NATIONAL CYBERSECURITY STRATEGIES: AUSTRALIA AND CANADA

JOÃO MANUEL ASSIS BARBAS

Coronel de Artilharia. Assessor de Estudos do IDN

INTRODUCTION

Globalization and information and communication technologies are two inseparable drivers of modern societies. Initially, the establishment of internet facilitated the integration of business networks with equipment from multiple vendors, facilitating internal communication, improving efficiency and productivity. Later and progressively, as internet became the global communications network, business, industries, cities and countries became also global, and easily accessible through a device with a simple browser.

As the use of technology expanded and facilitated globalization, information and technology also became global and more exposed to security breaches, easily explored by states or non-state actors.

Over the last years, especially since the cyber-attacks to Estonia (2007) and Georgia (2008), many countries published their National Cybersecurity Strategies, reflecting a progressive concern and understanding of the potential consequences of cyber incidents on their economies and social tissue.

These documents express principles and values, set strategic objectives and lines of action, driving their national approaches to cybersecurity. The purpose of this first article is to analyse the Cybersecurity strategies of two non-European countries - Australia and Canada - looking at their main building blocks and whenever possible identify trends and common elements.

Australian Cybersecurity Strategy

On December 4th 2008, the Australian Prime Minister, Kevin Rudd, on his first National Security Statement to Parliament, recognized publicly Australia's dependency on information technology making her potentially vulnerable to cyber-attacks by terrorists, exploiting internet to "operate beyond the law." He also stressed that the country should be prepared to "respond to new and emerging threats" and that partnerships between industry, governments and the community were vital to the national security policy (Rudd, 2008)

The Australian Cybersecurity Strategy articulates the aim and objectives of the Government's cyber security policy, identifies the strategic priorities to achieve these objectives and describes key actions to be undertaken.

The document recognises:

- Security, economic prosperity and social wellbeing depend of information and communications technologies;

- The high risk of computer intrusion and the use of malicious code by organised crime, in special on financial and commercial transactions and personal data;

- Threat Actors[1] are changing;

- The attribution of the source of attacks is hindered, due to internet's nature;

- The need to balance between risks and civil liberties, promoting efficiency and innovation;

- Online protection is not limited to the computer security but also depends of personal practices.

Aim

The aim of the Australian Cybersecurity policy is "the maintenance of a secure, resilient and trusted electronic operating environment that supports Australia's national security and maximises the benefits of the digital economy". Though its focus is on the "availability, integrity and confidentiality of Australia's ICT [Information and Communications Technology]" it should be articulated with other related policies, such as: cyber safety, identity security and privacy (Australian Government, 2009).

Principles

In accordance with the "enduring principles" of the National Security Statement the guiding principles of the Cyber Security Policy are: national leadership, shared responsibilities, partnerships, active international engagement, risk management and protecting Australian values (Australian Government, 2009).

Objectives

The strategy establishes the following key objectives:

- *"All Australians are aware of cyber risks, secure their computers and take steps to protect their identities, privacy and finances online".*

This objective focus on the promotion of a "robust" cyber security culture to increase awareness and confidence, essential to optimise the benefits and minimise the risks of the digital economy; reduce cyber-crime impact; mitigate threats to national critical systems; and improve security and resilience of web environment.

- *"Australian businesses operate secure and resilient information and communications technologies to protect the integrity of their own operations and the identity and privacy of their customers".*

Considering the majority of the national critical systems are owned by private sector, it is recognized the need to influence their policies and practices and identify those most critical to the national interest[2], based on a risk assessment. This requires the cooperation between Government and the owners and operators of critical systems and is capitalized through trusted information exchange mechanisms with mutual benefits.

- *"The Australian Government ensures its information and communications technologies are secure and resilient".*

Governmental ICT and associated information are considered a strategic national asset thus requiring security and resilience. A proactive approach identifying threats and vulnerabilities, developing mitigations strategies and creating an integrated framework[3] is to be developed by Government.

Strategic Priorities

To pursue these objectives the following mutually supporting strategic priorities are identified:

- *"Threat awareness and response: Improve the detection, analysis, mitigation and response to sophisticated cyber threats, with a focus on government, critical infrastructure and other systems of national interest."*

This priority encompasses initiatives to monitor threats, including:

- Establish of a Cyber Security Operations Centre (CSOC);
- Setup a new national Computer Emergency Response Team (CERT);
- Information sharing within and between public and private sectors, nationally and internationally, to facilitate situational awareness and threat response;
- Development of a cybersecurity crisis management plan;
- Implementation of a cybersecurity programme of exercises.

- *"Cultural change: Educate and empower all Australians with the information, confidence and practical tools to protect themselves online."*

This priority includes education and awareness raising activities such as:

- Cyber security information for home users and small business (www.staysmartonline.gov.au);
- Dissemination of information on cyber security threats, vulnerabilities and protection measures released by CERT;
- Dissemination of anti-spam practical tools and procedures;
- Promotion of an Internet service provider (ISP) Code of Practice to deal with cyber security issues;
- Implementation of cyber security education modules for primary and secondary education;
- Analyses of alternatives to "inform and educate" people on common cyber risks;

- *"Business-government partnerships: Partner with business to promote security and resilience in infrastructure, networks, products and services."*

This priority recognises that government and private sector must cooperate for the provision of secure products and services and maintenance of ICT infrastructures to secure customer information. It stresses the vulnerabilities in critical infrastructure and other systems of national interest covering initiatives to enable greater situational awareness.

The following actions are included:

- Strengthen trusted partnerships with the private sector to support cyber information sharing;

- Reinforce engagement with the commercial Internet industry to raise awareness on cyber risks, threats and vulnerabilities;
- Promotion of business continuous improvement to cyber security and critical infrastructure protection;
- Creation of a Critical Infrastructure Protection Modelling and Analysis (CIPMA) program;
- Promotion of education and training opportunities for industry representatives;

- *"Government systems: Model best practice in the protection of government ICT systems, including the systems of those transacting with government online."*

This priority addresses the protection of governmental and interconnected government systems and the reforms to the procurement of ICT and includes:

- Analysis of alternatives to reduce governmental internet gateways;
- Establishment of minimum security standards across government;
- Centralization of the procurement and management of ICT products and services;
- Risk assessment of major ICT projects;
- Promotion of security of governmental systems;
- Revision of the Australian Government's Protective Security Manual for adoption of commercial standards and best practices;

- *"International engagement: Promote a secure, resilient and trusted global electronic operating environment that supports Australia's national interests."*

International cooperation[4] is considered essential to improve networks security, develop standards, raise international legal system's ability to combat cybercrime, and disseminate best practices through a set of initiatives that include:

- Establishment of bilateral or multilateral agreements with "key allies";
- Regional capacity building initiatives;
- Participation on international organisations;
- Development of an international engagement strategy;

- *"Legal and law enforcement: Maintain an effective legal framework and enforcement capabilities to target and prosecute cyber-crime."*

As economy and society are affected by cybercrime, several issues are addressed, including the consolidation of the legal framework, the investigation and law enforcement capabilities and a "technically-aware" legal system, involving a wide range of measures such as:

- Enhance operational cyber capabilities of security and law enforcement agencies;
- Improve cooperation between cyber security and law enforcement through;
- Maintenance of the criminal and civil legal framework in accordance with the evolution of the technology and the conduct of criminals;
- Improve law administration though the provision of access to information and resources to legal professionals;
- Harmonization of the legal framework to smooth sharing of information and improve law enforcement cooperation.

- *"Knowledge, skills and innovation: Promote the development of a skilled cyber security workforce with access to research and development to develop innovative solutions."*

It is recognized the need of technically qualified human resources supported by innovative research and development to deal with future threats. This priority involves a set of initiatives to develop and retain that expertise within government and to mobilize the research community, such as:

- Setup of new recruitment and retention approaches;
- Funding of specific cyber security research and development activities;
- Setting annual priorities for Research and Development to inform science and innovation community;

The attachment A to the Australian Cybersecurity Strategy includes additional information about the CERT Australia, the Cyber Security Operations Centre and Government Agencies which will have an important role in the strategy's implementation.

Canada's Cyber Security Strategy

The Cyber Security Strategy recognizes that Canadian economy heavily depends on the Internet. Federal Government offers many online services and businesses are adopting most of the modern digital technologies and appliances. Cyberspace[5] is considered one of the "greatest national assets" (Government of Canada, 2010) requiring the protection of cyber systems – a extremely challenging task due to the difficulty to detect, identify and recover from attacks that have no "physical evidence" (Government of Canada, 2010).
The strategy identify power grids, water treatment plants and telecommunications networks as potential targets of sophisticated attackers, that may also affect the production and distribution of basic goods and services and undermine privacy. To address these threats Canadian Government is working with provinces[6], territories[7] and the private sector, having in mind that 86% of the Canadian organizations already suffered cyber-attack resulting in increasing loss of intellectual property (Government of Canada, 2010).

Cyber Threats

The strategy assumes four common characteristics of cyber-attacks:

- They are inexpensive, as many tools can be purchased or downloaded from Internet;
- They are easy to perform, as hackers with basic skills can cause extensive damage;
- They are very effective as minor attacks may

have significant impact;

- Low risk for attackers as they can avoid detection and legal prosecution.

Three types of threats are analysed in the document, having in consideration their targets, methods, motivations and intentions.

"State sponsored cyber espionage and Military Activities"

- Background: Existing reports confirm these attacks were extremely successful stealing industrial and state secrets, private data and other valuable information. For some states, they are a central element of their military strategy, to sabotage adversary's [critical] infrastructures and communications.
- Source: intelligence and military services from foreign states;
- Objective: gain political, economic, commercial or military advantage;

"Terrorist use of the Internet"

- Background: Cyberspace is being used by terrorist networks because they are aware of the Western World's dependence on cyber Information Systems.
- Source: Terrorist networks;
- Objective: Support recruitment, fundraising and propaganda.

"Cybercrime"

- Background: Criminals are shifting and expanding their operations to cyberspace. The most sophisticated cyber-criminals among them have been pursuing their illegal activities in Internet such as selling information stolen online, like debit credit cards, login passwords and malicious software;
- Source: Organized criminals (skilled cyber attackers)
- Objective: identity theft, money laundering and extortion.

Vision

"Canada's Cyber Security Strategy will strengthen our cyber systems and critical infrastructure sectors, support economic growth and protect Canadians as they connect to each other and to the world. We all have a role to play as we take full advantage of cyberspace to build a safe, resilient and innovative Canada" (Government of Canada, 2010).

Principles

The guiding principles identified in the strategy are considered to be aligned with the ones from some of Canada's closest "security and intelligence partners" (Government of Canada, 2010):

- Canadian values (e.g. rule of law, accountability and privacy);
- Continuous improvement to meet emerging threats;
- Integration of activities across the Government;
- Partnerships with citizens, Provinces, Territories, business and academy; and
- International cooperation with allies.

Pillars & Specific Initiatives

"Securing Government Systems"

Recognising the trust of citizens and private sector in Government for the protection of personal and corporate sensitive data, the availability of services, sustain national cyber sovereignty and economic interests, the strategy expresses the following initiatives:

- Establishment of "Federal Roles and Responsibilities". Under this initiative are given the following responsibilities:
  - Public Safety Canada: Coordination of the strategy's implementation on a "whole-of-government" approach.
  - Cyber Incident Response Centre: Monitoring and advice on cyber threats; direct reaction to cyber incident; and lead public awareness and outreach.
  - Communications Security Establishment Canada: Threat's detection and discovery; provision of foreign intelligence and cyber security services; reaction to cyber threats and attacks.
  - Canadian Security Intelligence Service: analysis and investigation of domestic and international threats.
  - Royal Canadian Mounted Police: Investigation of suspected domestic and international criminal activities against networks and critical information infrastructures.
  - Treasury Board Secretariat: Development of policies, standards and assessment tools to support cyber incident management capabilities and IT security within Government institutions.
  - Foreign Affairs and International Trade Canada: Advise on cybersecurity international aspects and policy.
  - Department of National Defence and the Canadian Forces: Defend own networks; cooperation on threats' identification and response; cooperation with allies for the exchange of best practices and the development of policies and frameworks.

-"Strengthening the Security of Federal Cyber Systems". The Canadian Government emphasises the continuous investment on expertise, technology and governance; self-monitoring of electronic operations; and technological risk reduction.
- "Enhancing Cyber Security Awareness throughout Government". Specific measures are not identified under this initiative. However, it recognises the success on securing Governmental systems depends of individual practices.

"Partnering to secure vital cyber systems outside the Federal Government"

Economic prosperity requires the normal operation of non-governmental systems and the security of intellectual and business property, transactions and

data; services and infrastructures. For that purpose, initiatives to reinforce global cyber resilience such as on critical infrastructures, improve global cybersecurity posture and information sharing, are to be undertaken.

- "Partnering with the Provinces and Territories." Partnerships are considered essential at all levels of government for the implementation of a comprehensible cyber strategy. Therefore, focus on education for the promotion of awareness and the security of private information and services delivered by central and regional authorities, is addressed under this initiative.
- "Partnering with the Private Sector and Critical Infrastructure Sectors". Existing cooperation between public and private sectors should be expanded on critical infrastructures, process control systems, training and exercises and sharing best practices.

"Helping Canadians to be secure online"

The strategy will pursue initiatives to assure that citizens may have access to protection information and will reinforce capabilities to combat cybercrime.

- "Combatting Cybercrime". To combat transnational cybercrime, Canada requires additional investigation powers and resources. A centralized Integrated Cyber Crime Fusion Centre was envisaged (and established in 2011) and additional legislative reforms were considered.

- "Protecting Canadians Online". The strategy ultimate goal is to develop a culture of safety in cyberspace and to promote awareness of security practices and of common cybercrimes.

CONCLUSIONS

The establishment of partnerships between public and private sectors, international cooperation with allies and the protection of national values are common principles of the two strategies. The objectives of both strategies, although with different structures, are similar and focus on a cybersecurity culture to improve cyber awareness; strengthen security and resilience of Governmental ICT and private sector, in special the owners and operators of critical infrastructures; reinforce the cooperation between public and private sectors associated with information sharing mechanisms; expansion of internal capabilities to detect, analyse and mitigate threats; reform national legal frameworks to better deal with cyber-criminals and actively engage with allies as cyber threats are not limited to borders.

The Australian strategy emphasizes the need of a strong national leadership, sharing of responsibilities and risk management, recognizing that dealing with cyber threats requires a clear engagement of all society and it is not possible to secure everything.

The Canadian strategy highlights the integration of activities across the Government and continuous improvement.

It suggests cooperation and sharing of responsibilities between public sector entities. Continuous improvement assumes the existence of a lessons learned capability and an associated information sharing framework.

NOTES

[1]"Hackers, terrorists, organised criminal networks, industrial spies and foreign intelligence services" (Australian Government, 2009).

[2]Systems of national interest are defined as "systems which, if rendered unavailable or otherwise compromised, could result in significant impacts on Australia's economic prosperity, international competitiveness, public safety, social wellbeing or national defence and security" (Australian Government, 2009).

[3]Policies, procedures and technical standards (Australian Government, 2009)

[4]United Nations and the International Telecommunication Union (ITU), regional forums and specific international groups (e.g. Forum of Incident Response and Security Teams (FIRST) and the International Watch and Warning Network (IWWN) (Australian Government, 2009).

[5]"Cyberspace is the electronic world created by interconnected networks of information technology and the information on those networks. It is a global commons where more than 1.7 billion people are linked together to exchange ideas, services and friendship." (Government of Canada, 2010).

[6]Alberta, British Columbia, Manitoba, New Brunswick, Newfoundland and Labrador, Nova Scotia, Ontario, Prince Edward Island, Québec, Saskatchewan.

[7]Northwest Territories, Nunavut and Yukon.

REFERENCES

Australian Government (2009). *Cyber Security Strategy.* Available at: http://www.ag.gov.au/RightsAndProtections/CyberSecurity/Documents/AG *Cyber Security Strategy* - for website.pdf.

Government of Canada (2010). *Action Plan 2010-2015 for Canada's Cyber Security Strategy.* Available at: http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ctn-pln-cbr-scrt/ctn-pln-cbr-scrt-eng.pdf.

Government of Canada (2010). *Canada's Cyber Security Strategy: For a Stronger and More Prosperous Canada.* Available at: http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/cbr-scrt-strtgy-eng.pdf.

Rudd, Kevin (2008). *The First National Security Statement to the Australian Parliament.* Available at: http://www.royalcommission.vic.gov.au/getdoc/596cc5ff-8a33-47eb-8d4a-9205131ebdd0/TEN.004.002.0437.pdf.