YMAX Speech 2022

Good morning to all delegates. My name is Hugo Chia and I'm a crew from Division 0 also known as Div0. Div0 is Singapore's largest techno-centric cybersecurity community. It is an open, inclusive, and completely volunteer-driven community. Div0 provides a platform where cybersecurity professionals, practitioners, and enthusiasts can meet like-minded people, explore and learn with peers, and contribute to the community. Div0 does so by organising events, driving programmes and initiatives, encouraging collaborations and contributions, and reaching out to the public.

Before I start, a disclaimer, views expressed here are solely my own based on my research of various organisations and the Singapore government's strategy. My presentation does not represent the views or opinions of YMAX and Div0.

I would like to thank the Secretary-General of YMAX 2022, Caleb Tan for inviting me as a youth guest speaker to speak on a topic I specialise in as well as have passion for - cyber security. I would also like to extend my appreciation to the organising committee for making this conference possible.

This year's theme for YMAX, "Futuring New Possibilities" is apt given the worries and uncertain world we live in. The past 2 years have certainly been volatile, from the COVID-19 pandemic to the largest conventional conflict in Europe since WW2, the Russia-Ukraine War, the repercussions are plenty, ranging from rapid digitalisation as more start to adopt remote working, to supply chain disruptions driving up inflation to levels not seen in 40 years and shortages of commodities worldwide.

The topic for the ASEAN Digital Minister's Meeting: Strengthening Cybersecurity to Protect the ASEAN Digital Economy" is very relevant, given ASEAN's position as the fastest growing internet market in the world. If ASEAN were a single country, it would be the world's fifth largest economy. According to research led by Google, 40 million new internet users came online in 2021 within the region.
Given ASEAN's geographic position, ASEAN is located at the crossroads between the East and West. As such, countries and businesses must be well positioned to capture the opportunities that come our way. Given our rapidly digitalising economies and as more people become connected, ASEAN's digital infrastructure and supply chains must be resilient against cyber attacks that would otherwise result in massive losses and disruptions to the supply of goods and services.

Singapore is a founding member of ASEAN and can also be considered the gateway to ASEAN given Singapore's openness to trade. Singapore is a hub in the submarine networks with 17 connections to multiple regions in the world. On top of that, Singapore is a hub for business, travel, talent, trade and is home to the largest number of regional headquarters in the Asia Pacific. This means we are very interconnected and trade-dependent, given our lack of a hinterland. Our strength lies in our people and our connections with the world. The COVID-19 pandemic showed that when supply chains are disrupted and our status as a hub challenged, livelihoods are affected.

There are many big trends happening in the technology and cybersecurity space and I will share a few. The COVID-19 pandemic furthered digitalisation, as companies moved to remote working. There are many risks associated with remote working, such as security controls being weaker.

Other digitialisation initiatives include the Smart Nation Initiative, which Singapore launched in 2014. Since then we have been digitising many aspects of our life. One such example is Singpass, the National Digital Identity initiative. It is convenient, as it allows us to interact with various government e-services and sign up for banking services with just a few clicks as opposed to filling up multiple forms. This cuts time and resources and helps to boost productivity. However, this convenience comes with its own set of challenges. If not properly secured, the National Digital Identity could become a central repository for bad actors to target.

Another trend that is happening is the “IT-OT” convergence. IT-OT convergence is the integration of information technology systems, IT, with operational technology systems, OT. In essence, supply chains which were previously disconnected from the Internet are increasingly being digitised, exposing more surface areas and vectors for attack, increasing the risk of attacks on these supply chains. This results in loss of profits to private sector firms, and disruption to the provision of public goods to citizens if key infrastructure such as energy, water or telecommunication comes under attack.

Amidst these trends, Singapore has been working hard to bolster our defences against said threats in a few areas. In 2015, the Singapore government formed the Cyber Security Agency of Singapore, also known as CSA, under the Prime Minister’s Office. In 2019, a 6th pillar was added to the total defence - “Digital Defence” signalling the importance of cyber and digital security. In a sign where the future of warfare is already here, the Singapore Armed Forces stood up the 4th Service - the Digital and Intelligence Service to defend against cyber attacks in the digital domain.

Before moving on to talk about cyber security, I want to talk about 2 words that are not just important to cyber security but relevant to the foundations of society as a whole. They are “Trust” and “Resilience” and it will be a recurring theme that I will come back to in my speech.

My first point is on “Trust”. Warren Buffet once said: “Trust is like the air we breathe--when it's present, nobody really notices; when it's absent, everybody notices.” I agree with this point. As we go about our daily lives, using iBanking services, communicating with our friends and family, we implicitly trust these systems to be safe, secure and reliable. Trust is also applicable to our daily lives, we trust the house we live in to be structurally sound, the mode of transport that we use to get around to be safe, reliable and many more.

The second word is “Resilience”. Resilience in this context, is the ability for our systems and society to withstand attacks and crises, but if it happens, to bounce back and emerge stronger together.

In fact, the root word resilient was mentioned 17 times in Singapore’s Cyber Security Strategy 2021 and other forms of it, such as resilience was mentioned 8 times. Resilient was also mentioned in the “Digital Defence” Pillar of Total Defence. The idea of a resilient society is a strategic one.

Our digital way of life increasingly comes under attack. We thus need to have digital resilience. Digital resilience is not just about cyber security. Digital resilience is about having digital security and being aware and on-guard against threats such as fake news and deliberate online falsehoods that may seek to sow discord in our society. In recent years, commentators have pointed out we live in a post-truth world, and Brexit and the 2016 US Presidential elections have shown that these are divisive and can threaten the fabric of society. Recent events such as the OCBC scam, shows that no one is spared and everyone plays an important role in both cyber & digital security. We have to be aware of phishing and scams.

Next, to help you understand what the Singapore government does with regards to cybersecurity, I would like to introduce our national cyber security agency - CSA and the Singapore cybersecurity strategy. This will set the ground for the rest of the speech. CSA was formed in 2015 and is given the task of protecting Singapore’s cyber space. CSA was established under the Prime Minister’s Office (PMO), and is administratively managed by the Ministry of Communications and Information (MCI).

CSA published Singapore’s 1st edition of the Cybersecurity Strategy which was announced by Prime Minister Lee Hsien Loong at the Singapore International Cyber Week in 2016. Strategy 2016 sets out Singapore’s vision, goals and priorities for cybersecurity. It engenders coordinated action and facilitates international partnerships for a resilient and trusted cyber environment.

In 2021, Singapore updated its Cybersecurity Strategy to reflect the rapidly evolving strategic and technological environment. Strategy 21 comprises 3 strategic pillars and 2 foundational enablers.
Compared to Strategy 2016, Strategy 21 takes a more proactive stance to address threats, broaden the scope of protection, and seeks to develop deeper partnerships with
industry and other organisations to adapt to the changes in our cyber operating environment. Strategy 21 also places greater emphasis on workforce and ecosystem development as key enablers of our cybersecurity.
One key observation is that Strategy 21 sets out 2 foundational enablers, namely “Developing a Vibrant Ecosystem” and “Growing a Robust Cyber Talent Pipeline”. These foundational enablers help to support the 3 strategic pillars which are “Build Resilient Infrastructure”, “Enable a Safer Cyberspace” and “Enhance International Cyber Cooperation”. This differs from Strategy 2016 where “Developing a Vibrant Cybersecurity Ecosystem” was a pillar itself. The government may have adjusted its strategy, as it felt that a strong ecosystem and also the newly included “Building a Cyber Talent Pipeline” is critical to the success in other areas, helping to support the 3 pillars.

I will share about one foundation enabler and one strategic pillar and I believe if there are any questions in other areas, we can discuss it in the Q&A session.

One of the foundation enabler of Strategy 21 is “Growing a Robust Cyber Talent Pipeline”. As I said earlier in my speech, our strength lies in our people and the successful execution of our cybersecurity strategy ultimately hinges on our people. CSA and the government partners with the industry, Institute of Higher Learning such as polytechnics and universities as well as professional partners to achieve these goals. The government will support people from a diverse range of backgrounds and support youths, women and mid-career professionals to pursue a cybersecurity career.

Youths are our future and grooming the next generation of cyber defenders is key. We need to expose them to cyber security when they are young so that they can consider it as a career in the future. One event I helped to lead when I was in polytechnic was the Youth Cyber Exploration Programme (YCEP) in short. YCEP is a cybersecurity bootcamp co-organised by CSA and the 5 polytechnics, to provide secondary school students with exposure to cyber security. Even if they don’t pursue cybersecurity as a career, these people could become advocates and ambassadors of cybersecurity, leading to a safer cyberspace for all.

Institutes of Higher Learning can help by providing a safe and trusted environment to experiment within a sandbox, fail and learn from mistakes too. In polytechnic, I was allowed to experiment and set-up a cybersecurity Special Interest Group, or SIG. Today the SIG is well established and has also inspired SIGs in other areas such as Artificial Intelligence, in short AI, and Cloud.

Having such entrepreneurial spirit and drive is what we need among our youths today and this ties in to the other foundation enabler "Developing a vibrant ecosystem", to have the innovative spirit to push the forefront of cybersecurity R&D in Singapore.

Upskilling is another key aspect of "Growing a Robust Cyber Talent Pipeline". The government is working on this area on several fronts. For example, the Government launched the Skills Framework for ICT and the OT Cybersecurity Competency Framework, which are tools that enterprises can leverage to enhance career pathways for cybersecurity professionals in their organisation. Programmes such as the Cybersecurity Development Programme, and training provided by CSA Academy helps upskill and train a pool of cybersecurity professionals for the public sector.

Another aspect of this enabler is to Foster a dynamic sector with strong professional communities. Even as the government sets the nation’s strategy and rolls out policies, a bottom-up grassroots community approach will help to enhance and make the local cybersecurity community more vibrant. The government aims to support and recognise such community efforts. For example, CSA supports the Cybersecurity Awards, an annual event organised by the Association of Information Security Professionals, that recognises enterprises and individuals who have made significant contributions to the local cybersecurity ecosystem. I am humbled to have received this award in the Student Category in 2020.

Div0 is one such volunteer-driven cybersecurity community. Div0 has quarters specialising in several areas such as AI Security, Bug Bounty, Car Security and Drone Security. One initiative by Div0 is Hacksmith. The aim of this hackathon is to promote the local and regional cybersecurity tools and development culture. Teams which developed outstanding tools were encouraged to present at prestigious international conferences such as Black Hat Asia Arsenal.

Div0 also helps to co-host the Global Cybersecurity Camp, GCC. GCC is an annual international week-long cybersecurity talent development camp organised by leading cybersecurity communities and institutes from Japan, South Korea, Singapore, Taiwan, Australia, Malaysia, Thailand and Vietnam. It aims to facilitate international collaborations and partnerships amongst cybersecurity institutions and communities to boost the quality of cybersecurity talents. This is good for interaction between countries in ASEAN and Asia-Pacific and helps foster trust and builds connections between countries. I participated in the 2020 edition, held in Tokyo, Japan. Apart from learning more advanced cybersecurity skills, I also got the chance to appreciate Japanese culture and meet people from various nationalities. Next year's edition will be hosted in Singapore, which should be the first in person run since 2020.

Moving on, I will now talk about the 1 of the 3 strategic pillars of Strategy 21 that is more relevant to this conference.

This strategic pillar is "Enhance International Cyber Cooperation". Singapore's stand has always been to uphold a rule-based order and international law, and must ensure that we are never bullied just because of our size. Cyber threats are international and cross-border. Given these two elements it is thus apt for Singapore to actively spearhead initiatives and establish cybernorms at the global level.

There are many platforms for regional and international cooperation and I will share a few. Singapore hosts the Singapore International Cyber Week, SICW for short every year, which forges deep public private partnerships and facilitates multi-stakeholder dialogue sessions. Singapore also hosts the ASEAN Ministerial Conference on Cybersecurity (AMCC) on the sidelines of SICW. The United Nations is a platform for all countries to develop norms, rules and standards. Singapore is currently chairing the Open-Ended Working Group on Security and in the Use of ICTs. Although we are a small country, it is good that Singapore can punch above our weight and lead such efforts, and the stability of our region ultimately depends on countries adhering to the rules based order.

Singapore also contributes to international efforts to combat cross-border cyber threats. We maintain bilateral ties with key countries, exchange best practices and coordinate capacity. Singapore will strengthen multilateral cooperation with regional partners. Regionally, Singapore conducts the annual ASEAN Cyber Incident Drill (ACID). Very relevant to this conference is the launch of the ASEAN Computer Emergency Response Team, known as CERT, Information Exchange Mechanism. It was launched in June 2021 at the first ASEAN Digital Ministers' Meeting. This initiative will support ASEAN CERT-CERT cooperation and improve information sharing among ASEAN members. INTERPOL also has its regional HQ based here and works closely with Singapore to combat cross-border cybercrime.

Apart from Strategy 21 which I have been sharing earlier which mainly deals with cyber security, we must have digital security as well. Digital security will lead to digital resilience enabling a more safe and secure Singapore. Given the proliferation of fake news on social media platforms and disinformation campaigns, I believe a whole of society effort will help in shoring up on resilience.

At a national level, the Singapore government has laws and various tools to tackle this challenge. Laws such as Protection from Online Falsehood and Manipulation Act (POFMA) and Foreign Interference Countermeasures Act (FICA) allow the government to deal with attempts to disrupt our domestic politics or social cohesion.

Companies and associations play their part too in building a more digitally resilient Singapore. For example, AI Singapore recently launched a competition to find solutions to detect fake media. The aim is to develop AI solutions to combat deepfakes. One of the ways to combat deepfake is to use technology to counter technology.

On the personal front, we can exercise our own discretion and always verify the information online first especially if it seems to be intended to evoke strong emotions from you. This is similar to spotting signs of scams. As the saying goes, “If it is too good to be true, it probably is”.

As a digitally savvy generation of youths, there are many ways to contribute your skills and talent, towards the betterment of Singapore, ASEAN and the world’s cybersecurity.

For secondary school students, do look out for YCEP by CSA and the 5 polytechnics where you will have the opportunities to have hands-on experience with cybersecurity. JC students can look out for Whitehacks organised by SMU.

You can also consider joining Div0 or various professional cybersecurity associations and volunteer at conferences where you get to meet people from the cybersecurity industry.

If you are a user of technology, which I assume all of you are, since you are “here” on Zoom, you can contribute to a safer cyberspace by educating your fellow peers and family members on how to stay safe online. You can volunteer with IMDA and various other organisations to help seniors navigate safely online just to name an example.

For guys who will serve National Service in a couple of years time, MINDEF-SAF has launched a new scheme called digital specialists in partnership with NTU. These digital specialists will develop AI applications and perform software engineering tasks in support of real-world military operations. NSFs will be able to take up modules at NTU, earning credits that contribute to a degree in Data Science and AI, Computer Science or Computer Engineering. This is on top of the cyber specialist scheme which was rolled out in 2018.

Before I conclude my speech, I would like to share some of my hopes for the future with regards to cybersecurity. I hope some cybersecurity can be moved upstream. This means protection at an Internet Service Provider level. For example, instead of asking all Singaporeans to install water filters at home, the government does it at a national level, by having PUB oversee our 4 national taps. Something similar could be done at a national level for cybersecurity as well. For example, I came across a prototype by the Singapore government which identifies websites that impersonate government websites and possibly take them down before they can even phish for information from the public. The current method of identifying scam calls using +65 and the app “ScamShield” developed by Govtech are good examples that demonstrate how such things can be done at a national level.

I also hope for a more heightened awareness of cyber and digital security among the population. Collectively as a country and a region, with improved awareness and cyber hygiene, we can all enjoy and maintain our digital way of life.

To conclude, I challenge delegates to dream, ideate, discuss and come up with solutions and pragmatic policies to foster more trust in our systems, build a more resilient system and society and solve the pressing needs of securing our cyberspace.

Thank you and I hope this speech has been insightful for you.