Speech by Senior Minister of State for Defence Mr Zaqy Mohamad at the 4th Singapore Defence Technology Summit on 22 Mar 2023, 1900hrs, at the Shangri-La Singapore

SPEECHES | 22 Mar 2023 20:00 (GMT+8)

Good evening senior defence officials, distinguished guests, ladies and gentlemen:

I am happy to be here this evening to welcome all of you to the fourth iteration of the Singapore Defence Technology Summit (SDTS).

To our overseas guests, a very warm welcome to Singapore.

This summit is a gathering of the best of minds from defence and security establishments, industry, academia, as well as think-tanks to examine emerging technology trends and issues of the day in the defence and security landscape.

I have been informed that there has been an overwhelming response to this year's summit.

We have more than 1400 in-person and virtual participants from over 25 countries. We are also appreciative of the great support from nearly 40 distinguished leaders who have agreed to speak at this summit.

We can be grateful for the impressive turnout this year, given that we have just overcome the pandemic restrictions of the past few years.

It shows that there is strong commitment and genuine desire from defence and technology leaders all around the world to come together and find ways to tackle the shared challenges of our times.

Your presence is testament to the immense opportunities but also non-trivial risks of emerging technologies.

I hope that this summit will serve as a useful platform for the defence technology community, to exchange views and ideas; agree, disagree or challenge one another; explore cooperation and help shape a more secure world going forward.

KEY SHIFTS IN TODAY'S TECHNOLOGICAL LANDSCAPE

At the last tech summit, participants discussed how best to build confidence amidst technological disruption, and the role of partnerships as stabilisers for enhancing our shared security.

These conversations remain important today.

Leaders worldwide need to take advantage of the opportunities from technological innovations, while mitigating the risks that come with them.

Cutting-edge and innovative technology continue to shape conflict, and affect the balance of power between states.

Digital and dual-use technologies, in particular, are undergoing a continued revolution, characterised by the rapid development and widespread availability of new technologies that have civilian or military applications.

This includes technologies such as artificial intelligence (AI), robotics, and nanotechnology, which continually transform various aspects of society, including warfare.

Since the last summit, we have unfortunately seen the re-emergence of major state-on-state conflict in the ongoing Russia-Ukraine war.

It came as a shock to many observers that conventional warfare on this scale could still break out on European soil.

Since the start of the war, hundreds of thousands have been reported killed or wounded, and millions have fled their homes as refugees.

Regrettably, the conflict has just passed the one-year mark, with the end not yet in sight.

Events in the Russia-Ukraine war have highlighted how digital and dual-use technology can be deployed in modern warfare.

Online is said to be the new frontline.

During the initial stages of the conflict, Ukrainian President Zelenskyy used social media to broadcast nightly addresses to the Ukrainian people, providing situational updates and appealing for support.

Using Telegram chatbots, hundreds of thousands of civilians shared videos, locations of troop movements and fighting, flooding the public domain with raw open-source intelligence, and real-time information of dangerous areas.

However, the information domain can also be easily be corrupted by fake news sources or orchestrated information campaigns.

Already, we have seen how generative AI can complicate trust and suspicion, with public figures impersonated in deepfake videos to push divisive opinions and falsehoods.

So it begs the question – how do we create systems that can take advantage of the opportunities in the digital and dual use space, while effectively dealing with the threats that they pose?

The war has also highlighted how technology with everyday civilian uses could be made "dual-use" with some adaptation and applied – often at low cost – to military objectives.

Using a 3-D printed fin, the Ukrainians improvised grenades that could be lifted by commercial drones, and dropped on troops.

In more destructive applications, we have seen how the Ukrainians developed unmanned surface vessels primarily based on commercial-off-the-shelf components, which successfully inflicted damage on several Russian naval vessels in the port of Sevastopol.

Iran's Shahed-136 drones, costing just US$20,000 a drone inflicted disruptive and significant damage on Ukraine's critical infrastructure and caused the loss of lives. Amongst countermeasures deployed by the Ukrainians were IRIS-T surface-to-air missiles, which at US$430,000 a missile, cost 21 times more. The cost asymmetry between such threats and their countermeasures is stark. It is not unimaginable that even terrorists would be drawing lessons from the conflict, and they, similarly, can build low-cost systems to threaten our shared security.

The implications of these shifts in technology and changes in the nature of warfare are no small matter, especially for all of us who have an interest in making the world a safer place.

It is therefore opportune that this year's summit focuses on the theme of "Digital and Dual-Use Technologies – Opportunities and Threats".

And over the next few days, I encourage tech leaders, industry captains and professionals to discuss the implications of these shifts in technology, and how they may apply to defence and security. I hope that every one of you will gain some new perspectives and a better understanding of how these technologies can contribute to peace and security.

ADDRESSING NEW CHALLENGES

In response to these myriad challenges, each of us will have to come up with our own strategies and approaches. But we will also have to develop partnerships.

Last year, Singapore announced the formation of the Singapore Armed Force's fourth Service - the Digital and Intelligence Service (DIS) - to tackle digital threats that will grow in scale, sophistication and organisation. The DIS also provides enhanced intelligence, advanced connectivity and resilient digital defence for the SAF.

Locally, the DIS works closely with technology partners such as our Defence Science and Technology Agency (DSTA), DSO National Laboratories (DSO) and ST Engineering to develop cutting-edge C4 and Cyber solutions.

Beyond Singapore, the DIS also seeks to learn from and partner with digital and cyber outfits in foreign militaries as it deals with a range of digital threats.

Outside of the defence sector, we can all also broaden and deepen our engagement with the wider technology ecosystem, given that the commercial sector and academia are key players in this technological revolution.

In Singapore, MINDEF and the SAF are working with Enterprise Singapore to engage promising start-ups and small companies to develop emerging solutions to future problems.

We have also deepened our engagement with academia, such as with the iTrust Centre for Research in Cyber Security at the Singapore University of Technology and Design (SUTD), to develop realistic cyber testbeds to train our cyber defenders.

Taken together, cross border and cross sector partnerships, can strengthen the sharing of expertise and collaboration on shared solutions.

For example, Singapore's Defence Science and Technology Agency (DSTA) has been working with the US Department of Defence's Irregular Warfare Technical Support Directorate, in partnership with ST Engineering, to conduct a data engineering Prize Challenge.

This competition, which ends today, has been seeking out innovative solutions from international participants to ingest and curate data for counter-terrorism intelligence analysis.

These solutions will in turn be applied in the real world by the users and partner nations operating at the Counter Terrorism Information Facility, here in Singapore.

Threats in the digital domain transcend physical boundaries, and collaboration is imperative to identify and tackle such threats.

In this regard, Singapore contributes to strengthening our cyber defences with regional Southeast Asian countries. One such example is the ASEAN Defence Ministers' Meeting Cybersecurity and Information Centre of Excellence (ACICE). This Centre seeks to promote research, information sharing and co-operation among partner nations on tackling emerging cybersecurity and informational threats.

Last month, we also launched a Malware Information Sharing Platform under the ACICE. This leverages the collective knowledge of the ASEAN Member States, shares information on cyber malware and other relevant threats, and will provide early warning, timely response, and relevant mitigation of cyberattacks.

CLOSING REMARKS

Ladies and Gentlemen, historically, as a trading post sitting at the nexus of East and West, Singapore has been a melting pot for diverse cultures and traditions, producing new and unique flavours.

Today, we continue to be a meeting point for the world in many other ways, at the intersection of modern information flows that criss-cross the digital domain.

Over the next few days, as global thought leaders from government, industry, and academia meet, I hope that this summit will serve as a useful platform for participants to share valuable insights and exchange ideas.

In closing, I want to thank each and every one of you for participating and gathering at this year's Tech Summit.

I look forward to the many stimulating and vibrant conversations that this Summit is known for generating.

I hope that these conversations will also strengthen existing partnerships, forge new ones for the future, and contribute to our shared security.

Thank you very much. Have a wonderful evening.