RSIS | S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES
Nanyang Technological University

RSIS COMMENTARY

www.rsis.edu.sg

No. 215 – 24 August 2016

Confronting Cybersecurity Challenges through US-Singapore Partnership

By Harry Hung

Synopsis

Cyber cooperation remains a prominent area of mutual interest between Singapore and Washington. Singapore's Cyber Security Agency (CSA) and the US Department of Homeland Security (DHS) recently established a formal cybersecurity partnership. This agreement will improve bilateral cybersecurity and potentially create mechanisms for ASEAN nations to better address cybersecurity challenges.

Commentary

AT THE invitation of President Barack Obama, Singapore Prime Minister Lee Hsien Loong paid a state visit to the United States from 31 July to 5 August 2016. It was the first official visit to the US by a Singapore prime minister since 1985, coinciding with the 50th anniversary of diplomatic relations. The two leaders subsequently released a joint statement, one highlight of which was cybersecurity commitments. These included "broadening and deepening our cooperation to promote an open, interoperable, reliable, and secure global Internet that supports innovation, economic growth and social development."

Both leaders endorsed a common approach to international cyber stability, affirming that international law applies to state conduct in cyberspace, and committed to promoting voluntary norms of responsible state behaviour in cyberspace. Both governments affirmed their support for a multi-stakeholder approach to Internet governance and for the protection of human rights online.

Bilateral Agreement to Enhance Cybersecurity

As a key deliverable to PM Lee's visit, Singapore's Cyber Security Agency (CSA) and the US Department of Homeland Security (DHS) co-signed on 2 August a Memorandum of Understanding (MOU) on the Cooperation in the Area of Cybersecurity, which lays a foundation for cooperation on cyber-related issues.

This agreement covers cooperation in key areas that include regular Computer Emergency Response Teams (CERT) to CERT information exchanges and sharing of best practices, coordination of cyber incident response, conducting new bilateral initiatives on critical infrastructure protection, and continued cooperation on cybercrime, cyber defense, and on regional capacity building.

Capacity building efforts include joint exercises, regular exchanges and visits, joint research and development, capability development, and regional cyber capacity building programs or initiatives.

David Koh, Chief Executive of CSA, noted that “Singapore and the US share long-standing warm bilateral relations and a shared vision to ensure international peace…Considering the interdependence in cyberspace between [both countries], the borderless nature of transboundary cyber-attacks would have a significant impact on both countries’ critical information infrastructure.”

Necessity and Importance

Singapore’s CSA has entered into four other bilateral cyber MOUs signed with France, United Kingdom, India and the Netherlands. The agreement with the US is the fifth and an important milestone for both countries. It is the first cyber agreement between an ASEAN nation and the US. While Singapore benefits from accessing knowledge about cyber threats and mitigation responses from the US, Washington will equally gain deeper insights into the cyber threats experienced by Singapore and potentially the South East Asia region.

As cyber threats continue to rapidly evolve, it is often difficult for one nation, corporation or entity to identify, characterise, mitigate, and respond in a timely manner. Both countries are uniquely postured to mutually support one another by bringing together their own global and regional expertise in understanding cyber threats.

Filling in knowledge gaps more rapidly and comprehensively is a key necessity that can only come from shared awareness and understanding, particularly with more advanced and sophisticated cyber threats originating from both state and non-state actors. These knowledge gaps may include specific attribution of adversaries, their capabilities, threat infrastructure, targeted victims, vulnerabilities exploited, mitigation and remediation measures and response actions. This agreement enables the critical information sharing needed to deepen these types of cyber threat awareness, understanding and responses.

Implications for the Future

Both Singapore and the US are becoming more digitally dependent, with Singapore having aspirations to be the world’s first Smart Nation. The creative use of information and communications technology (ICT) and Internet of Things (IOT) will undoubtedly bring about significant advances in the way we live, work and play through predictive and automated decision-making based on detailed collected data on individuals.

Public and private organisations stand to considerably improve efficiencies and deliver smart allocation of their resources and services through these innovative solutions. Realising these opportunities will be key motivators that drive rapid development, early adoption and integration of these technologies into day to day life.

However, often overlooked in the design stages of these technological innovations are the cybersecurity considerations and the potential security vulnerabilities. Cybersecurity frequently remains an afterthought that might, if at all, receive attention just prior to integration and or implementation into a larger network. Hackers exploit these vulnerabilities.

Regional cities and countries where cyber capabilities and capacities are still developing will find it increasingly important to improve their cybersecurity posture and response mechanisms. This is especially so as they adopt and integrate new smart technologies into their society. Both the US and Singapore can play a leading role in supporting the cybersecurity efforts for ASEAN nations.

First ASEAN Cybersecurity Workshop

From 16-18 August 2016, Singapore's CSA, Ministry of Foreign Affairs and the US Department of State's Third Country Training Programme hosted an ASEAN Cybersecurity workshop, the first of its kind. This Singapore and US lead diplomatic effort brought together ASEAN cyber officials from both policy and technical offices to discuss developing and implementing national cybersecurity strategies, cyber incident response, multi-stakeholder engagement, private-public partnerships and building a culture of cybersecurity.

Leading cyber experts from government, industry, and academia provided relevant presentations that supported daily country team exercises. The workshop concluded with each ASEAN country presenting their identified lessons learned for cyber coordination and initiatives. This type of diplomacy and engagement mechanism will likely become more frequent, in greater depth and with sharper focus as leaders in ASEAN countries become more accustomed to sharing their cybersecurity challenges, tactics, techniques, and procedures and best practices.

Finally, as Singapore continues to mature CSA and its national cybersecurity posture, this bilateral relationship can help inform current and emerging decisions related to the prioritisation of resources and investment allocations needed to enhance Singapore's cybersecurity. This remains the most difficult and elusive question in a highly fluid and dynamic global cyber operational environment: how much of what capabilities is enough to ensure there is sufficient and sustainable cybersecurity to allow our citizens, businesses, governments and critical infrastructures to function without significant loss or degradation?

Singapore is in a unique position to take the necessary technological leadership role in enhancing its national cybersecurity posture while supporting the region. The shared insights and experience by both Singapore and the US can be of considerable benefit to the ASEAN countries and to the larger global community as all nations continue to seek ways to improve their cybersecurity postures.

Harry Hung, Lieutenant Colonel, US Army, is a Visiting Fellow from the US Army War College at the S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University, Singapore. He is a career US Army intelligence officer whose command and staff assignments include Cyber, Signals Intelligence, and Information Assurance.