IDSS PAPER

20 July 2026

Building International Interoperability Through Cyber Defence Exercises

Marine Ourahli

RSiS S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES
Nanyang Technological University, Singapore

RSiS 30

RSIS S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES
Nanyang Technological University, Singapore
Ponder the Improbable since 1996

IDSS Paper
Ponder. Analyse. Prepare. Engage. Refresh.

www.rsis.edu.sg No.083– 20 July 2026

Building International Interoperability Through Cyber Defence Exercises

Marine Ourahli

KEY TAKEAWAYS

- *By participating in cyber defence exercises, Singapore has reinforced its position as one of the leading military cyber powers among small and medium-sized states; its approach can serve as a model for others of similar size.*

- *Singapore's participation in the Defence Cyber Marvel and Locked Shields cyber exercises demonstrates its growing cooperation and interoperability with leading military cyber powers.*

- *Singapore's approach encompasses both the technical and normative dimensions. Sustainable cyber cooperation goes beyond having interoperable capabilities and also encompasses interoperable legal and normative principles.*

COMMENTARY

In 2026, Singapore reinforced its position as a leading military cyber power among small and medium-sized states. From 9 to 13 February 2026, Singapore participated in the British Army Cyber Association's Defence Cyber Marvel exercise, which involved more than 2,500 cyber defenders from armed forces, government agencies, and industry partners across 29 countries. Furthermore, on 23 April 2026, a joint Singapore-Latvia team secured first place at Locked Shields 2026, the world's largest cyber defence exercise organised by NATO's Cooperative Cyber Defence Centre of Excellence (CCDCOE).

Singapore's regular and substantive participation in critical military cyber exercises reflects a recognition of the growing importance of cooperation and interoperability among states on cyber issues in the military domain. Singapore's approach also

illustrates how small and medium-sized states can develop their military cyber capabilities and achieve strategic relevance.

Multilateral Cooperation and Interoperability in Cyber Defence

Multilateral cooperation is essential to effectively respond to cyberattacks. Advanced persistent threat (APT) groups, which are sophisticated malicious actors that conduct cyber operations, often operate as transnational threat actors targeting multiple states or cross-border systems. In response to this trend, there has been a corresponding integration of cyber exercises into national and multilateral military training, demonstrating a shift in how militaries around the world are addressing cyber threats.

Since 2010, NATO's CCDCOE has been running Locked Shields, which is now considered the largest and most complex multilateral cyber defence exercise. Locked Shields fosters close coordination between states and private actors, as well as harmonise procedures, enhance interoperability, and strengthen military structures dedicated to cyberspace. As participating states develop the capacity to respond in a coordinated manner, they create a foundation for collective action. This helps mitigate the impact on compromised systems in the event of a cyberattack and acts as a form of deterrence by signalling collective resilience.

However, cooperation inevitably remains constrained by national sovereignty and the need to protect sensitive information. This also explains why multilateral cyber exercises are primarily aimed at establishing an adaptable approach to cooperation when necessary. More importantly, they enable states to develop shared understanding and experience, while deepening the expectation that a resilient cyberspace depends on the ability of all states to actively prevent, mitigate, and contain cyber threats.

Singapore's Position as a Military Cyber Power

Since 2022, the Singapore Armed Forces has had a fourth service branch dedicated to cyber operations, the Digital and Intelligence Service (DIS). This institutional development underscores the strategic importance attached to cyberspace in Singapore's national defence.

In addition, capacity building and multilateral cooperation are central elements of Singapore's cyber strategy. This has helped demonstrate Singapore's commitment to developing close cooperation and interoperability with the international community to tackle cyber threats. Since the publication of its first cyber strategy, Singapore has gradually established itself as a leading player in global cyber diplomacy, notably through its role in coordination and capacity building within ASEAN. This has put Singapore in a unique position to act as a bridge between ASEAN and broader global networks and initiatives, facilitating the exchange of expertise, norms, and best practices.

In this context, cyber exercises occupy a central place in Singapore's cyber diplomacy. They facilitate cooperation and confidence-building with the city-state's strategic partners, while demonstrating competence and operational readiness. Singapore's

ability to be a credible participant in multilateral cyber exercises is supported by its advanced domestic technological ecosystem and highly skilled cyber workforce.

Moreover, cyber exercises can serve as a platform to demonstrate the effectiveness of Singapore's approach, positioning the country alongside other small yet highly advanced military cyber powers such as Estonia. Indeed, Singapore drew lessons from Estonia when establishing the DIS, demonstrating how small and medium-sized states can influence one another.

For Singapore, participating in multilateral cyber exercises also involves a delicate diplomatic balancing act to avoid any misperception of excessive alignment with a particular geopolitical bloc. Rather than concentrating its cyber cooperation within a single framework, Singapore deliberately engages in a broad range of exercises involving different regional and Indo-Pacific partners. It maintains a strong regional role through ASEAN-led initiatives, notably by hosting the ASEAN CERT Incident Drill (ACID), an exercise designed to test incident response capabilities, strengthen threat intelligence sharing, and enhance the cyber preparedness of the Computer Emergency Response Teams (CERTs) of ASEAN member states and their partners. Beyond ASEAN, Singapore also participates in broader regional and multi-domain exercises like Bersama Shield 2026, conducted under the Five Power Defence Arrangements (FPDA) with Australia, Malaysia, New Zealand, and the United Kingdom, and Exercise Super Garuda Shield 2025, jointly organised by the Indonesian National Defence Forces and the United States Indo-Pacific Command, bringing together a wide range of Southeast Asian and extra-regional partners. By participating in exercises representing different cooperation platforms, Singapore diversifies its security partnerships and strengthens interoperability across multiple strategic frameworks.

Looking Ahead

Singapore's approach to cyber engagement demonstrates that effective cyber interoperability must also include normative interoperability. *Image credit: UN Photo/Eskinder Debebe.*

Beyond its recognised role within ASEAN, Singapore is now seeking to establish itself as an important actor for cyber capacity-building. This ambition is reflected in initiatives such as the UN-Singapore Cyber Fellowship Programme, which aims to strengthen UN member states' expertise in cyberspace. Rather than focusing exclusively on technical skills, this programme highlights that effective international cooperation also

depends on a shared understanding of the legal and institutional frameworks governing state behaviour in cyberspace.

Singapore's approach to cyber engagement demonstrates that effective cyber interoperability must also include normative interoperability. Technical cooperation alone can be constrained by divergent national interpretations of international law. Singapore's approach to cyber capacity-building combines the technical with legal, diplomatic, and policy dimensions. Alongside military cyber exercises that enhance interoperability and collective preparedness, Singapore also actively contributes to the development of international norms, notably as the Chair of the Open-Ended Working Group on the security and use of information and communications technologies. Through this strategy, Singapore seeks to position itself both as an actor engaging in cyber cooperation and as a contributor to international cyber governance.

Marine Ourahli *is a Senior Analyst with the Military Transformations Programme at the S. Rajaratnam School of International Studies (RSIS).*

Please share this publication with your friends. They can subscribe to RSIS publications by scanning the QR Code below.