COUNCIL FOR SECURITY COOPERATION IN THE ASIA PACIFIC (CSCAP)

2nd Meeting of the CSCAP Study Group on the Safety and Security of Digital Infrastructure

4-5 December 2025

Hanoi, Viet Nam

PROCEEDINGS

The second CSCAP Study Group Meeting on the Safety and Security of Digital Infrastructure was held in Hanoi from 4 to 5 December 2025. This CSCAP Study Group is co-chaired by CSCAP Singapore, CSCAP Viet Nam and CSCAP Korea.

The meeting was attended by experts from various CSCAP Member Committees and Vietnamese representatives of organizations and agencies from the CSCAP Viet Nam Committee. The CSCAP members present were Cambodia (virtually), Canada (virtually), China, EU (virtually), India, Myanmar (virtually), New Zealand, Singapore, Viet Nam, and other participants. The meeting focused on four main topics: (i) Geopolitical challenges to the security of digital infrastructure; (ii) Emerging technologies and the future of digital infrastructure; (iii) Submarine cables, power grids and the future of regional connectivity; and (iv) Public-private cooperation on digital infrastructure security.

OPENING REMARKS

Mrs. Nguyen Huong Tra, Acting Director-General, Institute for Strategic Studies, Diplomatic Academy of Viet Nam (CSCAP Viet Nam) welcomed distinguished experts and CSCAP colleagues, expressing appreciation for their commitment.

- Digital infrastructure has moved “from the background of public policy into the very center of strategic concern” as undersea cables, cloud platforms, energy grids and data centers underpin how economies function and societies stay connected.
- Three broad trends shaping regional challenges:
    - Shifting geopolitical environment: strategic competition is increasingly expressed through pressure on digital systems, from physical disruptions to contested standards and vulnerabilities in shared infrastructure;
    - Speed of technological change: AI, quantum computing, 6G and new connectivity architectures introduce powerful capabilities alongside unfamiliar risks, demanding regulatory frameworks that can adapt to a moving target;
    - Deep interdependence: economic integration, supply chains and public administration depend on uninterrupted connectivity, making resilience a regional public good.
- These dynamics frame the agenda: understanding the wider strategic environment; assessing how emerging technologies reshape resilience and

risk; and addressing the physical systems that anchor digital security and require coordination across borders and sectors.

- The private sector has an indispensable role as much of the world's digital backbone is privately owned and operated, making public-private cooperation foundational to stability.
- For Viet Nam, co-hosting the study group is both an opportunity and a responsibility as the country advances its digital-transformation agenda and strengthens national infrastructure security. As digital resilience cannot be pursued in isolation, Viet Nam values learning from participants' insights and experiences.
- In a complex strategic environment, CSCAP provides an essential platform for frank exchanges to identify areas of convergence, anticipate challenges, and build habits of cooperation that serve the region.

Mr. Kwa Chong Guan, Senior Fellow, S. Rajaratnam School of International Studies, Nanyang Technological University, Singapore (CSCAP Singapore) recalled CSCAP's earlier work on subsea fiber optic cables and elaborated the geopolitical challenges confronting this increasingly dense network, taking into account:

- CSCAP Singapore first organized a study group on subsea fiber optic cables in 2014. That study group issued a memorandum in 2014, but it did not generate further interest from ASEAN or the ASEAN Regional Forum (ARF) until last year. The group's revival in 2024 benefited greatly from the advice of Mr. Kent Bressie of the International Cable Protection Committee (ICPC), who highlighted the importance of collaboration between cable operators and governments and the need to share information on accidents and cable threats.
- Threats to undersea cables fall into two categories. Unintentional damage, which accounts for about 70%, mainly results from natural disasters and maritime activities, and regulatory obstacles can delay repair ships by up to a month. Intentional damage ranges from petty theft to acts of terrorism and hybrid warfare. He cited the Nord Stream sabotage and Red Sea cable cuts as examples of intentional damage in the grey zone, where attribution is inherently difficult.
- Growing geopolitical pressures are shaping regional connectivity. Severe disparities exist with ASEAN: e.g., Singapore and Malaysia each have over 20 cable connections, while countries such as Cambodia and Myanmar have only 4. It was also observed that new cable routes by technology companies increasingly bypass the South China Sea, routing south of the Philippines and through Indonesia, likely reflecting unstated geopolitical risks.
- It was noted that the Co-Chairs' report from both meetings should form the basis of a memorandum on best practices for protecting subsea fiber optic cables. Proposal for the meeting to consider whether to continue focusing specifically on subsea fiber optic cables or to broaden the agenda to include critical marine infrastructure in a future study group, which could include the electric cables (with focus on the ASEAN Power Grid), undersea pipelines for oil and gas, offshore oil platforms, and the impact of emerging technologies on critical marine infrastructure.

SESSION 1: GEOPOLITICAL CHALLENGES TO THE SECURITY OF DIGITAL INFRASTRUCTURE

Dr. Akekalak Chaipumee (CSCAP Thailand) spoke on the concept of a "digital interregnum", a political power vacuum in the global digital order where no single set of global rules or central authority exists to enforce order.

- Three competing digital empires have emerged: the US market-driven model; the China state-centric model focused on stability; and the EU rights-based model. This coexistence results in a fragmented and unstable global system.
- Imperial rivalries are occurring on two fronts: a horizontal state versus state front exemplified by US-China technology competition, and a vertical front involving the struggle for data control and data sovereignty versus data residency.
- Thailand faces an internal challenge of domestic fragmentation where numerous agencies (e.g., National Security Council, National Cyber Security Agency) lack interoperability, creating overlapping mandates and slow coordination despite efforts to align with international standards.
- ASEAN should offer a shared reference point for digital norms to help small and middle powers avoid being pulled entirely into one digital empire. It should act as a middle platform to bridge technical and regulatory standards, building resilience to maintain an open and stable region.

Ms. Irene Chan (CSCAP Canada, joining virtually) discussed the narrative in network challenge, arguing that the information space is now a strategic domain alongside land, sea, air, and cyber, where managing perception is as critical as managing systems.

- Decisions regarding satellites, cables, and platforms are not merely technical questions but political choices that create long-term dependencies.
- Three competing narratives dominate: the Russian view of a weaponized information space; the Chinese view of a sovereign, orderly space; and the US view of an open, rules-based space, which is sometimes perceived regionally as "digital imperialism".
- Southeast Asia faces three core obstacles to information resilience: fragmented responses with no dedicated ASEAN-wide process for foreign information manipulation and interference (FIMI); capacity asymmetries in forensic attribution; and sovereignty sensitivities where shared monitoring can be misinterpreted as interference.
- Practical recommendations include establishing a voluntary Track 1.5 regional information network for open-source analysis; linking information indicators with cross-domain monitoring of cyber and physical infrastructure; and investing in societal resilience through media professionalism and digital literacy.
- Guiding principles to avoid the perception of political interference or digital imperialism include: co-creation (Southeast Asian experts must lead the agenda), transparency (findings should be shared with member states), and genuine partnership (partnerships must be generated through exchange to create a distinctly Southeast Asian model of information integrity).

Dr. Bradley Jensen Murg (CSCAP Cambodia, joining virtually) introduced the concept of "weaponized interdependence", describing how states exploit their

centrality in networks to monitor, coerce, or exclude others, a pressure significantly felt by smaller ASEAN states.

- Geopolitics plays into the digital world through three mechanisms: financing and vendor lock-in; standard setting; and extraterritorial legal reach, such as laws extending state authority via corporate actors.
- The heterogeneity within ASEAN makes the region a target, with the CLMT countries (Cambodia, Laos, Myanmar, Timor-Leste) facing specific vulnerabilities due to financial constraints that incentivize them to accept offers from specific external powers.
- Domains of contestation include submarine cables, which are becoming politicized and bifurcated; cloud platforms, where choosing a provider is effectively choosing a "jurisdictional overlap"; and telecom networks.
- The ASEAN Digital Economy Framework Agreement (DEFA) brings security challenges regarding cross-border data flows and participation in trusted cloud ecosystems.
- Recommendations include treating submarine cables as shared strategic assets with a regional incident reporting system; attempting to embed minimum security standards into DEFA; and institutionalizing "quiet diplomacy" to de-escalate mutual incidents.

Discussion

Issue: The narrative that ASEAN nations "do not have to choose sides" in the digital domain is complex.

While some participants argued that ASEAN countries possess "strategic autonomy" and do not have to pick sides between major powers (maintaining complementarities with both China (e.g., 5G, AI applications) and the US (e.g., talent training)), it was also argued that while states may not choose sides diplomatically, they effectively choose sides regarding digital norms, regulations, and platforms. This decision is often driven by "path dependence", where the selection of a cloud platform or 5G provider creates long-term technical and financial lock-in, making future diversification difficult.

Issue: Financial constraints drive infrastructure choices more than political alignment.

For developing economies in the region, infrastructure choices are often dictated by the most affordable option rather than explicit political allegiance. Developing nations with limited access to Western credit are incentivized to accept offers that fit their national budgets. Consequently, decisions that appear to be strategic alignments are often driven by capacity asymmetries and the practical necessity of securing affordable connectivity.

Issue: Divergent national priorities hinder regional cooperation.

A significant barrier to genuine regional cooperation is that ASEAN members do not prioritize digital threats equally. For instance, some states prioritize immediate domestic issues like online scams over the security of submarine cables. Furthermore, domestic fragmentation within states (where multiple agencies lack interoperability)

serves as a lesson in the difficulties of coordinating a unified national response, let alone a regional one.

Issue: It is necessary to distinguish between intentional and unintentional threats to infrastructure.

Discussions highlighted the need to separate unintentional cuts (e.g., fishing, anchors) from intentional cuts (e.g., sabotage, grey zone tactics). While unintentional damage is a regulatory issue involving repair permits, intentional damage requires deterrence and surveillance strategies. It was noted that industry or states may need to deploy technologies such as automated underwater robots or "dark vessel detection" programs (using satellite technology to spot ships that switch off tracking systems) to identify suspicious behavior and enhance maritime domain awareness.

Issue: The potential for a regional information fusion mechanism.

There was a proposal to establish a regional information coordination center for submarine cables, like the information fusion center used for piracy monitoring. Such a mechanism would facilitate the exchange of information on threats and cable routes. However, challenges remain regarding the willingness of commercial operators and states to share confidential data, such as cable capacity and precise routes, with potential rivals due to jurisdiction and secrecy concerns.

Issue: Geopolitical maneuvering is influencing the physical routes of new submarine cables.

New cable projects by US tech giants are increasingly bypassing the South China Sea, routing south of the Philippines and through Indonesia instead. While companies cite stakeholder engagement as the reason, this is a geopolitical decision to avoid disputed waters, which has strategic implications for regional connectivity.

SESSION 2: EMERGING TECHNOLOGIES AND THE FUTURE OF DIGITAL INFRASTRUCTURE

Mr. Shashidhar T. K. (CSCAP India) provided an overview of the threat landscape shaped by emerging technologies, focusing on artificial intelligence (AI), quantum computing, and blockchain.

- The proliferation of IoT devices generates massive data but introduces vulnerabilities that criminals exploit for entry. The threat landscape has evolved from simple data theft to AI-driven attacks. Malicious actors now utilize AI to write polymorphic malware, conduct automated reconnaissance, and create deepfakes at scale (e.g., 20,000 deepfake videos were found in three months).
- India aims to make AI accessible across sectors like healthcare and manufacturing. The *India AI* platform serves as a knowledge hub for researchers, while the *Responsible AI for Youth* program engages the younger demographic.
- The government and private sectors are deploying AI to automate alert monitoring and response, detect anomalies across critical infrastructure, detect mule accounts and prevent fraud.
- Regarding quantum security, the "harvest now, decrypt later" strategy poses a critical strategic threat, where adversaries steal encrypted data today to decrypt

it when quantum computers mature. India's National Quantum Mission focuses on developing indigenous quantum capabilities and post-quantum cryptography to secure communications before threats materialize.

- Regarding blockchain and financial crime, while blockchain and Web3 technologies are adopted for securing financial transactions (e.g., land records, unified payments interface), cryptocurrencies pose money laundering risks.
- On international cooperation, India has signed cybersecurity MoUs with multiple partners (including Singapore, Malaysia, Japan, Vietnam, the UK, the US), facilitating threat intelligence sharing and joint investigations. It aims to act as a capacity-building partner for Global South by sharing Digital Public Infrastructure (DPI) models.

Ms. Farlina Said (CSCAP Malaysia) discussed the dual-use nature of AI and the governance challenges of critical infrastructure in the face of quantum and 6G developments.

- AI functions as a general-purpose technology that aids productivity but also empowers malicious actors to write malicious code, increasing the volume of cyber-attacks. Organizations must invest in "agent AI" to assist security officers in countering these automated threats.
- Quantum technology is not yet widely available or stable enough to break current encryption immediately, but the danger is the "store now, decrypt later" threat, where attackers steal encrypted data today to decrypt it years later when the technology matures.
- Preparedness requires migrating systems to quantum-safe encryption standards and building mathematical talent to understand complex encryption lattices.
- Preparation strategy: migrating systems to quantum-safe encryption standards; building mathematical talent to understand complex encryption lattices; assessing which data assets will still be sensitive/detrimental if decrypted 5 years from now.
- Regarding critical infrastructure and governance, a "one size fits all" approach to cybersecurity is ineffective. Standards must be sectoral because critical systems differ by industry; for instance, GPS is critical for maritime IT systems but less so for banking.
- Malaysia defines critical national information infrastructure as systems whose destruction negatively impacts national security, the economy, or public safety.
- Malaysia has launched many national initiatives: National AI Office to coordinate AI policies across ministries, National Quantum Cryptography Migration Plan (2025-2030). A new cybersecurity bill was passed to formalize these governance structures. The definition of critical national information infrastructure (CNII) focuses on "computer systems" rather than physical infrastructure to manage resource intensity.
- Regarding regional cooperation, it was acknowledged that while ASEAN has established frameworks like the ASEAN Cybersecurity Cooperation Strategy (2021-2025), success is hard to measure when incidents like ransomware still

occur. The focus remains on building resilience and incident management capacity.

Discussion

Issue: The concept of quantum migration and countries' experiences?

A question was raised for clarification on the concept of quantum migration. Entire ecosystems must migrate to post-quantum cryptography because once quantum computing matures, it will break current encryption standards (RSA/ECC). The migration is complex as it involves adopting new mathematical lattices and requires building specialized talent, as well as requires assessing which data assets will remain sensitive if decrypted in the future.

Issue: Feasibility international treaties for artificial intelligence.

A question was raised on whether ASEAN could move beyond non-binding guidelines to binding treaties or agreements to manage AI risks, noting that AI is a mature threat compared to 6G.

Instead of creating new treaties, it was suggested that countries amend existing mutual legal assistance treaties (MLATs) to explicitly include AI-related threats, facilitating faster cross-border cooperation. Conversely, it was noted that developing ASEAN states view AI as a catalyst for economic growth and may be hesitant to sign binding treaties that could stifle development or reduce competitiveness. Additionally, binding treaties are difficult because nations view AI as an economic catalyst (e.g., for semiconductor industries) and fear that strict regulations might stifle national competitiveness and development.

Issue: Establishing norms against cyber-attacks on critical infrastructure.

A question was raised on whether ASEAN could agree on a basic regulation to never use AI to attack critical infrastructure, like the Southeast Asia Nuclear Weapon-Free Zone (SEANWFZ) Treaty.

It was noted that such norms technically already exist in the United Nations Group of Governmental Experts (GGE) norms and ASEAN checklists (which cover critical infrastructure protection). The challenge is not the lack of text, but the political will to actively enforce and adhere to these voluntary norms.

Issue: Should researchers focus on distinguishing between what is real and what is potential/imaginary regarding emerging technologies like AI?

It was argued that cybersecurity requires imagination and policymakers must prepare for threats before they fully manifest; otherwise, it will be too late to react. AI-orchestrated attacks are no longer imaginary, citing recent reports of AI-executed cyber espionage campaigns.

Issue: A possibility for building a common platform regarding AI ethics and literacy?

The *India AI* platform and *Responsible AI for Youth* program were highlighted as models that could be scaled up for regional collaboration. AI literacy was framed as an existential question of human augmentation, requiring society to decide at what age and to what extent people should rely on AI for thinking and daily tasks.

Issue: What is the future of digital infrastructure given the tension between decentralized cryptocurrencies and state-controlled central bank digital currencies?

A question was raised regarding the conflict between the popularity of decentralized cryptocurrencies (investment) and the state's desire for control via central bank digital currencies. While blockchain technology is useful for transparency (e.g., land records), cryptocurrency poses severe money laundering risks due to anonymity. The recommended approach is not necessarily banning crypto but strictly regulating the exchanges to ensure law enforcement can attribute transactions and track illicit funds.

SESSION 3: SUBMARINE CABLES, POWER GRIDS AND THE FUTURE OF REGIONAL CONNECTIVITY

Mr. Kwa Chong Guan (CSCAP Singapore) noted that through these respective panels, the study group has widened its scope beyond submarine fiber-optic communication cables. He suggested possible areas for future research, including transport shipping lanes, the sustainability of fisheries and marine biodiversity, and electric grid cables. He stressed that because all of these issues face similar challenges, broadening the scope of a future study group would enable us to address them more holistically. Specific points made include:

- The ASEAN Power Grid (APG) is part of a wider ASEAN energy vision extending to 2045, which includes gas pipelines, renewable energy, and nuclear power.
- While the infrastructure for the APG technically exists (e.g., wires from Thailand to Malaysia), the implementation remains a technological rolling plan hindered by financing issues and policy coordination regarding tariffs and jurisdiction. However, he noted that such issues were beyond CSCAP's mandate, which focuses on matters related to security and confidence-building.
- The challenges confronting energy grids and pipelines, such as sabotage and resilience, are similar to those facing fiber-optic cables, justifying the potential for a new study group to explore how energy grids can further ASEAN connectivity.

Mr. Hoang Do (CSCAP Vietnam) used the three-level analysis framework (system, state, and sub-state) to assess recent developments in undersea cables and their impact on Vietnam's connectivity.

- At the system level, strategic competition has intensified with US legislative and executive efforts (e.g., FCC rules) to decouple from Chinese technology. However, alternative options have emerged, such as the EU's Global Gateway and other initiatives, which aim at enhancing connectivity.
- At the state level, governance gaps persist, with half of UN members lacking a definition for "critical infrastructure" and only 5% including undersea cables within that definition. A worrying trend is the increase in cabotage laws which impede foreign vessels from performing cable repairs. However, positive trends include Malaysia reenacting cabotage exemptions to facilitate repairs and the securitization of cables at forums like the Shangri-La Dialogue, which helps channel more resources into their protection.
- At the sub-state level, narratives regarding the avoidance of the South China Sea were challenged, noting that major projects like SJC2 and ALC are still

being laid in the area. Additionally, reports of a Chinese “cable cutting machine” were contextualized as standard repair technology capable of retrieving and fixing cables, similar to Western equipment.

Dr. Xu Longdi (CSCAP China) described submarine cables as vital arteries carrying over 95% of data traffic, while acknowledging that US-China tech competition has restricted Chinese participation in projects like the PLCN and SeaMeWe-6.

- Despite fierce competition, high-level communication between US and Chinese leadership indicates a desire to stabilize relations, suggesting that cooperation on maintaining the safety and integrity of cable networks is still possible.
- ASEAN can play an active role by establishing a liaison point for submarine cable safety to maintain working-level contact during incidents.
- Cable incidents should be depoliticized and treated as technical or business issues rather than exclusively as security threats. To safeguard submarine cable safety, a balance between political and security concerns and economic and technological interests should be maintained, following the principles of consultation, joint construction, and shared benefits. The positive role of the business and technology communities should not be neglected.

Ms. Lizza Bomassi (CSCAP EU, joining virtually) emphasized that Europe and Asia are connected to the same digital and energy system, citing the *Rubymar* incident in the Red Sea where a drifting ship cut three cables, demonstrating how disruption in one maritime corridor cascades across trans-regional systems.

- Maritime connectivity faces three types of vulnerability: physical (uneven redundancy where a single cut can cause national shutdowns); strategic/grey zone (below-threshold pressure like delays and ambiguous incidents); and governance (unclear responsibilities and overlapping agencies).
- Resilience requires aligning vision (seeing systems as connectivity lifelines), cooperation (practical routines to reduce downtime), and resources (long-term investment).
- The EU aims to be a predictable partner by sharing hard-learned experiences on resilience. Through the Global Gateway initiative, the EU is investing more in maritime security infrastructure in the Indo-Pacific, including supporting on-land capacities, as subsea cables traverse multiple geographies and require robust onshore management.
- Resilience is not separate from sustainability; the green transition and the integration of renewable energy grids are only possible if cross-border reliability is secured.

Discussion

Issue: The priority for countries with limited resources to ensure connectivity and transparency?

It was suggested that the priority is redundancy through diversification, not just of cable routes, but of partners and connecting points. To increase transparency without heavy costs, the use of maritime domain awareness (MDA) technologies and AI was

suggested to detect suspicious ship movements (e.g., loitering) that might indicate intentional sabotage.

For energy infrastructure, on-land capacities should not be ignored, as subsea cables traverse multiple geographies requiring robust onshore management. The EU's Global Gateway was highlighted as a source of investment for maritime security infrastructure.

Issue: Building trust and depoliticizing infrastructure.

A question was raised on how major powers can balance their role as global cable providers with concerns that they might control or undermine connectivity, and how can they rebuild global trust?

It was argued that trust cannot be built in a day, it was noted that time and frequent exchange are required to reveal reliability. To mitigate suspicion, parties should depoliticize incidents: if a cable is cut, it should be handled as a maintenance issue rather than a political security event. Re-establishing professional liaison points would allow experts to resolve faults efficiently, as was done in previous decades. The region should also consider land-based cables and power grids as options to supplement subsea routes.

Issue: Feasibility of the ASEAN Power Grid and public-private partnerships.

A questioned was raised on the potential for the ASEAN Power Grid to extend to countries like Myanmar through public-private partnerships? It was responded that while the grid is technically feasible, the primary hurdle is financing. Implementation depends on resolving banking and tariff coordination.

Furthermore, a truly regional grid requires regional stability in conflict areas and technical compatibility to ensuring green energy standards are met. It was noted that the process of negotiating these connections is valuable in itself for bringing ASEAN together, even if the physical grid takes time to materialize.

Issue: The feasibility and sustainability of decoupling or bifurcating cable infrastructure.

Questions were raised regarding whether it is technically feasible to completely bifurcate or decouple the submarine cable value chain between competing powers.

It was noted that while physical separation (disconnecting cables or landing stations) is possible, the total separation of data layers is harder; however, 100% decoupling may not be sustainable for any party. Observations of recent US legislative language suggest a shift from strict decoupling to de-risking or adversary-focused language, indicating a softening stance.

SESSION 4: PUBLIC–PRIVATE COOPERATION ON DIGITAL INFRASTRUCTURE SECURITY

Mr. Gavin Birrell (CSCAP New Zealand) spoke on the public private cooperation model (noting "public private partnership" implies debt and leverage financing in the New Zealand context) and the move from passive to active regulation.

- New Zealand follows the International Cable Protection Committee (ICPC) recommendations, having implemented 12 of the 16 best practices. Despite the existence of legal cable protection zones, mariners often ignore them, resulting

in numerous strikes (e.g., the Southern Cross cable suffered 180 strikes in 15 years). Industry has criticized the government's role as too passive, arguing that the government should enforce its own protection acts given the significant private investment ($600 million) in infrastructure.

- Facing fiscal constraints, a deal was negotiated where the private sector pays for surveillance (using Starboard Maritime Intelligence), while the government funds the warning function. This system uses algorithms to detect suspicious behaviors (e.g., trawling speeds) inside protection zones, triggering a human review and a radio warning to the vessel.
- New Zealand benefits from the security requirements imposed by the US and Australia as these are the countries at the other end of its cables (e.g., landing station physical security, reserve electricity generation minimum standards, personnel vetting, and logical security standards).
- Security roles have been devolved to the market. Employees of private companies can be designated as cable protection officers with the legal power to issue binding orders to vessels.
- Regarding future challenges, the "tyranny of distance" remains a challenge for repair ships, where one vessel covers a massive area; as other governments are exploring sovereign repair/response capabilities, the New Zealand government is exploring what it may need to do, noting the forecast deficit of half of one cable ship for the South Pacific Marine Maintenance Agreement area by 2040. That could include exploring opportunities to take a regional partnership approach to this with industry and Pacific Islands Forum partners.

Dr. Chyungly Lee discussed the legitimacy of security concerns and the nature of public-private interaction.

- Threat perception varies by country and region; while some feel secure, others face significant risks, justifying the legitimacy of discussing subsea cables as critical infrastructure. Infrastructure requires "security by design" - meaning infrastructure should be built with security features from the start to withstand future threats.
- Regarding public-private partnership (PPP) structure, although Chunghwa Telecom was privatized beginning in 1996, the authority and related agencies still hold a controlling stake (approx. 42%). Because subsea cables are public infrastructure, the authority must be involved, creating a close private-public partnership to support the private sector.
- To manage vulnerability, the focus is on redundancy and resilience. In addition to cables, microwave and satellite links are being developed as backup infrastructure. Due to the lack of repair ships, it is necessary to collaborate with international repair zones for maintenance.
- A strategic shift from "detecting and responding" to "prevention and deterrence" has occurred following recent cable disruptions. Early warning systems now use automatic identification system (AIS) to monitor suspicious vessels that loiter in the 96 identified cable protection zones beyond a reasonable time.

- Regarding the complexities of cooperation, the distinction between “cooperation” and “coordination” highlights the US shift toward a centralized agency for cable-security coordination, while the gap between redundant telecommunication cables and far costlier, non-diversifiable undersea power cables points to a deeper energy-security vulnerability.

Discussion

Issue: How can governments persuade profit-driven private operators to uphold high security standards without relying on pressure from major powers?

It was noted that countries like New Zealand employ a “free-riding” approach, relying on the strict regulations of the US (Department of Homeland Security) and Australia. Since international cables connecting to the US must meet American standards, other nations benefit from these high standards without imposing domestic costs. Additionally, some companies use “higher resilience” as a market differentiator to attract premium customers, creating a commercial incentive for security.

Issue: How does the dominance of “hyperscalers” (Big Tech like Google and Meta) change the balance of power in infrastructure governance?

A shift was noted as hyperscalers (whose GDPs often exceed those of the countries they operate in) become dominant cable owners. While traditional telecom companies cooperate voluntarily (e.g., seamlessly rerouting traffic), there is concern that these massive tech giants may exert undue influence that small states cannot regulate, potentially forcing regulation-averse governments to reconsider their hands-off approach.

Issue: How can the region address threats from “shadow fleets” operating beyond territorial waters?

A significant challenge is the operation of vessels registered to flags of convenience (e.g., Cook Islands) with weak management, known as shadow fleets. The *Eagle S* incident, which severed cables between Finland and Estonia, highlighted a gap in global governance beyond the 12-nautical-mile limit where coastal states lack jurisdiction. It was suggested that the Biodiversity Beyond National Jurisdiction treaty might offer a framework to address these gaps.

Issue: What is the genuine motivation for private companies to cooperate with governments?

Private companies are driven by profit and generally avoid government interference. However, when their infrastructure is physically disrupted and profits are threatened, they immediately seek government assistance for political and jurisdictional resolution, as they lack the capacity to handle relevant issues themselves.

Issue: What are the challenges in holding private actors accountable for transnational damage under current international law?

There is difficulty in assigning liability (e.g., should punishment target the flag state, the crew, or the cargo owner?). Due to the absence of clear international law and UNCLOS gaps regarding economic exclusive zones versus continental shelves, the focus remains on governance rather than strict legal penalties.

CLOSING SESSION

- It was proposed that the group produce a *memorandum* summarizing ideas from the first and second meetings regarding the safety and security of subsea maritime infrastructure. The memorandum must contain at least *three actionable policy recommendations* for submission to ASEAN Senior Officials and the ASEAN Regional Forum (ARF).
- On scope of future topics, a proposal was made to proceed to a new phase focusing on marine energy cables and the ASEAN Power Grid, aiming to transfer lessons learned from fiber-optic cables regarding maintenance and cooperation to the domain of energy security. Consensus leaned towards broadening the title to "Safety and Security of Critical Infrastructure" to encompass both digital cables and energy networks.
- There was a discussion on how deep the group should go into solving problems (e.g., establishing points of contact). It was clarified that CSCAP's mandate is policy exploration, not operationalization. Operational details (how to implement a specific center) are domestic executive issues and outside CSCAP's remit.
- On information sharing and security cooperation:
    - The need for a framework to map capacity was emphasized to identify who has the ability to ensure baseline services before enticing private sector action.
    - It was suggested that within CSCAP, visualizing progress through comparative tables or data sheets would be useful to motivate member states.
    - A call was made for renewed engagement from CSCAP Canada, with agreement to consult senior colleagues regarding contributions to the next phase.
    - Mapping of EU supported actions on the ground via the joint research services map for the Indo-Pacific was offered to assist with stakeholder and funding identification.
- **CSCAP Thailand's Recommendations:** as the CSCAP Thailand representative was unable to attend the final session in person, concise recommendations for the Study Group's consideration were submitted, including:
    - **Make "interoperability" the central organizing principle of ASEAN cyber cooperation.** AMS do not share the same level of cyber maturity or prioritisation, so progress must begin with achievable layers of cooperation: (1) shared norms, (2) shared infrastructure practices, and (3) shared implementation protocols. ASEAN currently sits at Level 1; Levels 2–3 should guide the next phase.
    - **Support and strengthen the development of the ASEAN Cybersecurity Cooperation Strategy (ACCS) 2026–2030.** The new strategy should clarify roles among AMCC, ASEAN Cyber-CC, and ASEAN-CERT, standardize incident reporting, and establish long-term capacity-building for less-resourced AMS.

- **Clarify and reinforce the mandate of the ASEAN Cyber-CC:** The Cyber-CC's current contribution is unclear. A formal coordination mechanism with the AMCC is needed, including a monitoring framework and regular deliverables.
- **Expand operational cooperation led by CERTs, building on the ACID drill**
  CERT-level cooperation remains the most effective and politically feasible. Annual ACID exercises and a "coalition of the willing" model should be encouraged for human-driven cyber threats.
- **Use interoperability models from multilateral CBDC frameworks as a guiding analogy:** ASEAN today resembles **Model 1** (fragmented but compatible). The region should move toward **Model 2** (interlinked systems), with **Model 3** serving as a long-term aspiration for a trusted regional cyber ecosystem.
- **Submarine-cable resilience:** ASEAN should develop mechanisms for rapid information-sharing and joint response to intentional attacks (sabotage, criminal damage) and unintentional disruptions (natural disasters, accidents). Cooperation here is critical and should be embedded into ACCS 2026–2030.

- Participants are to go back and consult their national committees regarding the proposal to expand the study group's mandate to energy infrastructure. The upcoming Steering Committee meeting (15-16 December 2025) will determine the future direction.