. The threshold that Australian officials have described for invoking the ANZUS Treaty is so high that, for a variety of reasons, it's hard to see the eventuality arising as a stand-alone incident.

It's sometimes argued that the ubiquity of cybersystems makes the new threat spectrum uniquely dangerous. That view is hard to sustain—the electromagnetic spectrum has been central to communications and military systems for at least half a century, but there's no joint statement on electromagnetic security that elevates it to the level of a treaty.

At the bottom line, it's hard to come up with credible scenarios that put cyberattacks into the same league as threats to territory or national security as it's traditionally been understood—which is the underpinning of the ANZUS Treaty.

Of course, it might be that the aim of the recent announcement wasn't to produce a practical operational doctrine, but instead to send a message about what's regarded as acceptable behaviour in cyberspace. In the case of the previous NATO agreement, the intended recipient was probably Russia, with the message being that hostile cyberactivity, such as that against Estonia, will be regarded as an act of aggression. In the Georgian case there was no ambiguity—cyberattacks were accompanied by physical acts of war.

In fact, those two instances provide a likely explanation of the echoing of Article III in the ANZUS announcement rather than Article IV or V. The Estonia attacks were a threat to security and thus look more like an Article III incident, whereas Georgia clearly comes under Articles IV and V.

In the ANZUS case, the intended recipient of any intended message is presumably China, and the message is that cyberattacks, while perhaps falling short of the seriousness of armed attack, are unacceptable and may attract a serious response.

Notes

1 Joint Statement on Cyberspace, Australian Minister for Foreign Affairs, 15 September 2011, available from http://www.foreignminister.gov.au/releases/2011/kr_mr_110916a.html.

2 Minister for Defence, interview on SKY News, 15 September 2011, available from http://www.minister.defence.gov.au/2011/09/15/minister-for-defence-interview-with-david-speers-on-sky-news-pm-agenda/.

3 While a second war against Japan seems unlikely with the benefit of hindsight, there's little doubt that the post-WWI experience of a resurgent Germany drove much of the allied planning for the post-WWII period. See, for example, Ernest R May, *'Lessons' of the past: the use and misuse of history in American foreign policy*, Oxford University Press, 1973.

4 The full text of the treaty is available at http://www.austlii.edu.au/au/other/dfat/treaties/1952/2.html.

5 US Defense Intelligence Agency, *Soviet electronic countermeasures during invasion of Czechoslovakia*, DIA Intelligence Supplement UP-275-68.

6 Cooperative Cyber Defence Centre of Excellence, *Cyber attacks against Georgia*, Tallin, Estonia.

7 In electronic warfare, these approaches are called 'suppression of enemy air defence' (SEAD) and 'destruction of enemy air defence' (DEAD). While there is no equivalent nomenclature in the public discussion of cyberwarfare, the acronym-rich environment within the Pentagon is sure to rectify that situation.

8 International law may have some catching up to do here. For example, a blockade is viewed as an act of war not because of its economic and social impact, but because of the physical presence of warships or other instruments of state power. There is no direct analogue in cybercoercion.

US perceptions of cyberthreats

James Lewis

An accurate assessment of threats in cyberspace is essential for effective policy. It's important to distinguish between the use of force through cyberspace and ongoing malicious activities. Early assessments focused too much on the potential for harm and the 'homeland security' aspect of the cybersecurity problem, to the detriment of policymaking.

We're now in a position (using available public data) to identify the current threats in cyberspace and predict what future threats will look like, although there are major areas of ambiguity—the role of proxies, the effect of the illicit acquisition of technology and the strategic implications of cyberespionage. We need to make an important initial distinction among the various kinds of malicious cyberactivity:

- There's the potential use of cyberattack for military purposes, but at the moment only a few nations have that capability and they're unlikely to use it outside of armed conflict. Non-state actors at this time don't have the most advanced and damaging cybercapabilities.
- There are threats to public safety (in the sense that private citizens and companies are at risk of financial harm), but that risk, like traditional criminal activity, doesn't aggregate into a threat to state survival and independence. By itself it isn't a threat to national security.
- There's long-term risk from espionage conducted against computer networks through ongoing technical collection programs that damage national economies and economic competitiveness. This may pose a long-term threat to national security, but

> in the near term neither national survival nor the independence of the state is at risk.

There's a question of aggregation—whether at some point the level of crime and espionage in cyberspace or the cumulative effect becomes a threat to national security. The questions of aggregation and cumulative effect are areas of ambiguity. Clearly, if the amount of cybercrime reaches a point at which legitimate online activity is greatly curtailed (and we're not at that point), that's a risk to nations. The cumulative effect of cyberespionage is harder to assess, as many other factors will shape the risk to national security—the growth and innovative capabilities of the victim country, the ability of the acquirer to use the technology, the global rate of technological change (if a design is 10 years out of date by the time it's introduced, the effect may be minimal).

In looking at these categories of threat—attack, crime and espionage—we can say that it's the ability of foreign national state opponents to exploit networks at will that poses an immediate national security risk. That they choose now only to steal information doesn't mean that they lack the capability to do more, to undertake actions that create immediate disruption and pose immediate risks to the state.

The principal source of threats to national security is other nation-states. There's some blurring of threats from crime and threats to national security because of the role that private actors, such as cybercriminals and hackers, play as proxy forces. Malicious actions in cyberspace provide nation-states with a new capacity to degrade opponents. The means for doing this involve gaining informational advantage—a traditional function of espionage—that provides deeper insight into opponents' intentions and capabilities, access to their technology, and new ways to coerce or damage them. Those capabilities are, in some degree, also available to private actors, and the lack of norms and law enforcement cooperation means that for a few countries, hacking into a business competitors' networks has become a normal business practice that's tolerated if not encouraged by the government.

One way to test the centrality of the threat from nation-states is to ask what would happen to cybersecurity if states ceased engaging in malicious actions. Were that to happen, most of the risk of coercion or attack and much of the damage from espionage and crime would be eliminated. In addition, if states no longer tolerated the activities of private hackers and cybercriminals and were willing to investigate and prosecute them, there would be a significant reduction in crime. It's the current monopoly of states over advanced cybercapabilities and their use of private actors as proxy forces that create most of the national security threat in cyberspace.

The reach of the black markets

That will eventually change as private actors not affiliated with states acquire advanced cyberattack capabilities. This is inevitable. Cybercriminals make extensive use of virtual black markets, which offer a range of attack and penetration capabilities, including information on vulnerabilities, personal information for use in phishing attacks, an ability to rent botnets[1], and malicious code for penetrating networks. The most advanced capabilities aren't yet available in these markets because either they must be supplemented with intelligence information from other sources (such as human agents or other kinds of technical collection) or they require advanced engineering knowledge to understand the dependencies of critical infrastructures and software. The general trend, however, is that these disruptive

technologies become 'commoditised' and available for purchase. What we don't know is whether these black markets would shrivel if states were to reduce their support for malicious cyberattack capabilities or whether they could continue to grow.

Non-state actors, whether they are *jihadis* or politically motivated groups like Anonymous, don't yet have such capabilities. If al-Qaeda or some other jihadist group had cyberattack capabilities, why would they wait to use them? We've never seen a terrorist use of cyberattack (as opposed to terrorist use of the internet). Similarly, the activities of groups like Anonymous, while annoying, pose little risk. A 'denial of service' attack is threatening only when it's linked to some larger coercive threat, as was the case in Estonia. We don't know the rate of improvement in non-state actor capabilities, but for the moment the threat from them is limited.

The identification of states as the primary source of malicious activity in cyberspace focuses the task of defence. Instead of an amorphous, anonymous threat, we now have a known set of opponents whose motives are already known or can be understood (even if their capabilities remain somewhat opaque). A nation developing its cyberdefence strategy can begin by asking who are its likely opponents and which countries engage in malicious actions (such as espionage) against it, and then look for evidence that this malicious activity has been translated into cyberspace. Those countries that pose a military threat probably also pose a threat in cyberspace. Those that engage in conventional espionage are likely also to be engaged in cyberspying. Once we've translated the cyberthreat into the traditional realm of national security, both risks and solutions become easier to identify.

The surprising element is how quickly so many nations have adapted cyberaction into their military and intelligence portfolios. The usual comparison is with aeroplanes—a rickety toy in 1913 and a crucial tool of war five years later. While perhaps only five or six countries currently have high-end cybercapabilities, more than 30 countries are developing military doctrine for cyberwarfare that includes examining how to incorporate cyberattack into offensive operations. An even larger number of nations engage in cyberespionage, both because the cost of entry is relatively low and because they can build on existing capabilities for monitoring domestic communications (a practice that almost every nation in the world engages in, subject to different national laws).

The use of cyberspace for military or attack purposes by (an expanding number of) opponent forces or, eventually, by non-state actors would involve three sets of actions. First, as we've seen in Estonia and Georgia, malicious cyberactivity provides a new tool of political coercion, to threaten and put pressure on an opposing state. This can involve denial of service attacks, website defacements or the spread of harmful information. It's likely that Russian doctrine for cyberwarfare puts a heavy emphasis on coercive political actions in the event of conflict. However, using international law as a guide, these should not be considered attacks, as they don't involve the use of force.

The struggle for informational advantage

Many militaries are exploring cybercapabilities that would degrade an opponent's 'informational advantage'. In the 1980s, the US began to develop concepts and doctrine that emphasised using intangible, informational and decisional tools to gain military advantage. The early lesson was that networked forces would outperform non-networked forces. The 1991 Gulf War was

an early demonstration of the informational advantages of combining combatants, sensors and weapons using space and network assets. Perhaps the greatest benefit comes from the reduction of uncertainty for military commanders, allowing them to make decisions faster and more effectively: networks reduce the fog of war. Therefore, informational advantage has become a logical target for opponents, who will seek to disrupt networks, damage or destroy data and create crippling uncertainty among opponent commanders. Chinese military doctrine probably combines electronic warfare, attacks on space assets and cyberattack as a means to degrade informational advantage (and other nations, while not as advanced or as capable, are likely to have similar doctrine).

Finally, there's a demonstrated capacity to do physical damage using software commands transmitted over networks. Public knowledge of this capability grew after the 2007 *Aurora* tests at Idaho National Labs demonstrated that a sequence of commands aimed at control systems could lead machines to self-destruct. *Stuxnet*, a complex cyberattack against an Iranian nuclear facility, was another public example of this destructive capability. There's been some public discussion by US officials of how potential US opponents have conducted cyberreconnaissance against critical US infrastructure in order to be able to launch destructive attacks if necessary. The strategic implications of that reconnaissance are not much different from those of a satellite passing overhead for nuclear targeting purposes, although space flight over national territories is lawful while cyberreconnaissance involves unlawful intrusion into opponent networks. As with satellite imagery, updating the target set is essential, and the update frequency required for maintaining an attack capability is probably greater for cybertechniques.

Escalation and retaliation

There's an implicit escalatory ladder from political coercion to physical destruction, and the use of cyberattacks by opponent militaries will probably depend on political–military judgements about the need for and benefits of escalation. Escalation is also determined by the nature and location of the target, ranging from deployed military forces in the combat zone to civilian targets in the opponent's homeland. We can think of an escalatory matrix of techniques and targets that allows an opponent to shape doctrine and strategy for cyberattack.

For the US, this means that the primary source of risk in cyberspace comes from Russia and China, both of which possess first-class capabilities equal to those of the US and its allies. There's a risk of military conflict with both countries (as episodes in Georgia and the China Sea illustrate), and both will use cyberattack should such conflict occur. In some ways, Russia and China have similar motives for engaging in malicious cyberactivity. Both seek to degrade US capabilities—they'd describe this as opposing US hegemony. Both seek to expand their ability to use what's become a critical military capability. Both engage in espionage to determine the intentions, capabilities and plans of the US and its allies. Both use cyberespionage to look for political threats to the regime (such as Tibetan activists). Both nations use proxy or irregular forces. The principal difference, to date, is that the Russian emphasis has been on financial crime, reflecting the close ties between the Russian state and organised crime, while the Chinese emphasis has been on the illicit acquisition of technology to increase China's economic and military strength.

Russia and China have invested heavily in systems to monitor domestic communications. There are no legal

impediments in either nation to the interception of traffic from and between citizens. While the primary purpose of these extensive surveillance systems is regime preservation, it does raise the question of the extent to which private actors can engage in illicit activities in cyberspace for long periods without the knowledge of these governments.

Proxies and protesters

This suggests a degree of state complicity in, or at least tolerance of, malicious cyberactivities carried out by private individuals resident in the two nations' territories, but it's easy to overstate the degree of control. While the Federal Security Service's control over Russian hackers and cybercriminals is probably greater than the Chinese Government's control over its hacking community, in neither case is that control complete. The monitoring systems of both nations are primarily focused on detecting political threats, meaning that criminal activity can evade interdiction to some degree. Both use criminals as proxy forces, but that doesn't mean that criminal activities are all centrally directed. The unspoken arrangement may well be that in exchange for a tolerance of malicious activities directed against foreign targets the hacker community is willing to accept direction from government agencies, may receive support in some instances, and may be required to share some of the proceeds of its malicious activities.

The situation in China is less clear. There are long-running national collection programs, usually using proxies. There are individual efforts by individual agencies that mightn't be centrally coordinated. There are actions by Chinese citizens and companies that are independent of any central control. The situation resembles traffic in Beijing—a semblance of order superimposed on a near-chaotic pattern of individual actions. But that there are many malicious Chinese actors in cyberspace, not all of whom are coordinated, shouldn't obscure the central role of the state in preparing for cyberwar, directing economic espionage, supporting proxies, and tolerating malicious behaviour aimed at foreign targets.

There's a degree of paranoia common among authoritarian states with communist backgrounds. Both Russia and China share a fear of the open access to information and the freedom of expression provided by the internet. Their conundrum is that open access is essential for business and research, and it's difficult to segregate the benefits from the political risk such openness poses for undemocratic regimes. Reacting to the use of social networks in Tunisia and Egypt, Russian President Dmitry Medvedev reportedly said, 'Let's face the truth. They have been preparing such a scenario for us, and now they will try even harder to implement it.' The belief that Western nations are wielding an 'information weapon' to destabilise other nations undergirds much Russian and Chinese thinking about cybersecurity—to the point where they assert that it's more accurate to speak of 'information security' and 'information space' than 'cybersecurity' and 'cyberspace'.

This emphasis on information operations is probably an indicator of how Russia (and perhaps China) may apply cybertechniques to warfare. Much of the discussion revolves around cyberweapons as an alternative to kinetic weapons or as a means of disrupting opponent data and information systems. It's also likely that Russia will use cybertechniques for both traditional political ends, seeking to influence opponent and third-party opinion in the event of conflict, and as a tool of coercion to undermine opponent morale.

Financial disruption

Warfare and attack aren't the most immediate threat, however. Nor is cybercrime (if we define it as extracting money from the unwitting) the most pressing risk. Some worry that China or Russia will use cybertechniques to destabilise the Western financial system, but that's unlikely. The Chinese are too heavily invested in Western financial institutions to disrupt them as anything other than an *in extremis*, suicidal action, and the Russians benefit too greatly from financial crime to disrupt a fruitful source of revenue. There's a possibility of an espionage exploit or crime inadvertently triggering some kind of highly damaging event in financial networks, but that wouldn't be intentional. The real and immediate threat comes from cyberespionage aimed at the illicit acquisition of technology and the acquisition of confidential political and business information. The deep insight into Western governments and economies provided by cyberespionage and the acceleration of technological developments will provide a tangible advantage—just as the ULTRA program gave the Allies a tangible military advantage in World War II.

The current dilemma goes well beyond conventional military espionage. Legislative bodies in the US, UK, Australia and Japan have had significant penetrations and data outflow. Financial agencies in Canada and France, along with international financial institutions, have been the target of attacks. Significantly, the penetration of French agencies occurred during the preparations for a crucial G-20 meeting that France was chairing, and much of the preparatory information was exfiltrated. In effect, a nation-state opponent was able to acquire information that could significantly improve its economic strategies and its negotiating positions. Reading your opponent's playbook at will poses serious risks to their national interests.

Cyberespionage provides new opportunities for political manipulation. The most salient example was the release of damaging emails in advance of climate change negotiations. The emails were used to discredit the scientific case for climate change. The first instance occurred before the 2009 Copenhagen conference (involving heads of state). Embarrassingly, a second incident involving the same scientists occurred in 2011 before the Durban conference. A more public but less successful attempt at political manipulation occurred with the release of confidential US diplomatic cables in 2010.

The theft of confidential business information provides immediate benefit. The Australian mining company Rio Tinto was the subject of more than 200 attempts to hack its networks at the time it was renegotiating contracts with Chinese companies.

The greatest threat, because it has the potential to change economic and military power, comes from the illicit acquisition of technology. Opponent weapons systems improve at a faster rate and opponent commercial firms can offer new products without the cost of investing in research and development. There can be a delay of some years in implementing stolen technology, and espionage programs work best when they are part of a larger strategic investment and industrial strategy, but Western nations have probably lost more since the exploits of the KGB's Directorate T and Line X, which focused on stealing technology to close the gap between East and West in the 1970s.

Reassessing cybersecurity

This reassessment of potential threats is important, as it helps focus and drive a transition to a new approach to cybersecurity. The old approach, encapsulated in Presidential Decision Directive 63 of 1998 and the 2003 National Strategy to Secure Cyberspace,

emphasised voluntary action by individual networks, loosely coordinated through a mixture of information sharing processes. The 2003 national strategy, with its emphasis in market solutions, was widely and correctly perceived as inadequate from the moment of its release. PDD-63 was a watershed document that laid out many of the ideas—information sharing, public–private partnerships, critical infrastructure protection—that still shape discussion of cybersecurity, but it and the ideas it put forward are badly outdated and inadequate for the threats nations now face.

Correctly identifying the threat in cyberspace as espionage (both economic and political) calls for different policies and priorities. Creating a computer emergency response team, sharing information for a technical 'point defence' and focusing on critical infrastructure are not an adequate strategy for national defence. The most important change for policy in the US is the recognition that cybersecurity is a national security problem. Espionage, transnational crime and potential military attack are governmental issues that are best dealt with by diplomatic, intelligence, law enforcement and military agencies, particularly if states are the leading threat.

This new approach to cybersecurity faces a number of serious issues that hamper (to varying degrees) the ability of Western democracies to create adequate defences. There's an ongoing debate over the role of government. Businesses fear additional regulation and privacy advocates fear government intrusion. Creating robust public–private partnerships is difficult. Defining the correct role of military forces in deterring cyberattack or defending civilian infrastructure raises constitutional challenges, as democracies don't use their military forces for routine internal security purposes. There's a deep ideological dispute, at least in the US, between cybersecurity advocates and internet pioneers, who argue that cyberspace should be unconstrained (to promote innovation and preserve rights)—a self-governing community led by civil society with little need for government intervention. Finally, cybersecurity is a new problem for international security and requires new diplomatic strategies for defence and trade. In key areas—security, trade, law enforcement—the US has made progress, but these issues complicate and slow the work of building better defences.

This slow pace is itself a source of risk. The future of threats in cyberspace will involve the 'proliferation' of attack capabilities. Currently, only a few states possess advanced attack capabilities able to create physical damage or serious disruption. Those nations are deterred from launching frivolous cyberattacks and are very unlikely to use cyberattack techniques outside of armed conflict. However, when less deterrable states and non-state actors acquire attack capabilities, they won't be as constrained. Risk will expand considerably if nations don't make greater progress in building international understanding to control cyber-risks and in building defensive capabilities at a national level. The likelihood of a damaging attack is now close to zero, but the situation isn't static and could change rapidly without a new, comprehensive approach to cybersecurity.

Note

1 A botnet is a group of compromised computers which are remotely controlled over the internet by an unauthorised user.

Cybersecurity: legal and normative issues

Jessica R Herrera-Flanigan

What is cybersecurity? The question's one that policymakers, companies, governments and individuals continue to ponder. Even the use of the terms 'cybersecurity' and 'cyberattack' raises questions about whether the underlying issue is an economic or defence issue. Interestingly, in the early years of global cybersecurity efforts, the struggle was one of commerce/economics versus law enforcement efforts on cybercrime. Only in recent years has the debate shifted to economic security versus national security. Even within the latter category, in the US there's a question about whether cybersecurity should be treated as a matter of homeland security and resiliency or as one of national defence and military capability.

The quest to define cybersecurity mirrors the struggle for global dominance. On one side, the US and its allies have agreed that cybersecurity is about creating, as US Secretary of State Hillary Clinton has stated, an 'interoperable, secure and reliable information and communications infrastructure that supports international trade and commerce, strengthens international security, and fosters free expression and innovation'.[1] Under such an approach, protecting systems against damage and compromise and assuring reliability is coupled with promoting intellectual property protections, human rights and privacy.

This approach was largely laid out in the International Strategy to Secure Cyberspace released by the White House in May 2011.[2] In that report, the Obama administration discussed the need to promote cyberspace cooperation, focusing particularly on the norms of behaviour for states and the need for bilateral and multilateral agreement, both in economic forums (the Council of Europe and the Organisation for Economic Co-operation and Development) and in military security organisations (such as NATO). The report also discussed openness and innovation in internet governance; building capacity, security and prosperity on the international level; and international freedom.

Contrasting with the US approach is one advocated by Russia and China, which defines cybersecurity in terms of controlling content, communications and social networking tools in a manner that does not undermine nations' cultural, political, economic and social stability.[3] In September 2011, those two nations, joined by Tajikistan and Uzbekistan, proposed to the United Nations an International Code of Conduct for Information Security that required nations to pledge:

> To cooperate in combating criminal and terrorist activities that use information and communications technologies, including networks, and in curbing the dissemination of information that incites terrorism, secessionism or extremism or undermines other countries' political, economic and social stability, as well as their spiritual and cultural environment ...[4]

Thus, underlying any global effort to put together legal norms for cybersecurity is an inherent conflict between promoting internet liberty and assuring internet sovereignty. The difficulty of resolving this conflict is significant. In many ways, it would be similar to putting an American football team against an Australian football team and telling them to play football. Without new rules and, by default, the creation of a new hybrid game, there would be no consensus on how to move forward. Reaching a consensus on cybersecurity will be one of the most difficult global policy issues facing nations collectively in the coming years.

Even if nations were able to move past the top layer of liberty versus sovereignty in the cybersecurity debate, they face even more significant legal and policy challenges. There are five areas where there are interdependent yet independent factors that must be addressed: national defence norms; criminal laws; standards and technical solutions; trade; and privacy. Layered over those five are intellectual property protections and economic espionage, which straddle criminal and trade efforts, and are incorporated here in discussion about those two efforts.

Cyberwarfare and the national defence

In the defence realm, in addition to the discussions at NATO and the United Nations about how nation-states should address cybersecurity, a number of bilateral efforts have attempted to address how allies will respond to cyberthreats, although the terminology used to describe cooperative efforts is vague and can be interpreted in multiple ways.[5]

For example, the 2011 US–Australia AUSMIN Joint Statement on Cyberspace mirrors Article III of the ANZUS Treaty[6] and appears to treat cyberattacks in the same fashion as a bombing or assault. The challenge, however, is in determining when self-defence is triggered in cyberspace. Unlike a bombing or assault, cyberattacks cross borders and nations, making it difficult to assess whether a nation-state or rogue actor is behind an attack. Quite simply, there's no international consensus on the application of the laws of armed conflict to cyberspace and cyberwarfare. This is due in part to both the definitional and cultural challenges of formulating a uniform global solution to cyberthreats.

Another part of the challenge is in determining whether attacks from within the borders of states should be attributed to those states as a norm. Any attribution would raise third-party sovereignty issues. In addition, increasing terrorist activity against the US and its allies over the past 20 years has changed the nature of war. In place of military-to-military engagements, there have been increasing attacks on civilian targets. If those attacks were to be carried out in cyberspace, intelligence-gathering and assessing the origins of an attacker would be complicated by the lack of traceability, remoteness, and the attackers' ability to hide behind others.

Interestingly, Russia has proposed for a number of years a global 'cyberarms control' approach, similar to actions that nations have taken in the chemical, biological and nuclear areas. The proposal would commit signatories to abstaining from developing offensive cybercapabilities or from engaging in cyberespionage. Unfortunately, verification that a nation is meeting its obligations is almost impossible, and most nations, at this point in the cyberdebate, would not agree to place themselves at a strategic disadvantage. The US has generally opposed the Russian proposals, although last year the Obama administration indicated that it was considering engaging with nations such as Russia on cyber-issues in order to try to establish some baseline rules for engagement.[7]

Cybercrime and procedural laws

When governments first began discussions on cybersecurity, much of the debate focused on cybercrime and the procedural laws that allowed for the enforcement of criminal laws. The most significant work in this area came out of the Council of Europe's 2001 Convention on Cybercrime.[8] The convention addressed both substantive and procedural laws. Substantively, it focused on the 'CIA' of cybercrime—the confidentiality, integrity

and availability of computer systems. It also addressed child pornography and copyright infringement, as defined by the World Trade Organization.

The convention didn't address issues such as hate speech, which was a point of contention between a number of nations and the US. The US couldn't sign on to the convention if hate speech were included because of its constitutional protections of free speech. Other nations, such as Germany, felt that the issue should be included as it was an important tool in their fight against xenophobia. To address all the concerns, an additional protocol to the Convention on Cybercrime was added in 2006, requiring participating nations to criminalise the cyberdissemination of racist and xenophobic materials.[9]

Procedurally, the convention addressed laws relating to the collection of evidence and to powers and procedures for criminal investigations. Among the areas addressed were the preservation of stored data, disclosures of traffic data, search and seizure processes, and transborder access to stored data without mutual assistance.

Australia introduced its cybercrime legislation in the summer of 2011, which, if passed, would allow the nation to ascend to the Council of Europe's Convention on Cybercrime. During debate, significant concern was raised about the privacy protections afforded to citizens. The US ratified the convention in 2006. In total, 17 nations are signatories of the convention but haven't ratified and 29 nations have ratified.

Standards and best practices

A number of ideas on international standards have been proposed by code organisations. The two most significant efforts have happened within the Open Group Trusted Technology Forum and the OECD.[10] The forum is focused on developing a global supply chain integrity program and framework in order to provide buyers of IT products with a choice of accredited technology partners and vendors.

In 2002, the OECD created its *Guidelines for the security of information systems and networks: towards a culture of security*, which consisted of nine principles that were designed to lead to the adoption of best practices for public awareness, education, information sharing and training in the cyber-arena.[11] More than 30 nations participated in the development of the guidelines. It's important to note that the nations that have implemented the guidelines have largely been nations that follow the 'liberty' approach to cybersecurity. They viewed the guidelines as assisting their efforts to promote economic growth, trade and development.

As nations move forward with the development of standards, policymakers must acknowledge the potential impact 'unilateral standards' can have on global cybersecurity efforts. For example, if the US insists on developing its own domestic standards, then other nations such as Russia, Brazil and China may pursue their own standards. The result? A technical Cold War in which nations develop networks that are not interoperable or technologically compatible. Those networks would be based on rules, protocols and practices that fit each nation's values and ethics, leaving us all the further from finding consensus on a global response to cybersecurity.

Trade

Trade's role in cybersecurity is only now becoming more of a force, especially as China's economic dominance grows and increased concerns about intellectual property protections emerge. We can expect the World Trade Organization and the World Intellectual

Property Organization to take more of a lead, especially on the intellectual property front. What remains to be seen, however, is how recent activity in the US to defeat legislative efforts to enforce intellectual property rights through the Stop Online Piracy Act (SOPA) and Protect IP Act (PIPA) will affect those efforts. Grassroots campaigns were successful in getting SOPA/PIPA pulled from consideration. Following that effort, a global movement was started to defeat the Anti-Counterfeiting Trade Agreement (ACTA), a multinational treaty that establishes international standards for intellectual property rights. Protest against ACTA occurred on 11 February 2012, causing a number of European nations to speak out against ACTA or to quietly set aside their implementation of the statute.

Within the trade space, another legal area to watch is how nations may turn to protectionism to further cybersecurity efforts, especially in today's global economy where technology products flow from nation to nation. Call it the 'Huawei problem', but several US policymakers have made it clear that they want stronger protections from imports that come from foreign companies with ties to nations of concern. Huawei is a Chinese telecommunications company with connections to the Chinese People's Liberation Army that was selling technology to Sprint for use in the US telecommunications network, before security concerns resulted in a reversal of the contract. The Australian Government blocked Huawei from work on the National Broadband Network in March 2012 for the same reason. How to balance trade and commerce requirements with the commercial emergence of foreign companies with ties to foreign governments, especially those governments known for their cyberespionage and intellectual property theft, is a question that we can expect much debate and discussion about in the coming years.

Privacy

Privacy is an issue that has developed into its own complicated area, attracting significant attention in many nations, especially those advocating for a cybersecurity liberty approach. As such, it won't be discussed in great detail in this paper. One thing that's worth noting, however, is that 'data breach and notification' laws have proliferated in the US but have done so as a privacy and not a cybersecurity issue. In the US Congress, the staffers who work on privacy are largely not the same staffers trying to address cybersecurity. As privacy becomes more complex through social media, mobile communications and cloud computing, the interconnect between it and cybersecurity will only strengthen and possibly complicate even further any effort to develop a global cybersecurity regime.

Conclusion

In sum, cybersecurity is and will continue to be a struggle to find global legal and normative solutions for a global problem on a global network. It's often said that 'a network is only as strong as its weakest link.' As more nations and applications go online, the need for a layered approach that combines liberty and sovereignty interests will only grow. As that approach is developed, it will have to be technology-neutral. It will also have to define roles according to defence, law enforcement, standards, trade and privacy but recognise that there's overlap and that traditional division lines won't necessarily work.

Notes

1 http://www.state.gov/secretary/rm/2011/05/163523.htm.

2 www.whitehouse.gov%2Fsites%2Fdefault%2Ffiles%2Frss_viewer 2FInternational_Strategy_Cyberspace_Factsheet.pdf.

3 See MSNBC.com, *Chasm widens in East–West 'Cyber Cold War'*, http://www.msnbc.msn.com/id/46254559/ns/technology_and_science-security/t/chasm-widens-east-west-cyber-cold-war/#.T1P0T3kx6So.

4 http://blog.internetgovernance.org/pdf/UN-infosec-code.pdf.

5 http://www.minister.defence.gov.au/files/2011/09/110915-Cyber-Joint.pdf; http://www.state.gov/r/pa/prs/ps/2011/09/172490.htm.

6 http://australianpolitics.com/foreign/anzus/anzus-treaty.shtml.

7 See 'US backs talks on cyber warfare', *Wall Street Journal*, 4 June 2010, http://online.wsj.com/article/SB10001424052748703340904575284964215965730.html.

8 http://conventions.coe.int/treaty/en/treaties/html/185.htm.

9 http://conventions.coe.int/treaty/en/treaties/html/189.htm.

10 http://www.opengroup.org/ottf/.

11 http://www.oecd.org/document/42/0,3746,en_2649_34255_15582250_1_1_1_1,00.html.

Responding to cyberattacks as allies: implications for the ANZUS alliance

James Mulvenon

Since 1952, the ANZUS Treaty has been a foundation for the military and national security relationships between the US and Australia. While the alliance has no integrated defence structure or dedicated forces, the two countries have 'fought side-by-side in every major conflict since the First World War'[1] and continue to maintain extensive ministerial consultations, joint exercises and intelligence sharing.[2] For most of this history, the parties to the ANZUS Treaty were concerned solely with kinetic military conflict, but the rise of cyberconflict necessitates an expansion of the scope of the alliance.

Why do we need cybercooperation?

Strategic cooperation in cyberspace between like-minded state actors such as the US and Australia is now absolutely critical to the national security of both countries. The main drivers are twofold: our collective reliance on cyberspace for an increasing percentage of global trade and commerce, and the corresponding rise of serious threats to what is universally acknowledged to be flawed technical architecture. Even as the world becomes more dependent on cyberspace in every facet of life, the threat environment has become more dire, exacerbated by a desire to prioritise connectivity over security.

The spectrum of cyberthreats ranges widely from lower level threats like defacements to intermediate threats like botnets and malware, and beyond to a new threshold of cyberattacks established by the *Stuxnet* worm.[3] Not only is the spectrum wide, but the potential actors and adversaries are proliferating at the speed of the

network. States and non-state actors, including state-sponsored organisations or proxies, have varying levels of capability and intent, but still comprise a significant level of threat in cyberspace. Increasing dependence on cyberspace across all dimensions of national power (political, economic, military, diplomatic, social) only increases our vulnerability and the potential negative consequences of not adequately understanding the threats.

While *Stuxnet* is considered the new pinnacle of cyberthreats, cyberespionage, not cyberattack or cyberwar, is currently the most pressing risk for the US and its allies in cyberspace. Strategic espionage against political, military and intelligence targets can change the outcome of interstate conflicts and even alter the balance of power, while economic espionage can result in substantial economic losses and can endanger future competitive advantage.[4] Within the espionage realm, 'advanced persistent threat' poses the most significant, sustained challenge to actors in cyberspace.

Another important class of threats against states includes activities designed to deny access to cyber-resources, such as the distributed denial of service (DDoS) attacks against Estonia in 2007, which took down the websites of many Estonian organisations, including the parliament, banks and media following increased tensions with Russia. The Estonian disruption also included defacements and other lower level methods, although the DDoS attacks caused the most significant, sustained damage. While some Russian hackers have taken responsibility for the attacks, no official connection with the Russian Government has been uncovered. The Estonian experience was repeated during the 2008 cyberdisruptions before and during the brief war between Georgia and Russia, including defacement and DDoS attacks against Georgian Government and media websites, again presumably by Russian-backed actors. Taken together, these various classes of cyberthreat present a significant threat to the viability of cyberspace as a usable domain for states, groups or individuals, necessitating a systematic examination of the dynamics of cyberconflict.

In short, the advanced persistent threat problem is global, so the solutions can't be isolated within an individual country. Instead, countries with similar values and institutional structures must band together in a 'coalition of the willing' to develop common strategies, policies, laws, standards and technical approaches. Given the long history of the relationship between Canberra and Washington, it's natural to see the ANZUS Treaty as the foundation of strategic cooperation between Australia and the US.

What cooperation strategies should we pursue?

Before discussing specific strategies, it's important to note a number of structural conditions and constraints that shape the cooperation environment. First, the governments of both countries are keenly aware that key resources for the effort, including time, bureaucratic energy and even travel dollars, are finite and must be optimised for the greatest potential gain. Second, we must recognise that the major 'problem' countries operating in cyberspace—China, Russia and Iran—are also the most difficult to talk to, and the cyber issue is inextricably intertwined with a wide array of other points of strategic tension and conflict with the three countries.

Given these factors, we should first align and normalise cybercooperation among ourselves before pursuing the more difficult challenge of cyberdialogue with adversary states. To this end, we can build

upon over a decade of successful bilateral and multilateral exchanges, led in the US by the State Department, to synchronise cyber-related laws and regulations and establish formal points of contact at the working levels. The intent of these exchanges has been to improve information sharing, joint investigations and our common defence. Strategically, we seek to create a cyber *cordon sanitaire* among Western, developed nations, while more starkly delineating the boundaries of the cyberthreat 'sanctuary'. Operating as a common bloc also unquestionably strengthens our bilateral and multilateral negotiations with adversary states, preventing them from playing us off against one another.

Why does this cooperation work? The answer lies in our similar political, legal and economic systems, as well as our long history of fighting together as an alliance. Our political systems share the same core values, including representative democracy, freedom of the press and governmental transparency. Our legal systems enshrine protections of privacy and civil liberties. And our economic systems are anchored in the encouragement of genuine private enterprise as opposed to the state capitalist systems of our main cyberadversaries. While the symmetries between Western systems aren't always exact, the similarities far outnumber the differences.

While these commonalities facilitate cooperation in peacetime, cooperation under conditions of cyberconflict is very different. We're very early in the development of strategic and military understandings of the nature of cyberconflict. In many ways, it feels like 1946, when the US had detonated atomic weapons but there had been very little strategic thinking about their employment.

But what is cyberconflict? One definition describes it as:

> the conduct of large scale, politically motivated conflict based on the use of offensive and defensive capabilities to disrupt digital systems, networks, and infrastructures, including the use of cyber-based weapons or tools by non-state/transnational actors in conjunction with other forces for political ends.[5]

Cyberconflict includes activities conducted by both state and non-state actors against a variety of targets. It encompasses a number of activities that pose threats to individuals, organisations and nation-states, as well as traditional military and intelligence operations. An alternative definition notes that cyberconflict is 'broader than cyberwarfare, including all conflicts and coercion between nations and groups for strategic purposes utilising cyberspace where software, computers, and networks are both the means and the targets.'[6] At its most basic level, cyberconflict encompasses activities conducted by many kinds of actors in order to achieve a strategic gain.

Given the huge stakes and potential damage to networked economies like those of the US and Australia, it's natural to begin with an examination of the notion of cyberdeterrence. While the US wisely retains the intention and capability to initiate cyberconflict at a time and place of its own choosing, it naturally seeks to deter other adversaries from the same goal, particularly given the asymmetric dependence of the US on cyberspace for economic, political and technological power. While it's well known that US government, military, and corporate networks have been the target of sustained computer network exploitation activities over the past 10 years, the country hasn't yet been the target of the type of large-scale computer network attack envisioned by Richard Clarke and others in their writings. How can we explain this apparent gap? Why

have adversaries not taken advantage of clear vulnerabilities to launch cyberattacks against the US? Is it because they haven't developed sufficient capabilities to do so? That's hard to believe, given the sophistication of the intrusions and methods. Has there not yet been the right combination of strategic circumstance and perceived payoff, such as the China–Taiwan contingency involving US military intervention, to justify using known capabilities? Or, despite its strategic confusion, does the US currently benefit from a form of tacit cyberdeterrence from computer network attack, and if so, what is the basis for this tacit deterrence?

When unpacking cyberdeterrence, the canon typologises deterrence into two categories: deterrence through denial and deterrence through punishment.

Cyberdeterrence through denial is also primarily based on computer network defence. One piece of good news is that the 'attribution problem', which occupies centre stage in the discussion of the dilemmas posed by cyberdeterrence by punishment, is not as significant an issue in cyberdeterrence by denial, because it isn't critical to know who might attack, only whether you're vulnerable to attack. Also, two primary methods for protecting retaliatory forces are mobility and concealment.[7] Cyberforces, by virtue of their form factor (a laptop is easier to conceal than a ballistic missile submarine), are already more mobile and more concealed than nuclear forces ever were. Finally, the inability to disarm an adversary's cyberattack capability has three benefits: reduced incentives for pre-emption; more focused and proportional retaliation; and reduced demand for immediate retaliation ('use it or lose it').[8]

But the cyber offence–defence balance is a huge problem for cyberdeterrence by denial. Fundamental security was not built into the architecture of cyberspace, and we have been gluing security onto the side of the network ever since. Without fundamental re-architecting of the network, which is unlikely in the short-term, is deterrence by denial even possible? In the short term, Rattray argues that these defensive dilemmas put a greater onus on risk management than impenetrable protection:

> Diffuse vulnerabilities and limited resources also require defensive efforts predicated on managing the risks of attacks rather than establishing comprehensive defenses capable of assured protection.[9]

But Owens et al. write that 'the gap between the attacker's capability to attack many vulnerable targets and the defender's inability to defend all of them is growing rather than diminishing.'[10] In addition, cyberoffensive capabilities are dramatically cheaper than effective cyberdefensive capabilities. As is often pointed out, the cyberwarrior, armed perhaps with a minimal kit (computer, internet connection and publicly available tools) only needs to find one way in, but the cyberdefender, protecting perhaps a huge network of thousands of heterogeneous nodes with dozens of access points, needs to bar every possible avenue of approach. Thus, cyberdeterrence by denial is also cost-prohibitive. For both of these reasons, it appears that cyberdeterrence by denial may be less credible than deterrence by punishment.

In the cyber-realm, deterrence by punishment theoretically offers better chances of success, especially against adversaries that have well-developed cyberinfrastructure. As Owens et al. argue:

> Deterrence by punishment is more likely to be an effective strategy against nations that are highly dependent on information technology, because such nations have a

> much larger number of potential targets that can be attacked. Nevertheless, even nations with a less technologically sophisticated national infrastructure are probably vulnerable to cyberattack in selected niches.[11]

Moreover, the will to retaliate is arguably less of a factor in cyberattack than in nuclear strategy, given its plausible deniability, potentially covert nature, and less physically destructive effects.[12]

Yet cyberdeterrence through punishment is also highly problematic. The main challenges for cyberdeterrence through punishment are:

- the so-called 'attribution problem', which makes it difficult to identify the attacker in the first place
- a series of credibility problems, including automaticity of response, unavailability of retaliatory targets, demonstration of effect, uncertainty of cybereffects, repeatability of effect, survivability of retaliatory capability, thresholds, signalling, command and control, and extended deterrence.

None of these challenges can be solved through policy measures alone, such as stated declaratory policies. All of these challenges create strategic instability in cyberconflict and undermine the utility of deterrence through punishment.

This leads us to the stark conclusion that the current cyberspace domain is inherently unstable. The strategic cyber-environment is marked by an inability to establish credible deterrence and effectively prevent the emergence of adversaries and conflicts in cyberspace detrimental to US interests. The sources of this instability are manyfold. First, the technical architecture undergirding cyberspace is highly permissive of cyberintrusions and attacks, resulting in a system that's extremely hard to defend and confers dominance on the offence. The defender can mitigate the asymmetry by reducing the degree of interconnectivity, or even disconnecting networks, but that's very costly, given the growing reliance of the US and advanced nations on those networks for a wide range of economic activity and military operations. Second, the design of the architecture often provides the attacker with anonymity and plausible deniability, aided by the lack of effective governance of the network focused on mitigating malicious activity. Third, the relatively low cost of technology and operations significantly lowers the barriers to entry for the attacker, enabling a wide range of actors to acquire capabilities. Fourth, cyberoperations running at the rapid 'speed of the network' deny defenders and the political leadership sufficient time for assessment and decision-making. Automation may mitigate this problem, but the risks are both high and unknown. Fifth, the pace of technological change and the breadth of network connectivity are outpacing both defensive approaches at the enterprise or engineering level and the policy and legal constructs promulgated to guide their operations. Moreover, these conditions are only getting worse with the proliferation of social media and mobile communications, and the migration to cloud computing. An internet underground capable of exploiting these trends is alive and well, with pirates and mercenaries thriving in a swampy ecosystem that makes hiding and attacking too easy. Last, while the issues are acknowledged, little progress is being made in improving security and resilience as a key aspect of internet governance.

Given this state of strategic instability in cyberspace, it's more important than ever for allies such as the ANZUS Treaty countries

to bolster their collective cyberdeterrent by coordinating information sharing[13] and technical cybercapabilities across all three realms of computer network operations (defence, exploitation and attack). This is a natural extension of the language in Article II of the treaty calling for all parties to 'separately and jointly by means of continuous and effective self-help and mutual aid [to] maintain and develop their individual and collective capacity to resist armed attack.' A higher and more complicated goal would be to link the nations' cyberdeterrence and declaratory policies such that cyberattacks would be covered under Article V's language that 'an armed attack on any of the Parties is deemed to include an armed attack' on all. If deterrence fails, however, it's equally important for the ANZUS Treaty partners to coordinate their kinetic and non-kinetic responses to a foreign cyberattack through information sharing about defensive signatures and the synchronisation of exploit and attack operations.

Current and future cooperation challenges

One current arena for cooperation and conflict between states involves what might be called the 're-sovereigntisation' of cyberspace. During the early years of the internet, when cyberspace was not the technological foundation for global commerce, states had the luxury of permitting the architecture to grow organically and not being concerned with its strategic value. Now that the situation has clearly changed, all states have come to an important realisation: every node of the network, every switch, router and computer, is either located within the sovereign boundaries of a nation-state and therefore governed by its laws, or travels on submarine cables or satellite connections that are owned by companies incorporated in sovereign nations and therefore bound by their laws. In other words, there's no 'commons' in cyberspace similar to air, sea and space, and there's no part of the global architecture that is 'sovereignty-less'. The implications of this realisation are profound, and explain why countries like China are keen on moving internet governance from non-governmental organisations like ICANN (the Internet Corporation for Assigned Names and Numbers) and the Internet Governance Forum to state-based organisations like the United Nations International Telecommunications Union. The battlelines have been clearly drawn (compare the White House's recently published International Strategy for Cyberspace with China and Russia's proposed International Code of Conduct in cyberspace), and Western nations need to develop policy responses that are properly aligned and mutually reinforcing.

Among the future cooperation challenges are the 'long game' issues in cyberspace, especially shaping the global information technology standards regimes. For many years, organisations such as the Internet Engineering Task Force and IEEE were dominated by knowledgeable technical personnel with little interference from governments, which had adopted a *laissez faire* approach to standards development. China's unwillingness to pay royalties for existing standards and protocols such as CDMA led Beijing to fund an aggressive, state-driven industrial policy to develop parallel, indigenous standards for nearly all of the existing protocols. While most of the Chinese standards have been rejected by the International Organization for Standardization and other governance bodies as technically inferior to the existing standards, China, exploiting its status as 'the world's IT workshop', has been able to force multinational companies assembling

equipment in-country to integrate the rejected standards into their products, thus distorting the standards regime.

Western countries were late in recognising this strategy and its implications, and have been playing 'catch-up' ever since. Because the standards debates today will define the nature of the technical architecture and the corresponding cybersecurity challenges of 5, 10 and even 20 years from now, it's important that the US and Australia develop a common approach on the standards issue and coordinate their efforts.

Notes

1 'Australia–United States Ministerial Consultations (AUSMIN) 2011 Joint Communiqué', media note, Office of the Spokesperson, San Francisco, California, 15 September 2011, available from http://www.state.gov/r/pa/prs/ps/2011/09/172517.htm.

2 Intelligence sharing between Australia and the US was referenced in the 2005 AUSMIN joint communiqué, available from http://www.dfat.gov.au/geo/us/ausmin/ausmin05_joint_communique.html.

3 William J Broad and David E Danger, 'Worm was perfect for sabotaging centrifuges,' *New York Times*, 18 November 2010, available from http://www.nytimes.com/2010/11/19/world/middleeast/19stuxnet.html. For more information on *Stuxnet*, see Ralph Langner, 'Cracking Stuxnet, a 21st-century cyber weapon', *TED*, March 2011, available from http://www.ted.com/talks/ralph_langner_cracking_stuxnet_a_21st_century_cyberweapon.html?awesm=on.ted.com_Langner&utm_content=awesm-publisher&utm_medium=on.ted.com-static&utm_source=langner.com.

4 Joseph Nye, *The future of power*, p. 145. For a specific example of cyberespionage, see Brian Grow and Mark Hosenball, 'Special report: in cyberspy vs. cyberspy, China has the edge', *Reuters*, 14 April 2011, available from http://www.reuters.com/article/2011/04/14/us-china-usa-cyberespionage-idUSTRE73D24220110414.

5 James Mulvenon, 'Toward a cyberconflict studies research agenda', *IEEE Security and Privacy*, 3(4) (July–August 2005), 52–55.

6 Jason Healey, 'Advanced intelligence support to cyber conflict', Delta risk fundamentals for cyber warfare (course presentation), Needham, MA, 28–30 September 2010).

7 Thomas Schelling, *The strategy of conflict*, Harvard University Press, Cambridge, MA: (1960, 1963), 1980, 243.

8 Martin Libicki, *Cyberdeterrence and cyberwar*, RAND Corporation, 2009, 61–62.

9 Gregory Rattray, *Strategic warfare in cyberspace*, MIT Press, 2001, 474.

10 WA Owens, KW Dam and HS Lin (eds), *Technology, policy, law and ethics regarding US acquisition of* ***cyberattack capabilities***, National Academies Press, 2009, 44.

11 Owens et al., *Cyberattack capabilities,* 41.

12 Libicki, *Cyberdeterrence and cyberwar*, 69–71.

13 Intelligence cooperation between Australia and the US was highlighted in the press release from the 2005 AUSMIN talks, held in Adelaide in November 2005.

Conclusion

All of our contributors point to the wide variety of actors in cyberspace and the breadth of threats they pose, but there's little doubt that, for the time being anyway, states remain the most capable and powerful actors in cyberspace. This is why treaties such as ANZUS are so important in dealing with national security cyberthreats.

From what little has been publicly articulated by Minister for Defence Stephen Smith, the type of cyberattack that would trigger the ANZUS Treaty would be one that could be a precursor to cyberwarfare or, more likely, a cyberattack that's either in combination with or would trigger physical, kinetic attacks. This sets a very high threshold for the type of attack that would invoke the provisions of the ANZUS Treaty.

In a situation like that, there would most likely be preceding hostilities and the actors involved would be apparent. Response would be relatively straightforward.

But even though only a very high order cyberattack would trigger a joint military response, the ANZUS alliance is also the basis for continued and strengthened cooperation and coordination on a multitude of levels concerning cyberthreats.

This is also important because, while states remain the most capable actors in cyberspace, there's no doubt that access to information via the internet and the growth of computer networks have greatly empowered individual actors, which poses a different challenge to the state. An individual or group with relatively few resources can bring down a critical computer network. Individuals or groups can use information technology and social networking to organise, promote and carry out actions or positions contrary to national security. Future cooperation through the ANZUS alliance structures would have to clarify whether the treaty could be invoked if a significant attack were perpetrated by a non-state actor.

In that instance, there are many lessons to be learned from our joint effort against global terrorism. Just as an individual act of terrorism can potentially spark a national security crisis, as it did after the September 11 attacks, so too can an act of cyberterrorism or a state-sponsored or quasi-sanctioned action. Greater American–Australian cooperation in cyberspace, aside from a joint military response in the event of a cyberattack within the context of a wider war between nation states, is critically important to managing this dynamic.

There are still differences within the international community about what type of cyberaction constitutes a cybersecurity threat on the part of individuals and small groups. Ultimately, as our contributors note, it's a case of information and internet freedom versus cybersecurity.

In societies where there are less openly contested politics and restrictions on information access, cybersecurity means not accessing and promoting certain types of information that would threaten the state. Authoritarian governments are seeking to frame and define cybersecurity in a way that allows them to limit and monitor online activity. The Shanghai Cooperation Organization approved an agreement put forward by Russia and China that defined online aggression and 'information war' as any effort to undermine another country's 'political, economic and social systems'. They want to frame the cybersecurity debate to include limitations on internet freedom—the ability to use the internet freely, anonymously and without monitoring.

However, cybersecurity is obviously framed differently in open democratic societies that promote freedom of information like Australia and the US. The previous position should be unacceptable for countries that believe in

universal human rights and the right to civil disobedience. Greater cooperation among close allies like Australia and the US can help clarify this debate and promote cyber-norms that protect internet freedom while also promoting cybersecurity.

Collaboration through the ANZUS alliance should also help the US and Australia shape, distinguish and define various cybersecurity concerns. A cyberattack should be clearly defined and distinct from an act of cyberespionage. Too often, an intrusion into a computer network for the purpose of stealing information is labelled as a cyberattack when it should be more accurately described as an act of cyberespionage. To label an act of espionage as an attack and therefore a potential precursor for an armed response is a major departure from accepted international practices. Breaking into a facility that stores classified information or information that's important to national security, whether it's a building or a computer network, is not an attack. It's espionage, an accepted and expected practice among states, including Australia and the US.

It's important to note that the ANZUS alliance, and in fact no other country or statement, has explicitly stated that this should be the case, but the absence of clarity in language leaves room for confusion. There's no shared concept of what constitutes a cyberattack, and using the cooperation afforded by the ANZUS alliance to shape and promote a definition is an important opportunity.

However, there's an important blurring between espionage and attack in cyberspace that doesn't exist in the physical space. The same intrusion method that's used to extract information from a network can also be exploited to conduct an attack to disrupt that network. This is a critically important distinction that policymakers must be aware of and account for. While every cyberintrusion can't be labelled as an 'attack' per se, it's critically important to assess whether or not an intrusion has exploited a vulnerability that could also be used to disrupt or destroy networks.

Additionally, as Dr Lewis points out in his paper, it's also a question of aggregation. Ongoing and unchecked cyberespionage carries national security risks. The sheer amount of data that is now carried and stored on computer networks is unprecedented. For relatively little effort, cyberspies can now access vast quantities of information that they never could before.

Clearly, the ANZUS alliance is an important and relevant mechanism in meeting and addressing national security challenges for both Australia and the US. Cybersecurity and the ability to shape and dominate the cyberdomain are future shapers of geopolitical power. The more that Australia and the US can act in concert as like-minded allies, the better they'll be able to ensure their security and economic and political wellbeing.

Equally important is the need of shaping and defining the terms of debate in the cyber-realm (internet freedom versus cybersecurity) and defining what action meets the threshold of a cyberattack. It's an ongoing conversation and effort, but one that Australia and the US can lead.

Acronyms and abbreviations

ACTA	Anti-Counterfeiting Trade Agreement
DDoS	distributed denial of service
IEEE	Institute of Electrical and Electronics Engineers
NATO	North Atlantic Treaty Organisation
OECD	Organisation for Economic Co-operation and Development
PIPA	Protect IP Act (US)
SOPA	Stop Online Piracy Act (US)
UN	United Nations

About the Authors

Dr Andrew Davies is the Director of the Operations and Capability Program at ASPI. He has written on the impact of Asian military modernisation programs, nuclear proliferation, defence acquisition projects and major Australian capability decisions.

James Andrew Lewis is a senior fellow and Program Director at CSIS where he writes on technology, security and the international economy. He was the Rapporteur for the 2010 United Nations Group of Governmental Experts on Information Security. He has authored many publications since joining CSIS. One series of reports explores the relationship between technology, innovation, and national power.

Jessica R Herrera-Flanigan is a partner at the Monument Policy Group, a strategic consulting and government affairs firm, where she focuses on the issues affecting our nation's security, technology, commerce, and entertainment markets. Previously, she served as the Staff Director and General Counsel of the House Committee on Homeland Security. She also has served as Senior Counsel at the Computer Crime & Intellectual Property Section, Criminal Division, US Department of Justice, where she led the Section's cybercrime investigation team.

Dr James Mulvenon is Vice-President of Defense Group, Inc.'s Intelligence Division and Director of DGI's Center for Intelligence Research and Analysis. A specialist on the Chinese military and cyber warfare, Dr. Mulvenon's research focuses on Chinese C4ISR (command, control, communications, computers, intelligence, and reconnaissance), defense research/development/acquisition organizations and policy, strategic weapons programs (computer network operations and nuclear warfare), cryptography, and the military and civilian implications of the information revolution in China.

ASPI
Tel +61 2 6270 5100
Fax + 61 2 6273 9566
Email enquiries@aspi.org.au
Web www.aspi.org.au

BECOME A MEMBER

JOIN NOW TO RECEIVE PRINTED PUBLICATIONS AND MORE

Join Australia's liveliest minds writing today on defence and strategic issues. ASPI produces ***Strategy***, ***Strategic Insights***, ***Special Reports***, and specialist publications including ***The Cost of Defence*** and ***The Australian Defence Almanac***.

ASPI's work is at the cutting edge of new thinking on defence and security.

Thoughtful, ground-breaking and often controversial, ASPI leads the public debate on these issues. Become a valued part of the ASPI team today!

Join now and we will post your choice of 3 free publications from our recent publications list.

Future subjects include:

- **Professional military and national security**
- **Comparative assessment of regional militaries**
- **Response to violent extremism**
- **Vietnam**
- **ADF future strike capability**
- **Transnational and organised crime**

TELL A FRIEND ABOUT ASPI

Join Australia's liveliest minds writing today on defence and strategic issues. Each year the Australian Strategic Policy Institute (ASPI) will produce up to six issues of ***Strategy***, six shorter ***Strategic Insights*** and a number of ***Special Reports*** on issues of critical importance to Australia and the Asia–Pacific.

Thoughtful, ground-breaking and often controversial, ASPI leads the public debate on defence and security issues.

JOIN ASPI

Name

Position

Company/Organisation

❑ Government **❑ Non-Government**

Address

City **State** **Postcode**

Country

Telephone

Email

SELECT 3 FREE PUBLICATIONS

- ❑ Two steps forward, one step back: Indonesia's arduous path of reform
- ❑ Beyond bin Laden: Future trends in terrorism
- ❑ Our near abroad: Australia and Pacific islands regionalism
- ❑ Forks in the river: Australia's strategic options in a transformational Asia
- ❑ Changing pace: ASPI's strategic assessment 2011
- ❑ Regionalism and community: Australia's options in the Asia–Pacific
- ❑ Southeast Asia: Patterns of security cooperation

INDIVIDUAL	❑ 1 year *$199*	❑ 2 years *$378*	❑ 3 years *$537*
STUDENT*	❑ 1 year *$99*	❑ 2 years *$188*	❑ 3 years *$263*
CORPORATE (Oct 06+)	❑ 1 year *$649*	❑ 2 years *$1233*	❑ 3 years *$1752*

* (STUDENT ID _____)

To join

1) Subscribe online www.aspi.org.au
2) Mail to Level 2, Arts House, 40 Macquarie St, Barton ACT 2600, or
3) Phone (02) 6270 5100 or fax (02) 6273 9566

❑ Cheque **❑ Money Order** **❑ Visa** **❑ MasterCard** **❑ AMEX** **❑ Diners**

Payable to Australian Strategic Policy Institute ABN 77 097 369 045

Name on card

Card no.

Expiry Date **/** **Total Amount $**

Signature

This will be a **TAX INVOICE** for GST purposes when fully completed and payment is made.
Please note specialist publications are not included.