MINDEF
SINGAPORE

SPEECH

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

WELCOME ADDRESS BY MINISTER FOR DEFENCE DR NG ENG HEN AT THE 3rd SINGAPORE DEFENCE TECHNOLOGY SUMMIT ON 12 OCTOBER 2021

Welcome Remarks

1. Senior defence officials, distinguished guests, ladies and gentlemen. First, a warm welcome to all of you to Singapore. I am very happy to meet and speak with you in person. A very warm welcome to the Singapore Defence Technology Summit (SDTS). This is the third since its inception. I think the strong showing at this year's Summit despite the global pandemic tells us two things. First, there is a strong desire to return to normalcy, albeit adjusted and scaled down because of COVID-19. Second, meetings like this Defence Technology Summit allow tech leaders, industry captains and professionals to discuss common challenges and differences, to shape a more secure future.

Relevance of SDTS Amidst Today's Conflict Landscape

2. I am a strong proponent for the SDTS and meetings of this genre because technological changes play a central role in conflicts. It is axiomatic that technology and science are neutral – humans start wars, not technologies. But all of us here would agree that technology, either its application or its availability, has inevitably shaped the conduct and outcomes of battles. I think this leads to the more relevant question: What role do defence technology leaders play in conflicts, either in its prosecution or prevention? Are they just suppliers of technological solutions, to reach desired outcomes, whatever the costs?

3. Take World War One (WWI) as a prime example, where I think a number of parallels with our time now exist. Historians agree that WWI was "the first modern mechanised industrial war". Oxford professor Margaret MacMillan in her book, *The War That Ended Peace,* described "a failure of imagination in not seeing how destructive such a conflict would be". This generation is in the midst of the 4th Industrial Revolution, with the pervasive Internet of Things to come. Similarly, for WWI's generation, their lived experience was the "Tele-net of Things". Modes of military communications were radically transformed from messengers on foot or horseback, dogs and carrier pigeons, or visual signalling to wired and wireless

telegraphy. Tens of thousands of miles of copper cables were laid, as was the exponential rise in the hardware for wireless transmission. Near instantaneous communication transformed trench warfare, accelerated and extended the mobilisation of troops and weapons. Coupled with advances in artillery that were more accurate, rapid and long-range, the scale and ferocity of modern armed conflict manifested itself vividly. After four years of global conflict in WWI, 20 million would lay dead and four empires extinguished. I am sure if you look though the historical archives of that time, that you will find some during that period, especially among leading scientists or engineers, who were concerned or even warned against the scale of devastation to come as a result of technological advances of that age.

4. This Technology Summit therefore seeks to give leaders and practitioners in defence technology a louder voice in shaping our future, and where possible, to prevent conflicts or at least to mitigate the loss of civilian if not military lives. Yes I know it is a high ambition, but one that is still worthy of our effort. To achieve that goal, there must be partnerships and consensus among friends and allies and even, perhaps especially, among those who disagree. The theme, "Building Confidence Amidst Technology Disruption", therefore, reflects this aspiration.

Threats and Responses

5. What specific areas need to be highlighted for discussion? I can name three which, similar to advances in the last century which preceded WWI, have great potential impact for destruction and disruption in our time.

6. The digital domain is a contested battle space. I don't think anyone will disagree. Real life examples abound from the effects of a digital virus on Iran's nuclear centrifuges, Ukraine's power grid in 2015, the recent Solarwinds hack and Colonial Pipeline ransomware attacks. Attacks in the digital battlefield pose a growing threat that can easily spill over, explode and wreck unintended havoc on the rest of society. These include disruption of hospital care, transport and power grids, as well as financial institutions, just to name a few. As the Internet and the Internet of Things (IoT) expand, the consequential impact may grow *pari passu*. The scale, scope and frequency of cyber-attacks are expected to rise, with non-state actors increasingly conducting attacks enabled by cyber and informational tools such as malware, ransomware, misinformation, disinformation and influence campaigns against private corporations and governments.

7. The Defence Technology Community ought to address in this Summit and elsewhere, on how and what rules should govern the digital domain. The need for frameworks to guide state and commercial behaviour in cyber, artificial intelligence (AI), big data and other emerging domains has become more urgent. Consensus will not be easy to achieve, but the conversations among corporations and countries must start, nonetheless. Just as in the kinetic world, the digital domain must move from an unfettered, no-rules based, "who dares, wins" architecture to one that prevents, at the very least, high-stakes catastrophes and disruption to civilian life.

8. There is also now a contest for dominance, if not supremacy, in space. Assets and capabilities in space are now critical to many facets of normal function of life on earth, which anti-satellite systems can cripple. As the number of private and state actors in space grow,

space can become a militarised zone and strategic miscalculations and inadvertent escalations can ensue.

9. Autonomous technologies and AI would be the third big area to discuss. Militaries, like other civilian organisations, want to exploit the potential of AI to deal with complex and voluminous data amid the fog of war, and make better and faster decisions. But can we tolerate mistakes, ultra-low statistically, but that result in loss of innocent lives or precipitate consequences from which there can be no retreat? What safeguards are needed, to be built in AI systems for robustness and accountability? These and other challenges, I think, are worth your attention.

Building Partnerships

10. Our search for stabilisers in this age of technological disruptions must necessarily involve partnerships. Countries need to come together to develop frameworks to guide behaviour and outcomes in digital, cyber, AI and other emerging domains. We should continue to support ongoing efforts at the United Nations (UN) to develop frameworks – whether on the application of international law, or fostering of norms and principles – to strengthen international order. Singapore, as Chair of the second Open-Ended Working Group on Security of and in the Use of Information and Communications Technologies, will do its part to enhance peace and stability in cyberspace.

11. Outside the UN, states can also pursue multilateral arrangements to address collective challenges. One such challenge is the risk of irresponsible use of AI in military applications. The AI Partnership for Defense has been effective in bringing together like-minded countries to promote and advance the responsible development and use of AI in the military. For its part, Singapore published the second edition of its Model AI Governance Framework last year, incorporating feedback and experiences from leading international forums such as the OECD [Organisation for Economic Co-operation and Development] Expert Group on AI and the European Commission's High-Level Expert Group. This year, we established the preliminary AI guiding principles of Responsible, Safe, Reliable and Robust for our defence establishment, and will continue to participate actively in multilateral cooperation on AI technologies, governance and policy.

12. This Summit hopes to serve as a platform and as a catalyst for industry, academia and government to build new partnerships and achieve virtuous outcomes.

Interagency Collaboration

13. Just as the kinetic services of air, land, and sea conduct exercises to enhance interoperability, build mutual confidence and understanding, their non-kinetic counterparts must follow suit. The cyber realm is one area we must rapidly invest in and develop to bring value to the nation's defence. In this regard, the Singapore Armed Forces (SAF) has established the Cybersecurity Task Force (CSTF), which brought together various cyber units across the Ministry of Defence (MINDEF) and the SAF for centralised command and control of cybersecurity operations across the defence sector. The taskforce conducted a range of cybersecurity exercises with valued partners from around the world. One such exercise was the Critical Infrastructure Security Showdown (CISS), an international cybersecurity exercise co-organised by the SAF and the Singapore University of Technology and Design (SUTD) that

was held in September this year. In this exercise, the SAF trained with specialists from our public utilities agencies and international military cyber teams to defend against attacks launched at testbeds that simulate our water treatment and distribution plants.

14. My Ministry has invested in non-kinetic infrastructure to spur ongoing developments. MINDEF has established a Digital Factory to allow project leads, developers, and designers to team up, build, test, and scale digital solutions securely. On the capabilities front, our Defence Science and Technology Agency (DSTA) acquires and adapts commercial AI, robotics and data analytics tools to realise new warfighting concepts and force multipliers. This includes adopting commercial cloud platforms to host less sensitive digital services, functions and data. In addition, in human capital, the SAF's Cybersecurity Task Force partners local universities to upskill military personnel through work-learn programmes and cybersecurity exercises.

Closing Remarks

15. In the week ahead, we will hear leading security and defence technology practitioners from around the world share their insights and experiences with building confidence amidst technology disruption. From C-suite executives in dominant technology firms, to senior government officials and distinguished academics, this Summit brings together a world-class gathering of minds to exchange ideas, forge partnerships, and realise new opportunities.

16. For gathering and participating here, I want to thank you very much. As with previous editions, I am confident that each of you will have a stimulating and productive summit. Thank you very much.

###