TRANSCRIPT OF OPENING ADDRESS BY DEPUTY PRIME MINISTER AND MINISTER FOR FINANCE, MR LAWRENCE WONG AT THE 4TH SINGAPORE DEFENCE TECHNOLOGY SUMMIT ON 23 MAR 2023 AT 0915HRS

Your Excellencies,

Distinguished Guests,

Ladies and Gentlemen,

1. I am very happy to join you this morning at the 4th Singapore Defence Technology Summit.

a. Let me extend a warm welcome to all our overseas guests.

b. The last summit was held in 2021, when Singapore still had pandemic-related restrictions. We had to scale back the number of in-person attendees and we largely had a virtual conference.

c. This year, we have opened up completely; we have removed all our restrictions, so it is very good to see so many of you here in-person. I am sure all of you are glad to have the chance to travel back in Asia, for some of you perhaps the first time, and to be able to interact face-to-face, because there is nothing that can replace that kind of personal contact, and virtual, remote meetings do not quite have the same effect. So thank you all for being here at this Summit and we value your participation.

2. We are meeting in a time of great change, in more ways than one. The pandemic has disrupted all our lives, and forced societies to adapt to new ways of living and working.

3. The geopolitical environment globally is fast evolving too.

a. The war in Ukraine has upended peace and stability in Europe, and forced countries everywhere to re-evaluate their security priorities.

b. Great power rivalry between America and China has continued to intensify across many domains.

c. The leaders of the two countries have said that they do not want a new Cold War after their meeting in Bali last year. Unfortunately, events since the start of this year have led to a more confrontational turn in the relationship.

d. In this new era of geopolitical contestation, we see strategic trust between countries continuing to erode, and that is pushing security considerations to the forefront of many countries' concerns and priorities.

4. Amidst these changes, it is even more important for countries to come together to engage in dialogue. After all, Governments everywhere, Governments in all countries, we want the best for their people. We seek to lift the human condition, and to maximise the potential of our citizens. But human nature is such that there will always be distrust and rivalry. That is why we really must continue to put diplomacy first and strive to engage, not just our partners, but also, perhaps more so, our adversaries and competitors. Amongst countries, there will inevitably be differences. Some of these differences may even be irreconcilable. But that does not mean we are destined for conflict. Instead, we have to learn how to set aside these differences, and focus on the many areas of common interests, where we can work together. That's how we can start to build trust, which is crucial. Because when trust runs empty, all hope is lost.

5. That is exactly what we hope to do through forums like this Defence Technology Summit. We started this summit about four years ago amidst rapid changes in defence technology. Our intent was to bring together the defence technology community – government and military officials, leaders from both national and private defence technology industries, and researchers from academia – to exchange perspectives and ideas on how the changes around us affect the defence and security landscape.

6. In recent years, one major change that all of us all grappling with is a shift in the development of technology from Governments to commercial enterprises, and the emergence of more dual-use technologies; hence the theme of the conference this year.

a. Historically, government-funded Research & Development (or R&D) played a central role in advancing technology for humankind. If we go back half a century ago, government-funded R&D far surpassed commercial R&D in both scale and in ambition.

b. For that reason, many cutting-edge technologies that we use today can be traced back to Government research.

   i. For instance, GPS technology, which we are all familiar with, and which we all use, was originally developed by the US military in the 1970s for missile guidance. Since then, its use has greatly expanded to a plethora of commercial uses, from personal navigation to helping businesses target services to consumers.

   ii. It was also the US Defence Department's research arm, called the Advanced Research Projects Agency back then, which developed packet switching and the ARPANET, and this eventually developed to the modern internet we all use today.

7. But the technology landscape has changed. In the vast majority of OECD countries now, the proportion of R&D funded by commercial enterprises has outstripped government R&D.

a. Spurred by competitive pressures, these commercial enterprises are innovating at a rapid pace, and are developing high-quality products at the cutting edge, including in areas such as Artificial Intelligence (AI), robotics, digital communications and bio-technology.

b. Moreover, because these products and their underlying technology often have widespread applications, they quickly achieve economies of scale and high cost-efficiency.

8. Given these developments, it is no surprise that more commercial technologies are finding applications in the military realm. We see this clearly in the digital domain, where advances in digital technologies have the potential to enhance the "network-centric operations" of modern militaries.

a. Such operations require militaries to make sense of large amounts of intelligence and operational data. And here, commercial offerings are already superior to existing traditional, bespoke defence solutions in some ways. For example, 5G and low-earth orbit satellite communications have the potential to allow faster and more reliable communications in the battlefield. Commercial cloud computing infrastructure can also enable militaries to better store and process large amounts of data securely.

b. As they continue to improve, the value they provide over bespoke defence solutions in certain areas will no doubt increase, and countries will need to figure out how best to adopt or deploy them. This is already happening. In a sign of the changing times, the Israeli Defence Forces is moving some of its data from their own self developed private cloud to one provided by Amazon Web Services and Google.

9. These changes will not be confined to the digital domain. We can expect to see commercial technologies increasingly play a direct role in the delivery of lethal force as well. Already today, commercial technologies are being used in unexpected and asymmetric ways on the battlefield. For example, in Ukraine, the military has successfully retrofitted commercial off-the-shelf drones used by aerial photography hobbyists to attack Russian tanks with bombs and grenades.

10. All these have blurred the lines separating traditional notions of civilian and military technologies and expanded the types of technologies that are considered "dual-use". And this has serious implications for defence establishments all over the world. Today, let me focus my remarks on three opportunities and challenges before us, and I will go through each of them in turn.

11. **First**, how can defence establishments effectively leverage on the opportunities presented by digital and dual use technologies?

12. Defence establishments will have to take a hard look at how to adapt and integrate commercial technologies for their defence and security needs. And to do this successfully, they must relook how they design, develop and procure defence systems and platforms.

13. Traditionally, all of you know, this has been a complex and drawn-out affair. A typical defence procurement involves multi-stage approval processes, with rigorous evaluations to ensure quality and safety. This is not without good reason; we all understand why this has to be done – it is well suited for military platforms like fighter jets, warships and tanks that are meant to last for decades.

14. But these traditional processes are not always “fit for purpose” when it comes to commercial technologies, where the typical product life-cycle is measured in years not decades. Moreover, for some emerging technologies, the most innovative companies are smaller start-ups which often lack the resources and time to engage in drawn-out procurement exercises.

15. Defence establishments will need to adapt to these new realities. Failure to do so would mean missing out on new capabilities, or worse, adopting solutions that quickly become obsolete the moment they are rolled out.

a. For a start, design and procurement processes can no longer be one-size-fits all – where they involve commercial technologies, they probably will need to be streamlined and simplified.

b. Processes aside, military units must also adapt to new ways of working with each other. Given the rapid pace of change, product development teams can no longer be comfortable working behind-the-scenes, separated away from operational units. This will only result in slow and outdated solutions. Instead, we must bring them closer, embedding them together if necessary. Only then can rapidly evolving new technologies be quickly adapted to meet operational needs.

16. These moves will not be easy. They involve not just organisational changes, but also cultural changes too. But they are necessary for the defence sector to fully benefit from digital and dual use technologies.

17. **Second**, as commercial enterprises continue to make technology breakthroughs across various fields, and I am sure they will, how can we guide their development to ensure these new technologies contribute to our collective security, rather than undermine it?

18. We must expect businesses to continue pushing the technological frontiers. There will therefore increasingly be a need for defence establishments and governments to step in to guide the development and application of these new technologies.

19. Of course, this is not something new – governments have always played this role. Take the example of nuclear energy. It is a powerful technology initially developed for military use during World War II. But it also has tremendous potential as a force for good. So governments collectively developed international protocols to harness nuclear technology effectively, in areas like civilian energy and medical use, as well as a system of controls to curb its proliferation to bad actors.

20. Today, we will have to consider how to do this for fast-developing technologies with wide ranging dual-use applications. One immediate issue is how we deal with the rapidly advancing and game-changing technology of Artificial Intelligence (AI).

21. Like so many modern dual-use technologies, AI is dual-use and is being advanced by commercial entities for profit. We have already seen glimpses of what generative AI can do, and these possibilities will only expand very quickly in the coming years. We can easily imagine a future powered by AI – improving all aspects of life, and enabling breakthroughs in different fields from medicine to transport. But AI is potentially also a very powerful weapon – it can accelerate the future of autonomous warfare, enabling weapons that are more precise, cheaper, faster and, with the capabilities to learn, making their missions virtually unstoppable.

22. All these will raise very difficult questions.

a. what degree of control should humans have over autonomous devices, and how should that be adjusted in different contexts?

b. How do we ensure accountability when unintended incidents occur?

c. Basically, how can the world get the best of AI while protecting ourselves against the worst possible consequences?

23. There are no easy answers. But what is clear is that we cannot leave commercial enterprises to answer these questions alone. Instead, Governments, industry, and civil society must all work together to set the international principles, norms and guidelines to guide the development of AI without holding back the innovation that is necessary to advance humanity.

a. I am glad an increasing number of countries are doing just that. Multilaterally, there are efforts such as the “Global Partnership on AI” to bring together countries and leading experts to guide the responsible development and use of AI. We have also seen positive moves on the defence front, such as the US’ recent declaration on the responsible use of AI in the military (released last month).

b. And while we are a small country, Singapore will do our part, especially as a technological hub in Southeast Asia. Apart from actively participating in forums like the Global Partnership on AI, we recently launched “AI Verify” (in May 2022), the world’s first testing toolkit to help companies objectively assess and verify whether their AI products are responsible and meet key international principles. We hope companies and other stakeholders will find it useful in evaluating and guiding their AI development efforts.

24. Third, as new technologies become more pervasive, how can we deal with the expanding range of asymmetric threats they have unleashed?

a. This is a particularly pressing issue in cyberspace, where a growing number of malicious actors have sprung up to exploit vulnerabilities inherent in computer systems, many of whom are capable of launching “best-in-class” cyber-attacks.

b. Take ransomware for example. In the past two years alone, criminal groups have launched ransomware attacks against major gas lines, global food supply chains, and hospital systems all over the world. This scope of damage has elevated ransomware from what was previously a petty cybercrime to a credible threat to national security.

c. Meanwhile, in the Asia Pacific region, the Dark Pink Advanced Persistent Threat (APT) Campaign has launched repeated espionage attacks on governments and militaries.

25. These emerging cyber threats are global in nature, and if we want to mount effective responses and stay ahead of these adversaries, global cooperation will be needed.

a. Where they involve malicious groups operating across geographical lines and jurisdictions, countries must work together to coordinate policy responses, share information, and even conduct joint operations.

b. Countries can also improve their collective resilience against cyber threats by collaborating on capacity building. This is something we have been focusing on in our part of the world in Southeast Asia, through the ASEAN-Singapore Cybersecurity Centre of Excellence (ASCCE). Apart from providing the region with cyber training, as well as information on the latest cyber threats and best practices, the centre also helps strengthen the region's research capabilities in this rapidly evolving field.

26. I have shared my thoughts on three implications and challenges today thrown up by the rapid change in the defence technology landscape. They involve complex issues which no single organisation or country can fully solve by themselves.

27. And that is why we have assembled here today a diverse set of thought leaders, industry experts and defence professionals. I am sure we won't have the answers now, but at least we can make progress by coming together and engaging in constructive dialogue. We may all have different background and interests, but I believe we all share the common desire to harness technology to benefit our countries, our peoples, and ultimately, our world. So I hope this conference will enable all of you to share your experiences and best practices, to spark new ideas, and ultimately, to help us deal with our shared challenges together.

28. On that note, let me wish everyone a fulfilling and productive summit ahead. Thank you.