ADMM Cybersecurity and Information Centre of Excellence

UPDATE ON THE CYBER DOMAIN

Issue 08/25 (August)

Digital Defence Symposium 2025

INTRODUCTION

1. The 3rd Digital Defence Symposium (DDS), co-organised by the S. Rajaratnam School of International Studies (RSIS) and the ADMM Cybersecurity and Information Centre of Excellence (ACICE), was held in Singapore from 22 to 23 Jul 2025. This year's DDS brought together over 300 senior defence officials, academics, industry experts, and international partners from 35 countries and international organisations. Lieutenant General Susan Coyle, Chief of Joint Capabilities at the Australian Defence Force delivered the keynote address for the 3rd DDS, while Germany's Chief of Cyber and Information Domain Service (CIDS) Vice Admiral Dr. Thomas Daum engaged in a Fireside Chat with Singapore's Defence Cyber Chief COL Clarence Cai.

Lieutenant General Coyle delivering the Keynote Address

2. The theme of the 3rd DDS was "Securing our Common Digital Frontiers", which was timely given the increasingly complex nature of today's threats. In view of the flux of the environment we live in, the Symposium centered around three key themes: (a) building effective digital military forces; (b) responsible behaviour in the cyber and information domains; and (c) how the defence sectoral can partner the civilian sector.

HIGHLIGHTS AND INSIGHTS FROM THE 3RD DDS

Building Effective Digital Forces

3. Militaries have been evolving to meet the threats posed by today's increasingly complex landscape. No country is immune from cyber and information threats, and recent developments and incidents have only reinforced the need for intelligence sharing and coordinated responses to deal with increasingly complex threats. Some militaries have adjusted their structures to tap on the strength of individuals who may not fit conventional military moulds while still instilling in them the discipline and expectations required of all service members. These individuals included those who possessed expertise related to and exceled working in the digital domain – such as cyber specialists and tech-savvy mid-career professionals – or those who did not prefer working in typical military environments. Militaries have done so through the likes of personnel policies that have allowed for flexible movement between departments, career tracks to help promote technical expertise and leadership qualities, and talent development programmes to help institutionalise digital mastery. Other militaries have started to place greater emphasis on ensuring that the leadership of their digital forces are sufficiently digitally literate. However, there is no best model of organising the military to effectively deal with digital threats as that would differ from military to military, based on variables such as resourcing, broader societal contexts and intended outcomes.

4. The 3rd DDS also recognised that regional and global cooperation could enhance our resilience in the cyber and information domains. The building of effective digital defence, for example, hinged on establishing shared protocols, procedures, and standards among partners. Strategic partnerships – both (i) regional and global; and (ii) public and private were highlighted at the DDS as key enablers of operational effectiveness of digital military forces.

Bridging the Civil-Military Divide

5. The 3rd DDS recognised the civilian sector as vital to national resilience and security, particularly because of its ability to innovate and develop technology rapidly. In her Keynote Address, Lieutenant General Susan Coyle spoke about the

need for defence forces to have healthy partnerships with the private sector to carry out their mission of providing effective digital defence. She also said that these partnerships needed to be based on agility and trust, which were necessary for innovation and timely responses to rapidly evolving technological landscapes and threats. These collaborations, which could include cyber threat intelligence sharing and enhancing interoperability, would be vital in securing our common digital frontiers.

6. Digital threats do not discriminate between defence and civilian sectors. As the boundaries between the defence and civilian sectors have become blurred by digital threats, discussants agreed that closer collaboration between both sectors was necessary. It was suggested that the defence sector was typically better at detecting advanced persistent threats (APTs), which were generally longer-term and strategically focused. In comparison, the civilian sector was typically better at detecting malware, as civilian sector tools were generally optimised for identifying widespread and opportunistic threats that follow certain patterns. Moreover, the civilian sector was often quicker at developing artificial intelligence (AI), cloud, and quantum technologies due to more agile innovation cycles. Thus, partnerships between the defence and civilian sectors were crucial, as by working together to share threat intelligence and develop defence capabilities both sectors can enhance their capabilities and achieve shared objectives. Agility in contracting and procurement as well as less risk-averse pilot programmes were suggested as practical remedies to ensure timely capability development.

Approaches to Responsible Behaviour in the Cyber and Information Domains

7. For the first time, the 3rd DDS discussed how militaries can contribute to the conversations on responsible behaviour in cyberspace. Norms such as those conceptualised by the UN Group of Governmental Experts (GGE) on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, and adopted by the UN General Assembly have provided a useful starting point. As the world becomes increasingly digitalised and connected, norms can help reduce risks to international peace and security by preventing conflict in cyberspace. However, the voluntary nature of these cyber norms as well as the lack of enforcement mechanisms has created gaps in implementation and operationalisation. Some countries have begun to embed behavioural norms into domestic legislation and standard operating procedures. Regional groupings such as the Association of Southeast Asian Nations (ASEAN) have subscribed in-principle and attempted to operationalise some of these norms, for example through the ASEAN Checklist for the Implementation of the Norms of Responsible State Behaviour in Cyberspace. However, these efforts needed to continue and in fact ramp up. In particular, regional approaches to developing and

adopting norms might be more feasible as they could be more context-sensitive and able to navigate geopolitical tensions.

8. The threats faced by the defence sectoral were becoming increasingly sophisticated as malicious actors blend cyber operations with information warfare and manipulation. Threat surfaces have also expanded as the defence sectoral now not only had to worry about threats to their own systems, but also threats to their vendors and supply chain providers. In particular, the rapid advancement of AI, especially in the quality of generative technologies, has blurred the lines between fact and fiction. We now live in a more uncertain information environment. Therefore, countries needed to shift from reactive approaches to dealing with misinformation and disinformation to proactive approaches such as pre-bunking, trust-building, and narrative shaping. Reactive approaches tended to be too slow and limited in impact, while proactive approaches could yield strategic advantages and long-term resilience. Long-term societal resilience would require enhanced government strategic communications, strengthened media literacy, and more integrated whole-of-government approaches

CONCLUSION

Discussions on how the defence sectoral can partner with the civilian sector

9. The discussions at the 3rd DDS affirmed that cyber and information threats were no longer abstract or distant issues. Rather, they were immediate and could have real effects on militaries and broader societies. Moreover, these threats have been evolving quickly increasingly straddling national borders and sectors. Therefore, these threats demanded responses that were integrated and agile. The path forward to securing our common digital frontiers has required both urgency and coordination. Crucially, defence could not be confined to conventional structures and must involve all strata of society to operate effectively.

Contact Details

All reports can be retrieved from our website at www.acice-asean.org/resource/.

For any queries and/or clarifications, please contact ACICE, at ACICE@defence.gov.sg.

Prepared by:
ADMM Cybersecurity and Information Centre of Excellence

• • • • •