

Event Overview

Date: Tuesday, September 29, 2026

Venue: Cisco Systems Tokyo Office

Organizer: Business Software Alliance

Supporting Organizations: AI Governance Association (AIGA), Japan Cybersecurity Innovation Committee (JCIC), Keidanren (Japan Business Federation), Japan Electronics and Information Technology Industries Association (JEITA), American Chamber of Commerce in Japan (ACCJ), Microsoft Japan, Cisco Systems G.K., Trend Micro Incorporated

While AI is changing the speed and scale of cyberattacks, it is also becoming a powerful tool for defenders by supporting vulnerability discovery and threat analysis. At the BSA Conference held on September 29, 2026, representatives from government and public institutions, domestic and international technology companies, critical infrastructure operators, and foreign embassies gathered to discuss the policies, initiatives, governance, and international cooperation needed to support cyber defense in the AI era. This report highlights the key points from the keynote speeches and roundtable discussion.

Opening Remarks



Aaron Cooper
(Senior Vice President, Global Policy, Business Software Alliance)

In their opening remarks, BSA and Cisco Systems expressed their appreciation to the policymakers, government officials, industry leaders, and supporting organizations participating in the conference. With the rapid advancement of AI making cybersecurity more important than ever, they emphasized the value of bringing together experts from government and industry to exchange perspectives on the future of policy, standards, and technology. They also expressed their hope that the discussions and insights from the conference would help translate dialogue into concrete actions to strengthen cybersecurity in the AI era.



Thimaya Subaiya
(Executive Vice President, Operations, Cisco Systems)

Part I ・National Cyber Defense in the AI Era: The Current State of Systems, Structures, and Technology

1）Keynote Speech: Masaaki Taira

Member of the House of Representatives; Chairperson, Headquarters for National Cybersecurity Strategy, Liberal Democratic Party



In his keynote speech, Diet Member Masaaki Taira described the work undertaken during his tenure as Minister of State for Cybersecurity to enact legislation strengthening Japan's cyber response capabilities and establish the National Cybersecurity Office (NCO), thereby building the institutional foundations for active cyber defense. He also highlighted coordination among the Financial Services Agency, the NCO, and the Japan AI Safety Institute (AISI), as well as Project YATA-Shield, an initiative designed to protect critical infrastructure and the technology foundations used by domestic businesses.

With AI advances rapidly transforming cyber threats, including the prospect of autonomous attacks by AI agents, he stressed the need to deepen cooperation not only across government agencies, but also with allies, like-minded countries, and private-sector technology companies. He further noted that the use of AI in cybersecurity requires an appropriate mix of high-performance AI and smaller open-weight models, safeguards for sensitive data, and solutions that extend beyond AI-versus-AI approaches, including confidential computing technologies. He emphasized the need to balance cost, security, and economic viability. Looking ahead, he identified AI misalignment, recursive self-improvement (RSI), and cognitive warfare as emerging challenges, and expressed his commitment to strengthening Japan's AI and cybersecurity policies through public-private and international cooperation while creating an environment in which companies can readily use trustworthy AI.

2）Keynote Speech: Aaron Cooper Senior Vice President, Global Policy, Business Software Alliance



In the second keynote address, BSA's Aaron Cooper observed that the rapid development of frontier AI and AI agents has made cybersecurity not only a technical issue, but also a critical matter of economic competitiveness and national security. He identified five priorities for the AI era. First, on public-private partnership, he emphasized the need to combine the distinct strengths of government and industry. Second, rather than rendering established cybersecurity principles obsolete, AI makes shared responsibility, risk-based approaches, and outcome-focused policies even more important. Third, AI has a dual role: it can make cyberattacks more sophisticated, but it can also strengthen threat detection and analysis and improve responses to vulnerabilities. Governments should therefore enable and encourage the use of AI for cyber defense.

Fourth, he discussed a security model for frontier AI. He introduced BSA's proposal, "Cybersecurity Professionals First," which calls to establish a voluntary public-private partnership to support a strategic, phased rollout of frontier AI models, under which trusted defenders would receive advance access before the model's market release, giving them time to identify and remediate critical vulnerabilities. Fifth, he underscored the importance of international cooperation in responding to borderless cyber threats. On digital sovereignty, he highlighted that policy should prioritize resilience, trust, and choice rather than restrict technologies based on the location of a company's headquarters, emphasizing that access to trusted technologies and interoperability are essential.



Cybersecurity Professionals First

3）Award Ceremony: Digital Diplomacy Champion

Honoree: Masaaki Taira, Member of the House of Representatives



BSA named His Excellency Masaaki Taira as one of eight government and policy leaders from around the world recognized as 2026 Digital Diplomacy Champions for advancing globally aligned digital policies and promoting international cooperation through engagement with government, industry, and civil society.

As Minister for Digital Transformation and Japan's first Minister of State for Cybersecurity, he worked to modernize government IT systems, strengthen Japan's cybersecurity framework, promote AI adoption, and advance the country's digital policy through international cooperation. The award recognized his leadership in digital policy and his contributions to global cooperation. Accepting the award, His Excellency Taira noted that many challenges remain, including those related to digital policy, AI, cybersecurity, and cognitive warfare. He said the recognition would encourage him to work even more vigorously to address these issues.







Part II・Roundtable Discussion　Public-Private Partnerships and AI-Enabled Cyber Defense



The roundtable brought together representatives from the National Cybersecurity Office, the Japan AI Safety Institute, domestic and international technology companies, and critical infrastructure operators to discuss how AI is changing cyber threats and cyber defense. Moderator Hiroaki Sakuma noted that as increasingly capable AI transforms both attack and defense, two dimensions have become equally important: “AI for Security,” which uses AI to protect systems, and “Security for AI,” which protects AI itself from attack.

He invited the panelists to discuss public- and private-sector initiatives and challenges, with particular attention to how advanced AI could be harnessed for cyber defense.

Moderator: Hiroaki Sakuma (Executive Director and Secretary General, AI Governance Association)



Yoichi Iida
(National Cyber Director and Deputy National Security Advisor)

Strengthening Cyber Defense and Public-Private Partnerships in the AI Era

Yoichi Iida explained that, in preparation for the implementation of Active Cyber Defense legislation, the government had been developing a new framework focused on enhancing public-private partnerships, using communications information and implementing remote access and neutralization measures. At the same time, he noted that the cyber landscape is changing rapidly due to advances in AI and shifts in the geopolitical environment. While AI is significantly increasing the speed and scale of cyberattacks, the fundamentals of cyber defense remain unchanged. He emphasized the importance of integrading measures such as multifactor authentication, zero trust architecture, timely patch deployment, and business continuity planning into everyday cybersecurity practices. He also emphasized the importance of defenders proactively leveraging AI. Early access to advanced technologies, including frontier AI models, is critical to securing the time needed to prepare for emerging threats.

Equally important, he argued, is ensuring that government agencies, critical infrastructure operators, and key industries have reliable and sustained access to these technologies. In his view, both “early access” and “sustained access” are indispensable to strengthening Japan’s cyber defense capabilities. He further explained that, by leveraging Project YATA-Shield and “Public-Private Cyber Community (PC2),” the government aims to share information more proactively and foster “collective intelligence” through collaboration with the private sector, allies, and like-minded partners, and translate that intelligence into “collective action.”

Strengthening Third-Party Evaluation of AI Models and International Cooperation



Suguru Nishimura explained that AISI is a public institution that analyzes a broad range of AI safety risks and provides direction and guidance for the safe deployment of AI in society. In the field of AI security, AISI is providing technical support for Project YATA-Shield while also building the capacity and environment needed to evaluate AI models independently from their developers.

This work includes security-focused evaluations of a range of overseas and open-weight models. He noted that no single company can address AI risks alone. AISI therefore has an important role in aggregating and analyzing knowledge from businesses and government agencies and returning the results to society in the form of guidance and practical approaches. He also highlighted cooperation with AISI counterparts in the United Kingdom and other countries as a means of supporting the safe adoption of AI.

Suguru Nishimura
(Deputy Executive Director and Secretary General, Japan AI Safety Institute)



Thimaya Subaiya
(Executive Vice President, Operations, Cisco Systems)

The Twin Priorities of "AI for Security" and "Security for AI"

Thimaya Subaiya identified the sheer speed of innovation as one of the most significant changes brought about by AI. The unprecedented compression of time – both in how fast technology evolves and how quickly AI executes complex tasks – creates significant operational opportunities, but also demands a new level of governance to manage emerging risks. He emphasized the importance of keeping humans firmly in control with AI, for example, by having people formulate hypotheses and validate conclusions while AI accelerates research and analysis. In cybersecurity, he stressed the need to pursue both "AI for Security," using AI for defense, and "Security for AI," protecting AI systems themselves. On the latter, he explained that protecting the data underpinning AI and establishing effective governance are essential. In particular, he stressed that governance is at the core as it cannot be differentiated across models and encouraged that governments and organizations such as BSA should work together to develop common standards, governance approaches, and data security frameworks.

Three Priorities for AI-Enabled Cyber Defense

Marcus Bartley Johns identified three priorities for strengthening AI-enabled cyber defense: data and intelligence; the use of AI tools best suited to the task; and partnerships. First, governments and companies should share the threat information available to them to build a more comprehensive picture of the threat landscape, enabling faster AI-supported detection and response. Second, organizations can build more resilient defenses by avoiding reliance on a single model and combining multiple models and AI agents according to the intended purpose. As an example, he described Microsoft's MDASH project, which combines many different AI models with hundreds of AI agents to dramatically accelerate vulnerability discovery. Third, he emphasized cooperation between global technology providers and Japanese companies. Citing collaboration between Microsoft and NTT, he highlighted the importance of bringing together leading global technologies and expertise to strengthen Japan's cybersecurity ecosystem as a whole.



Marcus Bartley Johns
(Senior Director, Head of North Asia, Microsoft Global Affairs)



Masashi Namatame
(Senior Managing Executive Officer, Group Chief Digital Officer and Group Chief AI Officer, Meiji Yasuda Life Insurance Company; Representative Director, AI Governance Association)

Accountability for AI Risk and the Formation of Collective Intelligence

Speaking from his perspective as a Senior Managing Executive Officer at Meiji Yasuda Life Insurance Company and Representative Director of the AI Governance Association, Masashi Namatame said corporate leaders have a responsibility to protect their companies and stakeholders from AI-related risks and to establish accountability for the use of AI. He identified three essential elements: promptness in responding, extensiveness in taking broad-based measures, and proactiveness in anticipating future developments. He added that maximizing AI's benefits requires stronger security and public acceptance.

Because the insights available to any single company are necessarily limited, he explained that the AI Governance Association is working to bring together insights from its 180 member companies and stressed the importance of building on this expertise and collaboration with AISI and the NCO to develop "collective intelligence" both in Japan and internationally.

Strengthening Critical Infrastructure Resilience Through Cross-Industry Cooperation

Tetsuhito Gima, who is responsible for strengthening cybersecurity and incident response at his company, explained that, as a critical infrastructure operator, NTT DOCOMO is preparing to comply with Japan's new framework for strengthening cyber response capabilities while also reinforcing its readiness for emerging threats, including those associated with frontier AI. While AI is changing the threat landscape, he stressed that the fundamentals of cyber defense remain unchanged. Against this backdrop, the company is reassessing established cybersecurity practices, including how patches are prioritized and deployed, to further strengthen the resilience of its infrastructure. At the same time, he noted that the increasing speed of AI-enabled attacks is raising new issues that need to be addressed, including how telecommunications providers should approach decisions to proactively suspend services when faced with critical vulnerabilities. He emphasized that such issues should be treated as areas for cooperation rather than competition, calling for closer coordination among industry players through forums such as ICT-ISAC, as well as the development of appropriate rules in collaboration with the government.



Tetsuhito Gima
(General Manager of CISO Office, Security Innovation Management Department, NTT DOCOMO, INC.)

Comments from Embassy Representatives



Sam Hall
First Secretary, Political Section, British Embassy Tokyo



Michelle Warren
Science and Technology Officer, Economic and Scientific Affairs, U.S. Embassy Tokyo



Eloisa Gye
Second Secretary, Political Section, Australian Embassy Tokyo

Representatives from the British, U.S., and Australian embassies, who participated as observers, shared the view that, even as rapid advances in AI create greater uncertainty in the cyber threat landscape, it remains essential to reinforce fundamental cybersecurity practices while further strengthening public-private and international cooperation. They emphasized that increasingly sophisticated AI-enabled cyber threats are inherently cross-border challenges that no single country or organization can address alone. In addition to government-to-government cooperation, they highlighted the importance of bringing together the expertise and strengths of trusted partners through public-private information and threat sharing, collaboration among institutions focused on AI safety and security, and the development of international standards. The embassy representatives also expressed support for Japan's efforts to strengthen its cyber response capabilities and underscored the importance of building on existing cooperation among Japan, the United Kingdom, the United States, and Australia to further deepen collaboration on AI and cybersecurity with like-minded countries and regional partners.

Strong Cybersecurity and AI Choice as Foundations for Digital Competitiveness: Roundtable Summary

In closing the roundtable, BSA's Aaron Cooper emphasized that digital transformation is essential to economic competitiveness and that strong cybersecurity is its foundation. To strengthen cybersecurity in the AI era, organizations need access to the most capable AI models while also retaining the ability to choose among a diverse range of models according to their needs rather than depending on any one model. Maintaining this choice, he concluded, contributes to stronger security across the ecosystem.








BSA Conference Participants

MC

• Tomoko Naoe, Country Manager and Director, Policy – Japan, Business Software Alliance

Keynote Speakers

• Masaaki Taira, Member of the House of Representatives; Chairperson, Headquarters for National Cybersecurity Strategy, Liberal Democratic Party

• Aaron Cooper, Senior Vice President, Global Policy, Business Software Alliance

Roundtable Moderator

• Hiroaki Sakuma, Executive Director and Secretary General, AI Governance Association

Roundtable Participants

• Yoichi Iida, National Cyber Director and Deputy National Security Advisor

• Suguru Nishimura, Deputy Executive Director and Secretary General, Japan AI Safety Institute

• Thimaya Subaiya, Executive Vice President, Operations, Cisco Systems

• Marcus Bartley Johns, Senior Director, Head of North Asia, Microsoft Global Affairs

• Masashi Namatame, Senior Managing Executive Officer, Group Chief Digital Officer and Group Chief AI Officer, Meiji Yasuda Life Insurance Company; Representative Director, AI Governance Association

• Tetsuhito Gima, General Manager of CISO Office, Security Innovation Management Department, NTT DOCOMO, INC.

• Aaron Cooper, Senior Vice President, Global Policy, Business Software Alliance

Roundtable Guests

• Sam Hall, First Secretary, Political Section, British Embassy Tokyo

• Michelle Warren, Science & Technology Officer, Economic and Scientific Affairs, U.S. Embassy Tokyo

• Eloisa Gye, Second Secretary, Political Section, Australian Embassy Tokyo