

**Speech by Professor Tan Eng Chye, NUS President
at the Inaugural International Alliance of Research Universities Cybersecurity Forum
4 April 2018, 9 am, Nexus**

Distinguished delegates from our partner universities under the IARU network,

Guests and colleagues,

Good morning to everyone and welcome to the inaugural International Alliance of Research Universities Cybersecurity Forum. To our friends from our partner universities, I bid you a warm welcome to Singapore and to the NUS campus.

[Section 1: IARU as a strategic alliance body](#)

Cybersecurity is a very pertinent and pressing issue confronting many organisations, including universities. Concomitant to the IT revolution, the past decade has witnessed incidents 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 May last year, a strain of ransomware called WannaCry spread around the world, and successfully targeted many organisations, including public utilities and large corporations. Notably, WannaCry disrupted National Health Service hospitals and facilities in the UK, hobbling emergency departments, delaying vital medical procedures, and creating chaos for many patients.

These incidents have raised awareness of the importance of protecting systems against cyber-attacks. Universities too, are not spared. I am thus glad that esteemed representatives from ANU, ETH Zurich, Peking University, University of Cape Town, University of Copenhagen and University of Tokyo are able to join us here today, to share ideas and perspectives, and to work together to tackle Cybersecurity challenges faced by higher education institutions.

[Section 2: Cybersecurity Initiatives at the National Level \(National Landscape\)](#)

Here in Singapore, where society and economy are highly empowered by IT, we have long appreciated the need for cybersecurity. As part of our quest to become a Smart Nation, Singapore has developed a Cybersecurity Strategy 2016 which rests on four pillars: Strengthening the resilience of our Critical Information Infrastructure, working with businesses and communities to create a safer cyberspace, developing a vibrant cybersecurity ecosystem comprising skilled professionals, technologically-advanced companies and strong research collaborations, and strengthening international partnerships as cyber threats know no borders.

To this end, Singapore has implemented initiatives such as the use of separate networks in the public service for internet surfing and work systems such as emails; we have strengthened laws to respond to cybercrime incidents, developed competency frameworks to recognize professionals in IT security, and so on.

[Section 3: University-wide Cybersecurity Initiatives](#)

Within NUS, we are fully cognizant of the increasing Cybersecurity risks that arise with evolving technologies, business practices and user expectations. These include phishing, cloud security and unsecured personal devices. Moreover, Universities typically have to manage a large number of users, accounts, networks, devices and servers amongst others.

As part of the National Cybersecurity R&D Programme, NUS set up a National Cybersecurity R&D Laboratory, as a testbed for creative solutions to tackle cyber threats. This Lab serves as a one-stop platform providing ready-to-use tools and environments for cybersecurity research and training. NUS is also in collaboration with Singtel, the largest Telco in Singapore, to facilitate R&D of solutions to cyber threats through novel data analytics techniques and new approaches to designing and implementing IT systems that are “secure by design”. The Lab will host research activities of over 100 research staff from NUS and Singtel and it will train 120 new cybersecurity professionals.

To support aspiring entrepreneurs who are venturing into cybersecurity solutions, NUS has set up a Cybersecurity Startup Incubation Hub known as ICE71 (Innovation Cybersecurity Ecosystem@Block71). This ecosystem helps entrepreneurs take their innovative ideas to the next step, by equipping them with financial and business know-how, and bringing them into the entrepreneurial ecosystem.

[Section 4: The Road Ahead](#)

But in tackling Cybersecurity, one cannot work alone. Given how cyber threats are borderless, constantly changing and increasing in sophistication, collaboration and harnessing the collective ideas and wisdom of likeminded experts, are key to enhancing Cybersecurity. It is increasingly difficult to outsmart and outdo the attackers, and as defenders, we have to amalgamate our strengths, expertise and resources.

It is thus most apt, that IARU partners are coming together today to deliberate on this pressing topic. We hope that this IARU forum will strengthen the exchange of information, and coordinate efforts among universities, so that we can respond more effectively against cyberthreats. We want our institutions to be able to harness digitization and technology to propel our education and research missions, yet without compromising on security.

On this note, I wish you a fruitful and productive forum, and I wish all delegates from overseas, an enjoyable stay in Singapore. Thank you.