RSIS COMMENTARY

2 July 2026

Defence Diplomacy in a Time of Digital Threats

Eugene E G Tan

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

RSIS 30

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

RSIS COMMENTARY

www.rsis.edu.sg No. 143 – 2 July 2026

Defence Diplomacy in a Time of Digital Threats

By Eugene E G Tan

SYNOPSIS

The United States Secretary of War, Pete Hegseth, delivered a stinging rebuke of defence diplomacy at the 2026 Shangri-La Dialogue, despite geopolitical realities that support it. Sector-based conversations that improve security among states, such as the Digital Defence Symposium, which supports the digital domain, may be the tonic the concept requires.

COMMENTARY

The concept of states acting in their own self-interest was prominently featured at the 2026 Shangri-La Dialogue. This brought the military's role and the use of military power to safeguard these interests into focus. This was evident in two contrasting visions presented during the dialogue on how military power should be exercised and the value of defence diplomacy.

In the first, United States Secretary of War Pete Hegseth urged allies to increase security spending and place greater emphasis on safeguarding the "conditions that have underwritten peace and prosperity in the region". In his words, "less Shangri-La, more ships, more subs".

The second vision, embodied by ASEAN Secretary-General Kao Kim Hourn's remarks, called for more practical cooperation grounded in common interests among ASEAN member states and with other interested parties, and for upholding the rules-based regional order.

In an increasingly complex security environment, including digital threats, where misunderstandings and miscalculations can have significant consequences, these security conferences are becoming invaluable for risk reduction and norm formation.

The value of conferences involving the military lies not in their ability to change the world through diplomacy, but in providing a platform for exchanging perspectives on regional and global security issues, clarifying policy positions, and facilitating formal and informal discussions.

Digital threats affect both civilian and military sectors, making it difficult for governments to lineate areas of responsibility, unlike the traditional military domains of air, land, and sea, where threats are clearly distinguishable between the military and civilian spheres. There is no guarantee that arming to the teeth will provide a state with security, especially given the proliferation of low-cost, dual-use, high-reward technologies that can be used against both civilian and military targets.

Diplomacy and Digital Threats

The definition of what constitutes a digital threat has also been multiplying and evolving, making an exact, commonly accepted definition difficult, if not impossible.

The primary discussions that shaped global understanding of digital concerns were the six Groups of Governmental Experts and two Open-ended Working Groups at the United Nations (UN), which have addressed the security implications of the use of information and communication technologies (ICTs) since 1998.

These processes have focused on the proliferation of cyber threats and the protection of critical information infrastructure, with some success in addressing threats posed by states, including the agreement on norms of responsible state behaviour and the recognition that international law applies to cyberspace.

This work is set to continue through the upcoming Global Mechanism on ICTs in the Context of International Security. Other groups at the UN are tackling related issues, including the use of Artificial Intelligence in the Military Domain, the use of lethal autonomous weapons, and the prevention of an arms race in space.

However, states are unable to collectively agree on threats in the digital domain – as captured in the emerging threat sections. Issues raised include the use of artificial intelligence, cybercrime, threats to critical underwater infrastructure, and the proliferation of misinformation and disinformation on social media platforms, among others.

The conduct of defence diplomacy in the digital domain is therefore not only about creating norms for states, but also about establishing the contours of common interests among like-minded partners and, in the process, establishing commonly acceptable practices in that domain, even when there is no agreement.

Defence Diplomacy and Why it Matters for the Digital Domain

When we speak of defence diplomacy, we often refer to the use of defence and military engagements to build trust, strengthen relationships, and promote cooperation among states. The goal is to foster communication and mutual understanding between defence establishments and armed forces, reduce the risk

of conflict, manage tensions, and create opportunities for collaboration on shared security challenges. Defence diplomacy is needed to build confidence and enhance transparency while supporting regional stability and the creation of a rules-based international order.

While the Shangri-La Dialogue is a mainstay of defence diplomacy, the topics discussed are broad and lack the precision needed to address domain-specific issues. The Digital Defence Symposium (DDS), organised annually by the ADMM Cybersecurity and Information Centre of Excellence (ACICE) and the S. Rajaratnam School of International Studies (RSIS), is a forum that addresses one of these issues, namely, digital threats.

While it does not have the broad security focus of the Shangri-La Dialogue, the Symposium gives states a platform to discuss the digital domain's challenges for the military and offers opportunities for militaries to work together to reduce risk and define what is acceptable and what is not.

The conduct of defence diplomacy against digital threats is not a reduction in security spending; rather, it helps create more inclusive rules of the road with like-minded partners across issues and ensures that the interests of all states are understood. Conferences such as the DDS should enable states to hold more focused discussions.

The Intensification of Digital Diplomacy for Defence

The digital domain is both a boon and a bane for states seeking to harness new and emerging technologies such as artificial intelligence, and there is a gap in how the space is governed. In his remarks at the Shangri-La Dialogue, Singapore's Minister for Defence, Chan Chun Sing, noted that states face a "Regulation Paradox": early regulation risks stifling innovation, while norms become entrenched and difficult to reverse if regulation comes too late.

But finding the sweet spot is not easy. Given ASEAN's digital growth and economic ambitions, substantial groundwork is needed to ensure the security architecture underpinning them is robust. This extends to areas where additional rules are needed to protect the use of technologies such as artificial intelligence and ransomware, and to safeguard critical underwater infrastructure.

Digital threats are not about to go away, and unilateral action will not resolve the insecurities a state may face. Confidence-building among states requires more dialogue to strengthen the existing rules-based order. Without platforms for defence diplomacy to bridge this gap in confidence and trust, collectively ensuring our digital security will be much harder.

Eugene EG Tan is an Associate Research Fellow at the Centre of Excellence for National Security (CENS), a constituent unit of the S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University (NTU), Singapore.

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