Briefing paper

June 2011

ARC Centre of Excellence in Policing and Security

Technological advances often outstrip governmental capacity to regulate, creating infrastructure vulnerabilities and opportunities for criminal exploitation and wrongdoing. These emerging threats and risks are compounded by the fact that new technologies (such as cloud computing) transcend borders. This environment poses serious challenges for policy makers and practitioners alike. On 30 June 2010, the Australian Government released its Critical Infrastructure Resilience Strategy which recognised 'the importance of engaging with the research sector to ensure policies and approaches remain responsive to change and identify and mitigate knowledge gaps identified by critical infrastructure stakeholders. The Government will foster a stronger relationship between the owners and operators of critical infrastructure and the research community to ensure the research needs of critical infrastructure stakeholders on a range of security issues are being met."

This Briefing Paper profiles the CEPS workshop on Information Technology Systems – Security and Risk held in early 2011. stimulated a rich set of ideas, as well as forging new partnerships. Bringing together the public and private sectors in a discursive forum, the workshop identifed a range of emerging issues for the purpose of the framing future research agendas within CEPS. This Briefing Paper is a tangible outcome of that forum, and an example of new levels of engagement between the government, private and research sectors that will assist in deepening our knowledge of the risks to infrastructure, and identify effective strategies of promoting resilience and risk mitigation.

Simon Bronitt

Professor Simon Bronitt
Director

Infrastructure Vulnerability and the Coordination of Government Responses

Information Technology Systems – Security and Risk

Ms Kate O'Donnell

Overview

The security of Australia's national infrastructures is of critical importance to its continued economic prosperity and well-being. Yet, the volatility of Australia's climates and the threat of terrorism present Australia's national critical infrastructures with a set of challenges almost unique in the world. Within the past 5 years, Australia's towns and cities have encountered tropical cyclones, droughts, catastrophic flooding and destructive bush fires. Into the future, Australia's energy, water, communications, transport, food chain, health and banking and finance sectors face severe and continuing natural and human-induced hazards.

The Australian Government's Critical Infrastructure Resilience Strategy (2010) and the accompanying Supplement sets out the Government's commitment to continuing a partnership with the owners and operators of critical infrastructures. The Strategy documents outline existing challenges and articulate the importance of risk management and building resilience.

Against this backdrop, the Australian Research Council Centre of Excellence in Policing and Security (CEPS) coordinated and hosted the next in a series of one-day workshops with partner organisations and researchers to identify joint research priorities for a stream of work aimed at strengthening the resilience of national critical infrastructure.

The objective of the workshop was to identify and agree areas where academic research could strengthen the knowledge and expertise of aspects of cyber security and risk to inform future policy development.

About the CEPS project on Critical Infrastructure and the Coordination of Government Response

This project has been set up to examine the attributes of Australian and regional infrastructures that are most vulnerable to exploitation and attack by transnational threats. A significant part of the project will explore ways that governments can

reduce infrastructure vulnerabilities and inform governmental planning and response to critical incidents. The project team will consider:

- Ways to increase the resilience and immunity of key infrastructures to transnational threats; and
- The impact such measures would have on our ways of life and modes of engagement with our regional neighbours.

The project will also map the range and variety of government arrangements at federal and state and territory levels devised to meet security threats. The team will explore the challenges confronting a whole-of-government response both within and between governments and identify ways different countries have sought to react and assess their policy and organisational impact. The research will examine the governance and function of the Australian Government's new approach to managing national security, including the impact of the National Security Statement (2008) and the Critical Infrastructure Resilience Strategy (2010).

Summary of Research Themes

1. Raising cyber-security awareness and building resilience -

   There was a consensus in the workshop that existing and emerging cyber-threats are a key priority for research into how to better protect Australia's critical infrastructure. While cyber-threats are not a new phenomena, some industry partners are better prepared than others to enhance their response to increasing cyber-threats.

2. The opportunities and challenges for policing social media -

   The continued emergence of social media is seen as both a challenge and opportunity for policing. Key issues for policing organisations include how to balance maximizing opportunities and identifying ethical issues and considerations.

3. Data protection – emerging threats and future policy -

   The emergence of new technologies continue to present new and emerging challenges for industry and governments. If and how to regulate cloud computing is a key emerging research issue to assist policy makers into the future.

Workshop Themes

The workshop focused on how critical infrastructures were vulnerable because of the impact of attacks on the information technology systems required to support them.

The variety of topics discussed at the workshop included:

- challenges with securing information systems now and into the future
- understanding the security implications of technological developments
- law enforcement challenges arising from technological developments such as the emergence of social networking sites
- how technological developments can be used as a policing tool
- the proliferation of malware
- security and policing challenges with the emergence of cloud computing

The workshop generated key themes and related learning / research priorities and research questions. These are set out below, identifying (i) the theme, (ii) the learning / research priorities, and (iii) research questions.

NB: Italicisied text indicates a participant comment transcribed from the notes taken during the workshop. These edited comments are not attributable to any agency or individual and are used simply to refine the research question.

Theme 1: Raising cyber-security awareness and building resilience

An awareness of the existing and emerging cyber-threats posed to Australian infrastructures, communities and businesses is an integral part of building organisational and infrastructure resilience.

"All systems rest so critically on IT structures."

While there is value in considering how historical cyber-attack methods may inform possible future attack methods, post-incident analysis is a critical component of developing a more predictive approach to introducing counter-measures against future attacks.

The government agencies and their specific roles in responding to cyber-incidents (tactical and policy) is not well articulated and consistently understood by industry or the public who wish to report cyber-crime.

"When looking at the Australian government from outside, it looks like a monolith – silos are a problem."

"In a lot of jurisdictions, when victims try to report cyber-crime, they can't do it."

"There appears to be a lack of coordination. Anything to help break that down and make it more cohesive has to come from the top … somewhere in the middle, proper coordination is missing."

While recognising the challenges of governments sharing information across the breadth of industry falling within the definition of critical infrastructure, there is a lack of consistency and transparency in how this is occurring.

"We need to understand the threat picture … by the time we've finished batting off the current threat, the next on is coming down the pitch."

"Some (owners and operators of critical infrastructure) need advice about what they need to be considering when introducing new technology from the concept / design phase"

There are opportunities to share information from the more 'mature' industry players (such as the banking and finance industry) to help build maturity in other sectors. The government may have a role in facilitating this in a more strategic way.

"As far as sharing of intelligence, sharing information, helping each other out, the banking sector is much more advanced."

Research Priority -

(Definitional Learning) To develop a shared understanding of the roles of Government and Industry:

- **in responding to cyber-incidents from a tactical and policy perspective**
- **in information sharing with industry (receiving and providing)**
- **supporting less mature industry players.**

Defining and articulating the role of Government and how it interacts with industry to support information sharing in terms of cyber-security will underpin how industry players further develop their specific resilience strategies.

Specific Activities -

Describe how government (inter-jurisdictional and inter-agency) is structured to respond to cyber-incidents from a policy and tactical perspective and the interdependencies with established groups such as the Trusted Information Sharing Network for Critical Infrastructure Resilience (TISN) who have established roles in communicating on security issues.

Describe how threat and attack information and future challenges such as the implications of introducing new technologies are shared with industry.

Describe how less mature industry players are supported by industry and government.

Describe how threat information is conveyed to industry and within industry.

Reconsider and review the scope and content of the previous AusCERT survey.

Understand what data and assistance AusCert and CERT Australia can provide to industry.

Research Questions -

- Should the role of government in responding to cyber-incidents be redefined?
- How can information sharing (federal, state, territory) within and between industry and government (including threat information) be better focused?
- How can cyber-security response teams better respond to cyber challenges? How can owners and operators of critical infrastructures understand the security implications of technological developments before they are introduced?
- Can available data help identify and define future strategic challenges?

Theme 2: The opportunities and challenges for policing social media

The continued take up of social media as a 'standard' communication tool presents unique opportunities and challenges. The prediction is that by 2014, there will be three billion people who transact using electronic mobile or internet technology.

The opportunities arise as law enforcement agencies can proactively use social media to communicate with the community. This is particularly useful in times of crisis where the public expects up-to-date and accurate information to dispel myths and provide facts.

"During the Brisbane floods, Council pages were overwhelmed … people turned to Facebook"

The strategic use of social media such as Twitter can also help build relationships between law enforcement agencies and specific sections of the community such as young people.

A key challenge for law enforcement is that offenders who use social networking sites are in different jurisdictions providing challenges for cross border police cooperation (within and external to Australia).

"Sharing information between states is still a problem."

The ongoing challenge is how to ensure law enforcement officers have access to technical expertise to deal with new crimes committed in new ways.

Research Priority -

(Comparative Learning) To explore the ways:

- **policing of social media has been operationalised in other countries**
- **police use social media to build relationships with key community groups**
- **police / private partnerships have been formed to lend technical expertise to investigations and prosecutions**

The approaches taken in the different Australian jurisdictions, the USA, UK and Canada could provide useful insights for Australian policy makers.

Specific Activities -

To identify how different models of police cooperation have been operationalised in different jurisdictions.

To identify laws and regulations in Australia that relate to the policing of social media.

To analyse how social media is being used by police in different jurisdictions

as part of its community engagement strategies.

To identify how different models of police / industry partnerships can be structured to ensure police have access to technical expertise for investigations and prosecutions.

Research Questions -

What lessons can be drawn from the approaches taken in different jurisdictions?

What legislative framework could be developed to support the policing of social media sites?

What models can be developed for police / private partnerships?

How can police meet the challenges of social media while remaining within both legal and ethical boundaries?

Theme 3: Data protection – emerging threats and future policy

Data protection and privacy is one of the biggest issues facing industry. Threats to data arise from internal and external sources. A key threat arising from internal sources is employees connecting mobile devices to their organisations' systems. External threats such as malware targeting individuals and consumers are having an increasing impact on industry (such as the banking industry). Industry is facing a situation where IT devices being used within their organisations though have no or limited security.

"The old security model is broken … the way we've been doing things has to change."

New technologies such as the rollout of the National Broadband Network, the rapid development of cloud computing and the emergence of large offshore data centres to support the rapid expansion of the market is intensifying the issues facing industry.

"Every piece of software is capable of being exploited".

Consumers, small and large business, not-for-profit business and governments are quickly identifying potential opportunities and advantages for from using cloud computing. However, the standards environment is quite unstable and key issues such as privacy, security and identity management remain of critical concern.

"Cloud service providers are emerging in healthcare, education, research and government service delivery."

"There are 24 different standards setting groups that are trying to develop different aspects of standards."

Research priority -

(Comparative Learning) To investigate ways:

- **that standards can be harmonised to provide guidance to industry**
- **that different organisations / sectors identify their data protection vulnerabilities**
- **that regulatory regimes are used to protect customers' rights and privacy.**

Specific Activities -

To identify existing standards and examine how harmonised standards may be constructed to provide guidance to industry.

To identify learnings from organisations / sectors relating to how data vulnerabilities, customers' rights and privacy are identified and managed.

Research Questions -

What legislative or policy levers can governments use to enhance the effectiveness of data protection?

How will harmonised standards assist industry protect data and build infrastructure resilience?

What are the industries most exposed to internal and external threats?

What future vulnerabilities are anticipated?

What future regulatory regimes may be applied to cloud computing to reduce threats to customers' rights and privacy?

References

Commonwealth of Australia (2010). *Australian Government Critical Infrastructure Resilience Strategy. Retrieved on 2 June 2011 from* http://www.tisn.gov.au/www/tisn/rwpattach.nsf/VAP/(9A5D88DBA63D32A661E6369859739356)~Australian+Government+s+Critical+Infrastructure+Resilience+Strategy.PDF/$file/Australian+Government+s+Critical+Infrastructure+Resilience+Strategy.PDF

Rudd, K. (2008). *The First National Security Statement to the Parliament. Retrieved on 2 June 2011 from* http://pm-rudd.archive.dpmc.gov.au/node/5424

About the Author

Kate O'Donnell is a Senior Officer with the Department of Transport and Main Roads on secondment to CEPS for 12 months.

While at CEPS Kate will focus on working to ensure the CEPS research program includes a focus on transport security, building strong linkages with CEPS and the transport sector and undertaking specific research on ferry security in Queensland.

Kate's public service career is diverse, spanning more than 25 years. Commencing her public service career as a nurse, Kate has held a variety of policy, change management and advisory positions in multiple agencies.

Kate's interest is in emergency management policy and transport security. During the 2009 influenza pandemic Kate worked as a key advisor to the Chief Health Officer and during 2010 as the Director of Transport Security.

Kate holds a Bachelor of Business (Health Administration) from QUT and a Mater of Arts in Criminology and Criminal Justice from Griffith University.

About this document:

This paper was prepared from notes taken by Alice Hutchings, CEPS PhD Student.

This paper is a thematic record of the workshop discussions and the associated research priorities identified by partner agencies. Your comments on this paper are welcome and will contribute to the directions of research arising from the workshop.

All papers in this series are subject to peer review.

General Editor: Professor Simon Bronitt, Director, ARC Centre of Excellence in Policing and Security.

For a complete list and the full text of the papers in this series, please visit www.ceps.edu.au

ARC Centre of Excellence in Policing and Security

M10_3.01
Mt Gravatt Campus
170 Kessels Road
NATHAN QLD 4122
Ph: 07 3735 6903
Fax: 07 3735 1033

www.ceps.edu.au