



## SUPPORT MESSAGE BY GENERAL DATUK HJ MOHD NIZAM BIN HJ JAFFAR CHIEF OF DEFENCE FORCE, MALAYSIA

I am honoured to extend my full support for CyberDSA 2025, a platform bringing together cybersecurity, defence, and digital technology professionals. From 30 September to 2 October 2025, Kuala Lumpur will become the epicentre of global discussions on cyber defence and national security, bringing together military leaders, government agencies, industry pioneers, and academia to collectively shape the future of our digital landscape.

The theme of this year's exhibition, "Pioneering the Future of a Resilient Digital Nation," is timely and significant. In today's rapidly evolving security environment, cyberspace has become the new frontline. Threats are no longer limited to traditional battlefields. They have moved into the digital domain, where adversaries seek to disrupt economies, compromise sovereignty, and undermine public trust through cyberattacks, espionage, and disinformation.

As the Chief of Defence Force, I am fully aware that a nation's cyber resilience is now central to its overall security. Cyber threats are no longer theoretical. They are real and growing, demanding urgent and coordinated responses across government, defence, and industry. From the vulnerabilities of critical infrastructure to the weaponisation of artificial intelligence, the cyber landscape is evolving rapidly. We must stay vigilant, adaptive, and united in our efforts.

Malaysia has made progress in strengthening its cyber defence posture. Yet, the scale and complexity of threats continue to increase. We must protect our critical infrastructure, military networks, and government systems from intrusion, espionage, and sabotage. Cyber defence must be fully embedded within our national security framework, ensuring resilience at every level.



Modern conflicts are no longer fought solely with conventional means. It now includes cyber warfare, digital espionage, and information operations. Malaysia must continue investing in both offensive and defensive cyber capabilities. This includes strengthening cyber situational awareness, developing real-time threat intelligence, and enhancing early warning systems. The adoption of Al-powered detection, predictive analytics, and automated responses will be crucial in securing our digital future.

Cybersecurity, however, is not a challenge any nation can face alone. In a deeply interconnected world, cyber threats do not respect borders. Malaysia remains committed to working closely with our ASEAN partners, the Five Power Defence Arrangements, and international allies. We must continue to improve intelligence sharing, conduct joint cyber exercises, and build stronger collective defences. The growing risks posed by state-sponsored cyberattacks, Al-driven malware, disinformation campaigns, and ransomware require a coordinated global response.

CyberDSA 2025 is more than an exhibition. It is a call to action. It presents an opportunity for defence leaders, cybersecurity experts, and technology innovators to shape future policies, demonstrate cutting-edge solutions, and build a safer digital environment. I encourage all stakeholders, including defence institutions, government agencies, private industry, and academic institutions, to participate fully and contribute towards enhancing our national and regional cybersecurity posture.

I look forward to CyberDSA 2025 and the meaningful collaborations emerging from this gathering of minds and expertise. Together, let us strengthen Malaysia's digital resilience, confront emerging cyber threats, and secure a safe, sovereign digital future for generations to come.

