Spring 2026 Aspen Digital Global Cybersecurity Group Meeting

May 25–27, 2026 | Tokyo, Japan

Convened by Aspen Digital, a program of the Aspen Institute, in collaboration with the National Cybersecurity Office of the Government of Japan

Executive Summary

Aspen Digital, a program of the Aspen Institute, in collaboration with the National Cybersecurity Office (NCO) of the Government of Japan, convened the Spring 2026 meeting of the Global Cybersecurity Group in Tokyo, May 25–27. This invite-only assembly of senior government officials, private-sector executives, and civil society experts met for two days of closed-door policy dialogue. Topics of discussion included strategic cyber priorities at all levels of government in areas both mature and emerging. Participants also examined the shifting global threat landscape, including the accelerating role of AI for both attackers and defenders.

The convening came at a moment when geopolitical tensions and rapid advances in AI are reshaping the threat environment faster than governments, defenders, and governance models can respond. Across every session, a common tension surfaced: offensive capability is outpacing defense, even as the cooperation needed to close that gap has become harder to sustain. Participants returned repeatedly to a reframing of cybersecurity away from a reactive, cost-centric discipline and toward proactive resilience and a strategic investment in economic competitiveness, national security, and digital sovereignty. The group recommended a series of practical actions that governments and industry can undertake together to move beyond dialogue toward coordinated, accountable action.

Strategic cyber priorities:

- **Tie national strategies to executable tasks and accountable institutions.** Across regions, participants stressed that a strategy without concrete actions, owners, and measurable outcomes risks becoming only a "piece of paper." Cyber policy must be a political priority, not solely a technical one, and international cooperation must be designed to respect different levels of maturity, political reality, and national sovereignty.

Public-private partnerships for critical infrastructure:

- **Move from goodwill to good governance through reciprocal, operational partnerships.** Operators and governments should commit to two-way information sharing backed by safe-harbor protections for good-faith disclosure, with Japan's designation of critical infrastructure categories and its proactive intelligence sharing requirements offered as a model to codify collaboration in law and practice.

Governance of emerging AI cyber capabilities:

- **Shift from vulnerability management to harm management.** As AI compresses the time between vulnerability discovery and exploitation, participants urged investment in segmentation, containment, runtime governance, and open-source security to reduce the "blast radius" of attacks rather than relying on patching alone.

Sub-national coordination:

- **Strengthen vertical coordination so national strategy reaches the local level.** National governments should supply the funding, standards, and workforce pathways that lift, not replace, municipal and regional capacity, recognizing that local authorities are closest to citizens and critical services, but often the least resourced to act at speed. Participants urged a move away from one-off grants toward continuous shared and managed security services, treating cybersecurity as a common good, since national resilience is only as strong as its least protected node.

Global cyber policy cooperation:

- **Build interoperable standards while avoiding "regulatory colonialism."** Shared frameworks for software bills of materials (SBOM), internet of things (IoT), and supply-chain transparency can provide neutral ground for cooperation across political systems but must be backed by capacity-building, technical support, and local flexibility.
- **Treat trusted relationships as strategic infrastructure.** Formal diplomatic processes move slowly, while smaller, trusted communities and ecosystems can produce faster outcomes. In a fragmented technology environment, resilience must be built through practical, trust-based cooperation rather than formal structures alone.

Strategies to disrupt the global scam economy:

- **Align incentives across the full digital and financial ecosystem.** Because most scam infrastructure runs through the private sector, effective disruption requires coordinated law-enforcement cooperation, telecommunication and financial regulations, identity security, anti-money-laundering action, and victim support, alongside public education and "digital mindfulness."

Cyber operations in modern warfare:

- **Prioritize resilience and preparedness over deterrence.** Participants emphasized hardening critical infrastructure, clarifying rules of engagement, and preparing for long-duration conflict and sustained operational capability before a crisis begins.

Integration of AI into national security:

- **Keep humans accountable while using AI actively for defense.** Governments should define clear AI use cases and limits, finance resilient assurance capabilities, and regulate for transparency and human responsibility in addition to preparing for emerging risks such as agentic insider threats and a coming wave of AI-generated vulnerabilities.

Full Summary of Outcomes

The Spring 2026 Aspen Digital Global Cybersecurity Group convened as cyber policy shifts from reactive defense toward a growing focus on raising the costs imposed on adversaries. Participants observed that this posture has become more publicly acceptable in the United States across recent administrations, as new policies have placed a heavier emphasis on offense and deterrence.

Cyber threats continue to grow in reach, pace and sophistication. Russia remains a persistent threat, evident in its attacks on Ukraine and European economic assets, while the Typhoon campaigns illustrate the reach of the People's Republic of China and other state-sponsored activity into critical infrastructure sectors. Japan, among others, has faced cryptocurrency theft, distributed denial-of-service, and ransomware attacks, including from North Korean cyber threats whose activities span both cryptocurrency theft and the infiltration of hiring pipelines. At least 10 percent of applicants screened at one participating organization at the Global Group meeting were assessed to be North Korean IT workers.

Attacks are also harder to detect as threat actors increasingly use valid credentials and native services, execute supply-chain compromises into continuous integration/continuous delivery (CI/CD) software delivery pipelines and open-source packages, target security tooling, and incorporate AI capabilities into their operations. The Google Threat Intelligence Group (GTIG) AI Threat Tracker, for example, now monitors AI-enabled exploits. Recent GTIG reporting documented a cybercriminal group generating an AI-assisted zero-day exploit and multiple threat actors shifting toward industrial-scale obfuscation, including automated scripts that open and close accounts for disposable attacker infrastructure.

Against this threat landscape, organizations confront a stifling reality: they cannot retire legacy technology fast enough, the attack surface keeps expanding, and timely patching can introduce supply-chain risk, because threat actors can seed open-source code with malicious components, while delayed patching invites compromise. New technology, moreover, rarely arrives with mature governance. This rapidly compounding risk environment is one that regulation and newly developed strategies must reflect and address. Defenders are now expected to patch faster, adopt AI faster, and share threat intelligence faster while absorbing nearly all the residual risk; participants argued they need a legal safe harbor when operating in good faith and following sound security practices.

Participants stressed, however, that intelligence sharing is a first step; the second is disruption, including taking down adversaries and adversarial infrastructure. And if patching alone is no longer sufficient, cybersecurity must shift from vulnerability management toward harm management: building systems that remain resilient to harm, much as the airline industry engineers for safe failure. The sections below capture the outcomes of each meeting session in turn.

Strategic Cyber Priorities for Governments

Examining how governments worldwide are approaching cybersecurity as a strategic policy priority, the discussion found highly varied legal, institutional, and capacity realities across regions. A common theme emerged: strategies must move beyond high-level commitments and translate into executable tasks, accountable institutions, and practical mechanisms for resilience. Participants from industry and governments across the following nations and regions provided these situational updates:

- **Japan:** Japan emphasized a shift from "cybersecurity" to "cyber resilience," anchored in the concept of Active Cyber Defense and the revised National Cybersecurity Strategy. At the core of this approach lies "deterrence and defense" through the continuous imposition of costs on malicious actors. Information was described as the indispensable bedrock of action, with the National Cybersecurity Office (NCO) positioned as a strategic hub that collects and analyzes information and translates it into action, both by the government itself and in collaboration with the private sector, including through a new Public-Private Collaborative Council, as well as through international cooperation. Japan has also launched a government-wide discussion on a fundamental reinforcement of its national security policy, with the cyber domain positioned at its very core as a vital axis intersecting every aspect of national defense.

- **United States:** Participants noted a comprehensive national cybersecurity law is unlikely to emerge soon. Instead, regulatory momentum is expected to continue sector by sector, echoing the logic of the European Union's (EU) Network and Information Security Directive 2 (NIS2) within a distinctly U.S. political context. Continuity across U.S. administrations includes the development of post-quantum cryptography standards and prohibiting communications equipment from untrusted foreign suppliers, including the Federal Communications Commission "Rip and Replace" program. For U.S. cyber policy to advance, participants argued, it must become a sustained political priority.
- **Czechia:** Cybersecurity was framed as a dynamic rather than static domain, building on obligations from both the EU and NATO. A strategy without executable tasks risks becoming "only a piece of paper;" the crucial question is which specific actions and mechanisms will produce greater security. For 2026–2030, priorities are expected to center on trust, democratic processes, and social cohesion, alongside capacity building, practical lesson-sharing, and deeper transnational collaboration.
- **Italy:** Italy is in the active process of drafting its national cybersecurity strategy, linking cyber policy to broader geopolitical and economic shifts and the growing role of governments in shaping a secure digital development. From an EU perspective, national efforts are also regional efforts, since the security of one member state strengthens the resilience of the wider European ecosystem.
- **Argentina:** Argentina is focused on practical national capability building. As of January 2026, critical infrastructure remains central to its agenda; the country is establishing a national security operations center while leveraging existing capabilities and is developing a CISO school to train cybersecurity leaders and practitioners.
- **African Union:** The discussion raised some of the most fundamental governance questions, as cybersecurity becomes continental before capacity is evenly distributed, particularly in the context of the African Continental Free Trade Area. Participants emphasized the importance of knowing who coordinates and who is accountable when governance fails, stating that [African nations] cannot wait for ideal conditions before acting. Different levels of maturity require different, tiered models of implementation to avoid producing "false compliance" in place of genuine resilience.

  Sovereignty increasingly operates through infrastructure. Questions around AI-for-defense agreements raised concerns about technological dependence and sovereign control. Many actors may be willing to coordinate, but far fewer will surrender authority, creating a central tension between shared resilience and national sovereignty.

- **Brazil:** Brazil, noting its youth as a democracy, shared its national cybersecurity strategy, offering a useful window into how major economies outside the traditional transatlantic frame are structuring priorities, aligning government action, and balancing domestic needs with international cooperation.

Cross-cutting themes: Several threads ran across the discussion: funding and implementation matters more than strategy alone; capacity remains a major constraint even in mature frameworks; critical infrastructure continues to dominate attention even as the definition of "critical" adapts with digitization; sovereignty is increasingly bound to digital infrastructure, supply chains, AI, and operational control; and regional and international cooperation, though essential, must be designed to respect different levels of maturity and national authority. The next stage of cyber policy will depend less on whether governments can produce strategies and more on whether they can turn them into coordinated, resourced, and accountable action.

Public-Private Partnerships for Critical Infrastructure

Turning to how better public-private partnerships can defend national critical infrastructure, participants recognized the severity and urgency of the current threat environment. The conversation centered on moving beyond goodwill toward building effective relationships between governments and industry.

- **Make partnerships reciprocal and accountable.** Effective partnerships require explicit expectations on both sides: incentives, accountability, and operational integration. Critical infrastructure owners possess deep operational insight, while governments often have broader visibility into threat actors and cross-sector risk. The private sector should share relevant operational data, while the government has a responsibility to return actionable information rather than simply collect it. Safe harbor protections for good-faith information sharing are essential, since without informed and balanced legal protection, operators are hesitant to share, and without useful feedback, reporting becomes a compliance exercise.
- **Codify collaboration in law and practice.** For example, Japan designates 15 sectors as critical infrastructure. Under the Cyber Response Capability Strengthening Act and Necessary Arrangement of Relevant Acts, the Japanese government collects and analyzes cybersecurity information, including information historically held by the private sector, and shares it in an appropriate form with both the public and private sectors. This reflects a purposeful government responsibility to share intelligence rather than keep it within government channels. Building on this, the May 2026 Project YATA-Shield

action package, compiled in response to the increasing speed and scale of AI-enabled cyberattacks, extends the public-private partnership mechanism beyond the financial sector to all critical infrastructure sectors and pairs it with support for cyber workforce development.

- **Reinforce this statutory framework through operational efforts.** In collaboration with the National Institute of Information and Communications Technology (NICT) and service providers, Japan monitors vulnerable IoT devices, such as routers and cameras, and notifies affected users. Its Cyber Defense Exercise with Recurrence (CYDER) runs simulated cyberattack response exercises involving more than 4,000 participants from national and local government and infrastructure. And it extends training to ASEAN members through the ASEAN-Japan Cyber Capacity Building Center (AJCCBC) in Bangkok, Thailand, and to regional partners in the Pacific such as Fiji. These efforts are demonstrating that resilience requires information sharing, technical monitoring, exercises, and countermeasures working in concert.
- **Elevate cybersecurity from a technical-operational issue to a business-resilience issue.** Executives should understand cyber risk in terms of safety, customer trust, operational continuity, and ecosystem resilience. Risk ownership and mitigation can start within private companies, but broader ecosystem risk, such as interconnected operational technology, requires government support through collaboration, regulation, incentives, and supply-chain engagement. Participants noted that these partnership frameworks are strongest when sector-specific and built in collaboration with industry. Priorities could include telecommunications collaboration, asset visibility and exposure management, supplier and customer transparency, and joint testing of critical components before deployment. Responsible supply-chain behavior also needs stronger positive incentives, financial, regulatory, and reputational, rather than penalties alone.
- **Address the growing asymmetry created by AI.** Recent reporting on state-sponsored threat activity has demonstrated how frontier AI models can support reconnaissance, vulnerability discovery, exploitation, lateral movement, and data exfiltration at speeds that are impossible for humans. Vulnerability discovery now operates at machine speed, while remediation operates at "calendar speed," shifting the cyber defense bottleneck from finding vulnerabilities to fixing them. Patching as a primary risk reduction strategy no longer scales for critical infrastructure. At the same time, because patching relies on testing and human oversight, fully automated patching can introduce unpredictable risk.

- **Treat frontier AI access as an equity and infrastructure question.** Because access to frontier AI models with advanced cybersecurity capabilities will likely be uneven, creating AI "haves" and "have-nots," participants identified several issues and recommendations:
    - AI compute as critical infrastructure: finding and fixing cyber vulnerabilities increasingly depend on compute capacity and on the power and cooling resources that sustain it. As such, AI compute now functions as a national resource even though in most nations, it has not been formally designated as one. Participants questioned whether AI compute should be treated as critical infrastructure, with contingency plans if cloud-based models or workflows fail during a crisis.
    - Access and equity: decisions about which governments and operators receive early access to frontier models carry direct implications for critical infrastructure security.
    - AI for defense: AI should be used to rewrite response playbooks, improve patching strategies, and perform security functions at machine speed.

The goal of public-private partnerships is to help critical infrastructure organizations detect, withstand, and recover from cyber incidents. As one analogy framed it, government and industry must play as one side by sharing the ball, controlling tempo, and moving together before the opposition can score. Partnership works when it is operational (embedded in shared workflows), AI-enabled (leveraging frontier or other useful capabilities for defense), leadership-driven (elevated from security teams to boardrooms), and human-centered (accounting for the people who operate, depend on, and are harmed by attacks).

Governing Emerging AI Cyber Capabilities

AI has "changed the game" by increasing the speed and scale of vulnerability discovery and exploitation, while countermeasures remain underdeveloped, even in advanced, cyber-capable nations. Session participants suggested several recommendations to reduce this incongruency.

- **Address the offense-defense imbalance.** AI-enabled tools are placing new capabilities in the hands of adversaries, who are often unconstrained by model access limits, norms, or governance. However, AI allows defenders to seize the initiative too. Defenders can use AI capabilities to find and close vulnerabilities before attackers discover them. Participants outlined an initial framework that treats AI infrastructure as a public good and funds it like one, so useful models reach defenders broadly.

Discussants cited Japan's Project "YATA Shield", an action package compiled in May 2026 in response to the increasing speed and scale of AI-enabled cyberattacks, as a near-term effort emphasizing enhanced vulnerability detection and patch management; alerts and guidance for critical-infrastructure operators, government agencies, and software vendors; deeper collaboration with international partners and AI developers; and NCO-led use of advanced AI to strengthen cyber response. Named after the Yata-no-Kagami, the sacred mirror in Japanese mythology said to illuminate the truth, this program of the Government of Japan calls for management-level leadership, fundamental cybersecurity measures, and disciplined vulnerability management.

- **Move from perimeter defense to dynamic protection and harm reduction.** Traditional boundary protection is no longer sufficient. Governments and organizations need more dynamic defensive systems. A priority is reducing the "blast radius" of successful attacks through network segmentation, containment, runtime governance, and harm management. This would be a shift from identifying vulnerabilities to limiting the damage they cause.
- **Strengthen open-source security as a strategic concern.** The Group discussed improving open-source software security, including whether nation-states should take more responsibility for patching open-source code themselves, especially ahead of quantum computing becoming realized. Of the thousands of vulnerabilities now surfacing, most fall into either proprietary software or open-source software. Proprietary software vendors have a market incentive to fix flaws, while open-source software maintainers have limited capacity and are increasingly overwhelmed by AI-enabled vulnerability findings. One approach is to create incentives for AI model providers to work directly with open-source maintainers on remediation efforts.
- **Recognize that access to advanced AI models is not enough.** The experience of organizations that gained access to powerful models to improve their cybersecurity posture showed that some lacked knowledge on how to use them effectively. Many organizations still struggle with basic cyber hygiene. Thus, model access must be paired with readiness, guidance, and operational maturity. In a world of advanced frontier and open-weight models with similar capabilities, successful integration of AI models into cybersecurity workflows is increasingly about organizational experience and knowledge, not simply exclusive model access.

Sub-National Coordination

Addressing how governments should coordinate at the sub-national level to secure the nation, participants agreed that effective national cybersecurity depends on strong

coordination among the central government, sub-national authorities, municipalities, and the private sector. The recurring theme was vertical coordination: national governments can set strategy, standards, funding priorities, and accountability mechanisms; but implementation depends on local and regional authorities who are closest to citizens and critical services yet often lack the resources, expertise, or mandate to act at the required speed.

- **Japan:** With 47 prefectures and approximately 1,700 municipalities accounting for about two-thirds of government expenditure, Japan has paired national initiatives, such as a cloud security framework and IoT labeling scheme, with four recent measures: a legal obligation for local governments to comply with national cyber standards (prioritizing security over decentralization), increased financial aid, an attack surface management system to monitor local government networks, and a workforce policy placing prefecture-hired security specialists into municipalities. Supply-chain risk is managed through a positive catalog of certified vendors. Yet, technology alone is insufficient. Human capital remains the most important resource, prompting university training pathways to build a long-term capacity pipeline.
- **Australia:** With about 28 million people across 8 states and territories and approximately 537 municipalities, Australia is now on the fifth generation of its national cyber strategy, but sub-national maturity falls away sharply. Two states still have no cyber strategy at all, and most municipalities receive no state funding for cybersecurity. Critical infrastructure "living labs" are a bright spot but inconsistent across states. Australia's extra-territorial responsibilities, such as in Antarctica, receive almost no cybersecurity attention.
- **Brazil:** Across a federal government overseeing 26 states and approximately 5,570 municipalities, Brazil described three coordination approaches: a cooperative federal incident response network that any organization can join by signing a membership letter, government shared services that states and municipalities can adopt at no cost, and a pending senate bill, modeled on the EU's NIS2, that would create a national cybersecurity agency with a public safety fund supporting state and municipal action. The discussion also emphasized partnership building and managing cascading, large-scale risks, drawing on cooperation with organizations such as the Shadowserver Foundation.
- **Canada:** With 5,162 municipalities, Canada has begun deploying federal cyber tooling directly into its three northern territories, Yukon, the Northwest Territories, and Nunavut, so that federal capacity defends sub-national infrastructure where local capacity does not exist. This Arctic example reinforced a broader point: sub-national coordination is

not only a question of authority but of capacity, in addition to connectivity, electricity, media access, and historical injustices in the region.

- **Chile:** Chile's recently established National Cybersecurity Agency holds oversight authority over essential services and operators of vital importance. After a 2025 breach of a private vendor serving the public health system, the Agency issued directives requiring basic controls such as multi-factor authentication and anomaly detection, reflecting a deliberate approach of starting with a small set of enforceable baseline standards instead of numerous controls that overwhelm institutions.
- **Finland:** With over 5.5 million people and a long border with a hostile neighbor, Finland mobilizes well-resourced private sector security leaders as national security infrastructure. Leaders across organizations participate in a shared operational chat that functions, in effect, as a national sensor network.
- **Germany and the European Union:** Across the EU's 27 member states as well as Germany's own 16 states and roughly 11,000 municipalities, most member states have exempted government itself from NIS2 requirements, leaving gaps where municipalities are excluded. The EU Cyber Solidarity Act focuses on shared detection and response capabilities as opposed to compliance. Separately, German states offer managed security services to municipalities through state-level IT providers. A German healthcare digitization fund that required 25 percent of hospital grants to be spent on cybersecurity was cited as a model for tying cyber to broader infrastructure investment.
- **India:** Spanning 28 states, 8 union territories, and more than 5,000 urban and 260,000 rural local bodies, India operates a hub-and-spoke model. The national government sets four foundational requirements for every state: 1) a notified cyber policy, 2) an empowered CISO, 3) a state security operations center (SOC) integrated with the national SOC, and 4) a cyber crisis plan, while states innovate locally. Examples include Bengaluru's public-private cyber center, Kerala's cyber safety awareness school curriculum and police Cyberdome partnership to counter cybercrime, Maharashtra's AI-enabled police unit, and Jharkhand's geographic information system (GIS)-based fraud tracking. Responsibilities remain distributed across agencies (e.g., telecommunications security with the Department of Telecommunications, cybercrime responsibilities with the foreign ministry) coordinated by a national cybersecurity coordinator. Participants acknowledged a deliberate trade-off: a slower operational tempo preserves federal trust.
- **Singapore:** Attendees discussed Singapore as a simpler coordination model owing to its unified government structure, where fewer layers make national coordination easier than in larger federal or highly decentralized systems.

- **United States:** Across 56 inhabited states (including Washington, D.C.) and territories, over 3,200 counties, and approximately 19,500 municipalities, the United States confronts a vast rural exposure: the 20 percent of Americans who live in rural communities span 97 percent of the country's land. The State and Local Cybersecurity Grant Program struggled to reach the highest-risk small communities. Water sector entities competed with the transportation and education sectors for the same state grant amount. Match-first, reimburse-later designs assumed cash flow that small utilities lacked. Competitive applications rewarded grant-writing capacity rather than risk exposure, and one-year funding cycles discouraged long-term investment. National Guard cyber elements and the Coast Guard's dual federal-state authority have emerged as promising, alternative cybersecurity capacity sources.

Cross-cutting recommendations: Participants drew several conclusions from this discussion. Two distinct problems are often conflated: the cybersecurity of state and local governments is different from the cybersecurity of critical infrastructure crossing jurisdictional boundaries, requiring different policy and funding tools. Awareness is no longer the bottleneck; capacity is, as sub-national leaders now understand the threat but lack resources, expertise, and consistent funding. Shared, managed security services delivered from a trusted, higher layer of government are preferred over one-off grants. Critical infrastructure entities desire consistent governance and oversight over local variation, since a utility operating across many jurisdictions cannot meaningfully comply with a different requirement in each. Cybersecurity investments should be bundled into broader infrastructure spending, built into every grid, port, and bridge by design rather than treated as a separate line item. Lastly, a small number of enforced baseline controls prevents more incidents than an extensive framework no one can implement.

Global Cyber Policy Cooperation

On how governments should coordinate global cyber policies, participants adopted the premise that cybercrime and cyber conflict cross national boundaries, with attackers exploiting differences between legal systems, regulatory approaches, and levels of capability. Cooperation must therefore be practical, timely, inclusive, and sensitive to local realities.

- **Develop interoperable standards and frameworks.** The Group urged moving beyond information sharing toward strategically harmonizing bilateral, regional, and multilateral policy frameworks, so that they reinforce one another. From a Japanese perspective, four areas stood out: 1) addressing the lack of international norms, with the new permanent UN mechanism, established as the successor to the Open-Ended

Working Group, seen as a critical forum for global rulemaking, 2) prioritizing practical collaboration for economic security, including promoting software bills of materials (SBOM) and IoT security to bring transparency and resilience to complex supply chains, 3) imposing costs on malicious cyber actors via enhanced international collaboration, and 4) strengthening resilience in the Indo-Pacific region.

- **Fit global rules to local realities and avoid "regulatory colonialism."** Developed regions should avoid exporting regulatory models to regions with less cybersecurity capability and capacity without adjusting to local conditions. Mature frameworks have been promoted in countries that lack the tools to comply and must simultaneously guard against regulatory capture by local and foreign companies. Cooperation should include capacity building, technical support, minimum thresholds for harmonization, and space for local adaptation, bearing in mind that one in three people worldwide have no internet access. Ultimately, regulatory policy must accommodate the underserved, the unserved, and future generations; not only the developed world.
- **Rebuild trust.** Before recent geopolitical tensions escalated to armed conflict in the Middle East and Europe, private malware labs and researchers often shared threat intelligence globally. As trust declined, this collaboration weakened, fostering safe havens for actors who exploit political divisions. With traditional diplomacy stalling, participants viewed public-private platforms, the World Economic Forum, the Aspen Institute, and regional or sectoral information sharing and analysis centers (ISACs), as faster vehicles for progress, observing that trusted networks and relationships are becoming strategic infrastructure. Some participants proposed a cyber-AI equivalent of the International Atomic Energy Agency (IAEA) to provide transparency and technical assistance at scale.
- **Draw lessons from digital resilience during conflict.** The war in Ukraine has shown the importance of digital resilience, offering lessons on how to prepare for, withstand, and recover from sustained cyber and digital disruption.

As threats and tensions grow, the need for cooperation increases, even as operational collaboration becomes harder to accomplish. Governments should pursue concrete, joint action focused on capabilities, speed, scale, and trust while aligning on interoperable standards, strengthening supply-chain transparency, improving public-private intelligence sharing, supporting countries with fewer resources, and building global rules that respect local realities. Such cooperation must be both principled and practical, fast enough to keep pace with technological change while respecting different national realities and drawing on the full range of bilateral, regional, multilateral, and multi-stakeholder mechanisms.

Disrupting the Global Scam Economy

Examining how to disrupt the global scam economy, participants described a transnational, for-profit criminal ecosystem responsible for an estimated US$442 billion in global losses related to financial fraud in 2025, according to Interpol's March 2026 Global Financial Fraud Threat Assessment. These scams are increasingly industrialized, often operating from hubs in Southeast Asia, where organized crime groups exploit weak regulation, open networks, and trafficked labor disproportionately targeting the underserved, especially the elderly. AI is sharpening the threat on every front, generating more convincing emails, cloning voices, and powering more persuasive romance scams.

- **Align incentives between government and industry.** Scams are not only a law-enforcement problem; much of the ecosystem's enabling infrastructure runs through private sector systems: telecommunications networks, financial institutions, cloud service providers, cryptocurrency platforms, hosting providers, and messaging channels. Some parts of the problem can be addressed significantly by the private sector, including real-time detection, threat intelligence sharing, insider threat monitoring, identity protection, and payment disruption. Participants suggested the private sector may need to lead in certain areas, such as detection, while governments work to align national objectives with commercial ones.
- **Build on proven public-private cooperation.** Fraud and scam investigations are complicated because suspects often reside overseas, rely on encrypted messaging, and launder proceeds rapidly using cryptocurrency across borders. Strong public-private and international cooperation help close the gap. For example, the Japanese Cybercrime Control Center, founded in 2014 as a public-private partnership organization to address cyberspace threats, collaborates with some 120 partner companies. Japan's establishment of the National Cyber Unit in 2022 marked a significant shift in national policing. Under the Police Law of 1954, only prefectural police held real investigative authority, but the NCU can now investigate cybercrimes and collaborate with international partners. This provides other nations with a sound model.
- **Confront consistent tactics and the human toll.** Threat actors rely on deception, emotional manipulation, and story-based attacks. Whether synthetic media is involved matters less than the fabricated story itself, which provokes an emotion that drives the victim to act against their interest. Romance scams and investment fraud often build trust over months before asking for money. Elderly victims are particularly vulnerable, suffering substantial financial losses and lasting trauma. Sextortion is an especially

urgent harm: deaths by suicide can occur within hours in some cases and even well-educated, cyber-aware people can fall victim. International collaboration is hampered by data protection and jurisdictional barriers. Participants argued that trauma-informed victim support should become a formal part of cybercrime response rather than an afterthought and noted that payment systems remain a critical enabler of fraud.

- **Pair technical controls with "digital mindfulness."** As part of a broader, human-centric approach, participants discussed building cognitive resilience and digital mindfulness across society. Drawing on the Japanese concept of Ma, or deliberate pause, the discussion emphasized helping people recognize emotional triggers, slow down before reacting, and identify their own vulnerabilities before scammers exploit them. The same predictable human vulnerabilities, urgency, fear, distraction, and loneliness, are exploited by information warfare and disinformation actors as well, so strengthening human judgment can complement technical controls.
- **Deploy practical disruption strategies.** Mobile network operators can scan for malicious traffic at scale, potentially protecting hundreds of millions of users, and wider adoption of passkeys can reduce account takeover risk. Participants cited Amazon Retail for large-scale deployment across hundreds of millions of accounts. Bulletproof hosting remains a major challenge, as many providers offer no practical route for takedowns or accountability.
- **Learn from national regulatory responses.** National efforts worth studying include the United Kingdom's anti-fraud initiatives, which have made it among the least affected nations, and China's anti-scam alliance efforts. The Group presented Thailand as another case study: its open visa policy and payment networks are vital to a tourism-dependent economy but also create vulnerabilities for cybercrime, so authorities have used know-your-customer rules to limit individual accounts across telecommunications, banking, and cryptocurrency to mitigate abuse, tightened the visa application process, and strengthened the powers of anti-money laundering agencies. Participants also pressed for greater use of sanctions, economic tools, and attribution, noting that many organizations lack a CISO and are ill-equipped to respond. Disrupting the scam economy ultimately requires coordinated pressure across the full ecosystem: law enforcement cooperation, private sector intelligence sharing, telecommunications and financial controls, identity security, victim support, anti-money laundering actions, and public education with incentives aligned, so every part of online infrastructure has reason to detect, prevent, and disrupt scams before victims are harmed.

Securing Digital Ecosystems in Modern Warfare

Exploring how to secure digital ecosystems as cyber operations become embedded in modern warfare, the session concluded that AI should not be considered a deterrent, even after extensive debate over whether new cyber capabilities could create such an effect. The emphasis fell instead on resilience, preparedness, and sustained operational capability.

- **Prepare for a new way of warfare.** Modern warfare is being reshaped rapidly by drones, data, AI, and cyber capabilities. A kinetic attack may be preceded by information warfare and accompanied by cyber operations, as observed in the armed conflict involving the United States, Israel, and Iran. Decision superiority in the form of more accurate and rapid decisions than an opponent, increasingly with AI support, is a central feature of modern conflict, alongside the indispensable use of cloud technology. As the group considered hypothetical scenarios in modern warfare, they concluded that cyber and information operations could amplify, synchronize, modify, and disseminate propaganda, with disinformation and generative AI influence operations a significant concern. Securing against cognitive warfare and avoiding rigid civilian-military or peacetime-wartime distinctions emerged as key recommendations. East Asia is where the strategic consequences of frontier AI are likely to be felt most acutely, as technology competition, cyber operations, semiconductor supply chains, and military modernization become increasingly interlinked, making the region a primary theater in which the rules of AI-enabled competition will be tested.
- **Sustain operational capabilities for long-duration cyber-physical conflict.** Once fighting begins, conflicts are difficult to stop quickly, making it essential to prepare for a longer campaign and ensure reliability across the entire supply chain. Targets now extend beyond military infrastructure to supply-chain attacks on private companies, which can disrupt critical sectors and undermine a nation's sustained operational capability, highlighting modern governments' obligation to protect society as a whole. Physical protection of the infrastructure that supports cyberspace (subsea cables and data centers) grows in importance, reflecting the erosion of clear distinctions between civilian and military targets.
- **Reduce diplomatic and legal ambiguity.** Rules of engagement in cyberspace remain unclear, and norms are often written by diplomats rather than engineers. Engineers may seek clear binary answers, while diplomatic language allows multiple interpretations. Cyberspace is increasingly an instrument of power used to synchronize and amplify effects in the physical world, support kinetic operations, and steal intellectual property. Yet, while there is a reasonable body of law for using cyber operations to destroy or steal, there is minimal jurisprudence governing operations to pre-position within critical infrastructure, as seen with the Volt Typhoon campaign. This activity is not considered

by many nations as a 'cut and dried' violation of existing norms, so governments must decide individually, and political commitments are non-binding.

Integrating AI into National Security Functions

Participants observed that AI is rapidly becoming a strategic capability across cyber defense, intelligence, and public sector decision-making. The question is no longer whether AI will be used, but how to devise, finance, regulate, and use it responsibly without creating unmanaged national security risk. Some attendees described current AI policy as closer to a manifesto without guidelines than a mature operational framework for safe AI use. The prevailing view was not that governments should shoulder all risk, but that they should demand safety from the companies that build these systems.

- **Keep final authority and accountability with humans.** AI can accelerate analysis, coding, and operational support, and improve the speed and quality of decisions, but it also surfaces new risks. Biases from skewed or contaminated training data, model selection, or the operating environment exist and must be considered by users. Human-in-the-loop governance is critical, especially where AI model outputs may influence targeting, vulnerability discovery, intelligence assessments, or law enforcement actions. AI systems should support human decisions, not replace responsibility for them.
- **Operationalize AI governance as a cybersecurity discipline.** AI governance cannot be separated from cybersecurity requirements. Model integrity, misuse prevention, and information assurance are now foundational security questions. Participants argued the next phase of policy must move past broad principles toward operational approaches for model testing, incident response support, and international coordination.
- **Options to constrain AI models with advanced cybersecurity capabilities.** The cyber defense landscape has shifted rapidly from finding a vulnerability to the gap between finding and remediating it. Compressing vulnerability patch cycles helps but cannot solve the root issues of insecure software by design or limited cybersecurity capacity at many organizations. Participants weighed three options for managing powerful vulnerability discovery capabilities: limit advanced AI model development (though the power to find a flaw is also the power to fix it, so constraining one constrains the other); build models but withhold them; or release models with designed safeguards. There is no singular ideal option and policymakers should always re-evaluate their approach in light of changing circumstances.
- **AI agent measurement and oversight.** Governments need rigorous measurement of what activities AI agents are asked to do, how they perform, where bias appears, and

how non-deterministic agent behavior occurs. Just as humans have flaws, agents can hallucinate or make errors in their action processes. Without comparable evaluation standards for agents across borders, AI risk will be hard to govern.

- **Rethink insider threat models for agents.** Decades of counterintelligence and security experience with human incentives, coercion, and betrayal have no equivalent for autonomous or semi-autonomous AI agents. As agents gain access to systems, data, credentials, and workflows, governments must ask what an insider threat looks like when the insider is not human.
- **Prepare for "Vulnageddon."** AI-assisted coding and vulnerability discovery will likely generate an unmanageable wave of updates across open-source and proprietary software in the coming months, faster than defenders can absorb and remediate. This challenge will strain national-level cyber resilience unless governments and industry invest heavily in secure-by-design development and prioritized remediation solutions.
- **Address both nation-state threats and criminal misuse.** State-sponsored cyber actors can already afford expensive exploits and will continue to use them, but AI advancements will likely drive down cyber exploit prices, benefiting cybercrime groups and commoditizing sophisticated computer network exploitation. Responses must therefore span both ends of the threat spectrum. To mitigate risk, governments should pursue four near-term priorities: 1) devise clear AI use cases and limits; 2) finance resilient cyber defense capabilities; 3) regulate AI for accountability, transparency, and human responsibility; and 4) use AI for defense.

Participant List

The Spring 2026 Aspen Digital Global Cybersecurity Group was an invite-only, closed-door convening of government officials, private sector executives, and civil society experts. Delegations included representatives from Japan, the United States, the United Kingdom, Australia, New Zealand, Canada, India, Singapore, Taiwan, Thailand, Brazil, Argentina, Chile, South Africa, France, Germany, Italy, Czechia, and Finland, together with representatives speaking to the perspectives of the European and African Unions.