SECU-149
3.30
20 Fev. 2019

Cybersecurity in the financial sector as an economic security issue

Submission to the House of Commons Committee on Public Safety and National Security

Professor Jill Slay, La Trobe Optus Chair of Cyber Security

Introduction

In this brief, I look at some key cyber security challenges that I believe both Australia and Canada (and to some extent other 5 Eyes partners) are facing and offer some recommendations to deal with these challenges.

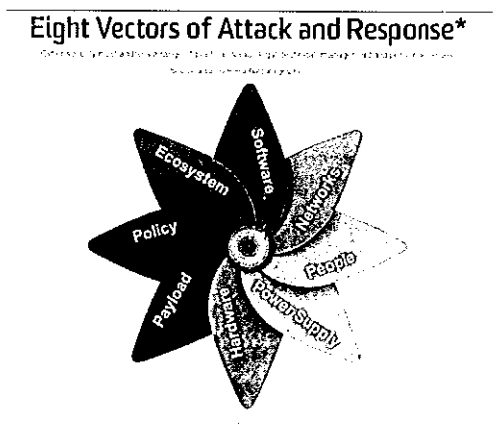
- Development of a clear understanding of the nature of cyber threat
- Cyber Security as part of National Security
- Developing a clear and culturally appropriate set of National Cyber Security certifications (summary of Australian Computer Society work)
- Developing an appropriate academic and government research agenda in cyber security especially machine learning for cyber, other AI approaches and IoT security

Background

One of the major cyber security problems that Australia, Canada and allies contend with is the large volume of attacks on government, industry and home users. While some are targeted and of high value, the trend across the board is one of uncontained growth in threat level, and exponential growth in economic cost. These national problems were brought into stark focus in May of 2017 during the WannaCry ransomware campaign. According to a Europol report (2017), the attack affected an estimated 200,000 computers worldwide by encrypting them and demanding a payment in cryptocurrency. In the UK, the National Health Service alone had 70,000 devices affected including MRI scanners, blood-storage refrigerators and theatre equipment. An estimate puts the world-wide economic cost of WannaCryat $4 billion.

WannaCry's spread was halted due to a programming limitation, but what would have happened if that limitation did not exist? What if WannaCry had targeted our Systems of National Interest? Most importantly, how will Australia and Canad defend against the next, more sophisticated version of WannaCry? How will we deal with issues of cyber intelligence and the human interpretation of the threat that this intelligence conveys? How will we respond under attack? How do our National Security policies support the implementation of appropriate solution? Who will do the research and practice in this specialised field?

There are a large number of issues that I touch on here but, in 10 minutes, I will touch on 3 of them.



Development of a clear understanding of the nature of cyber security

Cyber security is a term that is still misunderstood and it is often seen as 'computer and network security'. When we think of the economic security issues we face, we have to consider the cross-disciplinary nature of cyber security.

'Cyber security' has at least eight foundational components, some of which are narrowly technical (but involve people and organizations); and others of which are simultaneously technical and deeply dependent on non-technical inputs. One view of these ingredients is captured here in a graphic which describes them as vectors of attack and response. This graphic is adapted from an approach developed by engineers in Bell Labs to address problems of defence of connected computers and devices (Gupta and Buthmann 2007). This concept provides understanding of what shapes cyber security and the nature of cyber defence. There is also a wider national perspective since strategy and planning for cyber security depend on the political, legal and social environment as much as they do on engineering and systems approaches, as conceived in the original Bell Labs work.

Cyber Security as part of National Security

Cyber security is, to some at least, still a portion of computer science and a theoretical science looking for formal solutions. In academia in particular, the link between Cyber Security, Cyber Defence, Espionage and Foreign Interference are important linked concepts that are only beginning to be understood.

Cyber security (or cyber warfare) for National Security and Defence is a fairly new concept to technical experts. Cyber security, as a national security issue, was identified first in Australia in the Defence White Paper of 2000 (Defence 2000). The Howard government in 2001 launched an E-Security Initiative, which formed collaboration between federal government agencies, and the Trusted Information Sharing Network, representing major sector groups that were identified as critical infrastructure for the purposes of national security (Parliament 2013). The Rudd Government reviewed Australia's e-security policies, programs and capabilities in 2008. The table below summarises the cyber security initiatives since 2008, the source of policy or advice, and the implications for research and the professional workforce.

Cyber Security Need	Putative Policy/Advice Sources	Socio-Technical Research implications
• Cyber Security • Cyber Warfare and Cyber Defence • Cyber Intelligence and Espionage	• Australian Signals Directorate Top 4 Strategies (ASD 2013) • Defence White Paper 2016 (Defence 2016) • Defence White Paper 2009 (Defence 2009) • ASIO Report to Parliament 2011/12 (ASIO 2012) • ASIO Strategic Plan 2013-16 (ASIO 2013)	Cohort of innovative academic researchers, government and industry leaders in: • Network and data security • Incident response and digital forensics • Software development and reverse engineering • Cyber effects • Open-source Intelligence • Law and Policy • International Defence and Security relations

- The policy and advice of the last eighteen years in Australia (and I believe Canada will not be different) have suggested the need for a highly qualified workforce to deal with cyber warfare, defence, security and to protect all aspects of society.
- My research, and knowledge of the Australian context, indicates that there is limited research in Cyber Security for Australian National Security.
- There is no public-domain link between the National Security Agenda and technical research outputs that continue to be funded, but not necessarily applied.
- There is no established framework on which this kind of relationship may be built, and, while there is an interest in researching new and challenging cyber security issues such as Defensive Cyber Operations, automated Cyber Intelligence and evidence collection, deception and some of the human issues involved, there is no credible and sustained national research focus on the issue of linking the technical cyber security and Defence, law and policy agendas.

Advice

- There is a need to create a framework to specify how the Cyber Security and Cyber Defence of Canada's economy and its Critical Infrastructure might be carried out, incorporating technical, socio-technical and policy perspectives, and to test and validate this framework.
- The alternative to using such a framework is a piecemeal approach to academic cyber security research which draws on the strengths of an individual researcher or research leader and their track record. This work might be publishable in a good outlet, but misses out on providing a solution that is both theoretically cutting-edge, and also devices or techniques that are immediately usable by the National Security community, and potentially commercialisable.

National Cyber Security Professional Standards, Common Body of Knowledge, Curriculum and in

Australian Computer Society is national computing and cyber accrediting, curriculum and ICT standards body with around 40,000 members. It has worked on a set of National Professional Standards in Cyber Security so that Australia can answer the question 'Who is a cyber security professional?' and "What kind of skillis does Australian need in tis cyber security professionals

National Professional Standards

These were launched in September 2017 after work by the ACS Task force at the request of Prime Minister's Special Advisor / Head of ACSC Alastair MacGibbon. The standards have been implemented, assessors recruited and trained and there is teady flow of new members taking the opportunity to achieve this certification. Candidates come from Australia and SE Asia and from a range of cyber security and IT backgrounds. In summary the standards, gained from synthesis of NIST, ISC2 and ISACA work provide an Australian focused certification:

Certified Professional - Cyber Security

Cyber security specialism assessment requirements are equivalent to existing ACS Certified Professional assessment criteria and pathways with the addition of demonstrating in-depth competence in 4 SFIA skills at SFIA level 5.

SFIA skills must be from the following skills:

- IT Governance
- Information Management
- Information Security
- Information Assurance
- Business Risk Management
- Penetration Testing
- Security Administration
- Programming/Software Development
- Systems Software
- Testing
- Asset Management

Certified Technologist - Cyber Security

Cyber security specialism assessment requirements are equivalent to existing ACS Certified Technologist assessment criteria and pathways with the addition of demonstrating in-depth competence in 3 SFIA skills at SFIA level 3.SFIA skills must be from the following skills:

- Information Management
- Information Security
- Information Assurance
- Business Risk Management
- Systems Development Management
- Asset Management
- Change Management
- Security Administration
- Incident Management
- Conformance Review

We also have 2 projects developing micro-credentials and academic curriculum guidelines in for cyber security. I would suggest that Canada also needs the same so as to determine the nature of the work force and to ensure that curriculum matches workforce need. I see these as major issues to share but can also answer questions on other research issues such as Critical Infrastructure , IoT and Deception Systems.