Keynote Address by Minister for Communications and Information Mrs Josephine Teo at the Operational Technology Cybersecurity Expert Panel (OTCEP) Forum 2022 on 12 July

Distinguished panellists

Colleagues and Friends

Introduction

1. Thank you for inviting me.

2. Modern life as we know is unimaginable without technology. Much of it is Operational Technology or OT.

3. They include the air traffic control and landing systems that helped our overseas guests arrive safely in Singapore, and the immigration clearance and baggage handling and systems that got you out of Changi Airport in less than 30 minutes.

4. At hotels, clean, drinkable water flows from your tap. At night, the cityscape lights up from uninterrupted energy provided by our power grid. Without the electrical systems that power air-conditioning right now, we would be breaking out in heavy perspiration.

5. Most of the time, operational technologies work well enough that we have no need to question their reliability or resilience. However, in recent years, they have also become vulnerable to cyber-attacks.

6. This is because many OT systems are now inter-connected with IT systems. Cyber-attacks that used to disrupt IT systems only can now impact physical operations. We have already witnessed such occurrences in the water, energy, and other critical sectors.

OT threats are always evolving, and we must keep up.

7. Of course, some of these attacks are intended to disrupt critical supply chains that will make our lives on a day-to-day basis very uncomfortable. Last September, US company

140 Hill Street #01-01A, Old Hill Street Police Station, Singapore 179369
1800 837 9655 mci_connects@mci.gov.sg www.mci.gov.sg

New Cooperative, which accounts for nearly half of the nation's grain production, was hit by a ransomware attack. Fortunately, they managed to avoid serious supply chain issues by quickly containing the breach and developing manual workarounds.

8. Attacks could also have knock-on effects beyond an immediate target, which amplify their impact. Earlier this year, a cyberattack on a Viasat communications satellite caused service interruption for tens of thousands of customers across Europe. This included a wind turbine operator in Germany that lost remote control over their assets. There was no lasting harm from the incident, but it clearly demonstrates the long reach of OT cyberattacks.

9. Other attacks can be even more malicious, intended to cause direct harm to people. In April 2020, an attack on several Water Authority facilities in Israel aimed to raise chlorine to dangerous levels, causing widespread poisoning. Israeli authorities managed to stop the attack short of any damage, but this is a stark reminder of what is at stake or the vulnerabilities that we face for OT systems.

10. In the cyber world, a hacker on the other side of the globe is as close to our systems as the hacker in the basement next door. The long reach of attackers unimpeded by distance means that we must always be prepared to mount a defence against best-in-class threat actors.

11. Unfortunately, best-in-class threat actors have started selling their services and tools to lesser threat actors. As a result, there are far fewer barriers now to mount an attack with the latest and most sophisticated modalities and tools. The lucrative nature of this business also creates powerful incentives for innovation of the wrong kind.

12. There is no way of avoiding the risks without systematic efforts to find and patch vulnerabilities. We must also keep abreast of new cybersecurity threats, share our knowledge and collaborate to help each other.

<u>To uplift OT cybersecurity posture in Singapore, we must improve our People, Process, and Technology.</u>

13. To be effective in OT cybersecurity, our people, processes and technology are our critical assets. This is why we invest in them. Events such as this OT Cyber Experts Panel

140 Hill Street #01-01A, Old Hill Street Police Station, Singapore 179369
1800 837 9655 mci_connects@mci.gov.sg www.mci.gov.sg

Forum are also important, to raise awareness and knowledge levels within Singapore's OT community. For this reason, I want to thank the members of the OTCEP for making your way to join us again this year.

14. Let me briefly explain Singapore's efforts in the areas of People, Process, and Technology.

15. First, People. Talent is the anchor that undergirds our cybersecurity posture so it is important to invest in developing OT cybersecurity professionals.

16. Last year, the Cyber Security Agency of Singapore (CSA) launched the OT Cybersecurity Competency Framework[1]. It is a systematic compilation of relevant job roles with the corresponding technical skills and core competencies. It carries all of these articulations and puts them together in a comprehensive compilation.

17. With this Framework guiding skills development, we can better design programmes to support the training of cybersecurity professionals in OT, and the training of OT Professionals in cybersecurity.

18. For example, to encourage STEM professionals to enter the field of OT cybersecurity, CSA is funding 80 scholarships over 3 years to pursue the Master of Science in Security by Design, at the Singapore University of Technology & Design (SUTD). This is a specialised programme that is offered by SUTD to encourage involvement and take up. The cybersecurity research centre at SUTD, iTrust, hosts industrial testbeds that simulate critical infrastructure. These scholars can therefore readily access some of the world's best research, design, and training facilities for cyber-physical systems. Applications for the scholarship are open, and we encourage interested applicants to apply.

19. Second, Process. To coordinate our defensive efforts, we need good processes. But even good processes must keep evolving to meet the needs of our organisations, especially so in a fast-paced environment like cybersecurity. We talked about this when we met with the panellists this morning. They expressed concern that even when systems are being designed with cybersecurity in mind and the first iteration is good

[1] OTCCF launched on 8 October 2021.

140 Hill Street #01-01A, Old Hill Street Police Station, Singapore 179369
1800 837 9655 mci_connects@mci.gov.sg www.mci.gov.sg

enough, we need to have a continued emphasis on updating the processes, as the cybersecurity measures in OT systems need to be kept up.

20. Last week, CSA published the revised Cybersecurity Code-of-Practice. Applicable to both IT and OT systems that are designated as Critical Information Infrastructure, the Code-of-Practice has been updated to keep pace with developments in the cyber threat landscape, taking into account learning from its first iteration.

21. So that brings me to the third area, Technology. It takes a community to develop technology that works well. Practitioners and researchers need to come together to ensure that the tools are fit for purpose and make improvements when necessary.

22. Take security evaluation for example, which involves testing hardware and software to ensure compliance with standards. Security evaluation is important for OT systems because there needs to be assurance that system components are not rife with vulnerabilities. Researchers and product evaluators need to work together to figure out how they can improve security evaluation technology.

23. This is why in May this year, CSA and Nanyang Technological University launched Singapore's National Integrated Centre for Evaluation. The Centre is a 'one-stop' facility for cybersecurity evaluation and certification. It has advanced equipment for available for use, and holds professional training courses. It seeks to bring together the different players in the security evaluation ecosystem, to form a community of practice that will learn together and advance the field.

24. In implementing these initiatives in the areas of People, Process, and Technology, we have deepened collaboration throughout our cybersecurity ecosystem. The Government, industry sectors, and academia will continue to learn together, and continually raise the bar.

Conclusion

25. This conference is another way to enhance our mutual learning. There is much to be gained from bringing people with different experiences here, so we can share our unique perspectives, and put our minds together to address our challenges in OT cybersecurity.

140 Hill Street #01-01A, Old Hill Street Police Station, Singapore 179369
1800 837 9655 mci_connects@mci.gov.sg www.mci.gov.sg

26. This year, we have added two new panellists to the OTCEP. Mr Daniel Ehrenreich has over 32 years of engineering experience across a range of OT sectors including energy and water, which we will all agree are essential in any setting. Ms Sarah Fluchs is currently leading a government-funded research project on security by design for industrial control systems, in partnership with academia and industry representatives. Both Daniel and Sarah bring so much to the table. I am very excited by the new perspectives that they will be able to share with our participants. I am certainly very confident that they will both be valuable contributors to the already remarkable expertise of the panel.

27. The OTCEP forum agenda also features representatives from a range of organisations, including OT companies Schneider Electric and Honeywell, cybersecurity company Claroty, government agencies GovTech, HTX, and MINDEF, and professional services firms Deloitte, KPMG, and Ernst & Young. As OT cybersecurity becomes more mature, we expect an even wider range of organisations to participate.

28. Let's learn as much as we can from one another so that collectively, we can do an even better job keeping OT safe and secure.

29. I wish all of you a pleasant and fruitful conference. Thank you.

+++

140 Hill Street #01-01A, Old Hill Street Police Station, Singapore 179369
1800 837 9655 mci_connects@mci.gov.sg www.mci.gov.sg