ACICE
ADMM Cybersecurity and
Information Centre of Excellence

Monthly Digest

Issue 08/24 (August)

A monthly round-up of significant news around the world

1. The 2nd Digital Defence Symposium (DDS), co-organised by the S. Rajaratnam School of International Studies (RSIS) and the ASEAN Defence Ministers' Meeting (ADMM) Cybersecurity and Information Centre of Excellence (ACICE), was held in Singapore from 24 to 25 Jul 2024. This year, the DDS was expanded beyond ASEAN countries, and brought together over 200 senior defence and military officials, academics, industry experts, and international partners from across 22 countries. The DDS, involving both the public and private sectors, discussed the latest developments and challenges in the domains of cybersecurity and information amid rising geopolitical tensions.

2. Opening the event was the Welcome Remarks by Executive Deputy Chairman of RSIS and Director of the Institute of Defence and Strategic Studies (IDSS) in RSIS, Ambassador Ong Keng Yong. This was followed by the keynote address given by Vice-Admiral (VADM) Dr Thomas Daum, Chief of Cyber and Information Domain Service (CIDS) in the German Armed Forces. In his keynote address, VADM Daum addressed the evolving challenges of the new battlefield that is cyberspace itself, as well as the blurring of lines between the civilian and military sectors. He stressed the need for speed, agility, and mutual cooperation in mitigating these new and unprecedented threats.

VADM Daum delivering Keynote Address at 2nd Digital Defence Symposium

3. Comprising four panels, speakers for the first panel explored the growing demands of the evolving cyber and information landscapes, and drew from their own respective backgrounds as military commanders to provide perspectives on the changing vulnerabilities and challenges, and possible mitigation strategies. For the second panel, speakers spoke on countering cyber threats in defence and provided perspectives on various apparatus and defence systems that different countries and international organisations had in place to respond to cyber threats, as well as the value of collaborating across various sectors. The third panel focused on understanding the cognitive domain; speakers spoke about the complexities of the domain, and how factors within the physical and virtual environment interacted with the cognitive dimension in an interconnected matrix, influencing the perceptions, opinions and attitudes of people in society. Last but not least, the fourth panel brought together speakers representing international organisations, research institutions, and technological companies to provide perspectives on how various stakeholders can establish collaborative relationships to manage the various risks brought upon by the demands of the cyber and information landscapes.

Highlights and Insights from 2nd DDS

4. Latest Trends in the Cyber and Information Domains. Technical advancements in the modern age are actively changing the landscape of the battlefields. The ongoing war between Russia and Ukraine had demonstrated these fundamental changes in modern warfare, illustrating that developments within the cyber and information domains not only impacted the land, sea, and air domains of combat, but had also become a battlefield in their own rights. Understanding and effectively managing the information highway had become

crucial for military planning, command and control, and achieving strategic objectives. Cyber and information threats straddle across the civilian and military sectors. Military geo-positioning operations may be conducted by civilian satellites, and data interception operations by malicious actors can target both civilian and military domains. Troops are exposed to the same news and social media landscape as civilians. There is recognition for a growing need for greater collaboration across whole-of-society and among nations in dealing with the increasing cyber and information threats. The ACICE Malware Information Sharing Platform (MISP)[1] and ACICE Chat[2], launched in Feb 2023 and Jul 2024 respectively, were steps for the ASEAN region to come to grips with the growing cyber threats through enhanced information sharing.

5. Different Military Structures to Respond to Growing Threats. Many militaries in different parts of the world are responding to the growing cyber and information threats with evolving structures and organisations. Germany's CIDS was established in 2017 as a military service of the German Federal Armed Forces to respond to the threats and challenges in an increasingly networked world in an agile and innovative manner. The aim was to enable quick and coordinated planning, action and reaction in the cyber and information domain. CIDS brought together German Federal Armed Forces' key players in cyberspace, the electromagnetic spectrum and the information environment under one command, operating on an equal footing with land, air, sea and space. Likewise, the UK recognises five domains in multi-domain operations: space, cyber, air, land, and maritime, and three dimensions: physical, virtual, and cognitive. In the ASEAN region, Singapore Armed Forces had established the Digital Intelligence Service as a 4th service after Army, Navy and Airforce in 2022 to respond to the growing cyber and information threats. Malaysia and Thailand had also started to develop national strategies and frameworks to deal with these threats.

6. Increasing Awareness of Hybrid Threats. The DDS recognised the increasing importance of understanding the nexus between the cyber and information domain and the cognitive implications of these threats, often played out amid hybrid warfare. Cognitive warfare refers to the conduct of operations using available tools to impact adversary attitudes and behaviour. Hybrid warfare combines digital compromise and influence operations. In India, a polarised political spectrum provides a fertile ground for such operations. Deepfakes and other AI-driven technologies can convince electorates and amplify kinetic actions on the ground. Domestic fault lines create dissonance, leading to distrust in the

[1] ACICE's MISP is an online platform that provides ASEAN member states exclusive access to real time information on threats in cyberspace as well as malware incidents.

[2] ACICE Chat is a dedicated channel on the mobile device that automatically broadcasts and shares cyber and information news with ASEAN member states. It provides daily updates on cyber threats to facilitate swift response and mitigation efforts, and weekly broadcasts featuring curated cyber and information news.

government and weakening national resilience. Only by understanding the impacts that cognitive warfare had on the virtual and physical dimensions, could militaries operate effectively to attain competitive advantage over their adversaries.

RSIS
ACICE
2nd Digital Defence Symposium
PANEL 3:
UNDERSTANDING COGNITIVE DOMAIN –
OPPORTUNITIES AND THREATS FOR DEFENCE

Discussions on the opportunities and threats that the cognitive domain brought to defence

7. Need for Cyber Norms and Regulations. Participation in cyber discussions such as at the UN Open-Ended Working Group on Information and Communication Technologies had allowed for greater public awareness and knowledge on cybersecurity issues. In 2015, the UN General Assembly adopted 11 voluntary norms defining acceptable and unacceptable behaviour in the ICT domain through resolution 70/237. Currently, states are working on advancing the UN Framework of Responsible State Behaviour for a Secure Cyber Environment, based on international law, confidence-building and capacity building measures. As discussions on international norms on cybersecurity progress, it is important to consider how these norms could be applied to individual states. For example, building the nation's digital literacy would act as a rising tide that lifts all ships in enhancing the region's collective resilience against digital threats. However, given that different countries still used varied languages to describe the digital domain and its threats, the choice of words in discussions might sometimes become politically charged. There was therefore a need to first establish trust and understanding among nations. To this end, the DDS provides a useful platform for communication and cooperation.

8. Cybersecurity and Information Resilience as a "Team Sport". Discussions at the DDS highlighted the importance for public-private partnerships (PPPs) to adopt a multi-stakeholder approach that involved government, industry and academia to promote resiliency in cyberspace. As defined by IBM, cyber resilience is an entity's ability to prevent, withstand and recover from cybersecurity incidents. The line between the military and civilian sectors in the

digital domain is blurred because militaries do not own all the systems and networks that we need to protect. Many militaries rely on civilian-driven innovations in areas like cloud computing, Artificial Intelligence, and telecommunications to power modern defence infrastructures. Meaningful engagement at the national level is therefore essential for cyber resilience, encompassing all phases from planning and preparation to post-incident learning and after-action reviews.

Conclusion

9. As ACICE Executive Director Yeo Seow Peng said in her closing remarks, the DDS "represents a yearly culmination of ACICE's efforts to promote information sharing and capacity building in the cybersecurity and information domain in our region." By keeping communication channels open, the exchanges enabled by the DDS are useful to inculcate best practices in the region, and raise the bar in collective resilience against common digital threats.

With input from: RSIS

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