RSIS S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES
Nanyang Technological University

RSIS COMMENTARY

www.rsis.edu.sg No. 214 – 13 October 2015



# Singapore's Smart City: Securing It From Emerging Cyber Threats

*By Michael Mylrea*

**Synopsis**

*As Singapore and other smart cities become increasingly connected to the cyberspace so too does their risk of cyber threats. Smart cities need to develop a cyber-smart workforce, technology, policies and new risk management solutions.*

**Commentary**

FIFTY YEARS after its establishment, Singapore is a smart city-state success story at the forefront of a third industrial revolution. Today, the Internet of Things (IoT) increasingly interconnects Singapore's cyber and physical systems, sensors and smart technology into the digital fabric that links society and critical infrastructures such as transportation, health, finance and defence. Infrastructure investment is expected to grow by 50 percent to about S$30 billion by the end of the decade.

But as Singapore and other smart cities become increasingly connected to cyberspace, so too does their risk of cyber threats. For the next 50 years to be as prosperous as the last, Singapore and other smart cities and nations need to develop a cyber-smart workforce, technology, policies, and new risk management solutions.

**Cyber Smart City: opportunity and challenge**

*The Cyber Smart City Opportunity* of new IoT-inspired products, services and markets could boost the GDP of the world's 20 largest economies by $14.2 trillion by 2030, according to a recent study by Accenture. This trend can be seen in Singapore's smart buildings, where converged information and operational technologies infrastructures, control systems and sensors integrate multiple electronic systems to support building management and business functions. Smart building technology is increasing energy efficiency and conservation of natural resources. Smart transportation is making cities more efficient. Smart health solutions are making cities healthier and providing early warning against pandemics.

*The Cyber Smart City Challenge* is to secure all of these converged networks and devices from cyber threats. Hackers continue to exploit smart devices to steal, manipulate and disrupt cyber and physical systems. Cyber attacks have been used to infiltrate corporate networks through smart building controls, blow up furnaces in steel plants, and cause generators to fail. In 2013, Target, a large US

retailer, was hacked through its smart heating ventilation and cooling system, exposing corporate networks and over 40 million customer's credit cards. Similar vulnerabilities are prevalent in thousands of networked smart systems.

A cyber-secure smart city will require a more holistic cyber security approach that fosters a culture of cyber security. Traditional information assurance solutions to risk management are challenged by IoT's expanded attack landscape: more networked devices exchanging larger data sets. Secondly, many industrial control systems need to be running 24/7, lack secure communication protocol and include legacy devices that are not interoperable or secure when combined with new IoT technology.

So what can Singapore do to realise the smart city opportunity and overcome the cyber security challenge?

*Developing a Cyber Smart Workforce* is imperative. Even as some technical cyber security defences improve, humans remain the weakest link in cyberspace. A secure architecture requires a workforce to be continually trained in best cyber security policies, practices, and technology. A cyber smart city workforce must understand how to secure converged information technology (IT) and operational technology (OT) (e.g., control systems, actuators, intelligent energy devices) environments.

Investments in human resource development should foster skills in the both "hard" and social sciences such as human and organizational learning, complex systems and behavioral psychology. The IT and OT cyber security skill set will be increasingly necessary to secure the smart technology, while the social sciences encourage smart decisions that optimize the technology and help protect us from ourselves.

**Cyber smart policies and solutions**

*Cyber Smart Policies and Regulations* are imperative for Singapore's continued success and survival. Cyber smart policies should help increase cyber security of critical infrastructures such as financial institutions, transportation systems and hospitals. Smart cities depend on these inter-related and symbiotic infrastructures for their economic livelihood, security and survival. Unfortunately, increased networking of critical infrastructure has also made it increasingly vulnerable to cyber threats.

Smart Cities are fueled by prodigious amounts of data that becomes more valuable as it is aggregated and analysed. However, big data needs to be protected by policies that curtail industrial espionage and strengthen intellectual property protection. One incentive for doing so is increased foreign direct investment as international corporations will increasingly move and expand in nations that protect intellectual property, encourage ingenuity and seek new ways to marry man and machine through education, not malware and hacking.

*Cyber smart risk management solutions* should provide a holistic defence in-depth approach to secure how data is being collected, shared and stored. Advanced intrusion detection systems and firewalls combined with encrypted data between servers, devices, sensors and enterprise networks are a good place to start. New security solutions for machine-to-machine secure communications are needed.

Technical solutions are only as strong as the risk management policies in place to respond to and prevent attacks. Secure standardisation of communication protocol in IoT can help facilitate more secure and interoperable smart cities. Any effective cyber risk management solution should quickly adapt to the threat, helping to limit damage and assure continuity of operations.

**The next 50 years**

In considering what Singapore will look like in the next 50 years, IoT is both transformational and inspiring, but not without challenges. Smart technologies continue to be developed and deployed in our cities without a holistic cyber security strategy. As a result, Moore's law is playing out to hackers' advantage in that as data processing and storage costs fall we become less discerning about what data we store and send and how we store and send it.

For our future smart cities to prosper and bring in a new era of value creation, cyber security needs to

be part of the IoT design and human resource development criteria. This new wave of innovation will continue to be disruptive, but it does not have to be destructive to smart cities with smart cyber solutions.

---

*Michael Mylrea is Manager for Cybersecurity and Energy Infrastructure at Pacific Northwest National Laboratory, USA and works on energy and cyber security issues for industry and government. He is also a National Science Foundation, Executive Cyber Security Doctoral Fellow at George Washington University who contributed this RSIS Commentary.*

---

**Nanyang Technological University**
Block S4, Level B4, 50 Nanyang Avenue, Singapore 639798
Tel: +65 6790 6982 | Fax: +65 6794 0617 | www.rsis.edu.sg