MINDEF
SINGAPORE

SPEECH

Visit http://www.mindef.gov.sg for more news and information about MINDEF and the SAF

Speech by Second Minister for Defence, Mr Ong Ye Kung, at the Cyber Defenders Discovery Camp Awards Ceremony Held at the Singapore University of Technology and Design

08 Jun 2017

Introduction

This is the fifth edition of the Cyber Defenders Discovery Camp (CDDC), and it is encouraging to see growing interest amongst our youth in this area of expertise. This year, we have participation from 400 students, 26 schools. I hope that all of you have found the camp fun, enriching, and fascinating.

Some people say we are at the cusp of the "Fourth Industrial Revolution". I tend to think technological advancement is a continuous process. You cannot quite mark it by chapters or by versions like software updates.

But what we know for sure is that the digital realm has become integral to our way of life, and its penetration into our lives will get deeper with time. It is driven by the Internet, it is linking up machines, gadgets, appliances, connecting economies, societies, systems and people in more ways than ever before, and reshaping the world as we know it.

Cyber Good vs Evil

But there is always a dark side to every bright side. For every Jedi, there is a Sith. For every risk, there is a gain. So, as more and more devices are connected to the Internet, in a phenomenon known as the "Internet of Things", the possibilities to improve lives are immense. But at the same time, cyber attackers now have more points of intrusion and the greater potential to cause havoc and cause harm.

Unlike conventional warfare, cyber threats transcend geographical limitations and physical boundaries. As David Koh, Deputy Secretary (Technology) always said, "Cyber Defence, there is no SEA games. Straight away you would be in the Olympics." Cyber attackers use bytes instead of bullets. They can strike from anywhere in the world, even disguise their locations. They are faceless and they are nameless.

Last October, the largest Distributed Denial of Service attack on record brought down Twitter, CNN, PayPal and other popular sites across the US and Europe. The attack was caused by malware-infected devices such as webcams, printers and baby monitors.

Last month, a massive ransomware virus attack, Wannacry, spread to more than 230,000 computers in over 150 countries within a day. It is very sophisticated. The ransom demands were made in 28 languages.

Military networks are not spared. December last year, the South Korean military announced that its networks had been hacked, and a malicious code had been injected into its command and control networks, as part of a deliberate and prolonged cyber campaign. The German defence ministry also reported that in the first nine weeks of the year, their IT systems have been targeted more than 280,000 times.

Closer to home, you all may know, a few months ago, (Ministry of Defence) MINDEF's Internet-facing system was infiltrated, but fortunately it was not connected to any of our operating systems so there was no significant damage. Two of our universities suffered separate IT network breaches in April. These attacks were targeted, well-planned and professionally executed.

In the third quarter of 2016 alone, 18 million new malware were captured. Every day, more than 4,000 ransomware attacks occurred worldwide in 2016.

Light Triumphs over Darkness

We are like the Mexican Aztecs or Peruvian Incas in the past, never exposed to the world. But when they were exposed to the world because sea lanes were open, new immigrants came into their territories, they were exposed to new viruses, and many of them died. Unlike these tribes which died in big numbers, we must make sure we can fend off these new Internet viruses and attacks.

When Singapore became an independent nation in 1965, one of the key priorities was to ensure we could defend ourselves against external threats. This was the precondition for us to grow our economy and develop our society.

Now as Singapore aspires to be a smart nation, the same considerations must apply. We must defend ourselves against cyber threats and the dark side of the Internet. That is the precondition for us to derive maximum economic benefits and opportunities from digital connectivity. It also provides the basic conditions to build a healthy, positive cyber community which facilitates learning, sharing, socialisation and collaboration, rather than spread messages of hate and fear.

Just like national defence requires the participation of all, everyone - individuals, private companies and the Government, have a part to play in enhancing our cyber defence.

The Government will take the lead. We are investing more to strengthen government systems and networks. Through the Cyber Security Agency, we will also work closely with the private sector to shore up their cyber defences.

In defence, cyber is now an entirely new battlefront domain, adding to the existing domains of air, sea, land, and space. MINDEF has established the new Defence Cyber Organisation or DCO to strengthen and institutionalise our efforts in cyber defence.

DCO will collaborate with our Defence Technology Community, which has been working hard to exploit cutting-edge technologies to strengthen our cybersecurity.

Our local institutes of higher learning are stepping up to equip youths with the skills and knowledge in cybersecurity. NUS and SIT have introduced undergraduate degree programmes in Information Security. SUTD, where we are today, will begin inaugural classes for Master of Science in Security by Design in September this year. Singapore Polytechnic is also offering a specialist diploma in cybersecurity management and Republic

Polytechnic has set up a cluster of five labs with a group of leading cybersecurity companies to tackle new cybersecurity challenges.

Combat Fit Cyber Defenders

The critical success factor in building up cyber defence in Singapore is really the availability of people and talent. A new cyber defence vocation has been established in the SAF and in MINDEF. We should learn from our elite combat forces, to develop our cyber defence force also as an elite force comprising people with exceptional talent. Hence, recruitment must be highly-selective, and the demands on the vocation will be exact, will be intense.

MINDEF will work with the education institutions to identify potential cyber defenders for defending Singapore. The best way to do so will be through nation-wide cyber competitions such as this, such as the CDDC. So to the winners and outstanding performers of this camp, you will take home your medals and prizes and you will be invited to go through the selection process to join the cyber defence vocation. For those in JCs and Polytechnics, who have not gone for your NS yet, if you win and perform well in this camp, you will be invited. This means that if you are selected, for Full-time National Service, you serve by defending Singapore's cyberspace.

We will expand future camps and make them more rigorous to better identify cyber talents. As for ladies - your talents are much needed too, so please consider us as you make your career choices and as you decide on your course of study and then step into the workforce later.

In a similar vein, past winners who are active in the cybersecurity industry, or those of you who are in University and completed your NS, you will also be considered for possible reassignment to an NS role in cyber defence.

Lest you are still wondering, it is no longer the case that only men who are physically unfit or have medical problems, get to work on computers during NS. We need cyber talents - combat fit or not. Because as long as you can fight in cyberspace, you are fit in our eyes. And if we find someone who is a talent in cyber defence, and at the same time fit to join other elite combat vocations, we will have a difficult dilemma but that is a good problem to have.

Conclusion

I would like to conclude by congratulating all participants who have completed our CDDC challenge today and to the winning teams, well done!

This camp has given all of you just a glimpse into the exciting and challenging world of cyber defence to spur your interest in this area. Take for example Eugene Lim. He participated in the camp twice while he was studying computer science in NUS. On his first attempt, in 2013, he was new to cybersecurity, but by the time he joined the camp again two years later, in 2015, his skills had improved so much that he won the "Best Defender" award and also clinched 2nd place in the team competition.

During those two years, Eugene actively pursued his newfound interest in cyber defence - he read up more on his own, participated in other online competitions, and even completed an internship with DSTA's Cybersecurity Programme Centre in 2014. After graduating, Eugene turned his passion into his career and returned to DSTA and worked full-time as a cybersecurity engineer. He is now part of a team that tackles cyber incidents faced by MINDEF and the SAF.

I am heartened to see how the CDDC helped him discover his passion for cybersecurity and kick-started his career in this field, and I hope it will do the same for many of you here.

On that note, I hope that you will be inspired to continue your journey and I look forward to seeing many of you as Singapore's cyber defence engineers and defenders in the near future, starting with your NS.