Ministry of Communications and Information
An Engaged and Connected Singapore

SPEECH BY MRS JOSEPHINE TEO, MINISTER FOR COMMUNICATIONS AND INFORMATION, AT THE OPERATIONAL TECHNOLOGY CYBERSECURITY EXPERT PANEL (OTCEP) FORUM 2023 ON 22 AUGUST 2023, 9.05AM

Embracing New Perspectives in OT Cybersecurity

Distinguished panellists
Colleagues and Friends

Introduction

1. Thank you for inviting me to join you at this third edition of the OTCEP forum. I am glad to see familiar as well as new faces since the forum was held last year.

2. We live in uncertain times. The geopolitical situation remains highly charged with an ongoing war in Europe. Inevitably, tensions in the physical world spill over into the cyber arena.

3. Technologies like Artificial Intelligence (AI) and quantum computing, while exciting, also make the cyber threat landscape more challenging to navigate.

4. The OT cybersecurity sector, which you are part of, has seen more than its fair share of disruption. OT systems are traditionally placed in protected environments, managed and monitored separately from Internet-facing IT systems.

5. However, in recent years, digitalisation has accelerated in the OT industry, with more companies tapping on IT solutions to streamline and enhance the efficiency of their work processes.

6. Unfortunately, the same technologies that enable OT operators to readily control their systems via a web interface can also allow bad actors to hijack OT systems and manipulate them to cause damage and destruction.

7. For example, you will be familiar with a suspected ransomware attack targeted a major German oil and gas supplier, Oiltanking.

8. This attack reportedly affected the company's supply and distribution of petrol around Germany. The company was forced to declare "force majeure". Its customers, the petrol companies, had to seek out other suppliers to minimise disruption.

9. We have also seen hacktivist groups attack OT systems to gain public attention. In April, water irrigation and wastewater treatment systems in Israel were hit by a cyber-attack as part of an annual hacktivist campaign "OpIsrael".

10. The attack disrupted the treatment processes of some water processors and disabled the automated irrigation systems of some farms, forcing them to switch to manual irrigation.

11. The OT cybersecurity sector faces challenges on many fronts. How should defenders deal with threats and disruptions to mitigate the risks while maximising the opportunities?

12. Here in Singapore, we believe three lines of effort are critical. They are the 3Ts - technology, talent and teamwork.

Emerging technologies are both a threat and an opportunity for cybersecurity defenders.

13. Let me begin with technology.

14. Advances in **artificial intelligence (AI) and machine learning (ML)** are threatening to disrupt the cybersecurity industry. They can be weaponised by threat actors.

15. For example, cybercriminals could use AI chatbots like ChatGPT to craft convincing phishing emails at scale. It is already happening.

16. Without human intervention, advanced malware could also tap on AI to alter the behaviour to evade detection. One example is Emotet, an advanced malware targeting banks.

17. But AI also represents tremendous opportunities in enhancing our defensive capabilities.

18. Companies have developed products that utilised AI and Machine Learning to detect abnormal behavioural patterns in control systems, thwarting malicious cyber activities before they create greater disruption. AI-powered systems have been used to enhance available tools, such as firewalls, to bolster our defence capabilities.

19. **Quantum computing** is another area that carries both peril and potential.

20. The lightning computing speed of quantum computers means that good actors - like us - could also use it for public good – to create new, stronger cryptographic algorithms that are resistant to attacks from traditional computers. This could provide better, more secure ways for us to encrypt our data and communicate securely, for both IT and OT systems.

21. As a community, we should harness these technologies to improve our collective defences. It is therefore useful to start discussing these possibilities at international platforms, such as the Forum today.

We need to invest in building up talent for the OT cybersecurity industry.

22. The second ‘T’ I want to cover is ‘Talent’.

23. The best AI tools and quantum computers cannot fully replace the need for humans to be in the loop. The OT cybersecurity sector, specifically, requires a niche pool of talent with both IT and OT capabilities.

24. With this consideration in mind, Singapore launched the **OT Cybersecurity Competency Framework** two years ago. It provides guidance on the competencies that OT cybersecurity professionals need, and supports OT cyber talent attraction and development in Singapore.

25. At the last OTCEP Forum, I announced the launch of the **CSA-iTrust Master of Science in Security by Design Scholarship Programme**, which seeks to encourage STEM professionals to enter the field of OT cybersecurity. I am glad to announce the launch this week of the **inaugural Singapore-Industrial Control Systems Cybersecurity 301 (or SG-ICS301) course**.

26. Singapore's own CSA Academy has worked in partnership with the U.S. Cybersecurity and Infrastructure Security Agency (CISA), to design this programme. It equips participants with the concepts, theories and practical hands-on experience for protecting OT networks and securing our CII systems from cyber-attacks.

27. The inaugural run of the course will involve around 40 participants from Singapore, ASEAN, Bangladesh and Maldives. It is a good beginning, and I am certain that the course – held alongside this Forum – will benefit many more batches of participants, thus enhancing OT security within this region.

We need to work as a <u>team</u> to tackle emerging challenges in OT cybersecurity.

28. The third piece of the puzzle is teamwork.

29. When attackers come at us on multiple fronts, it is even more important that we work together across government, industry and academia, to build up the interdisciplinary expertise and partnership mechanisms to respond effectively.

30. Cybersecurity is after all, an international team sport, and we can only win if we're playing as one against our common enemy.

31. Another area where we should cooperate is in the creation of technical standards. Technical standards are important to any industry – they help companies to promote public trust in the industry's products and services.

32. For rapidly developing sectors such as OT cybersecurity, there is an added challenge of needing to keep abreast of new developments. The Government therefore needs to work closely with industry experts and other stakeholders to develop standards that are relevant, accurate and up to date.

33. Most recently, CSA contributed to the development of the cybersecurity **Technical Reference (TR) on "Securing Cyber-Physical Systems for Buildings"**.

34. The development of the standards was industry-led, and involved a range of experts from the public and private sectors who contributed in their individual capacity.

35. The Technical Reference was published in May and is the first in Singapore which provides guidance on securing cyber-physical systems of buildings and facilities.

36. These initiatives show CSA'scommitment in working with partners on all fronts. To this end, I am pleased to announce two MOUs that will be signed at this Forum:

a. CSA will be signing an **MOU with Dragos**, a global industry leader in OT cybersecurity, to fortify Singapore's OT cybersecurity capabilities through collaborations in threat intelligence, consultancy and risk assessment, incident response and training. The MOU will facilitate more information sharing and cross-fertilisation of ideas, foster alignment with industry best practices and

provide CII sectors access to expert knowledge. Local cybersecurity companies will also have opportunities to work collaboratively with Dragos through this MOU.

b. Another MOU will be signed today between ST Engineering and Siemens Energy. Where Siemens Energy provides the experience and innovation as a global OEM, ST Engineering empowers regional integration and execution. The collaboration between these companies on OT cybersecurity will enhance the resilience of our national critical infrastructure in Singapore. The MOU will facilitate knowledge sharing, information exchange, and joint exploration or entry into new markets and use cases for both companies. I wish them a successful and fruitful partnership.

37. To everyone else in the audience, the OTCEP Forum is the ideal platform for you to forge and strengthen partnerships with others in the industry, academia or government.

38. I urge you to consider how you may also be able to realise untapped potential opportunities for your organisation through this platform.

Conclusion

39. In conclusion, we cannot be sure what new challenges we might face in the digital domain, and specifically in the field of OT cybersecurity.

40. But by making better use of advances in technologies, nurturing the capabilities of our talent pool, and fostering stronger teamwork across the ecosystem, I am sure we can make the OT cyber arena – and by extension, the physical world – a safer one.

41. I thank you all and wish all of you an enriching Forum.

+++