ADMM Cybersecurity and Information Centre of Excellence

UPDATE ON

THE DIGITAL DOMAIN

Issue 09/26 (September) – Special Edition Op-Ed

Beyond Hacking Defence…Into the Era of Digital Security

By H.E. Mr Yun Byung-se

First published in Korean for Maeil Business (MK) Newspaper, Republic of Korea, 27 Jul 2026

1. Last week, the Ministry of Foreign Affairs announced the details of an unprecedented cyber-attack and information leak. While an investigation into the perpetrators is underway, this incident cannot be dismissed as a mere security breach. Given that cyber intrusions targeting the government, military and related agencies have become increasingly sophisticated in recent years, this must be understood as a new form of threat aimed at national security.

2. Coincidentally, at the very moment the Ministry of Foreign Affairs made its announcement, I was delivering the fireside chat at the 4th Digital Defence Symposium (DDS) in Singapore in my capacity as the former Chair of the Global Commission on the Responsible Artificial Intelligence in the Military Domain (GC REAIM). The conference was attended by over 300 cyber and information warfare commanders, defence policymakers and cyber experts from 35 countries, including the United States, the United Kingdom, NATO, the European Union and ASEAN. It is evolving into the "Shangri-La (Security) Dialogue" of the digital field.

3. DDS is a consultative body seeking to proactively respond to the shift in the national security paradigm itself, viewing it as a transition from 'cyber security to digital defence'. Digital defence is an expanded security concept that goes beyond the technical dimension of protecting networks to safeguarding the nation's entire digital ecosystem, including cyberspace, the information

environment, AI, critical infrastructure, supply chains and the electromagnetic spectrum.

4. Today, cyber-attacks targeting nations or critical infrastructure, as seen in the current conflicts in Ukraine and Iran, are unfolding as part of complex "hybrid threats" and AI is automating these attacks and spreading them on a massive scale. Supply chain disruption, attacks on satellites and communication networks, the paralysis of critical infrastructure and even the electromagnetic spectrum are combined. The boundaries between peacetime and wartime, military and civilian, and physical and digital space effectively disappear.

5. Recognising that cyber defence alone is insufficient, NATO, the European Union, the United Kingdom, France, Singapore and others are transitioning to more comprehensive digital defence systems. There is a growing consensus that prevention, response and recovery must be linked into a single system covering the entire digital domain – beyond land, sea and air – and that a national cooperative framework involving not only the government and the military but also telecommunications, finance, energy and platform companies must be established and managed in an integrated manner. They are even conducting joint exercises to share threat intelligence in real time with allies and friendly nations. Furthermore, they aim to counter disinformation through strategic communication and organically link diplomacy, law enforcement, intelligence agencies and military responses. Consequently, the targets of defence, the participating entities and the methods of response are all undergoing transformation.

6. In particular, moving away from the concept of 'perfect defence', greater emphasis is placed on robust 'resilience'. In the digital age, defensive capabilities, as well as resilience, determine national competitiveness as well as security.

7. In the era of hybrid threats, the cyber and intelligence domains are inextricably linked and the core message of DDS is that we must establish a system of collective response – internally as a single whole-of-nation team and externally with relevant countries. There is a need to build a national platform where our government, military, intelligence agencies, local governments and private companies can respond jointly within a single digital defence system.

8. It is significant that the trilateral foreign ministers meeting among South Korea, the United States and Japan, held before and after the announcement of the Ministry of Foreign Affairs hacking, agreed to 'cooperate in responding to North Korea's cyber threats and illegal activities' and that strengthened cooperation on 'cyber and hybrid threats' was highlighted at the South Korea-European Union summit in June. Now, the important task ahead is to activate an operating system that concretises this into action.

9. I hope that this hacking incident will serve as an opportunity for South Korea to move beyond ‘cyber security’ and advance toward ‘digital security’ by protecting the entire digital ecosystem at the level of national security.

**The views expressed in this ACICE Digest are that of H.E. Mr Yun Byung-se. H.E. Mr Yun is the Chairman of the Seoul International Law Academy; he also served as the Chairman of the Global Commission on Responsible Artificial Intelligence in the Military Domain, and former Minister of Foreign Affairs of the Republic of Korea. H.E. Mr Yun headlined the 4th Digital Defence Symposium, where he was engaged in a fireside chat during the Official Dinner.*

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

• • • • •