



## **ASPI-SACF Summary**

The Australian Strategic Policy Institute hosted a 1.5 track dialogue on 5 May 2016 with the Spain Australia Council Foundation addressing 'How Australia and Spain face cybersecurity challenges'.

### **Welcome Remarks**

Mr Peter Jennings, ASPI's Executive Director, opened the event by welcoming distinguished guests, outlining the increasing prominence of cybersecurity issues and his confidence in the practical utility of the dialogue.

Mr Jose Revuelta, President of the Spain-Australia Council Foundation, noted that a key goal for the Spain-Australia Council Foundation is pursuing new areas for cooperation to ensure the sustained growth of the bilateral relationship. There have been significant attempts to undermine Spain's security in cyberspace, and cooperation between Spain and Australia's government and private sectors to enhance the resilience of their societies to cyber threats is increasingly valuable.

Mr Richard Sadleir, First Assistant Secretary International Security Division at the Department of Foreign Affairs and Trade (DFAT), replied, noting that Spain and Australia share a strong defence materiel relationship, particularly in naval shipbuilding, and are operational partners in the coalitions in Iraq and Afghanistan. Australia and Spain have a shared interest in reducing the risk of conflict in cyberspace that they pursue in their respective regional multilateral fora such as the ASEAN Regional Forum.

HE Ignacio Ybañez, Spanish Secretary of State for Foreign Affairs, noted that the growing seriousness of non-traditional security threats means that it is important for democratic governments to act based on their shared values. As members of the Global Forum on Cyber Expertise (GFCE), there is significant potential for Spain and Australia to engage on enhancing the cyber protection of third party critical infrastructure. Cooperation between likeminded countries with similar ideals, such as Spain and Australia, is important in a world where increasing interconnectedness is making geographical distance irrelevant.

### **Dialogue**

The dialogue commenced with a discussion on the national security implications of cyberspace. The contested nature of cyberspace, its constant evolution and plurality of actors was highlighted as a fundamental basis for the challenge posed to both Australian and Spanish governments and companies. It was agreed that in the face of such a threat, network resilience and defence in depth was an essential component of proactive planning. Spanish participants offered insight into their

national approaches to cybersecurity and their Australian counterparts gave brief overviews of the recently released Cyber Security Strategy. Discussions identified the human element of cybersecurity as crucial. A significant proportion of security protocols rely on human implementation/compliance and such systems are only as strong as the weakest link. The metaphor of herd immunity was used to depict this notion, and emphasise the importance of collective responsibility. In light of this dynamic, it was agreed that personnel must be educated and solutions must be accessible so they can be adopted by the average individual in order to facilitate whole of workforce implementation.

The second panel addressed the task of protecting critical national infrastructure. The groups exchanged outlines of their respective government structures/architectures/responsibilities in regards to dealing with this issue, as well as approaches to risk analysis, strategic planning and coordinated responses. It was agreed that public-private cooperation is vital in securing infrastructure systems. Substantial time was dedicated to the question of companies' moral and legal obligations to report a breach of their cybersecurity. There were slight differences in national philosophies on government's role in regulating private industry's cybersecurity: the Spanish approach consisting of negotiated standards of infrastructure security with the private sector, while the Australian approach was described as less hands on and more reliant on free market forces to generate security standards. This debate was extrapolated to considerations of international companies and the complexities of regulation compliance across multiple jurisdictions. The group also identified the potential for bilateral cooperation and agreements between their national CERTs, to develop trusting relationships and facilitate sharing of information and best practise.

The dialogue closed with a discussion on the issue of cybercrime. Participants from both sides laid out their impressions of the threat landscape, painting a mutual picture of innovative criminals and an understanding of the impossibility of totally eliminating the problem. Participants agreed that the difficulty of attribution and borderless nature of the crime pose significant challenges to taking a traditional law enforcement approach to cybercrime. As such, the need for a radical paradigm shift was identified. It is challenging to prosecute cybercrime after the fact, so instead governments have to focus on interjecting earlier in the law enforcement process. It was agreed that this should be achieved through promoting awareness, education and prevention.

The point was also made, that whilst cybercrime is in many ways new, in other ways it is simply a new iteration of traditional issues: theft, fraud, denial of service, activism and the propagation of illegal goods. From this perspective, it was highlighted as important not to isolate cyber issues to the margins of law enforcement as hi-tech – but instead integrate it across normal operations. Addressing this issue successfully was described as not only a national security issue but also specifically an economic security issue: tackling cybercrime is an essential step in making Australia and Spain safe places to do business. It was agreed that hardening networks to sustain a reputation of prosperity should be a national priority, but that doing so would require policy and legal frameworks to catch up to the practical challenges. Establishing clarity on issues such as the utility and legality of white hat hackers was identified as important element of this process.

Lastly, the point was made that cyberspace can represent a national capability as much as a vulnerability. As such, it is important to take steps to sharpen strengths. The group discussed the value of simulations and exercises, such as CyberEx. Similarly, the groups addressed their capacity building efforts in the Asia Pacific and Latin America, respectively.

The dialogue facilitated fruitful discussions on the shared challenges of cyberspace and the potential for greater bilateral cooperation in this area.

**Authored by Zoe Hawkins & Liam Nevill**