ASIA-PACIFIC LEADERSHIP NETWORK

BUILDING NUCLEAR CYBER RESILIENCE IN THE ASIA-PACIFIC

Ali Alkis, Junior Associate Fellow at NATO Defense College

13 August 2026

What happens when a cyberattack disrupts a nuclear facility without directly affecting the reactor? Communications may fail, security records may become inaccessible, monitoring data may be compromised, and access systems may stop working. These disruptions could delay critical decisions, obstruct emergency response, and weaken public confidence through false or misleading information.

Many Asia-Pacific countries treat cybersecurity as an integral part of nuclear governance, several have also taken steps to strengthen it in recent years. Cybersecurity at nuclear facilities will continue to evolve beyond preventing unauthorised access to computer systems, and toward preserving essential functions, reliable information, and decision-making under severe disruption. The region should further integrate cyber resilience into nuclear regulation, emergency preparedness, supply-chain oversight, and regional cooperation.

Why the Asia-Pacific?

The Asia-Pacific combines substantial reactor fleets in Japan and South Korea, rapid nuclear expansion in China, and renewed interest in nuclear energy across Southeast Asia. IAEA data show that Japan and South Korea operate 14 and 26 reactors respectively, while the International Energy Agency reports that approximately half of the nuclear capacity under construction worldwide are in China. These programs face different institutional challenges.

For example, Japan's Nuclear Regulation Authority regulates nuclear facilities, while the National Cybersecurity Office coordinates national cybersecurity policy and individual ministries retain sectoral responsibilities. South Korea's Nuclear Safety and Security Commission has responsibilities spanning nuclear safety, security, safeguards, and emergency preparedness, with the Korea Institute of Nuclear Nonproliferation and Control providing specialized technical support. Despite their different structures, both countries must ensure effective coordination among regulators, operators, cybersecurity bodies, and emergency authorities. The risk is that a cyber incident can cross these mandates at once: unclear leadership, different reporting thresholds, or slow information-sharing can delay assessment and produce inconsistent technical, emergency, and public-communication decisions.

China's National Nuclear Safety Administration supervises nuclear and radiation safety. A 2025 IAEA review found that China had strengthened its regulatory framework and made innovative use of digital tools and artificial intelligence. However, the review also stressed that regulatory staffing must keep pace with the industry's rapid growth and recommended further improvements in inspections and emergency preparedness. With 60 reactors operating, 37 under construction, and another 21 planned, China illustrates how rapid expansion can place pressure on regulatory personnel and consistent oversight across projects and suppliers.

Southeast Asian states are not all at the same stage. Viet Nam has revived the Ninh Thuan project which was suspended in 2016, and the National Assembly authorized its restart in 2024. It is now developing the infrastructure needed to negotiate and implement its first nuclear power plant. An IAEA review conducted in December 2025 assessed 19 infrastructure issues and proposed further steps for program development. Singapore, by contrast, has not committed to any deployment yet and is pursuing a regulator-first approach, including preparations for an IAEA infrastructure review and cooperation with experienced foreign regulators. These different paths show why regional support must be adapted to national readiness rather than applied through a single model.

For newcomers, investment in cybersecurity understandably competes with regulator development, workforce training, emergency infrastructure, and independent technical expertise, and governments are working to sequence these priorities sensibly. Even so, front-loading cybersecurity considerations where possible can help avoid dependence on vendors and systems whose vulnerabilities may be difficult and expensive to correct after procurement or construction.

Vulnerabilities Across the Facility Lifecycle

Three connected vulnerabilities deserve particular attention.

First, nuclear facilities have long operational lifetimes. Older equipment may eventually interact with software and systems developed in a different technological environment. Modernization can reduce some risks while introducing others, especially when external connectivity, remote access, or new digital capabilities are added without adequate security assessment.

Second, nuclear facilities rely on extensive supply chains. Vendors, contractors, software providers, equipment manufacturers, and system integrators may have access to sensitive systems or information. The IAEA describes the nuclear supply chain as a potential attack surface through which existing protections could be circumvented. It recommends a defense-in-depth approach covering people, processes, and technology throughout the supply-chain lifecycle.

Third, human and organizational weaknesses can undermine sophisticated technology. Insufficient training, poor reporting practices, negligence, coercion, or misuse of

legitimate access can all create vulnerabilities. Clear authority is particularly important where responsibilities are distributed among regulators, operators, national cybersecurity bodies, law-enforcement agencies, and emergency organizations.

A Practical Resilience Agenda

Building on existing regulatory and cooperative frameworks, four priorities could help Asia-Pacific governments deepen this progress.

First, continue adapting governance to program maturity. Countries that already coordinate among established regulators, operators, cybersecurity bodies, and emergency authorities could formalize a lead authority for nuclear cyber incidents, common reporting thresholds, protected information-sharing channels, and joint decision protocols, then stress-test these arrangements regularly. Others that have strengthened their regulatory frameworks can continue expanding regulatory staffing, inspections, and supplier oversight in step with construction. Newcomers are already building regulatory authority and specialist capacity, and can prioritize this groundwork before committing to technologies whose security they may otherwise lack the capacity to assess independently.

Second, expand exercises to cover compound crises. Building on existing emergency and technical exercises, future scenarios could combine cyber disruption with physical damage, loss of electricity, compromised monitoring information, and misleading public reports. Broadening these exercises to test decision-making, continuity of operations, communication, and recovery, alongside technical defenses, would further strengthen preparedness. Each exercise could produce a corrective action plan with assigned responsibilities, deadlines, and follow-up testing.

Third, extend supply-chain requirements across the full lifecycle. Existing cybersecurity requirements could be extended more consistently from procurement and installation through operation, modernization, and decommissioning. Contracts can further address software integrity, vulnerability reporting, remote access, component authenticity, and protection of sensitive information. Newcomers with limited specialist capacity could draw on common procurement guidance, shared training, and external peer review to complement their own developing capabilities.

Fourth, resource regional cooperation properly. The ASEAN Network of Regulatory Bodies on Atomic Energy (ASEANTOM) already supports regulatory exchange, human-resource development, emergency preparedness, radiation monitoring, and nuclear security cooperation. Its activities draw on the IAEA, ASEAN dialogue partners, and other external organizations. These foundations could support joint cyber exercises and specialist training, but an expanded role would require dedicated personnel, predictable funding, and clear responsibility for maintaining programs between annual meetings.

ASEANTOM could begin with a modest pilot supported by voluntary national contributions, seconded specialists from member regulators, and technical assistance

from the IAEA and dialogue partners. A small coordination unit could maintain reporting templates, organize exercises, manage access controls, and track corrective actions. This would avoid burdening every member with building the same capabilities while ensuring that the initiative does not depend entirely on occasional workshops.

The pilot could include a protected mechanism for sharing anonymized incident summaries, exercise findings, and regulatory lessons. Governments need information about recurring weaknesses, but excessive disclosure may expose sensitive details. Agreed classifications, anonymization, and controlled access could separate shareable lessons from restricted technical information. Reports could omit facility-specific details while identifying broader problems in training, supply chains, communications, and emergency response.

Prevention Is Not Enough

No cybersecurity system can guarantee complete prevention. Nuclear facilities and responsible authorities must also be able to detect and contain incidents, communicate under degraded conditions, maintain critical functions, and recover safely.

While resilience complements rather than replaces strong technical protection, cyber resilience must become a shared responsibility across operators, regulators, governments, suppliers, and regional partners. The Asia-Pacific's nuclear future will depend not only on how well its facilities resist cyberattacks, but also on how effectively its institutions respond when digital, physical, and political pressures converge.

Ali Alkis *is a junior associate fellow at NATO Defense College and a Ph.D. candidate at Hacettepe University in Ankara, Turkey. Alkis is also a 2025 Nuclear Futures fellow at Ploughshares and a 2025-2026 fellow for the Arms Control Negotiation Academy (ACONA). His research interests encompass nuclear security, non-proliferation, and nuclear terrorism as well as Turkish nuclear and foreign policies.*

The opinions articulated above represent the views of the author and do not necessarily reflect the position of the Asia-Pacific Leadership Network or any of its members.

This commentary is also published on the APLN website.

ABOUT APLN

The **Asia-Pacific Leadership Network (APLN)** is a Seoul-based organisation and network of political, military, diplomatic leaders, and experts from across the Asia-Pacific region, working to address global security challenges, with a particular focus on reducing and eliminating nuclear weapons risks. The mission of APLN is to inform and stimulate debate, influence action, and propose policy recommendations designed to address regional security threats, with an emphasis on nuclear and other weapons of mass destruction threats, and to do everything possible to achieve a world in which nuclear weapons and other WMDs are contained, diminished, and eventually eliminated.