The Case for a Regional Cyber Security Action Task Force

Gary Waters

The impact of increasing globalisation, greater connectivity via the internet, and increasing access to information via the World Wide Web suggest that states should look at multilateral security cooperation through fresh eyes. This necessarily encompasses the cyber domain. Indeed, cyberspace sits at the centre of many changes and new challenges that affect the security and safety of nations, societies and individuals.

Most Asia-Pacific states today recognise that they are increasingly vulnerable through their greater connectivity and dependence on cyberspace. The internet has become an integral part of the everyday lives of people in the Asia-Pacific region. Business and banking are increasingly being conducted online, which supports national and regional productivity and improved social well-being. The enormous attraction of social networking is resulting in the sharing of a lot of personal information online. While the internet offers many benefits, its use also carries several safety and security risks. It is imperative that governments, industry and individuals of the states in the Asia-Pacific take action to mitigate these risks.[1]

Cyber intrusions are occurring today, in which intellectual property, sensitive government and commercial information, and the identities of individuals are all being stolen. The threat from cyberspace is likely to worsen as it becomes more tightly enmeshed across society and within the economy. Users of the World Wide Web have increased from sixteen million in 1995 to 1.7 billion in 2010.[2] Recent media reporting indicates that figure had exceeded two billion by the start of 2011.[3]

Cyber crime affects the profitability of companies and threatens the networks over which commerce and trade are conducted. Critical services, particularly those that rely on Supervisory Control and Data Acquisition[4]

[1] The Government Response to the House of Representatives Standing Committee on Communications, *Hackers, Fraudsters and Botnets: Tackling the Problem of Cyber Crime,* Department of Broadband, Communications and the Digital Economy, December 2010, p. 1.

[2] 'A Strong Britain in an Age of Uncertainty: The National Security Strategy', Her Majesty's Government, October 2010, para 3.28.

[3] See 'Net Users Reach Two Billion', *The Canberra Times*, 31 January 2011, p. 13.

[4] Supervisory Control and Data Acquisition (SCADA) devices are used to automate tasks such as opening and closing valves in pipes and circuit breakers, monitoring temperatures and

devices, can be targeted, as can government services delivered online. Finally, terrorists use cyberspace to organise, recruit, communicate, obtain funds, and influence those most vulnerable to radicalisation.

Governments and businesses in all Asia-Pacific states need to work closely together in partnership to identify, monitor, and manage risks; deal with the vulnerabilities; enforce domestic law; strengthen international law and norms; and improve resilience. This will demand collaboration to anticipate future threats through all-source assessment, continuous scanning and early warning, and feeding that into regional policy-making through periodic risk assessments and reviews. Asia-Pacific states should collaborate on improving cyber security, and set up a regional Cyber Security Action Task Force to achieve practical progress to this end.

Dealing with the Cyber Threat

The threats arising from actions in cyberspace bear at least three characteristics—they are broad, embedded and diverse.[5] The nature of the threat is broad because any aspect that depends on cyberspace is at risk. Challenges can range from ensuring the protection of critical national infrastructure, maintaining the integrity of the financial and banking system, protecting intellectual property whether that is commercial in nature or is of national security importance, or preventing other activities that might significantly undermine the nation's ability to pursue its objectives.

Threats to cyber security arise from potential vulnerabilities in software applications, operating systems and hardware. Because this is an intrinsic feature of cyberspace and cannot be eradicated entirely, such threats are referred to as embedded. The threat in cyberspace is diverse, characterised by a large number of potential attackers or perpetrators, including nation-states, criminal gangs, independent terrorist organisations and hackers. Each poses a distinct type of threat, requiring tailored responses.

Governments and businesses can adopt a defence-in-depth approach against cyber intrusions, noting that both the information and the systems must be protected. This includes:[6]

- Static defence, such as firewalls, anti-virus software, and patches.

pressures, and managing machinery on assembly lines. SCADA device vulnerability is discussed further in Gary Waters, Desmond Ball, Ian Dudgeon, *Australia and Cyber-Warfare*, Canberra Papers on Strategy and Defence no. 168 (Canberra: Strategic and Defence Studies Centre, The Australian National University, May 2008), pp. 95-6.

[5] *National Security Threats in Cyberspace: Post-Workshop Report* (Workshop Jointly Conducted by American Bar Association Standing Committee on Law and National Security, and National Strategy Forum), September 2009, p. 1.

[6] John Blackburn and Gary Waters, *Optimising Australia's Response to the Cyber Challenge*, Kokoda Paper 14 (Canberra: Kokoda Foundation, February 2011), p.12.

- Situational awareness and active deception, which demands sophisticated technology using anomaly detection to detect threats and vulnerabilities in real-time.

- Dynamic cyber defence, which demands a sophisticated detection capability and dynamic re-configuration of systems.

- Protecting critical information from social engineering (manipulating people into divulging information) and the insider threat (malicious activity carried out by employees).

However, each layer of security also potentially represents a barrier to efficiency in operations as well as a cost that will have to be borne by someone.[7] Nations will need to learn to tolerate a certain amount of insecurity as threats are both impossible to eradicate and can be exceedingly costly to counter even to the extent where that is possible. This means that systems will need to be able to operate under the assumption that security breaches will occur, which suggests a strong emphasis on system architectures that employ multiple tiers of defences, that can be segmented when under attack, and that have sufficient resilience to allow speedy recovery.[8]

Governments need to have in place mature arrangements that ensure clarity of roles and responsibilities across their agencies in optimising cyber security so that they can prioritise and allocate resources to mitigate the various cyber threats. Governments should also ensure a coordinated policy interface with their key cyber partners—the public, industry, the jurisdictions, and international partners.

Three distinct legal regimes are potentially applicable to a government’s response to cyber threats: criminal law for law enforcement; international law, including the law of armed conflict, for war-like kinetic and cyber responses; and intelligence law for actions relating to covert actions and the collection and analysis of data about cyber adversaries.[9] But national governments generally struggle to make substantive change to their domestic laws in timely fashion. In the international context, many years have been required to simply start to construct a set of procedural rules for cyber crime that can be agreed.[10]

Need for International Action

Security across the entire cyber spectrum is a global problem that has to be addressed globally by all governments together. It is a risk that has to be

[7] *National Security Threats in Cyberspace*, p. 2.
[8] Ibid., pp. 2-3.
[9] Ibid., p. 12.
[10] Ibid., p. 13.

managed through a combination of defensive technology, astute analysis and traditional diplomacy. Governments need to take appropriate steps in their respective countries to create necessary laws, promote the implementation of security practices and incident management, develop information sharing mechanisms, and continuously educate both corporate and home users about cyber security.[11]

International cooperation at several levels is critical for making nations secure: law enforcement and information sharing to bring criminals to trial; incident management; information sharing on threats and vulnerabilities; international cooperation to create an intelligence mechanism to combat cyber threats; and private-sector cooperation across countries.[12] Acceptable legal norms for dealing with cyber crimes are needed, particularly in terms of territorial jurisdiction, sovereign responsibility, and reconciling differing national laws for investigating and prosecuting cyber crimes. The problem of existing cyber laws that do not carry enforcement provisions also needs to be addressed.[13]

Government-to-government, multilateral behaviour should be the way of the future. Interactions among National Computer Emergency Response Teams (CERTs) of multiple states can underpin this. Relationships are much easier to establish operationally through CERTs than through broader Departments of State or Foreign Affairs. These CERT-to-CERT relationships will mature and be important elements of any framework, but they will depend on a willingness to share, not just to receive. Nations might find that CERTs operate more effectively as part of a public-private partnership in future.

Asia-Pacific states have established strong engagement and beneficial relationships within some forums with respect to cyber security. The Organisation for Economic Cooperation and Development (OECD), the ASEAN Regional Forum (ARF), Asia-Pacific Economic Cooperation (APEC), International Telecommunications Union (ITU) and its development sub-committee are all involved in coming to terms with the challenges of cyber security. The Council for Security Cooperation in the Asia Pacific (CSCAP) has initiated a regional cyber study to be conducted in 2011. The challenge for regional governments is to maximise opportunities for cooperation across all of these bodies and to remain alert to those organisations and forums that could exert the greatest influence and be prepared to work with them.

In respect of cyber crime, the Council of Europe Convention on Cybercrime is the only binding international treaty on cyber crime seeking to adopt appropriate legislation and foster international cooperation. Other

[11] Kamlesh Bajaj, ‘The Cybersecurity Agenda: Mobilizing for International Action’, EastWest Institute, 17 June 2010, <http://www.ewi.info/system/files/Bajaj_Web.pdf> [Accessed 9 February 2011], pp. i, ii.
[12] Bajaj, ‘The Cybersecurity Agenda’, pp.1-2.
[13] Ibid., p. ii.

international collaborative activities to combat cyber crime have evolved, such as the London Action Plan, which is the preeminent international collaboration on anti-spam that also fosters links between international law enforcement authorities.

These developments highlight that international consensus can be reached over time, and effective action can be taken. The challenge from here is to broaden such cooperation and reduce the time taken from concept to action.

Improving Collaboration in Cyber Security

There are different approaches that nations can take to cyber security, perhaps best illustrated by the US and Russian approaches: the United States focuses on a law enforcement approach at the domestic level with voluntary international collaboration, while Russia focuses on developing binding international regimes. There are also quite different philosophies at work: Russia favours social control of the internet as a medium, while the United States, for the most part, does not.[14]

Despite these differences, the United States and Russia agreed in December 2009 at a meeting of the United Nations Committee on Disarmament and International Security to begin talks on strengthening internet security and limiting military use of cyberspace. They identified possible areas of cooperation such as public key infrastructure, rapid response to cyber crime, and deliberation on international cyber law, that together with another key initiative identified during a cyber security workshop held in Singapore in July 2010[15] can be used as a basis and developed further to broaden multilateral cyber cooperation in the Asia-Pacific:

- *Public Key Infrastructure*: Asia-Pacific states should champion in the International Telecommunication Union (ITU) the idea of a binding multilateral agreement on Public Key Infrastructure (PKI) to promote internationally a system of trusted identities. There can be no exclusively national system of trust because of the global interdependence of cyberspace. Some form of trusted centre is needed to deal with the attribution problem as without it there can be no real progress on PKI.

- *Cyber crime emergency response*: Asia-Pacific states should develop around-the-clock contacts for combating high-tech crime, including

[14] Franz-Stefan Gady and Greg Austin, 'Russia, the United States, and Cyber Diplomacy', EastWest Institute, 14 September 2010, <http://www.ewi.info/system/files/USRussiaCyber_WEB.pdf> [Accessed 9 February 2011].

[15] Ng Sue Chia (ed.), 'Towards a Secure and Resilient Cyberspace', Report on the workshop jointly organised by the Centre of Excellence for National Security (Singapore) and the Global Futures Forum (International) with the support of The National Security Coordination Secretariat (Singapore), 12-13 July 2010.

support for a global program of capacity building in law enforcement and cyber investigation for all countries connected to the internet.

- *International cyber law*: Asia-Pacific States should undertake joint policy assessments of legal aspects of regulating cyber warfare activities, especially in the area of critical infrastructure and rules of engagement. In terms of international cyber crime, the existing jurisdictional differences through inconsistent laws and legal systems, law enforcement processes and priorities, the different rules of disclosure for information sharing arrangements, and the different levels of capacity and resourcing, all need to be addressed.

- *An operational definition of cyberspace* would reduce conceptual ambiguity and allow for workable solutions to be devised.

Improving international cooperation in securing critical information infrastructure could start with the following set of actions:[16]

- *Trusted identities:* Develop a private-public forum to discuss issues concerning certificates, authentication and other aspects of civilian security infrastructure.

- *Emergency warning networks:* Determine the best approach for countries to develop emergency warning networks regarding cyber vulnerabilities, threats, and incidents.

- *Awareness raising:* Determine the best approach for raising awareness to facilitate stakeholders' understanding of the nature and extent of their critical information infrastructures, and the role each must play in protecting them.

- *Threat assessment:* Identify the key infrastructures and any interdependencies that exist among those infrastructures, and decide the actions needed to enhance the protection of these infrastructures, including interdependencies.

- *Private-public partnerships:* Determine the best approach for promoting partnership among stakeholders, both private and public, to share and analyse critical infrastructure information in order to prevent, investigate, and respond to damage or attacks on such infrastructures.

- *Crisis communication networks:* Determine the best approach for creating and maintaining crisis communication networks and for testing them to ensure that they remain secure and stable in emergency situations.

[16] Gady and Austin, 'Russia, the United States, and Cyber Diplomacy'.

- *Tracing attacks:* Determine the best approach for tracing attacks on critical information infrastructures, as well as those measures that can be used to best facilitate the disclosure of that attack-tracing information between countries.

- *Preventing dissemination of illegal or dangerous information:* Websites are ideal tools for disseminating information and disinformation on a regional or global scale. Terrorist groups increasingly use the Internet for their propaganda as well as recruitment. Electronic mail has become one of the most important forms of communication in the world. Terrorists can take advantage of the anonymity and accessibility of cyberspace. Determine the level of cooperation and the consequent actions between the private and public sectors needed to prevent the use of the internet for terrorist purposes.

A Regional Cyber Security Action Task Force

Countries have little to lose by talking with one another even though they will need to develop separate agendas and strategies in certain areas. Together, the Asia-Pacific states could seek to create a stronger set of international regimes to fight crime in cyberspace and secure the internet's underlying technologies. The Asia-Pacific states could show leadership by securing their national networks, ensuring their systems are not being used in international cyber intrusions, and cooperating on criminal investigation of cyber intrusions with foreign victims.[17]

States cannot call on others to take action without also curbing cyber criminals at home and taking steps to reduce malicious activity on their networks. This means that states should be expected to secure their networks to a reasonable standard, pass laws outlawing international cyber crime, and have mechanisms in place to act on requests for assistance in shutting down attacks, and investigating and prosecuting them.

Multilateral initiatives are needed that provide countries with assistance in developing legal frameworks and enforcement capabilities, a mechanism for judging the effectiveness of national efforts at combating cyber crime, and a process that provides both positive and negative incentives that promote adherence to international legal standards.[18]

Diplomatic initiatives like the OECD's Financial Action Task Force (FATF) have used international standards and shaming to cause countries to improve their responses to money-laundering issues. The FATF allows member states to cooperate in setting standards, monitoring compliance with

[17] This is broadly consistent with that argued in Robert K. Knake, *Internet Governance in an Age of Cyber Insecurity*, Council on Foreign Relations, Special Report no. 56, September 2010, pp. 3-4.

[18] Knake, *Internet Governance in an Age of Cyber Insecurity*, p. 16.

those standards, and identifying new and ongoing financial threats.[19] A similar effort would yield useful results in the cyber domain.

A regional Cyber Security Action Task Force (CSATF) should be established to deal with cyber crime and could begin by developing model policies based on the Council of Europe Convention, the ITU Toolkit for Cybercrime Legislation, and other recognised best practices. Once the recommended policies have been developed in the first year, the organisation could begin assessing member countries against the developed standards. The assessments could also provide a roadmap for correcting any problems identified and establish a process for periodic review of progress made in addressing the identified problems.[20]

The CSATF could operate in similar fashion to the FATF, which began by establishing a set of forty recommended policies that countries should adopt. FATF quickly expanded, and now covers thirty-four countries that together account for most global financial transactions. With an accepted set of standards and objective mechanisms for monitoring compliance, the FATF has created the basis upon which countries can threaten non-compliant nations with the loss of access to international financial networks.

The CSATF could also conduct an annual global review of both member and non-member countries that assesses countries' legal frameworks, enforcement capabilities, and overall levels of cyber crime. For other transnational problems, compiling an annual index or report of the best and worst states based on objective metrics has prompted many states to improve their behaviour. Such rankings would be an effective mechanism for 'naming and shaming' countries to address cyber criminal activity and to become members of the new organisation. Countries that do not clean up their cyberspace could have their international internet traffic subjected to deep packet inspection or other higher levels of scrutiny that would slow the flow of the traffic. As a last resort, failure to improve could result in the blacklisting of national IP ranges of the worst offending states.[21]

The CSATF could institute a set of planning processes that promote the development of members' cyber defence capabilities. These processes could optimise information sharing, collaboration and interoperability. The CSATF could also assist individual members upon request. The CSATF would not develop specific technologies, which would remain the responsibility of individual members; although, there would be scope for the CSATF to facilitate sharing of technologies.

[19] *National Security Threats in Cyberspace*, p. 26.
[20] Knake, *Internet Governance in an Age of Cyber Insecurity*, p. 19.
[21] Ibid., pp. 19-20.

Finally, the CSATF could persuade states to focus not only on limiting the development of cyber weapons, but, more importantly, to also focus on limiting state actor penetration into civilian systems that have limited, if any, intelligence or military value. If cyber attacks become an acceptable form of international conflict, the effects could be extremely destabilising economically and could lead to conventional military conflict. International agreements to set power grids, the financial sector, and other components of civilian infrastructure off limits would be in the interests of most nations. In addition, proposals could be developed to address separately the security and sanctity of root operations that allow the internet to function, and to improve internet governance.[22]

It will be important for the CSATF to forge strong links with the International Multilateral Partnership Against Cyber Threats (IMPACT) that was established in Cyberjaya, Malaysia, in 2009. IMPACT hosts the ITU's Global Cyber-security Agenda (GCA), which promotes international cooperation to make cyberspace more secure. The CSATF would need to establish strong links with the ITU in a strategic and policy sense and with the GCA in an operational sense, leveraging the ITU's capability for early warning, crisis management, and real-time analysis of global cyber threats.

A key consideration would be the leadership and political framework for the CSATF. The ARF might appeal as an option; however, while it has achieved much over its seventeen years the ARF has struggled in dealing meaningfully with sensitive issues, and gaining traction has been inhibited through the lack of a Secretariat. In this latter respect, Barry Desker[23] has recommended expanding the ASEAN Secretariat to provide financial, economic and law enforcement cooperation to the ARF more broadly and co-locating it with the APEC Secretariat. Indeed, an important initial step has been taken already with the establishment of an ARF Unit within the ASEAN Secretariat; although the Unit's role is to support the ARF Chair and some eight years were needed to move from initial proposal to establishment of the Unit.

The Secretary General of the ASEAN Secretariat has been able to show genuine leadership in implementing ASEAN-agreed actions, which could be broadened to support the ARF if the ASEAN states agreed. Significant additional resources would be required, however, to make this work.

An ARF Secretariat built around an expanded ASEAN Secretariat could also forge stronger and closer links with the ASEAN-Plus Defence Ministers' Meeting (ADMM+) which brings together Defence Ministers from the ten

[22] Ibid., p. 23.

[23] Barry Desker, 'CSCAP: Shaping the Future of the ASEAN Regional Forum', in Desmond Ball and Kwa Chong Guan (eds), *Assessing Track 2 Diplomacy in the Asia-Pacific Region: A CSCAP Reader* (Singapore: S. Rajaratnam School of International Studies and Strategic and Defence Studies Centre, Canberra, 2010), pp. 237-8.

ASEAN nations plus Australia, China, India, Japan, New Zealand, Republic of Korea, Russia and the United States. The ADMM+ will strengthen and deepen trust and cooperation on defence and security matters throughout the Asia-Pacific region, and while its initial focus will be on counter-terrorism, humanitarian and disaster relief, maritime security, and peacekeeping, one could anticipate that cyber will be added to its agenda sooner rather than later.

Another option might be to use the ARF to provide political leadership and move to some form of a public-private partnership that might be managed by a small cadre of regional countries such as Australia, Singapore, Malaysia, India and Indonesia. It is through just such a public-private initiative that IMPACT was set up. Bringing together governments, industry leaders and cyber security experts within the region and working closely with the ITU and IMPACT, the CSATF could improve the Asia-Pacific's capacity to prevent, defend and respond to cyber threats and improve the cyber security of the region's governments, private sectors and societies.

Conclusion

Cyber has intruded into so many aspects of everyday business and life. It provides wonderful opportunities but brings with it attendant vulnerabilities. It is an intrinsic part of globalisation and thus the challenges around optimising cyber for the benefit of all need to be addressed globally. The states of the Asia-Pacific can take a lead in this respect by developing a regional approach to a safe and secure cyber environment.

There are several broad areas that could usefully come together and serve as an agenda for multilateral cyber cooperation in the Asia-Pacific. There are also several actions that could be carried out cooperatively and quickly for securing critical information infrastructure. This should all be brought together effectively through a regional Cyber Security Action Task Force which would provide a useful focus to practical cyber cooperation in the Asia-Pacific to the benefit of all regional states. The CSATF might best be initiated as a public-private partnership, led by a small cadre of regional states, within the overall political framework of the ARF.

Dr Gary Waters is currently Head of Strategy for Jacobs Australia. He also consults in the areas of strategy, national and cyber security, capability development, risk management, preparedness and logistics. Gary served for thirty-three years in the Royal Australian Air Force (retiring as an Air Commodore) and for four years as an SES officer in the Australian Public Service. He has written over a dozen books on doctrine, strategy and historical aspects associated with the use of military force. His latest book released in February 2011, co-authored with Air Vice Marshal John Blackburn, is entitled Optimising Australia's Response to the Cyber Challenge*. Gary gained his doctorate in political science and international relations from the Australian National University.* Gary.Waters@jacobs.com.au.