NUS at the Opening Ceremony of the 2nd Singapore Cyber Security R&D Conference (SG-CRC) 2017

Speech by Prof Tan Eng Chye,
Dy President & Provost

21 Feb 2017, 9.00 am
Stephen Riady Centre, University Town,
National University of Singapore

Guest of Honour Mr Gabriel Lim, Permanent Secretary, Ministry of Communications and Information

Mr Quek Gim Pew, Chair of the NCL Governing Board and Chief Defence Scientist of the Singapore Ministry of Defence

Distinguished Guests,

Colleagues, Ladies and Gentlemen,

A very good morning to everyone and on behalf of NUS, I would like to bid you a warm welcome to our campus. I am delighted that so many of us are gathered here today, for the 2nd Singapore Cyber-Security R&D conference, and to mark the special occasion of the launch of the National Cybersecurity R&D Lab, an important and critical infrastructure that will augment Singapore's research innovation and capabilities in Cybersecurity.

GLOBAL IMPORTANCE OF CYBERSECURITY

Our lives in this day and age are dominated by Information Technology. Smart mobile devices, cloud computing, digital services and so on, have all transformed the way we organize and conduct our personal lives, business operations, and even in the delivery of public services.

Concomitant to the IT revolution, the past decade has also witnessed the adverse impact when underlying information systems were being compromised. Organisations had to incur hefty costs to regain access to their own data following ransomware attacks. Hacking incidents can have severe repercussions. In December 2015, hackers were able to successfully compromise information systems of three energy distribution companies in Ukraine, resulting in a blackout that disrupted the electricity supply to more than 200,000 residents.

These incidents have raised awareness of the importance of protecting systems against cyber-attacks. The Global State of Information Security Survey 2017 found that many organizations have factored cybersecurity into their operations, products and services, not only to safeguard themselves against attacks, but also to build customer trust and to gain market advantage. It is becoming a business imperative.

CYBERSECURITY EFFORTS IN SINGAPORE

Here in Singapore, where society and economy are highly empowered by information technology, we have long appreciated the need for cybersecurity. Way back in 2005, the first Infocomm Security Masterplan had identified building capabilities to mitigate and respond to cyber threats as a priority. This focus has expanded over the years as the nation's capabilities grew and we aimed to become a Secure and Trusted Hub. Most recently, Singapore has developed a Cybersecurity Strategy 2016 which rests on four pillars: Singapore will endeavour to strengthen the resilience of Critical Information Infrastructures, work with businesses and communities to create a safer cyberspace, develop a vibrant cybersecurity ecosystem comprising skilled professionals, technologically-advanced companies and strong research collaborations, and to strengthen international partnerships as cyber threats know no borders.

As part of the national effort to develop R&D expertise and capabilities in cybersecurity, as well as grow a strong and vibrant R&D community, the National Research Foundation has established the **National Cybersecurity R&D (NCR) Programme**. Amongst others, this programme offers annual postgraduate scholarships to nurture a strong talent pipeline in cybersecurity; it also offers grants to support research projects in key cybersecurity areas, and to seed innovations that will meet the cybersecurity needs in Singapore and beyond.

To enhance industry academia collaboration, and to reap synergies between industry and academic research, the **Corporate Laboratory@University Scheme** by the National Research Foundation has enabled the establishment of two corporate laboratories in cybersecurity research, between Singtel and NUS, and the other between ST Electronics and Singapore University of Technology and Design. The interplay between in-depth corporate domain knowledge of companies and the deep research foundations at universities will accelerate industry-relevant innovations in cybersecurity.

And in September last year, with support from the National Research Foundation, the **Singapore Cybersecurity Consortium** was created to foster closer interaction and greater engagement between industry, government agencies, and research institutions to encourage use-inspired research. As an engagement platform, it provides companies and agencies access to emerging technologies in the research stage, while facilitating use-inspired research and technology translation. The consortium currently has more than twenty companies as members.

CONFERENCE OVERVIEW

This year's Singapore Cyber-security R&D conference showcases all these efforts in a vibrant program under the theme of Systems Approach to Cyber Security. It is most apt that the conference is being hosted by the TSUNAMi centre at the NUS School of Computing, which is engaged in cutting-edge research to build **Trustworthy systems from untrusted component amalgamations**. Speakers from this project, as well as from the other ongoing national cybersecurity R&D projects, will show us the latest developments in their respective missions.

In line with the theme, the conference will feature presentations of novel ideas that address the issue of constructing resilient systems by improving the security of the underlying hardware and software. Successful translation of these ideas to effective solutions will strengthen our critical information infrastructures, enabling them to withstand cyber-attacks and minimizing adverse impact on the society and the economy.

A panel discussion on Cybersecurity Education will take place tomorrow It will address the crucial issue of developing human talent in cybersecurity; the future workforce who will lead practices and innovations in cybersecurity. Not only must they possess deep technical understanding, they must also embrace adaptability, acumen and the spirit of lifelong learning, as cyber-security is a dynamically evolving and demanding discipline.

I would also like to commend the organisers for a successful pre-conference cyber-camp that was held over the last two days at NUS; participants from both academia and industry attended lessons conducted by international experts, and put on their active thinking hats in an intense hackathon.

LAUNCH OF NATIONAL CYBERSECURITY R&D LAB (ANNOUNCEMENT)

The Cybersecurity eco-system in Singapore is a growing and thriving one, and the collective efforts are beginning to bear fruit. Today, I am pleased to announce the launch of the National Cybersecurity R&D Laboratory or NCL, a timely and significant initiative that will add to and enhance Singapore's cybersecurity efforts. The National Cybersecurity R&D Lab is a national shared infrastructure that provides ready-to-use environments and hosts realistic data repositories for experimentation and education in cybersecurity. Researchers, businesses, and educators can embark on experiments and achieve results more quickly, as this lab will help to save time, effort, and costs associated with setting up one's own environment.

NCL is established with the support of NRF, alongside the Singapore Cybersecurity Consortium and the NUS-Singtel Cyber Security R&D Lab. With this shared anchor, the three units will work in synergy and support each other's efforts in advancing cybersecurity R&D. NUS is privileged to be hosting this new facility and the concentration of these cybersecurity R&D activities at NUS also creates positive network effects and excellent opportunities for manpower training and entrepreneurship. Experts across the industry, research community, and government agencies can come together to share, exchange and build on ideas quickly and spontaneously, and these innovations will further strengthen Singapore's resilience as a smart and cybersecure nation.

On this note, I wish the National Cybersecurity R&D Laboratory every success, and I wish all delegates here a fruitful and productive conference. Thank you.