MINDEF
SINGAPORE

SPEECH

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

SPEECH BY SENIOR MINISTER OF STATE FOR DEFENCE MR HENG CHEE HOW AT THE 22ND ASIA-PACIFIC PROGRAMME FOR SENIOR MILITARY OFFICERS ON "THE EVOLVING SECURITY ENVIRONMENT IN THE ASIA PACIFIC AND ITS CHALLENGES" ON 5 OCTOBER 2021

1. Ambassador Ong Keng Yong, distinguished speakers, ladies and gentlemen. A very good morning to everyone. First, let me thank the S. Rajaratnam School of International Studies for inviting me to speak at this 22nd Asia-Pacific Programme for Senior Military Officers (APPSMO), and thank you to everyone for joining us from all over the globe.

22nd APPSMO

2. The 22nd APPSMO is a unique one – this is the first time that the entire programme is being conducted virtually. While it is a somewhat a regret that COVID-19 has prevented us from meeting physically, I think we can also be thankful that technology has enabled us to meet for this programme amid the disruptions caused by the pandemic.

3. APPSMO was established in 1999 by Singapore's former President, the late Mr S.R. Nathan. He had envisioned a "summer camp" in bringing together military officers from across the Asia-Pacific and beyond to discuss defence and security-related issues in a frank and open manner, and to forge relationships with one another. The idea then, as is now, is that an informal setting such as APPSMO would be the most valuable opportunity for officers to get to know their counterparts and benefit from the candid discussions that might not be possible during official meetings. While this virtual setting is somewhat less conducive than in-person meetings, I think with everybody's contribution and participation, it will still be an enriching programme.

4. Over the past two decades, APPSMO has grown and developed, and has become an established feature in the regional calendar. Over the years, the programme has brought together experts, practitioners, and participants from over 30 countries around the world, including those from Europe and the Middle East. Such inclusive platforms for military officers to exchange views have become more essential as we confront the numerous security challenges in this period of geopolitical flux.

Geopolitical Trends and Challenges

5. Let me begin by talking about some of the trends that we are seeing in the evolving security environment around us today. I will speak on just three, which I think are particularly pertinent in our time.

6. The first is great power competition. In recent years, the US-China rivalry has intensified. Antagonism between the two countries now covers several areas beyond defence, to include trade, technology and finance. One particular domain that I will highlight in my speech is technology, where the US and China are competing for leadership. In our region, we are also witnessing the emergence, or re-emergence, of new regional partnerships, including the Quadrilateral Security Dialogue, or Quad, and more recently, a trilateral security pact between the US, Australia and the UK. As these initiatives develop, we hope that they will contribute constructively to the peace and stability of the region and complement the regional security architecture.

7. The second is new, non-traditional security challenges that have emerged. The ongoing COVID-19 pandemic is a prime example. Climate change is another one. On COVID-19, many countries were unprepared to deal with the challenge when it came, and the cost of getting caught unprepared again will indeed be very great for any of these non-traditional challenges that might have yet emerged.

8. The third is the disruption and increasing security risks brought about by technology and changes in technology. While technological advances have given rise to new opportunities, these have also come with their attendant risks. These same technologies have enabled threat actors to exploit our vulnerabilities with greater ease and at a lower cost.

9. The three developments that I have briefly described here have one thing in common, and that is there is a strong nexus between technology and security. Technology is a battlefield in great power competition. But it also offers the means to address the challenges of a global pandemic and climate change. It brings both enormous opportunities and risks. For these reasons, I would like to talk a little bit more about the impact of technology and the accompanying challenges, and share our thoughts on how defence establishments could adapt and respond to these developments.

Technology as a Disruptive Force

10. The Fourth Industrial Revolution has led to technological breakthroughs in fields such as biotechnology, autonomous systems, quantum computing, and artificial intelligence (AI) to bring about ever-greater productivity and convenience. We will experience these changes and their impact in our lifetime. From our smart phones to electric vehicles, the massive conveniences afforded by technology have not only transformed our day-to-day lives, but also changed our physical world and our sense of space, and powered our economies.

11. I think we are all aware of the benefits of technology. I am also confident that all of us here, being from defence establishments, are fully cognisant as to how technology has also opened up new vectors through which hostile actors can threaten our security. Let me cite two examples. One is the cyber domain. The connectivity and availability afforded by cyberspace today are essential to supporting our way of life. Our virtual infrastructure is just as important as our physical infrastructure, physical infrastructure like our sanitation systems and our power grid, although our virtual infrastructure is somewhat more vulnerable than our physical infrastructure. For example, if a road is blocked or a power line is cut, the impact is typically more localised. However, the scale and effects of a major cyberattack are harder to isolate and control. Take the Colonial Pipeline cyberattack that occurred in May earlier this year, when a ransomware attack forced the shutdown of oil pipelines over a six-day period, resulting in fuel shortages across south-eastern US.

12. Another example is in the information domain. This is an avenue which hostile actors exploit to further their malicious aims. In September this year, a terrorist attack was carried out in New Zealand, in which six people were stabbed by an ISIS-inspired lone attacker. That attacker had previously been found to possess ISIS content on his personal computing devices. While self-radicalisation over the Internet is not new, it is likely to become more prevalent moving forward.

Sophisticated social media applications will allow for misinformation and disinformation to not only be spread more extensively and at a faster pace, but to also be customised to the individual, thereby reinforcing the impact of the echo chamber that self-radicalised individuals find themselves in.

13. With the onslaught of the global pandemic, the pace of digitalisation has accelerated, making societies and countries more vulnerable to threats in these domains. We have become even more dependent on technology, and as our dependency on technology grows, so too will new a challenges surface. Given the new challenges and threats brought about by technological changes, all militaries will need to adapt in order to respond effectively. So what can militaries do? I propose three lines of effort.

Need for Militaries to Adapt

14. First, armed forces should rethink our traditional concepts of defence. In conventional warfare, there are a few constants that we often take for granted: a clearly identified adversary, an accountable chain of command, and defined objectives, just to name a few. Against novel threats in the domains which we have just discussed like in cyber and information – these constants are not the same. For example, when we are faced with attacks from the cyber or information domains, how can we be sure who the perpetrator is? How do we differentiate between a criminal attack and an attack from a hostile political actor? Then, how do we respond, and who should respond? I think militaries will need to review their doctrines, structures and capabilities to be able to respond effectively to these threats in this changed environment.

15. In other emerging areas such as autonomous systems, biotechnology and AI which have defence applications, militaries will need to confront questions on ethics and legality. For instance, while AI can act as a force multiplier, there can also be serious consequences if AI behaves in an unanticipated manner. It was in view of this consideration that Singapore established our preliminary guiding principles of Responsible, Safe, Reliable and Robust in the defence sector to promote and advance the responsible development and use of AI.

16. Second, there needs to be greater cooperation between the public and private sectors to enable effective national responses. Upending our traditional conceptions of warfare, today's conflicts often circumvent geographical borders and take place outside the bounds of clear

battlefields. Aggressors exploit soft targets, which are less readily defended. Threat actors have used social media to spread false information, embark on influence campaigns and polarise and tear apart societies. Multi-ethnic and multi-religious societies such as Singapore are particularly vulnerable. Critical information infrastructures (CII) have been targeted as well. In view of the large attack surface afforded by our dependence on technology, an effective defence would entail a national effort with effective partnership between the relevant public agencies and the private sector. It is for this reason that Singapore takes a national approach to our cybersecurity strategy. Our lead agency, the Cyber Security Agency of Singapore, supported by our home front and defence agencies, works closely with the private sector to protect our networks and CIIs.

17. Public-private partnerships can also help defence and military establishments leverage opportunities afforded by technology to become more capable and more effective. Doing so would enable defence establishments to grow their talent pools, cross share ideas and innovate, as well as optimise resources to tackle collective challenges to the economy and to society.

Multilateral Cooperation

18. Third, given the transnational nature of these new emerging threats, greater multilateral cooperation will be key to dealing with them effectively. In support of civilian agencies, defence establishments could work together to foster common rules, norms and principles in cyber, information, AI, and other emerging domains. In the defence sectoral, militaries are well-positioned to leverage existing relationships and networks with international partners to tackle transnational security challenges. We therefore encourage our partners in the region and beyond to fully leverage platforms such as the ASEAN Defence Ministers' Meeting (ADMM)-Plus and the Experts' Working Groups.

19. On our part, Singapore has always been a strong advocate for multilateral cooperation as a means to promote regional peace and prosperity, in line with our interest to promote an open and rules-based order. We continue to build on existing networks to enhance practical military cooperation in key domains. In this vein, and as a timely response to the threats in the cyber and information domains that I just spoke about, we announced earlier this year that Singapore would establish the ADMM Cybersecurity and Information Centre of Excellence. The Centre will promote information sharing and research to help the region develop a deeper shared understanding of

cyber malware, misinformation and disinformation threats that have implications for defence. Moving forward, it is important for all defence establishments to build on this strong foundation of practical cooperation within the region and explore new opportunities to collaborate in new and emerging domains.

Conclusion

20. Let me conclude. Today, COVID-19 has limited the opportunities for militaries around the world to engage and build ties. But far from turning inwards and focusing just on our own problems, I hope that my arguments have convinced everyone joining us today that there are more reasons than ever for all our countries to work together to tackle common security threats. I also hope that armed forces will consider ways to adapt and respond to the widening range of security challenges. Over the next few days, you will have opportunities to discuss these ideas in detail, and in the process develop long-lasting professional relationships.

21. We hope that through candid discussions and sharing of views, you will be able to get to know each other better. We also hope that these conversations will continue long after this programme has concluded. Countries, like friends, may share common interests and perspectives. At the same time, they may not always agree with each other on issues, particularly when conflicting national interests are at stake. However, the peaceful resolution of disputes requires leaders who are open and willing to talk through their differences. This is where strong relationships that you build with your counterparts – a familiar face at the other end of the phone, or in our current context, on the other side of the screen – can make a huge difference.

22. This is the long-term value of APPSMO – to bolster our regional security architecture by fostering friendships and cooperation among military officers. So on this note and in conclusion, I wish everyone a most productive and fruitful week ahead. Thank you very much.

###