RSIS COMMENTARY

8 April 2026

Developing Capacity for Cyber Defence: Insights from Finland

Asha Hemrajani, Esa Pollari and Eddie Lim

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. 074 – 8 April 2026

Developing Capacity for Cyber Defence: Insights from Finland

By Asha Hemrajani, Esa Pollari and Eddie Lim

SYNOPSIS

Frequent cyber-attacks on Singapore's critical infrastructure have demonstrated that cyber resilience depends on sustained defence, not just prevention. Finland's reservist model, supported by its volunteer-driven National Defence Training Association's cyber training and exercises, offers key lessons for Singapore: skills-based, inclusive pathways; wider participation; and building an exercise-to-reserve pipeline.

COMMENTARY

Singapore has had multiple brushes with sophisticated cyber-attacks on its critical information infrastructure (CII), including an attack by an Iranian threat actor targeting Singapore universities and the intrusion of UNC3886, a cyber espionage group, into four of Singapore's major telecommunications service providers (Singtel, StarHub, M1, and SIMBA Telecom).

The UNC3886 attack triggered Operation Cyber Guardian, Singapore's largest multi-agency cyber response effort to date, involving over 100 defenders working for more than 11 months to contain the threat. Although the response successfully mitigated the threat before significant damage occurred, the episode highlighted the complexity of defending against highly capable and well-resourced adversaries.

From an operational perspective, the key issue for Singapore is not just prevention, but also sustainable defence over time.

In this context, there is a need for a system that identifies and invites relevant cyber expertise from the civilian population, trains that expertise to a high standard, and integrates it into cyber incident response and recovery teams across the CII sectors.

Singapore's Enhanced Expertise Deployment Scheme (EEDS), launched in 2022, facilitates the redeployment of NSmen at various stages of their Operationally Ready National Service (ORNS) cycle, enabling the SAF to harness civilian-acquired expertise better. It also has the Expertise Deployment Centre (EDC), which matches skills to deployment needs. To date, more than 850 NSmen have been redeployed across over 20 areas of expertise, including legal services, counselling, intelligence and digital domains.

Finland's Use of Reservist Expertise for Cyber Defence

To further enhance this capability for Singapore's cyber defence, the Finnish Defence Forces (FDF) can serve as a reference, as it has a mandatory national service system similar to that of the Singapore Armed Forces (SAF).

According to the Finnish Security and Intelligence Service (SUPO), Russia and China represent the most significant sources of intelligence and cyber threats facing Finland, with state-linked actors continuing to conduct cyber espionage and influence operations against Finnish institutions.

To boost its cyber talent pool to defend against hostile foreign cyber operations, Finland identifies and selects the people needed from its entire population, and trains and exercises them for mobilisation in a national crisis. This system is reflected in Finnish defence thinking on cyber manpower, including the emphasis that the skills base can be expanded through closer cooperation with the private sector.

Finland has also shown demographic pragmatism by adjusting its reserve policy to retain experienced talent, including raising the reservist age ceiling to 65, effective from January 2026. The United Kingdom has recently announced the same.

Role of the National Defence Training Association of Finland

The National Defence Training Association of Finland (MPK) provides national defence training within an established legal and organisational framework, offering structured courses open to any member of the public who wishes to acquire relevant defence and preparedness skills and contribute on a volunteer basis. The MPK's role is significant because it supports expanded training and access to relevant competencies, including cyber defence.

The scale is significant; the MPK reports record-high demand for training that enhances participants' skills and performance, including reservists and members of the public not mandated for national service.

Finland's participation in NATO's Operation Locked Shields, the world's largest and most complex live-fire cyber defence exercise, also involves personnel from MPK, with the exercise environment bringing together participants from legal,

communications, and other non-technical functions to contribute alongside technical teams. Finland's cyber environment similarly assumes a mixed-skills ecosystem, drawing on a range of experts from among its cyber defence personnel.

A further lesson is that Finland does not treat mobilisation as a first response to aggression or crisis escalation. Rather, mobilisation is embedded within a broader system of whole-of-society readiness, sustained through ongoing cooperation and training.

Recommendations

Singapore already has in place institutional levers, such as the Digital and Intelligence Service (DIS) and EEDS, to tap into cyber talent. The following measures are recommended to further enhance cyber defence capacity by diversifying the sources of cyber talent.

1. Make EEDS/EDC pathways of ORNS personnel skills-based rather than degree-gated, using transparent cybersecurity competency benchmarks and credible certification or assessment pathways where appropriate.

2. Actively encourage more women in cybersecurity to play a role in cyber defence.

3. Leverage permanent residents for less sensitive cyber roles, while maintaining strict access controls and supervision for higher sensitivity tasks. One possible avenue is the Singapore Armed Forces Volunteer Corps (SAFVC), a uniformed volunteer scheme open to permanent residents. Expanding the range of roles offered by the SAFVC to include cyber specialist positions could help tap additional expertise.

4. Raise (or remove) upper age limits for cyber volunteering and reserve participation, recognising that experience and judgment are critical for leadership and coordination during cyber incidents.

5. Build an exercise-to-reserve pipeline: Use national exercises, including the Critical Infrastructure Defence Exercise (CIDeX) series, to identify high-performing cyber talent and place them into roles where they can be most effective.

A practical approach could focus on creating a bridging function using a "Cyber MPK-equivalent" coordinated by DIS and the Cybersecurity Agency of Singapore (CSA), responsible for:

1. A regular training schedule with periodic cyber skills recertification.

2. Cyber talent selection from major cyber exercises and channelling the talent into a vetted reserve pool; and

3. Pre-agreed mobilisation arrangements with CII operators, setting out activation triggers, tasking, supervision and access controls so that surge support can integrate smoothly into cyber incident response without introducing new security risks.

Conclusion

Finland's approach to developing surge capacity for cyber defence underscores a key point in its battle to protect its cyber domains: an understanding that effective cyber defence depends on a system to mobilise women and men cyber specialists already in the workforce. For Singapore, aligning EEDS/EDC with structured training, exercise-based selection, and clear mobilisation arrangements would create a cyber defence exercise-to-reserve resource surge model for sustained CII defence.

Asha Hemrajani is a Senior Fellow at the S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University (NTU). Esa Pollari is a technologist and a reservist with the Finnish Defence Forces (FDF). Eddie Lim is Head of Outreach at RSIS, NTU.

S. Rajaratnam School of International Studies, NTU Singapore
Block S4, Level B3, 50 Nanyang Avenue, Singapore 639798

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