POLICY ANALYSIS ASPI

ASPI
AUSTRALIAN STRATEGIC POLICY INSTITUTE

Your system might be at risk—Australia's cyber security

by Andrew Davies

80

31 May 2011

Executive summary

Illicit activity in cyber space is increasing markedly and represents a threat to national security and to the broader economy. Hostile and criminal cyber activities probably cost the Australian economy billions of dollars per year, and national security is threatened by state-sponsored acts. However, many cyber threats represent an extension of existing criminal and espionage activity in more traditional physical domains.

Some of the 'worst case' scenarios of the impact of hostile or illegal cyber activity are just that—worst case. They accurately represent the likely outcome of an increased dependence on networked systems in the absence of either a coherent government policy or market responses in the form of improved security products and services. There is certainly enough awareness of the problem today to ensure that governments and industry will respond—the Australian Government has already made good progress—but the question is whether the response is proportional to the threat.

Because of the breadth of the problem, it represents a difficult public policy challenge. While there is a widespread expectation that government should 'fix' the problem, the reality is that the government has a limited (although important) role to play. A whole of community response involving the various tiers of government and their respective agencies, industry and the wider populace is the appropriate way to address the issue—a fact already recognised in the national cyber security strategy. Provided the strategy is agile enough to keep up with a rapidly evolving threat, Australia is reasonably well placed, although our efforts to date have been in 'catch-up' mode.

Within the defence/national security sector, the scale of Australia's response should be set by the gravity of the threat to national security. That's a matter of judgement for those with access to the relevant (classified) information.

For issues of lower national security concern, the scale of the governmental response—and hence the resources and funding allocated—should be determined by a rigorous cost-benefit analysis. Cyber security will necessarily compete with other calls on government funding. The level of investment should be set by the expected reduction in losses that can be achieved—noting that success will never be complete.

In the private sector, the level of investment in cyber security will also be driven by cost-benefit analysis. Just as companies with physical retail stores balance losses due to theft against the cost of security measures, online business will balance losses from cyber activity against the cost of prevention and remediation.

Introduction

It's not hard to find breathless accounts of the dangers of lapses in cyber security. Here's a typical example:

> The next large-scale military or terrorist attack on the United States, if and when it happens, may not involve airplanes or bombs or even intruders breaching American borders. Instead, such an assault may be carried out in cyberspace by shadowy hackers half a world away. And Internet security experts believe that it could be just as devastating to the U.S.'s economy and infrastructure as a deadly bombing.[1]

The implied comparison of cyber attacks with the events of September 11, 2001 in this CNN report seems extraordinary, but it is by no means unusual—it was picked at random from Google search results that included hundreds of such pieces. As well, there's no shortage of stories about Chinese espionage and Russian criminal activity in cyberspace and general cyber gloom and doom reporting. Recent reports in the Australian press revealed that there is more than one significant attack on a government website every day.

Some of this reporting is based on a reasonable analysis of the situation. Some of it is exaggerated for effect. And some of it is generated by those who would profit from a greater uptake of bespoke technical solutions. For the lay reader, it's hard to know how worried to be.

That's why this analysis starts off with a conceptual framework for understanding cyber security threats. This isn't just an abstract exercise; by framing the problem in the right way, it's possible to identify not only the scope and possible severity of cyber security threats but also to identify who should have primary responsibility for managing them.

The second part of this paper, using the conceptual framework, examines current and proposed Australian arrangements for cyber security. It concludes that it's neither practical nor desirable for governments to be responsible for all cyber security. Rather, the burden of cyber security should be shared between the users and providers of IT—government, industry and individuals, with the government being responsible for systems that have national security implications (in the narrow sense of the term).

But there is also a role for the government to provide guidance, regulatory frameworks and, in some instances, even to promulgate technical mechanisms and tools. The trick is to work out what the balance should be between government-led and market-led solutions.

Understanding cyber security

Cyber security has many facets. The gamut of concerns runs all the way from amateurish nuisance activity through to sophisticated state-sponsored intrusions into government networks. Some hostile cyber activity is criminally-motivated, some is malicious 'fun' and some is intended to procure information of interest to states and/or to provide their military arms with a useful adjunct to other warfighting capabilities.

To break down the problem to 'first principles' it's useful to think about the range of potential targets of hostile cyber activity. The following list of categories (which are not mutually exclusive) shows the breadth of challenges for those hoping to conduct their online activities securely.

Action:

against computer systems

- obtaining remote access and/or control (as a prelude to other activities)
- use as a 'cut-out' or unwilling proxy to disguise the origin of illicit activity

against data at rest (information systems)

- steal it (copy)
- delete it
- corrupt it (make data useless by replacing with garbage)
- spoof it (replace it with data designed to mislead)

against moving data

- interception (eavesdropping)
- compromise it (receiver cannot be sure data is reliable/unseen by intruder).

against industrial and civil and military infrastructure control systems

- disrupt them (stop them working)
- control them for sabotage (cause them to operate in an unintended mode)

against access points (ISPs, websites)

- denial of service
- corruption of data
- replacement of data with alternatives (propaganda, protest)

against the end-user

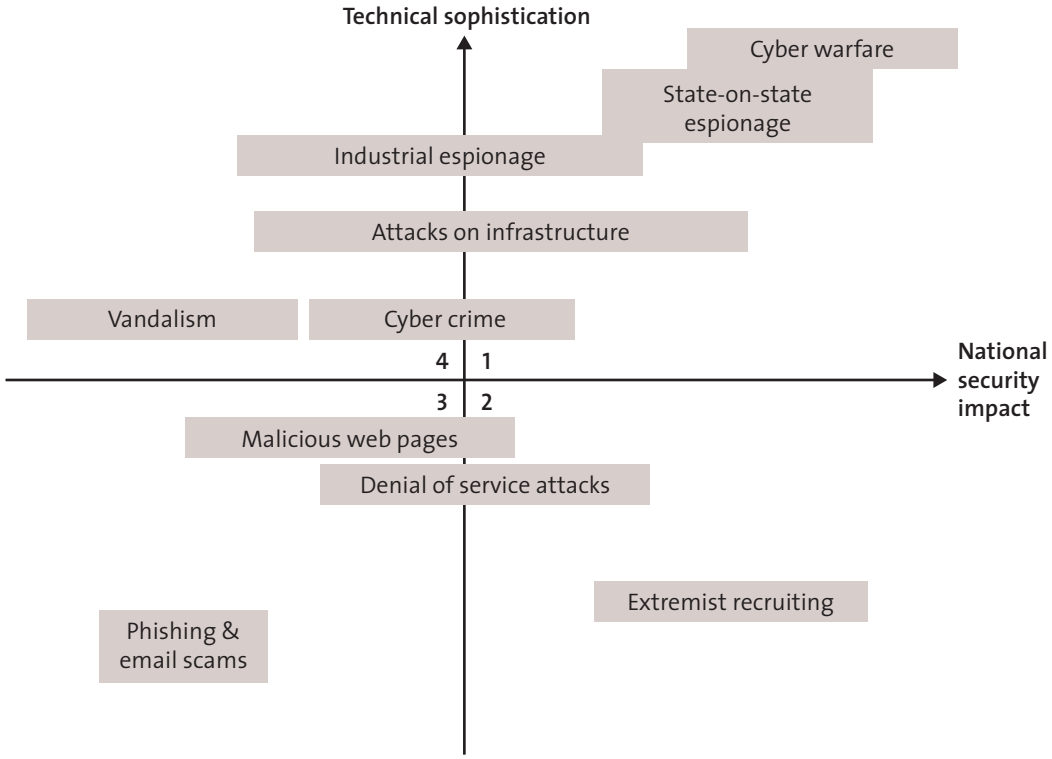
- theft of authentication information—passwords, login details etc
- fraudulent activity (phishing emails)
- vandalism (corrupting hard drives).

The internet as a facilitator of illicit activity

- dissemination of extremist messages and recruiting
- communication between terrorists/criminals
- dissemination of cyber-crime tools
- dissemination of contraband including confidential information (e.g. WikiLeaks) or illicit products (e.g. child pornography)
- issue motivated groups attacking infrastructure including government sites
- scams, fraud, extortion and medium for human exploitation
- hosting services that provide on-line facilities for illegal activity.

A list like the one above is OK as far as it goes, but a visualisation is helpful to make sense of the problem. Figure 1 schematically maps a range of cyber activities according to two of their most important characteristics; technical sophistication and national security impact. While acknowledging the limitations of this sort of representation—some activities overlap significantly with others and the range of technical skills exhibited by malicious individuals varies widely to give just a couple of examples—it nonetheless allows us to begin to sort through the panoply of cyber threats. We'll return to this representation in several different contexts—like most complex problems, it is possible to 'slice' cyber security in several different ways, each of which providing a different view. Collectively they allow a coherent picture of cyber security responsibilities to be developed, from which good policy can follow.

Figure 1: A framework for thinking about hostile cyber activity



Enemies of the state

Quadrant 1 (top right) is the one most written about. It is the space in which sophisticated antagonists are working directly against systems and institutions with high national security value—largely (but not exclusively) in the '.gov' sector. This quadrant contains the cyberspace version of the traditional espionage and sabotage threats against the state, as well as the emerging field of cyber warfare.

Cyber warfare, which consists of attacks against and exploitation of the computers, digital control and information systems of an adversary's military or civil systems, is a complex topic in its own right and won't be discussed at any length in this paper.

In some ways cyber spying is simply a new version of an old problem. While espionage is (arguably) the second oldest profession, it has translated into cyberspace more effectively than its rival for first place. The amount of government and commercial information available online, and the number of points of connection between internal and external systems required to facilitate access to it has considerably expanded the scope of spying activities.

In principle the countermeasure to cyber espionage is straightforward—keep the systems hosting sensitive information or required for warfighting isolated from the outside world while implementing high-grade encryption on any data that has to be passed outside secure systems. In practice it's more difficult than that. Anecdotal reports of computer viruses that originate on the internet spreading rapidly onto classified systems suggest that there are multiple points of contact between the two. And breaches of cyber security can amplify human failure (or treachery).

As well, material that is important for national security is increasingly to be found on systems in the commercial world. In the military world this is due to the outsourcing of many support tasks and to the role played by industry in developing cutting edge technologies. In the United States, firms like Lockheed Martin, Boeing and Raytheon are frequently the targets of cyber infiltration and espionage activities. Major defence programs such as the F-35 Joint Strike Fighter attract considerable attention from cyber infiltrators. It's not a big stretch to imagine that Australian

subsidiaries of those firms and local companies involved in defence business are similarly of interest to outside players. Many of these activities have been ascribed to foreign governments—with China being the most prominent of the 'states most likely to'.[2]

Given the sort of press reporting this paper opened with, the reader might be surprised that 'cyber terrorism' doesn't feature in Figure 1. That is because there is no serious evidence (at least in the public domain) that terrorists see any great value in cyber attack as an end in itself. The aim of terrorist groups is to conduct attacks that are highly visible and which result in mass casualties. The nature of cyberspace makes both of those objectives hard to achieve. The well-documented continued appeal to terrorists of attacks on aeroplanes—probably the most psychologically potent target—testifies to the nature of their thinking.[3] And there is a technical hurdle to overcome. A sophisticated attack on infrastructure is not easily done. For example, the *Stuxnet* worm that was apparently used to attack Iranian nuclear facilities likely had man-years of sophisticated software engineering effort behind it.[4]

However, as a risk management strategy it would be prudent to assume that terrorist groups might turn their attention to cyberspace in the future. Perhaps the most credible threat is an attack in cyberspace on response authorities, such as fire and ambulance services, and civil infrastructure *in conjunction with a physical attack* to exacerbate its effects. The appropriate preventative measures are a combination of physical separation of critical systems where possible and 'hardening' of system security when physical separation isn't feasible.

Terrorists can also use the connectivity of modern digital communication systems to their advantage like any other user group. Recruiting, coordination and command and control activities inimical to national security can all be facilitated over the internet using readily-available tools such as chat rooms, message boards and websites.

Those activities can be found at the bottom right in quadrant 2—technically straightforward, but with potentially high national security impact. As well, like any other users, terrorist groups can be involved in other disruptive or criminal cyber activity for political or economic gain.

Every computer a target

To the left of the vertical axis we find the overwhelming bulk of computer and communication systems—those in homes and the wider business world. The proliferation of computers, smart-phones (which blur the line between computers and communication devices) networks and applications has been accompanied by the development of a rich array of schemes and software technologies designed to exploit new opportunities for criminal activity, malicious fun or just curiosity-driven exploration. And just as technical advances have moved computers from mainframes to desktops to laptops, networks now allow computing and communications devices to exchange data in ways unthought-of just a few years ago—like car systems that connect with the internet. These provide new avenues for unauthorised access.

Fraudulent email is a daily occurrence for most users; malware packages such as viruses, spyware and Trojans are constantly being updated and promulgated; networking allows remote users to probe all of the machines on the network for vulnerabilities to exploit. The technical sophistication of these attacks runs all the way from naive (such as 'Nigerian' email scams) through to highly advanced—such as a recently-developed application for a smart phone that can recognise a credit card number being spoken, record it and exfiltrate the data. (Fortunately that one was developed by security researchers, but similar developments can be expected from less benign sources).[5] And even low-tech threats that aren't of concern to

savvy users nonetheless can impair the ability of less sophisticated users to make use of computers.

The impact of these activities ranges from nuisance value through to serious criminal acts such as identity theft and credit card fraud. And there is a national cost even in instances where national security is not directly threatened. While banks and large corporations aren't national security institutions in the narrow sense, they constitute critical infrastructure because the general health and wellbeing of the economy relies on them being able to conduct their business affairs online and to be able to safely store corporate information. In a broader sense, the ability to safely conduct online business is now an important part of consumer confidence, an important indicator of the national economy. Flow-on effects of a loss of confidence in online institutions would include loss of some of the productivity gains that have come with widespread use of the internet for business.

Responses and strategies

It's not all doom and gloom—each of the potential threats in cyberspace can be countered. But there is no 'one size fits all' response. Sophisticated intrusion detection systems designed for government networks are not going to stop a neophyte home user from clicking on a link in a scam email, or prevent an extremist group from proselytising online. It's a matter of identifying the appropriate response to each of the threats that are out there.

And at each point in the threat spectrum there will be a combination of approaches that provide layered security. Technically sophisticated threats require responses that are not just technically sophisticated themselves but which also take into account the human factors and poor practices that even the most technically accomplished adversaries require to access some systems. In the case of protecting high-end government systems, for example, the layered security approach might include:

- isolating those systems carrying highly-sensitive material from the outside world ('air gapping')
- providing systems administrators with tools that allow them to identify unauthorised activity
- minimising the number of internet gateways into other computer systems
- limiting the ability of users to access data for which they have no 'need to know' and circumscribing the ability to download data onto portable devices
- improving security practices and awareness (ensuring that passwords are strong and regularly changed
- systems assurance—testing and checking for vulnerabilities and/or functionality beyond what is required or expected
- encryption.

In short, the answer is a combination of system tools and security measures, education of users on good security practices and the quarantining of sensitive information wherever practicable. There is no doubt that the Australian Government is active in protecting its systems in these ways. For example, an extensive public key encryption infrastructure and accompanying policy frameworks are in place to allow government departments to securely deliver their products and services online.[6] And the government's information security manual sets out roles and responsibilities and best practices for government systems.[7]

This layered approach generalises to other IT users, with the balance between the elements and the degree of direct involvement in management being the main variables. For example, a home user doing online banking is protected by

a combination of operating system features, local firewall and malware detection software and strong encryption of the connection between the home computer and the bank in the form of SSL or other protocols. Much of that is done in a way that is transparent to the user. For example, there is no need for a bank customer to manage encryption key settings—that's all done 'behind the webpage'.

As well, the ISP providing that home connection will also have in place a range of systems and tools that allow system administrators to protect their customers. Similar arrangements also apply to small and medium businesses. Larger businesses have their own IT support arrangements, which allow them to apply their own security measures on top of those provided by hardware and software vendors and ISPs.

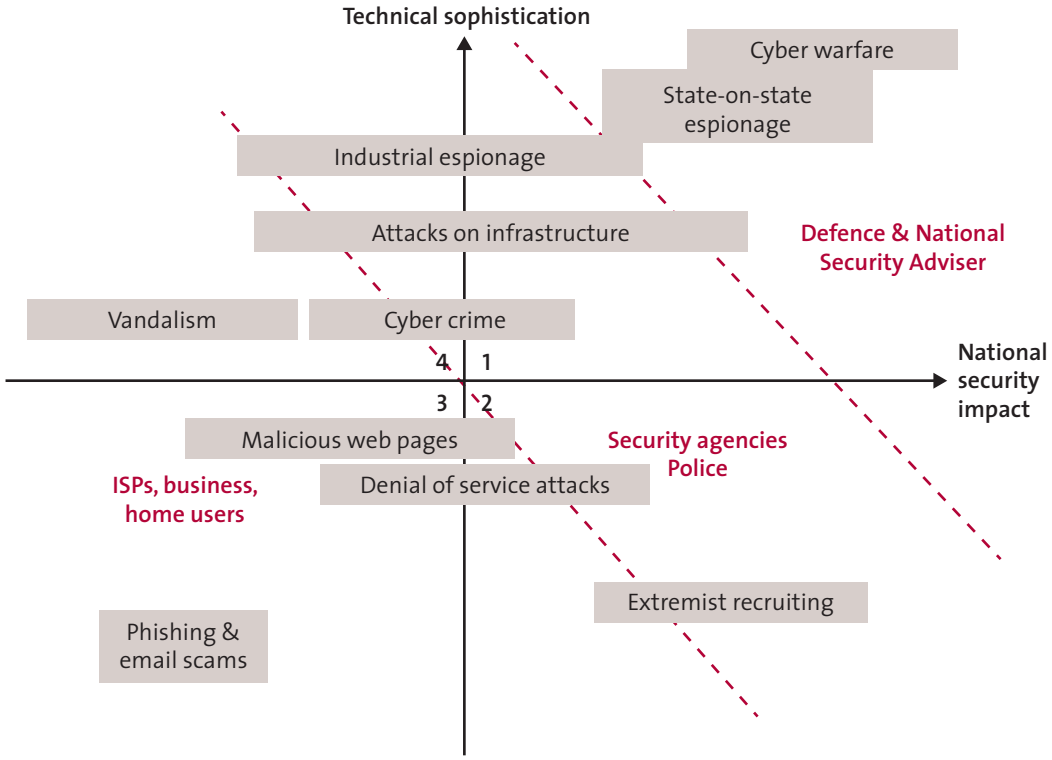
In short, when formulating cyber security policy, as well as working out *what* is to be done, it's necessary to work out *who* is best placed to do it. Sometimes the decision is easy. As the guarantor of national security, the federal government clearly has the responsibility to ensure that 'quadrant 1' government and warfighting systems are afforded protection commensurate with their importance. As well, there are criminal aspects of cyber security which necessarily require the attention of law enforcement agencies. Government security agencies also have a remit to monitor and sometimes act against terrorist groups promulgating a radical agenda or recruiting new members online. And where the government is working with private sector partners in this quadrant—as it often does—it's up to the government to set and monitor appropriate security standards.

But there's a limit to what can be expected from government. And in fact the worldwide internet community has proven to be effective in self-regulating to an impressive extent. The self-interests of diverse government, commercial and private parties around the world have conspired to produce a 'network of security' that is surprisingly effective. In the week prior to writing this passage, security software on the author's home PC downloaded and installed almost 100 new files. As well, there were half a dozen new system patches. Each one required a new threat (or system weakness, which is at least a nascent threat) to be identified and analysed before a solution could be implemented, tested and promulgated.

This level of security service is the international norm, and the scale and speed of activity is such that governments can't (and shouldn't) be expected to be directing those efforts. However, it's not perfect, and the level of penetration of state-of-the-art technical remedies and best practice is incomplete. It is in that space that governments have a role to play, as setters of standards and—if necessary—as regulators.

The national response to cyber security is going to require a collaborative effort between the various arms of government, the IT security industry and the wider community of computer users. Figure 2 shows schematically who has primary responsibility for the various cyber threats. There are some subtleties here—it makes sense to break down responsibilities into *prevention, detection* and *response*. Figure 2 shows responsibilities for *prevention.* The breakdown of responsibilities for detection and response will generally be different. For example, ASIO has the responsibility to 'investigate electronic attacks conducted for purpose of espionage, sabotage, terrorism or other forms of politically motivated violence' and the Australian Federal Police have a response role at all points in the diagram.

Figure 2: Where the responsibility falls for the prevention of hostile cyber activity



Policy and organisational responses

It's probably fair to say that Australia's response to date has been 'after the event'—it has taken consistent penetration of national and commercial systems and substantial commercial losses to wake us up to the need for a coordinated response. But a national strategy has emerged that has many of the right elements.

In setting policy, the government has to do two things. Within its own domain it needs to ensure that all government departments and agencies have a consistent and effective approach to cyber security. To strengthen the cyber resilience of the nation's business infrastructure, the government can promulgate advice and technical assistance more broadly. And in doing both of those things, the government can draw on the technical expertise developed for its quadrant 1 activities to provide advice on technological and implementation strategies appropriate for each type of user.

The evidence shows this is exactly the thinking that has underpinned the government's approach to cyber security. Work is underway—and good progress is being made—to develop a whole-of-government policy framework, coordinated by the Department of Prime Minister and Cabinet under the auspices of the National Security Adviser. The Cyber Security Operations Centre (CSOC) set up by the 2009 Defence White Paper is housed within the Defence Signals Directorate (DSD)—an appropriate location given DSD's legislated role as the Commonwealth's authority for information security.

Some good work has been done to extend the hand of cooperation into the public domain. The Computer Emergency Response Team (CERT) Australia initiative is a good example. Building on earlier efforts coordinated through a non-profit centre at the University of Queensland, the federal government instituted a national body

> … to work with the private sector in identifying critical infrastructure and systems that are important to Australia's national interest, based on an assessment of risk, and to provide these organisations with information and assistance to help them protect their information and communication technology infrastructure from cyber threats and vulnerabilities. [8]

Figures 3a and 3b provide a complementary view, drawing on the interests identified above. The right hand side of Figure 3a is dominated by government agencies, which follows naturally from the national security aspects. The left hand side is mostly the domain of the wider community of users, with an overlap of interests towards the middle of the diagram. (Again, this most accurately represents *prevention*.)

Figure 3b shows the policy and technology 'flows'. The arrows are two-headed because commercial technologies and experience and the work of law enforcement and security agencies necessarily inform and influence the work being conducted in quadrant 1.

Figure 3b also suggests an area where further policy development may be beneficial. The bottom left quadrant of low national security impact and low technical sophistication—where the bulk of home users are to be found, is today largely self-regulated. Some government work has been done to raise awareness of the potential pitfalls that users face, and there are advisory notices and educational videos on government websites. But, for the most part, security solutions are left up to users and their ISPs to implement.

The extent to which it's desirable and possible for government to intervene at that level is a good topic for further exploration. Governments have a responsibility to provide security for Australians beyond what falls into the national security rubric. For example, we have police on the beat to provide an overall level of civil security, and extra resources are allocated where there is a raised possibility of harm to the community from whatever source. There's no reason for that concept not to translate into cyberspace. Indeed, to some extent it already has. The Australian Federal Police cybercrime unit provides definitions of high-tech crime, security advice, online resources and policing services.[9] The Australian Competition and Consumer Commission (ACCC) is active against online scams.[10]

No doubt much of this effort is appreciated by law-abiding computer users. However, the internet brings its own challenges in terms of public support for government activity. Nobody complains when the ACCC or the Australian Federal Police (AFP) prosecute people for breaking the law using online means. But the public has shown itself to be extremely unwelcoming of what it sees as government intrusion into a 'free' cyberspace. A good example is provided by the backlash against the notion of subjecting internet content to the same censorship standards that apply to other media.

Figure 3a: Two domains of cyber security

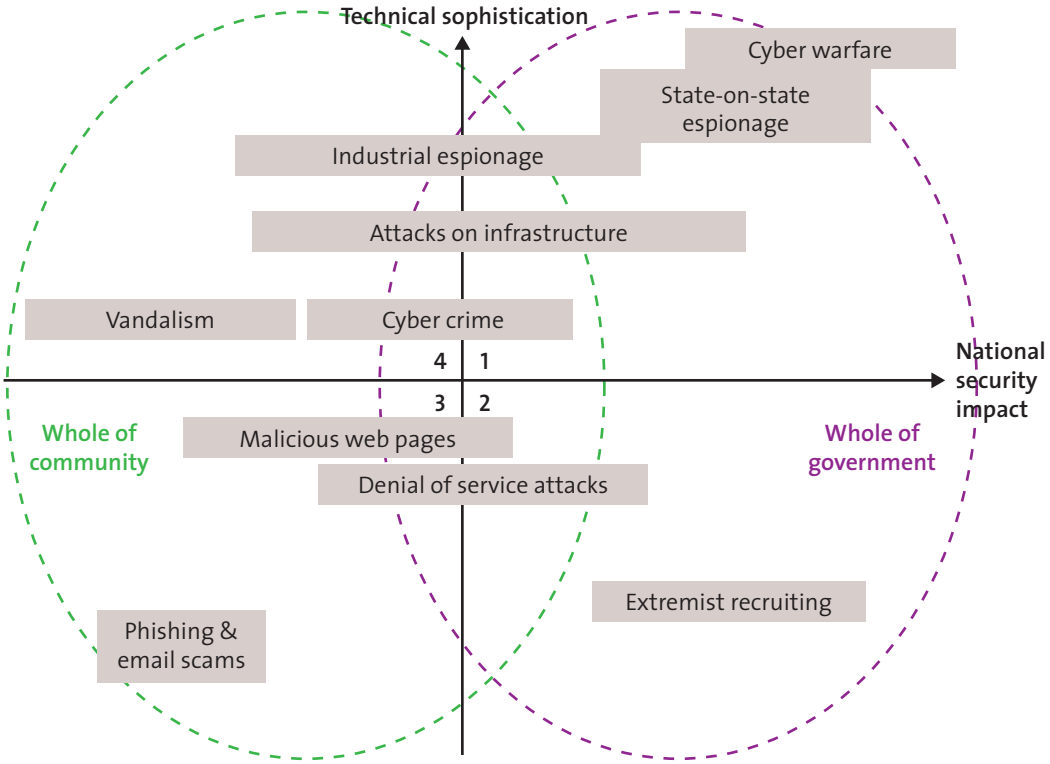
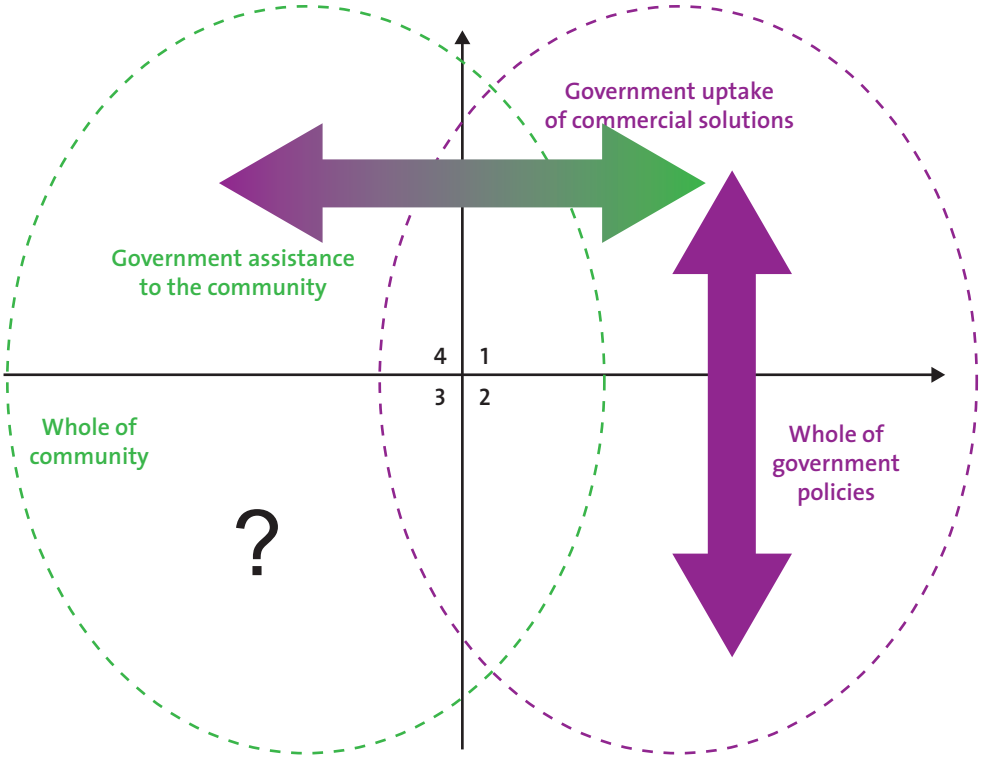


Figure 3b: Government cyber security initiatives



Governance

Given the breadth of the challenge presented by cyber security, it's not surprising that the responsibility within government is spread across a number of organisations. In fact, that follows quite naturally from the breakdown of responsibilities sketched out in Figure 2. But that doesn't mean that governance can be left to become an emergent property of the actions of multiple government departments, which is always the risk when a new issue comes to the fore. Some sort of structured approach is required.

The government's answer is sketched out in the *Australian Government Cyber Security Strategy*.[11] Reflecting the 'shared responsibility' approach argued for in this paper, the strategy states that all users should take 'reasonable steps' to secure their systems. (The only quibble there is that the language could be a little stronger.) It goes on to say that, given the scale and complexity of the challenge, national leadership is required, thus placing government at the centre of the national response.

The question then becomes how the government goes about doing that. One possibility is to assign primary responsibility to one position/department, and letting them assign tasks. In a study published earlier this year, the Kokoda Foundation discusses the desirability of appointing such a 'cyber Czar'.[12] They concluded that such a move would be counterproductive, preferring a goal of normalising cyber security as part of the wider national security framework. That view is correct for part of the spectrum of cyber threats, but runs the risk of focussing effort disproportionately on the 'quadrant 1' activities that are the natural province of Defence and the National Security Adviser within the Department of Prime Minister and Cabinet.

Instead, a more 'decentralised' model is appropriate and this is already reflected in the national strategy. There responsibilities are shared between several government departments. As well as the expected role for Defence, the Attorney-General's (AG's) Department takes responsibility for protective security policy across government and for law enforcement policy (the Australian Federal Police is responsible for actual law enforcement). ASIO is responsible for investigating acts of suspected cyber espionage, sabotage and terrorism. The interface between government and the wider community effort is mediated by the Australian Communications and Media Authority and the Department of Broadband, Communications and the Digital Economy. The overall government effort is coordinated by the Cyber Security Policy and Coordination (CSPC) Committee.

The overall government approach strongly reflects the conceptual model shown in figures 2 and 3. It is a sensible approach that recognises the breadth of the problem. But there are two cautions worth noting. Firstly, there is likely to be a tendency for the 'quadrant 1' aspects of the problem to become preeminent and crowd others off the agenda. Secondly, it's likely that the model will require frequent revisiting due to the dynamic nature of the ICT world.

Technical solutions

From a policy perspective, there is a question as to whether the government should be setting technical standards and/or prescribing technical solutions for cyber security in the wider community and, if so, to what extent. As argued above, the internet has been remarkably good at 'self-regulating', but there is little doubt that significant weaknesses exist, especially at the top end of the technical sophistication scale.

Many of the leading multinational defence firms have entered the field of cyber security/operations.[13] This was likely influenced by the decision of the United States to establish a military cyber command in response to the level of activity against US military and industrial computer systems.[14] Activities in the 'high-end' space of cyber defensive and offensive operations almost certainly require specialist tools—resulting in some systems being bespoke solutions. Some of those tools have probably been developed from tools in use in the private sector and others are likely to be unique 'government use only' solutions. This may put the government into the interesting position of having technical perspectives and expertise that would be of value in the wider community.

This is not an entirely novel development—government-owned cryptographic capability, developed over decades of experience in two world wars and the Cold War, has often been ahead of the private sector. In the United States, the National Security Agency (NSA, the equivalent of Australia's DSD) played a leading role in the development of the Data Encryption Standard (DES) used widely by the US Government (for protecting sensitive but not national security classified information), banks and other businesses from 1977–2001 (when it was replaced by the Advanced Encryption Standard).

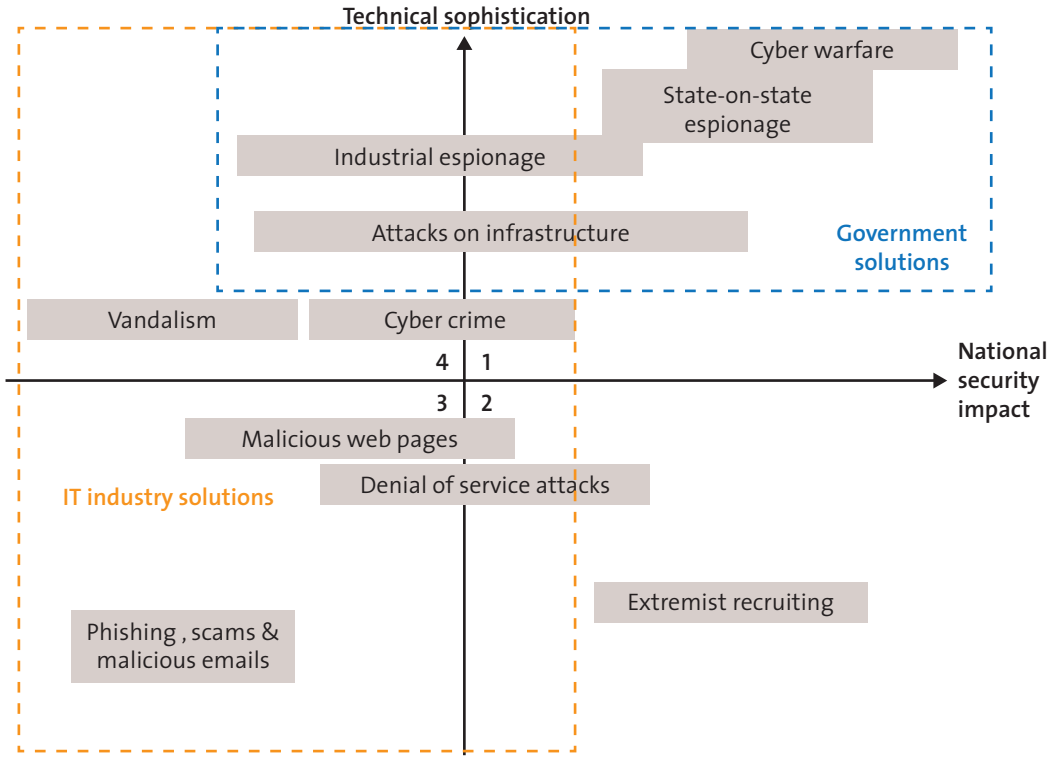
Some of the suspicions of government motives referred to earlier played out in the roll-out of DES. The NSA promulgated a modification to the scheme at one stage, prompting suspicions that the scheme was being deliberately weakened to allow NSA access to encrypted material. In fact, the changes suggested strengthened DES against a cryptologic attack known to NSA, but not discovered in the 'outside' world until some years later. As a result, the NSA significantly strengthened the ability of the wider community to safely store and transmit data.

So there is certainly the potential for a similar government role in broader cyber security. Whether this should occur through direct government intervention (the DES model) or by the private sector working directly with those firms contracted by the government for quadrant 1 systems and services should be worked out on a case-by-case basis. In some instances (like the protection of public infrastructure) the government may wish to impose solutions. In the wider community it may choose to offer advice tools and allow businesses and end users to make their own choices. The US Defense Department has begun a pilot program along these lines.[15]

To some extent, the Australian Government is already working in this space. The Defence Signals Directorate as the national information security authority runs the InfoSec Registered Assessor Program (IRAP) and maintains an evaluated product list (EPL). And as mentioned earlier, CERT Australia is a point of contact for the private sector when they are seeking assistance with cyber security. The current situation is certainly an improvement compared to a couple of years ago, but the IRAP and EPL both have a governmental focus. For example, the IRAP assessment and accreditation is based on the Australian Government's Protective Security Policy Framework and Information Security Manual. As the scale of cyber activity grows, there's likely to be scope for more programs, and ones that are more tailored to private sector 'customers.'

One final overlay on the conceptual diagram shows how technical solutions might fit into the overall scheme. Government solutions may have their origin in quadrant 1 (or may in fact have been coopted from the broader IT industry in the first place). General users in quadrant 3 are well-served by the multi-billion dollar IT security industry for cost-effective levels of protection. In quadrant 4, there is the most scope for a mixture of 'inside' and 'outside' solutions, with the mix to be determined by policy settings and fitness for purpose.

Figure 4: Possible sourcing of technical solutions for cyber security



Resources

It is easy to identify cyber security as a growing challenge and to conclude that it is likely to require greater resources. It is much harder to work out exactly what the appropriate level of resources is. Like every other issue that has a call on government funding, ideally the level of funding should be determined through a rigorous cost-benefit analysis. In practice that's hard to do because the diverse nature of cyber activities makes it hard to pin down a cost of inaction. And while it might be possible to put a dollar figure on business losses, at the high national security risk end of the spectrum the costs are much less tangible.

Within the defence/national security sector, the scale of Australia's response should be set by the gravity of the threat to national security. That's a matter of judgement for those with access to the relevant (classified) information and with an understanding of the technical complexities of dealing with sophisticated threats.

In the wider government sector (including the interface with industry and the public), to work out what the appropriate level of public funding is, it's necessary to make an 'apples versus apples' comparison of offline and online costs and benefits. That's much more complex than comparing the level of investment made in cyber security with losses that can be identified. The crux is to work out how the level of funding for response activities relates to the proportion of the losses that might be prevented.

The British Government went through the first part of the exercise during the development of its 2010 Strategic Defence and Security Review. The result was an increase in spending on cyber security at a time when 'traditional' defence and national security assets were being cut:

> The Government will introduce a transformative national cyber security programme to close the gap between the requirements of a modern digital economy and the rapidly growing risks associated with cyber space. The National Cyber Security Programme will be supported by £650 million of new investment over the next four years…[16]

This additional expenditure was predicated in part on the results of a study commissioned by the Cabinet Office that found that the cost to Britain of cyber crime was £27 billion per year.[17] That headline figure has to be treated with caution. Around £10 billion is ascribed to fraud, extortion and theft, all of which can be readily quantified. The remaining costs are put down to IP theft (£9 billion) and espionage (£7.5 billion). While IP can be costed (it is a saleable commodity), it's far from clear that the value is actually lost. Espionage is even harder to cost accurately. Nonetheless, it's probably accurate to conclude that the cost to Britain is some billions of pounds per year. But the level of rigour is insufficient to draw a clear link between the additional £650 million pounds to be spent and the fraction of the purported £27 billion pounds of losses that might be prevented.

Nonetheless, assuming that the cost scales with the size of the economy (a reasonable assumption for similarly developed countries), Australia's losses would be billions of dollars. The question is what is the appropriate scale of response? As noted earlier, cybercrime is often the extension of crime in the offline world. The cost of offline crime is borne collectively by governments through the provision of policing services and by the business and wider community through insurance and through the writing off of losses. To give a concrete example, it would be possible to essentially eliminate shoplifting by having a security guard in every aisle of every store—but it would be ruinously expensive compared to the losses prevented. While unpalatable, there is a level of criminal activity that will be tolerated on rational grounds. The same model will necessarily apply to cyberspace.

It's likely that there are cost-effective investments that the Australian Government could make in the realm of cyber security. But a rigorous study that takes into account losses and the cost and effectiveness of prevention, detection and response mechanisms is required to work out what those investments are.

Similarly, businesses (and individuals) have to assess their vulnerabilities and perform their own cost-benefit calculations. There's anecdotal evidence that many businesses do not understand either the costs they are incurring or the potential benefits of remediation measures. There's scope for government to run awareness raising campaigns and provide standards and tools where appropriate, but industries and individual businesses ultimately must take responsibility for their own cyber security.

Conclusions

Despite the hyperbole sometimes associated with the topic, cyber security is not an entirely new and novel threat to national security. In many ways it is an extension of pre-existing threats into a new technical domain—albeit one that is more extensive in reach and pervasiveness than its predecessors. And it moves at a prodigious rate due to the rapid rate of change of technology and the quick uptake of new technologies by users ranging from households to central government agencies.

All of those aspects present challenges to governments, where the timeframes for policy development and acquisition projects are typically longer than the market lifetime of many technologies. (Early buyers of the iPad got eleven months at the leading edge of commercially-available tablet technology.)

There's little doubt that Australia, like many other nations, has been the subject of cyber attack from criminals, hackers and foreign states. And there's no doubt that economic harm has been done and that information with national security significance has been compromised.

Despite that, the evidence available suggests that the Australian Government has the right conceptual cyber security frameworks in place, although agility in

governance structures will be required as the threat evolves and as technology blurs the lines between previously separate domains.

Whether the resource allocations are adequate or correctly apportioned is harder to judge. More work needs to be done to get a clear picture of the costs Australia is incurring, and the likely benefits that could be achieved through further investment in cyber security.

Endnotes

1 *U.S. at risk of cyberattacks, experts say*, CNN, 18 August 2008, available at http://articles.cnn.com/2008-08-18/tech/cyber.warfare_1_hackers-internet-assault-web-sites?_s=PM:TECH

2 *Capability of the People's Republic of China to conduct cyber warfare and computer networkexploitation*, report prepared for the US-China Economic and Security Review Commission, November 2009. Available at http://www.uscc.gov/researchpapers/2009/NorthropGrumman_PRC_Cyber_Paper_FINAL_Approved%20Report_16Oct2009.pdf

3 See for example *The Challenge of Aviation Security*, Stratfor.com, 16 September 2009. Available at http://www.stratfor.com/weekly/20090916_convergence_challenge_aviation_security

4 The *Stuxnet* worm has over 15,000 lines of code and is very precise in its effect, which suggests careful engineering and extensive testing. The industry standard for similar software is about 15 lines of code per programmer per day, giving an estimate of about four man-years of engineering effort. *Vanity Fair* magazine published a good popular level account of *Stuxnet* in the April 2011 edition: Michael Gross, *Stuxnet worm: a declaration of cyber war*, available at http://www.vanityfair.com/culture/features/2011/04/stuxnet-201104

5 *Surprisingly sophisticated mobile malware targets Android*, IT World, 8 February 2011, available at http://www.itworld.com/security/136344/surprisingly-sophisticated-mobile-malware-targets-android

6 http://www.finance.gov.au/e-government/security-and-authentication/gatekeeper/index.html

7 The manual is available at http://www.dsd.gov.au/publications/Information_Security_Manual_2010.pdf

8 Web site at http://www.cert.gov.au/www/cert/cert.nsf

9 The AFP's cyber-crime website is http://www.afp.gov.au/policing/cybercrime/hightech-crime.aspx

10 See the *Scamwatch* website: http://www.scamwatch.gov.au/content/index.phtml/itemId/693900

11 See http://www.ema.gov.au/www/agd/agd.nsf/Page/CyberSecurity_CyberSecurity#h2strategy

12 John Blackburn and Gary Waters, *Optimising Australia's response to the cyber challenge*, Kokoda Foundation Report No.14, February 2011, p20.

13 Including Boeing, Lockheed Martin, Northrop Grumman and Raytheon.

14 'U.S. Creates Command for Cyber Battlefield', *Defense News*, 23 June 2009, available at *http://www.defensenews.com/story.php?i=4154004*

15 *Pentagon to Help Internet Providers Get Military Cyber Tools*, Bloomberg, 17 March 2011, http://www.bloomberg.com/news/2011-03-16/pentagon-to-help-internet-providers-get-military-cyber-tools.html

16 *Securing Britain in an Age of Uncertainty: The Strategic Defence and Security Review*, British Government, 2010. Available at http://www.cabinetoffice.gov.uk/content/securing-britain-age-uncertainty-strategic-defence-and-security-review

17 *The cost of cyber crime*, Detica/UK Government Cabinet Office, 2010. Available at http://www.detica.com/uploads/press_releases/THE_COST_OF_CYBER_CRIME_SUMMARY_FINAL_14_February_2011.pdf

About the author

Dr Andrew Davies is ASPI's Operations and Capability Program Director.

About Policy Analysis

Generally written by ASPI experts, the **POLICY ANALYSIS** series is provided online to give readers timely, insightful opinion pieces on current strategic issues, with clear policy recommendations when appropriate. They reflect the personal views of the author and do not in any way express or reflect the views of the Australian Government or represent the formal position of ASPI on any particular issue.

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