May 2026

Technology Standards as Foreign Policy

Japan, the United States, and Europe must coordinate to compete with China.

Editor

Dr. Sayuri Romei

Authors

Lindsay Gorman
Gautam Kamath
Shotaro Nagino
Alexandra Pugh

G | M | F

G | M | F

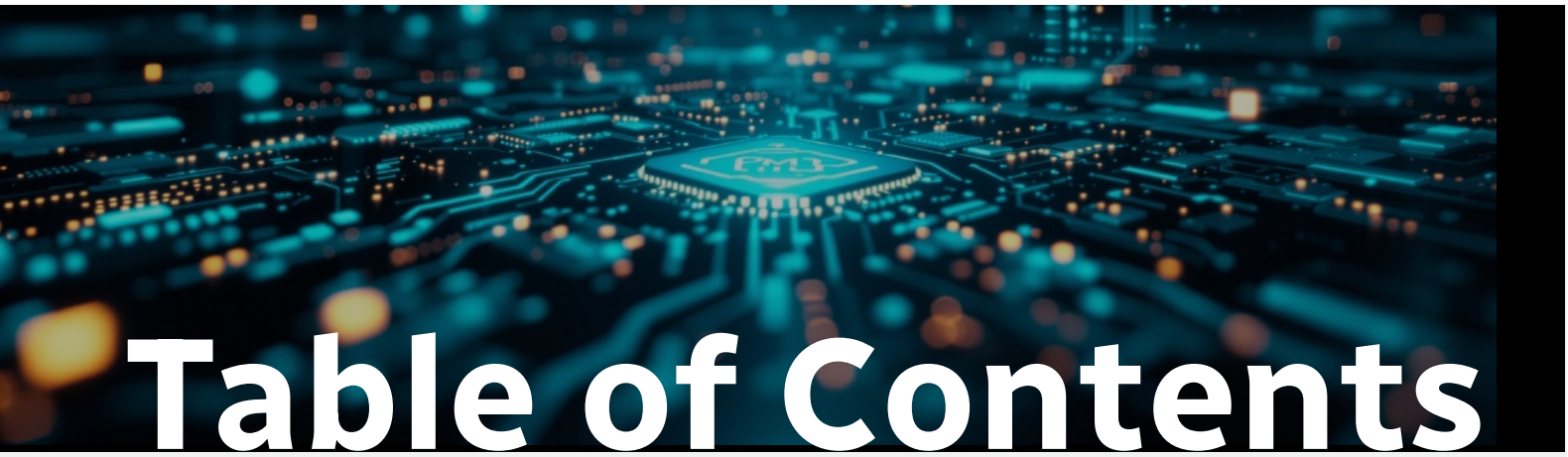


Table of Contents

Setting International Standards for Emerging Technologies

Introduction by Dr. Sayuri Romei

The rapid evolution of emerging technologies, ranging from artificial intelligence (AI) and next-generation telecommunications to quantum computing, is reshaping not only global markets but also the foundations of geopolitical power. At the center of this transformation lies a less visible, yet decisive driver: international standards-setting. Technical standards, often perceived as neutral or purely technical, are in fact powerful instruments that determine market access, shape innovation pathways, and embed societal values into the infrastructure of the digital world. Reflecting the growing importance of this issue, GMF's Indo-Pacific program has compiled an edited volume to examine how like-minded partners can better coordinate in this space. As China expands its influence across international standards bodies, leveraging state-backed industrial policy and coordinated participation, the urgency of the need for these partners to respond collectively has become increasingly clear.

This volume brings together perspectives on how the United States, Japan, and Europe can enhance coordination in setting international standards for emerging technologies. Together, these partners possess unparalleled strengths in innovation, market size, and institutional capacity. Yet differences in regulatory philosophy, industrial organization, and approaches to public-private collaboration have at times limited their collective effectiveness. Addressing these gaps is essential not only to maintain competitiveness, but also to ensure that the global technological ecosystem reflects shared commitments to openness, transparency, and democratic governance.

The contributions in this volume highlight both the risks of fragmentation and the opportunities for alignment. The first contribution, by **Shotaro Nagino**, underscores that international standardization has become a frontline issue in economic security, particularly as China's growing role in standard-setting organizations enables it to shape standards in ways that advantage its firms and its governance model. Nagino argues that the United States, Japan, and Europe must work together to secure supply chains, coordinate on technical standards, and, when necessary, develop mechanisms to reject or counter standards that undermine their economic and security interests.

The second analysis, by **Gautam Kamath**, examines the broader geopolitical competition over standards in emerging technologies, emphasizing that technical standards function as the "invisible glue" of the global digital economy. The author highlights contrasting approaches across regions (China's coordinated state-industry model, Europe's regulatory leadership, and the more market-driven systems of the United States and Japan) and calls for deeper trilateral cooperation to align incentives, strengthen institutional coordination, and prevent technological fragmentation.

The final contribution to the volume, by **Lindsay Gorman and Alexandra Pugh**, illustrates how standard-setting, innovation, and economic security are increasingly intertwined across emerging technologies, particularly in the critical domain of quantum systems. It shows that while the United States, Japan, and Europe are each investing heavily in quantum research and commercialization, their ability to maintain leadership will depend on closer collaboration in areas such as defense innovation, supply chain resilience, and the development of shared standards. At the same time, the authors highlight the tension between growing ambitions for technological self-reliance and the clear benefits of partnership, suggesting that carefully targeted cooperation can reconcile these dynamics.

Taken together, these analyses point to a common conclusion: Standard-setting is no longer a technical afterthought, but a central pillar of strategic competition and cooperation. To succeed, the United States, Japan, and Europe must move beyond ad hoc coordination toward a more deliberate and sustained approach. This includes engaging the private sector more effectively, aligning regulatory and industrial policies, investing in the next generation of standards experts, and building coalitions with partners beyond the transatlantic and Indo-Pacific spaces. In doing so, they can help ensure that the rules governing emerging technologies support innovation, strengthen economic security, and reflect the values that underpin open and democratic societies.

Sayuri Romei *is the senior fellow for Japan at GMF's Indo-Pacific program. She leads work on Japan and heads the Japan Trilateral Forum and the Young Strategists Forum. Her research focuses on US-Japan-Europe relations and security issues in the Indo-Pacific.*

Economic Security and the Future of International Standards

Japan, the United States, and Europe must cooperate.

By Shotaro Nagino

Economic Security Risks in International Standardization

In discussions of collaboration in international standardization among like-minded countries such as Japan, the United States, and European states, the economic security dimension is critical. The Japanese government, for example, refers to economic security more than ten times in the New International Standards Strategy[1] announced in 2025. International frameworks—for instance, the G7 Leaders' Statement on Economic Resilience and Economic Security[2] issued at the 2023 Hiroshima Summit, where the G7 for the first time agreed on a definition of economic security—highlight cooperation on international standardization as a response to harmful practices that undermine international rules and norms. At that summit, the seven governments declared that they would cooperate on standardization grounded in democratic values. Thus, a consensus has emerged among these countries that international standardization is an unavoidable domain for ensuring economic security.

The primary driver of this policy direction is China's rise on the stage of international standardization. According to an analysis[3] by the US Studies Centre at the University of Sydney, over the decade from 2013 to 2023, China increased the number of secretariat positions it holds in the International Organization for Standardization (ISO) by 233, while the United States lost 139 and the United Kingdom 86. In terms of participation in ISO committees as well, China overtook the United Kingdom and Germany in 2021 and, by 2024, held the largest number of memberships at 763. As these numbers show, China is implementing state-led efforts, under the banner of its "China Standards 2035" campaign to raise its profile in international standardization bodies. A Heritage Foundation report[4] analyzing China's growing influence in the telecommunications sector argues that cumulative government support has translated into growing influence. For instance, the Chinese government reportedly covers the roughly $300,000 participation fee for Chinese technical experts in the Third Generation Partnership Project (3GPP), a standard-development project for specifications aligned with International Telecommunication Union (ITU) guidelines in the field of international mobile communications. In other countries, private-sector engineers must pay their own way.

A prominent case in which China expanded its market share by wielding international standardization as a weapon—thereby eroding the economic security of other countries—is the adoption within 3GPP standards of Polar Code, an error-correcting coding scheme in which Huawei had made large-scale investments.[5] In 2016, 3GPP adopted Polar Code as part of the global standard for wireless connectivity in 5G networks. As a result, Huawei—which holds close to two-thirds of all patents related to Polar Code—was able to supply telecommunications equipment compliant with international standards at low prices to markets including those of Japan, the United States,

and Europe, while forcing firms such as Qualcomm and Ericsson to pay licensing fees and gradually chipping away at the competitiveness of like-minded countries' firms in the 5G sector. Consequently, particularly during the first Trump administration, as Huawei, ZTE, and other Chinese firms came under suspicion of enabling surveillance via their infrastructure and began to be perceived as national security threats, the United States and European countries embarked on replacing Chinese-made equipment. This effort imposed enormous costs on both governments and the private sector. In addition, the decline in competitiveness among firms from like-minded countries led, for example, to NEC in Japan announcing its withdrawal[6] from the 4G/5G equipment business, which ultimately undermined economic-security-driven autonomy in the telecommunications domain among like-minded countries.

Areas for Collaboration in International Standardization

In a situation in which so-called countries of concern are expanding their influence in international standardization organizations with explicit backing from their governments, what forms of collaboration are required among like-minded countries? Broadly speaking, three main subjects are on the agenda for standardization: definitions of terms; technologies and products such as communication protocols and physical form factors; and evaluation methods and performance thresholds. Of these, defining terms is important as a foundation for advancing standardization in the other two domains, but once an international common vocabulary has been agreed through deliberation, it is not a particularly high-risk area. By contrast, collaboration on the standardization of technologies and products and on the standardization of evaluation methods is of critical importance.

In the realm of technology and product standardization, there are several areas where like-minded countries can work together to secure autonomy (meaning, strengthen the resilience of one country's supply chain and critical infrastructure to counter economic coercion from foreign adversaries) and indispensability (supplying indispensable critical goods or technologies to other jurisdictions to create choke points that could deter economic coercion from that jurisdiction) from the standpoint of economic security. One is to coordinate in responding to attempts by countries of concern to internationalize standards that are already widely adopted domestically or that enjoy a technological edge globally to prevent such countries from locking in technological hegemony. In addition, if like-minded countries are to establish technological superiority at an early stage, they can promote the standardization of components and modules that they themselves can manufacture. This can help secure supply chains for interchangeable components that conform to the same specifications, and by dividing development work according to comparative strengths under a common standard, like-minded countries as a bloc can seek to achieve global technological leadership. For example, within the Quantum Development Group, where Japan, the United States, Europe, and other countries collaborate in the quantum domain, governments are analyzing quantum-related supply chains in each country, reflecting efforts to strengthen those supply chains not on a purely national basis but at the level of like-minded countries as a group. Moreover, if these countries can dominate global technology in a specific area, they can turn strategies such as countering economic coercion—using chokepoints in the supply chains of countries of concern—into sources of strength.

With respect to the standardization of technology evaluation methods, first and foremost, when a standard requires disclosure of the inner workings of a technology as a precondition for evaluation, the

evaluation process itself creates a risk of information leakage. Like-minded countries should therefore resist such standards. For instance, when measuring a computer's processing performance, it is preferable to use evaluation criteria defined in terms of the ability to carry out specified calculations at specified speeds or with specified accuracy, without prescribing or revealing the underlying technical methods. Furthermore, as countries that share democratic values, they should also work to embed those values into performance evaluation. In the case of surveillance technologies, for example, event-trigger-based privacy-enhancing techniques should be standardized, and assessment should focus on whether privacy-preserving functionality grounded in democratic values has been implemented. Trigger-based privacy technology has already been incorporated into management standards such as ISO 27701,[7] but going forward, like-minded countries should push for such techniques to be standardized at the product-specification level as well. For emerging technologies such as AI, similar forms of cooperation aimed at codifying these countries' values into standards will be indispensable.

An "Economic Security Exception" in the Adoption of International Standards

Ideally, international standards would consistently be shaped in ways favorable to like-minded countries. Yet, as the statistics above indicate, China's influence in international standardization fora is expanding rapidly. Under such circumstances, it is necessary to engage not only like-minded countries, but also the "Global South" and countries such as India that place a premium on neutrality. However, China's influence over these countries is also growing, driven by initiatives such as the Belt and Road and the Digital Silk Road, and there is a real possibility that international standards unfavorable to like-minded countries will be adopted.

To prepare for such contingencies, countries must be ready, as a matter of strategy, to refuse the adoption of certain international standards and to reject standards that would undermine their economic security. Conceptually, this resembles the security exceptions under the WTO Agreements, but unlike in the WTO framework—where each country makes independent determinations—what is needed is coordination among like-minded countries to protect their markets and to block, as far as possible, efforts by countries of concern to enhance their competitiveness through standardization. In practice, again taking telecommunications as an example, the policies of like-minded countries to exclude Huawei from 5G network equipment has had the effect of rejecting the standard that incorporated Polar Code. However, by the time the United States moved to restrict federal procurement from Huawei under the 2019 National Defense Authorization Act, Huawei products had already made deep inroads into markets in like-minded countries. Even after the US decision, it took considerable time before the governments of Japan and European states followed suit and imposed similar bans. In emerging technology domains that will see rapid development in the coming years, it will be essential not to wait until after standards are adopted to devise countermeasures. Rather, it will be necessary to develop, in parallel with the international standardization process, contingent scenarios for refusing standards in cases where like-minded countries fail to secure standards that preserve their competitive edge. In doing so, even if de jure international standardization efforts fall short, like-minded countries should seek to leverage the combined markets of Japan, the US, and Europe—which together are three times the size of China's GDP—to establish de facto standards at an early stage.

An Economic Security-Oriented Management Standard Concept

In parallel with the strategies for international standardization of emerging technologies discussed above, it will also be important to consider standardizing management practices that promote the diffusion of economic security-oriented management as a means of ensuring the economic security of like-minded countries. It is easy to imagine objections that, unlike the Information Security Management System (ISMS) based on ISO/IEC 27001, it is impossible to pursue international standardization in the realm of economic security, which is inherently subject to political discretion. However, among the measures required to safeguard economic security, there are indeed items that can be adopted without taking a specific political stance. For instance, in the context of supply chain dependence, it would likely be impossible to reach international agreement on a standard that explicitly demands "no dependence on China". By contrast, a requirement such as "no dependence of 30% or more on any single country" could be adopted as a neutral management control that does not single out any specific state. While the practical effect would be to counter China's "dual circulation" strategy, as a standard it would be framed as generally desirable guidance for securing economic security, applicable to any country.

Recommendations for Japan-US-Europe Collaboration in International Standardization of Emerging Technologies

- Like-minded countries should cooperate in international standard-setting fora to prevent countries of concern from imposing standards that favor themselves and should negotiate with the aim of embedding their values into those standards.

- If international standardization efforts favorable to like-minded countries may at times fail, these countries should, along with such efforts, consider an "economic security exception" and coordinate in leveraging their markets to establish de facto standards.

- In tandem with strategies for international standardization of emerging technologies, like-minded countries should cooperate in pursuing international standards for economic-security-oriented management practices that, in effect, reduce the influence of countries of concern.

Shotaro Nagino *is an adjunct fellow at Pacific Forum. He also leads economic security consulting at EY Strategy and Consulting Co., Ltd. He has extensive experience in policy research, risk and opportunity assessments, business strategy formulation, internal system design, and internal system reform in various areas of economic security. He also leverages his network with government agencies, think tanks, and academia to support numerous companies and government institutions as a consultant connecting international relations and business.*

Endnotes

[1] *Prime Minister's Office of Japan, "A New International Standardization Strategy," [新たな国際標準戦略], 2025: https://www.cas.go.jp/jp/seisakukaigi/titeki2/tyousakai/kousou/2025/dai5/siryou2-2.pdf*

[2] *「G7 Leaders' Statement on Economic Resilience and Economic Security, Ministry of Foreign Affairs of Japan, May 20, 2023. https://www.mofa.go.jp/mofaj/files/100506768.pdf*

[3] *United States Studies Centre, University of Sydney, "Standards Development Organisations in an Era of Strategic Competition". https://www.ussc.edu.au/standards-development-organisations-in-an-era-of-strategic-competition*

[4] *Dean Cheng and Matthew Turpin, "Countering China's Growing Influence at the International Telecommunication Union", Heritage Foundation, March 7, 2022. https://www.heritage.org/global-politics/report/countering-chinas-growing-influence-the-international-telecommunication#_ftnref30*

[5] *Matt Burgess, "Huawei, 5G, and the Man Who Conquered Noise", Wired, November 16, 2020. https://www.wired.com/story/huawei-5g-polar-codes-data-breakthrough/*

[6] *Nikkei Asia, "NEC Halts Development of 4G and 5G Base Station Equipment, Setting Back Domestic Production Efforts; Defense-Related Development to Continue" [NECが4G・5G基地局の機器開発中止、国産化後退　防衛用は継続], December 27, 2025: https://www.nikkei.com/article/DGXZQOUC193NF0Z11C25A2000000/*

[7] *ISO/IEC 27701:2019, "Security techniques—Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management—Requirements and recommendations," International Organization for Standardization. https://www.iso.org/standard/27701*

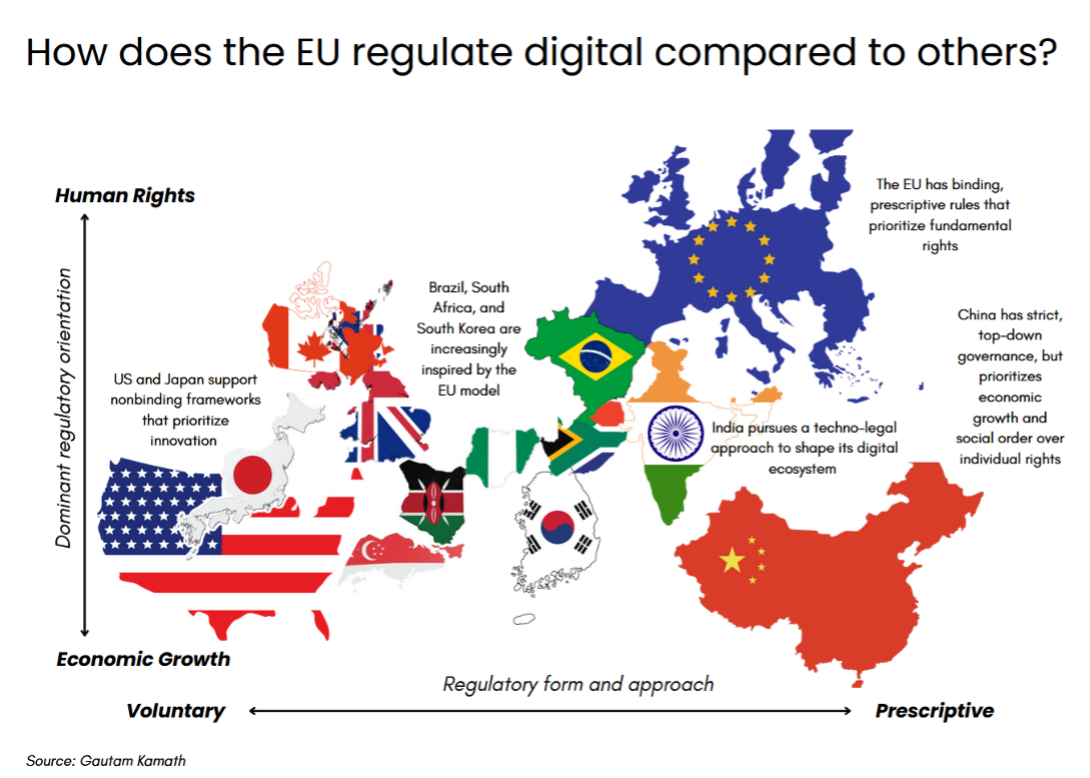
Shaping Emerging Disruptive Technology Standards

A view from Brussels.

By Gautam Kamath

Regulations and standards on governing digital technologies differ among major geographic regions. My recent article, "Beyond the Brussels Effect", argues that approaches vary based on economic and regulatory priorities. As Figure 1 shows, Japan and the United States take a more industry-led, innovation-focused stance while Brazil, the EU, and India emphasize human rights and are more legally prescriptive.

Figure 1



China sits alone in the graphic. Its push to engage with and shape international standards on emerging technologies such as artificial intelligence (AI), 5G/6G, and quantum computing at standards organizations (SDOs) is well known.[1] The Standardization Administration of China (SAC) acknowledges the effort, as does the Chinese government, which in October 2021 published the "Outline for the Development of National Standardization". It explicitly includes an objective to harmonize at least 85% of local and international standards. The EU has acknowledged China's role as an emerging hub for standards development and has consequently run the Seconded European Standardization Expert in China (SESEC) for over 20 years. The project helps increase Chinese participation in the development of international and European standards through policy alignment, reciprocity in access, and technical cooperation, among other areas.

China's approach to standardization development is increasingly driven by the private sector, with strong coordination among local, regional, and sectoral standards coordination bodies. The SAC under the State Administration for Market Regulation manages China's de jure national standardization. Mirroring the structure of the International Organization for Standardization, the SAC operates through a network of specialized technical committees.

China's AI standardization is largely centralized within the China Electronics Standardization Institute (CESI). Specifically, the Technical Committees for Information Technology (TC28) and Cybersecurity (TC260), which drafted key mandates such as the machine learning data labeling code and generative AI security requirements, operate under CESI's leadership. Because it manages these secretariats and publishes the final standards, CESI serves as the primary engine for China's AI regulatory output. However, while a "top-down approach" to standardization is commonly assumed, the development of AI standards is in practice led by more than 20 companies and research institutions including Huawei, JD, Alibaba, Baidu, China Mobile, and DJI. They are known collectively as the "AI team".[2] The consortium works together on multiple levels—on technical committees (TCs) and as SAC representatives at international SDOs. Beijing incentivizes participation in standard-setting bodies by rewarding companies with subsidies and tax breaks based on their number of representatives and technical submissions.[3]

The EU trails the United States and China in AI data, adoption, and talent, but the bloc has secured a strategic advantage by spearheading global governance. Through its General Data Protection Regulation and the AI Act, Europe has long adopted a "regulation-first" strategy, using its position as a preferred venue for technical standards development as a primary tool to drive international competitiveness (see "Beyond the Brussels Effect").

Many observers, however, question whether the Brussels effect still holds. Lacking a "national team" of homegrown AI giants to dictate market norms, the EU must cultivate its own "community of practice" and remain an open and inviting venue for the private sector, including for players from China, Japan, and the United States. This collaborative approach is essential to drive and harmonize AI standardization across the EU.

Coordination is also important due to Europe's complex standards development process. In addition to formal SDOs—such as the International Telecommunications Union, the European Committee for Standardization (CEN), and the European Committee for Electrotechnical Standardization (CENELEC)—producing de jure standards mandated by law, the EU hosts quasi-formal SDOs that are led by private-sector consortia to develop technical standards similar to formal standards, including for the Institute of Electrical and Electronics Engineers (IEEE), the World Wide Web

Consortium (W3C), and the 3rd Generation Partnership Project 3GPP. CEN-CENELEC also hosts national SDOs from more than 30 member countries including the 27 EU member states, Switzerland, Türkiye, and the United Kingdom. Finally, in addition to the emergence of de facto standards, EU regulations can mandate specific standards and request the development of new standards to ensure legal compliance.

With an open, private sector-driven standards development ecosystem, the EU has long been regarded as a preferred venue for nation states and private actors to align emerging and disruptive technologies. Recent geopolitical volatility has meant this position has grown in importance, with the EU and organizations such as NATO introducing initiatives to foster innovation in emerging and disruptive technologies (EDTs). Notably, these efforts overlap significantly in their technological focus, despite disparate policy goals (e.g., defense and competitiveness). Regarding defense, NATO prioritizes nine key areas—including AI, big data, quantum, and biotechnology—while the European Defence Agency (EDA) targets a similar list of six critical fields, ranging from robotics and hypersonics to advanced materials and space technologies. Disruptive technologies can "disrupt" different domains, including "the economic system; the military and defense; democratic debates and the 'infosphere'; social norms, values and identities; international relations; and the legal and regulatory system".[4]

Coordination on EDTs Is Key

Technical standards are the "invisible glue" of the modern world, and EDTs such as AI and quantum are the difference between global progress and fragmented chaos. Standardization serves as the primary framework for global technological and economic systems, granting "first-mover" advantages and dictating market access to proactive ecosystems. Standards ensure interoperability. Without these "common rules", the digital world would split into incompatible technological islands. By establishing the groundwork for interoperability, safety, and quality, standards prevent the industry fragmentation and trade barriers that stifle innovation. Conversely, a lack of standards leads to higher consumer costs and vendor lock-in. As global competition intensifies, the ability to set benchmarks has evolved into a critical geopolitical lever, for which diverse technological approaches vie for dominance in the international arena.

For AI, standards establish ethical and safety benchmarks—such as data privacy and bias mitigation—that build the public trust necessary for mass adoption. With the EU AI Act requiring the development of all types of technical standards in the CEN/CLC/JTC 22 technical committee, the process behind this effort is being scrutinized for its slowness. Article 9 of the EU AI Act for example, requires "high risk AI providers" to establish a continuous, documented, and iterative risk management system to mitigate risks to health, safety, and fundamental rights. This was one of the first standards to be tackled yet work on it is still ongoing.[5]

While "legally requested" standards take a long time and follow a complex process,[6] AI risk management standards already exist, namely within the National Institute of Standards and Technology (NIST) AI Risk Management Framework (AI RMF) or with related AI risk-management standards (RMS) such as ISO/IEC 23894. The Organization for Economic Co-operation and Development, in collaboration with the University of California, Berkeley, has also published an RMS catalog to serve as a companion to the NIST AI RMF. The catalog is meant for developers of frontier models (general purpose AI providers or the Global Partnership on Artificial Intelligence (GPAI)) and builds on existing international commitments such as the G7 Hiroshima

code of practice. EU, Japanese, and US firms should adopt and champion these standards and commitments from GPAI providers. Japanese companies, for their part, are closely monitoring and requesting clarification of the deployment of fine-tuned models, but none has formally signed an EU code of practice. Interestingly, Chinese companies are also absent from the list of signatories.

In quantum, there is a standards race to define post-quantum cryptography, quantum communication, and global security before the first "cryptographically relevant" quantum computers come on the market. While Europe boasts strong research and development (R&D) but is weak on deployment, the United States is focused on developing and scaling quantum computing (reflecting private-sector interests), and the Chinese are building applications and investing strategically in hardware, platforms, and communications networks.

China has adopted a proactive enterprise-led strategy to dominate SDOs such as the International Organization for Standardization, the International Electrotechnical Commission (IEC), and the ITU, and European institutions including CEN-CENELEC. By embedding its proprietary quantum key distribution (QKD) protocols into international frameworks, Beijing aims to create a "first-mover" lock-in. This is particularly evident in their Digital Silk Road initiative,[7] for which China exports quantum-secure infrastructure to partner nations, effectively making Chinese standards the default for a significant portion of the "Global South".

This proactive strategy is also found in their efforts at European standardization organizations (ESOs). QKD is important as this shifts quantum security from "mathematical" to "physical", providing "theoretically safe" real-time notice of any attempted interception. QKD requires specialized hardware (satellites, repeaters, and routers), and vendor lock-in and standards dominance eventually enables any state or non-state actor to dominate the global market and create strategic dependence, and, potentially, security risks (e.g., backdoors).8 Huawei was a top contributor to the Focus Group for Quantum Technologies (FGQT, the predecessor of CEN/CLC/JTC 22) between 2020 and 2023, specifically on QKD proposals,[9] and the company is an active member of the QKD Industry Specification Group (ISG) of the European Telecommunications Standards Institute (ETSI).

To counter foreign interests shaping standards, the EU has adopted a defensive posture with its 2022 Strategy on Standardisation and with a proposal to amend the standardization regulation by changing ESO governance (e.g., allowing only them to take leadership roles in technical committees on EDTs) when devising "legally requested" standards. The EU also announced a quantum strategy that is based on five pillars: research and innovation, quantum infrastructures, ecosystem strengthening, space and dual-use technologies, and quantum skills. The strategy is expected to be codified through the Quantum Act, which is due later this year. The legislation should include a focus on standardization and investment in post-quantum cryptography (PQC).

Policy Recommendations

Standard-setting is no longer a purely technical exercise. It is the new frontier of geopolitical statecraft. Technical standards function as a multifaceted lever, exerting influence across the five pillars. In the ideational realm, they shape global reputations and perceptions of technological leadership, effectively embedding specific values into the global infrastructure. Legally, standards serve as critical benchmarks for nontariff trade barriers, affecting over 80% of global trade and providing the regulatory certainty required for cross-jurisdictional compliance. The political

dimension highlights how standards create long-term dependencies and "lock-in" effects, both with serious geopolitical consequences. Economically, standards harmonize regulations to reduce technical barriers and foster innovation through expert collaboration. They are also inextricably linked to standard essential patents (SEPs), which grant actors the power to control technological evolution. Collectively setting standards is not merely a technical exercise but a primary method of projecting allied power over global markets and reinforcing shared societal values. Therefore, to prevent fragmentation of technological ecosystems, the EU, Japan, and the United States must move beyond high-level dialogue and implement specific financial and institutional mechanisms, including:

Setting the right incentives for trilateral collaboration on EDTs. These include:

- standard-participation tax credits (SPTC) and grants. National governments should harmonize domestic tax codes to allow smaller firms a 150% deduction for expenses related to international standard-setting activities (travel, engineering hours, and ISO/IEC/IEEE membership fees). They should also establish a joint fund to subsidize the "seat at the table" for startups, small- and medium-sized enterprises, and think tanks, ensuring that incumbents do not dictate EDT standards.

- reciprocal incentive recognition to ensure that an R&D tax credit claimed in one jurisdiction (e.g., in the United States under its CHIPS Act) is recognized for collaborative trilateral projects. This would avoiding double taxation on joint EDT ventures.

- funding for public interest technologies to ensure EDT standards are human-centric and ethically grounded. Civil society must be financially empowered to provide technical inputs and oversight here. Support could include a pooled fund managed by the United States, Japan, and the EU to provide multi-year grants to NGOs, academic labs, and consumer rights groups. A "Public Interest Technologists" group could bring together voting members in key technical committees to propose standards on AI safety, quantum communications, biometric data, and neurotechnology.

Improved institutional coordination among the EU, Japan, and the United States. This effort should:

- involve CEN/CENELEC/ETSI, the Japanese Industrial Standards Committee, and the NIST, and transcend economic incentives. A formal interface is required to coordinate and implement industrial strategy and security requirements for technical workflows. This interface could be a funded, permanent, rotating administrative body that synchronizes calendars and aligns positions. The body could focus on specific EDTs such as AI and quantum and follow a joint submission process for technical standards to key working groups in the ISO and IEC.

- improved public reporting at SDOs (ISO, IEC, ITU), including creating reliable granular data on votes and proposals to better track state-led influence and to strengthen organizational legitimacy. The effort should also create a joint "Tech Watch" registry that identifies overlapping EDT research in areas

such as AI, quantum, and 6G before standards diverge at each of the partner SDOs. In addition, SDOs should start implementing risk-based categorization, developing a shared taxonomy of "critical standards" that identifies workplans for 10-15 EDTs. A pool of trilateral funding for security-vetted experts should help support the participation of independent security researchers in SDO meetings on these areas.

- fund tech accessibility that enables hybrid participation and invest in translation tools and other inclusive governance mechanisms

- assess interoperable risk to create a common security baseline (CSB) for vendors in critical sectors (AI, quantum, telecommunications, and cloud) and monitor participation in standards development. Criteria could include ownership transparency, data laws of home countries, and histories of intellectual property compliance.

Strategic cooperation on key EDTs and R&D including:

- standardization, which often happens in silos. A centralized hub would synchronize the technical roadmaps of the EU's Smart Networks and Services Joint Undertaking (SNS JU) and Joint Research Centre (JRC), Japan's JISC and National Institute of Information and Communications Technology, and the United States' NIST, and identify areas for joint cooperation.

- cooperation in critical areas such as joint R&D credits for Open-RAN architectures, preventing vendor lock-in on key EDTs (e.g., 6G equipment standards, QKDs) and ensuring network modularity, investing in cross-border "quantum sandboxes" for private firms,[10] grants for startups developing critical technologies, R&D on adapting commercial AI, drones, advanced communications, and geospatial tech for national security applications. Japanese researchers from JISC and the National Institute of Advanced Industrial Science and Technology (AIST) should have access to EU and US open innovation testbeds for semiconductors and quantum, and help support the transition from classical encryption (Rivest-Shamir-Adleman and Elliptic Curve Cryptography) to PQC.

- aligning technical specifications for export controls so that definitions of "dual-use" are consistent in the EU, Japan, and the United States to prevent "regulatory arbitrage" and security leakages. The three should jointly establish shared standards and metrics for export-controlled hardware to supplement "clean supply chains".

- launching EU, Japanese, and US AI safety institutes that must move beyond information sharing to functional interoperability with network effects. Landmark initiatives could include joint red-teaming protocols that harmonize the "stress tests" used to evaluate frontier models; create a secure, trilateral incident repository of "near-miss" AI incidents and vulnerabilities; establish joint metrics that standardize the measurement of AI energy consumption; and found a rotating "safety diplomat" program in which technical experts from the EU AI Office, Japan's Ministry of Economy, Trade and Industry, and the NIST serve one-year terms in partner institutes.

Broadening international cooperation with other key countries by:

- expanding alignment on standards development to key regional leaders such as Brazil, India, and South Korea, and blocs such as ASEAN and Mercosur, to ensure global interoperability. Frameworks such as Pax Silica11 should be explored further in lieu of EDT standards development.

- building on work done within the EU-India Trade and Technology Council to create a "Quad-plus" standard setting framework for advanced telecommunications, digital public infrastructure, and to encourage coordination on semiconductor supply chains (e.g., manufacturing in India and Latin America). Technical assistance should be provided, and "standard-setting training hubs" in Singapore and Vietnam should be established to counter state-centric models. The 2026 EU-Mercosur Partnership can be leveraged to align data privacy and cybersecurity standards.

References

Anthony M. Barrett, et al., "AI Risk-Management Standards Profile for General-Purpose AI (GPAI) and Foundation Models". UC Berkley, Center for Long-term Cybersecurity. January 2025. https://cltc.berkeley.edu/wp-content/uploads/2025/01/Berkeley-AI-Risk-Management-Standards-Profile-for-General-Purpose-AI-and-Foundation-Models-v1-1.pdf

Tom Barrett, "Standards Development Organisations in an era of strategic competition", University of Sydney United States Studies Centre, December 16, 2024. https://www.ussc.edu.au/standards-development-organisations-in-an-era-of-strategic-competition

Philip Boucher, et al., "Disruption by technology: Impacts on politics, economics and society", European Parliamentary Research Service, September 21, 2020. https://www.europarl.europa.eu/RegData/etudes/IDAN/2020/652079/EPRS_IDA(2020)652079_EN.pdf

European Commission, "An EU Strategy on Standardisation: Setting global standards in support of a resilient, green and digital EU single market" , Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs, 2022. https://ec.europa.eu/docsroom/documents/48598

European Commission, "Proposal for a Regulation amending Regulation (EU) No 1025/2012 as regards the decisions of European standardisation organisations concerning European standards and European standardisation deliverables", Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs, 2022. https://ec.europa.eu/docsroom/documents/48599

Alexandre Gomes, et al., "Standardisation with Chinese Characteristics: The Missing Pillar in Rebooting Europe's Industrial Policy", Clingendael, July 2025. https://www.clingendael.org/pub/2025/standardisation-with-chinese-characteristics/

Alex He, "The digital Silk Road and China's influence on standard setting", CIGI Papers No. 264, Centre for International Governance Innovation, April 2022. https://www.econstor.eu/bitstream/10419/299736/1/cigi-paper264.pdf

Gautam Kamath and Chloe Teevan, "Beyond the Brussels effect", ECDPM Brief, December 3, 2025. https://ecdpm.org/work/beyond-brussels-effect

Matt Sheehan and Jacob Feldgoise, "What Washington Gets Wrong About China and Technical Standards", Carnegie Endowment for International Peace, February 27, 2023. https://carnegieendowment.org/research/2023/02/what-washington-gets-wrong-about-china-and-technical-standards?lang=en&center=global

US Department of State, Pax Silica, 2026. https://www.state.gov/pax-silica

US House of Representatives, H.R.3220 - Quantum Sandbox for Near-Term Applications Act of 2025, 119th US Congress, June 5, 2025. https://www.congress.gov/bill/119th-congress/house-bill/3220

Oskar van Deventer, et al., "Towards European standards for quantum technologies", EPJ Quantum Technology. Vol. 9, article number 33, November 29, 2022. https://doi.org/10.1140/epjqt/s40507-022-00150-1

Valentin Weber, "Data-Centric Authoritarianism", National Endowment for Democracy, February 2025. https://www.ned.org/wp-content/uploads/2025/02/NED_FORUM-China-Emerging-Technologies-Report.pdf

The White House, "Ensuring Safe, Secure, and Trustworthy AI". White House, 2023. https://bidenwhitehouse.archives.gov/wp-content/uploads/2023/07/Ensuring-Safe-Secure-and-Trustworthy-AI.pdf

The White House, "Red-Teaming Large Language Models to Identify Novel AI Risks", August 29, 2023. https://bidenwhitehouse.archives.gov/ostp/news-updates/2023/08/29/red-teaming-large-language-models-to-identify-novel-ai-risks/

The White House, "Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence", Executive Order 14110, 2023. https://www.federalregister.gov/documents/2023/11/01/2023-24283/ safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence

Junhua Zhu, "China's Approach to AI Standardisation", Finnish Institute of International Affairs, August 2024. https://fiia.fi/wp-content/uploads/2024/08/bp391_chinas-approach-to-ai-standardisation.pdf

Acknowledgements

This working paper was prepared for GMF. The author has benefited from insights shared in the Japan Trilateral Forum in Brussels in October 2025 and in "Setting International Standards for Emerging Technologies: Enhancing Coordination among Japan, the US, and Europe", a January 2026 online, closed-door roundtable supported by the Embassy of Japan in the United States. All errors or omissions are attributable to the author and are unintentional. The contents of this working paper do not reflect the views of any institution or organization with which the author is associated.

Gautam Kamath *is an independent, Brussels-based policy consultant managing Eurus Advisory and acting as senior adviser for ECDPM, a think tank. He has served for over a decade in global tech and policy roles at leading tech companies and international institutions including at the UN and World Bank. He holds degrees from Harvard Kennedy School, National Taiwan University, and Maastricht University. He advises business leaders and think tanks navigating complex EU and global issues.*

Endnotes

[1] *See, e.g., "Standardisation with Chinese Characteristics: The Missing Pillar in Rebooting Europe's Industrial Policy", Clingendael, 2025. China tops the list for participation in ISO technical committees, and its position has grown exponentially between 2013 and 2025. See also "Standards Development Organisations in an era of strategic competition," University of Sydney United States Studies Centre, December 2024.*

[2] *Junhua Zhu, "China's approach to AI standardisation: State-guided but enterprise-led", Finnish Institute of International Affairs, August 2024.*

[3] *Matt Sheehan and Jacob Feldgoise, "What Washington Gets Wrong About China and Technical Standards", Carnegie Endowment for International Peace, February 27, 2023. https://carnegieendowment.org/research/2023/02/what-washington-gets-wrong-about-china-and-technical-standards?lang=en&center=global*

[4] *Philip Boucher, et al., "Disruption by technology: Impacts on politics, economics and society", European Parliamentary Research Service, September 21, 2020. https://www.europarl.europa.eu/RegData/etudes/IDAN/2020/652079/EPRS_IDA(2020)652079_EN.pdf.*

[5] *See, e.g., "Shaping European Standards Supporting the AI Act", CEN/CENELEC press release, July 29, 2025. https://www.cencenelec.eu/news-events/news/2025/newsletter/ots-64-etuc/*

[6] *Simplified view of the creation of harmonized standards for the EU AI Act, beginning with the standardization request and following the order of the clock through the drafting, enquiry, final vote, assessment, and OJEU publication. Picture taken from https://artificialintelligenceact.eu/standard-setting-overview/*

[7] *Alex He, "The digital Silk Road and China's influence on standard setting", CIGI Papers No. 264, Centre for International Governance Innovation, April 2022. https://www.econstor.eu/bitstream/10419/299736/1/cigi-paper264.pdf*

[8] *Valentin Weber, "Data-Centric Authoritarianism", National Endowment for Democracy, February 2025. https://www.ned.org/wp-content/uploads/2025/02/NED_FORUM-China-Emerging-Technologies-Report.pdf*

[9] *Oskar van Deventer, et al., "Towards European standards for quantum technologies", EPJ Quantum Technology. Vol. 9, article number 33, November 29, 2022. https://doi.org/10.1140/epjqt/s40507-022-00150-1*

[10] *See, e.g., US House of Representatives, H.R.3220 - Quantum Sandbox for Near-Term Applications Act of 2025, 119th US Congress, June 5, 2025. https://www.congress.gov/bill/119th-congress/house-bill/3220*

[11] *Pax Silica is a new US-led strategic alliance launched in December 2025 to establish secure and resilient global supply chains for semiconductors, critical minerals, and AI infrastructure among a network of „trusted" partner nations. The initiative aims to reduce coercive dependencies and coordinate policy. US Department of State, Pax Silica, 2026. https://www.state.gov/pax-silica*

Entangled Interests in Quantum Technology

The United States, Japan, and Europe should pursue aligned economic security policies.

By Lindsay Gorman and Alexandra Pugh

The People's Republic of China's (PRC) China Standards 2035 strategy[1], coupled with its growing leadership in 5G and influence in international standards bodies, served as a wakeup call to the United States and its allies: Abstruse technical standards, often left to the private sector, are a geopolitical battleground. Today, this competition is unfolding across critical technologies from 6G and AI to quantum and biotechnology, with increased attention among the United States, Europe, and Japan to standard-setting as one driver of technology power.[2]

Quantum technologies hold transformative potential across sectors and remain largely in a pre-competitive stage, making early alignment on standards a critical opportunity to shape global markets. As these technologies move from the lab to deployment, democratic allies should prioritize de facto standards alignment by increasing cooperation on both innovation and economic security.

Coordinated economic security measures can translate technical strengths into global leadership and strategic advantage by securing critical supply chains and protecting technological advances. As quantum markets materialize, US, allied, and PRC economic security postures will shape which technologies are built, by whom, and on what scale. The countries that protect and grow their quantum industries today will see their technical approaches become the international standard tomorrow. Aligned toolkits supporting the build-out of allied quantum supply chains are critical if the United States, Europe, and Japan are to lead in future quantum standards.

Standard-Setting on Quantum Technologies

The year 2025 was the UN's "international year of quantum", while 2026 will operationalize national commitments and thrust quantum technologies firmly into the spotlight as a domain of active—and not just theoretical—great-power competition. In the face of intensifying technological rivalry with the PRC, the United States, Europe, and Japan each seek to expand their economies and international influence through global quantum leadership. International standard-setting is increasingly part of their strategies.

In the United States, the National Institute of Standards and Technology's (NIST) "Strategy for American Technology Leadership in the 21st Century" prioritizes[3] bolstering US leadership in standards and a scale-up of the US quantum industrial base. The EU's Quantum Strategy notes the importance of technical interoperability and promises[4] a European Quantum Standards Roadmap in 2026 to facilitate industrialization. Japan's 2025 New International Standards Strategy[5] includes a dedicated section on quantum, calling for public-private collaboration on technical standards to create markets, define norms, and solve societal challenges.

At the international level, the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) established[6] Joint Technical Committee (JTC) 3 in 2024 to standardize quantum technologies. Japan secured[7] a working group leadership role, the United Kingdom's British Standards Institution managed the group's inaugural secretariat, and NIST swiftly created a US Technical Advisory Group for the committee. In coordination with JTC 3, the EU's European Committee for Standardization (CEN) and European Committee for Electrotechnical Standardization (CENELEC) Joint Technical Committee on Quantum Technologies (CEN-CLC/JTC 22[8]) build European standardization roadmaps. They work across quantum metrology, sensing, and enhanced imaging; enabling technologies; quantum computing and simulation; and quantum communications and cryptography.

While allied coordination on formal standard-setting can help blunt PRC influence, the United States, Japan, and Europe should also employ a de facto standardization strategy by aligning approaches to promoting and protecting quantum technologies. In this framework, allies can borrow and adapt successful strategies for technological competitiveness and economic security, and uncover cooperation opportunities—particularly in pre-competitive technologies and in areas where critical supply chains are globally distributed. All three partners, however, must balance strong currents toward stated goals of technological self-reliance in quantum with the advantages they recognize of international partnership.

The Economic Security Toolkit for Quantum Technologies

Amid concerns over the security of advanced technology supply chains and competition from the PRC, the United States, Europe, and Japan are each expanding their techno-economic security toolkits, including on quantum technologies. Allies should coordinate on threat-intelligence sharing, shoring up supply-chain vulnerabilities, and blunting the economic impacts of restrictive measures such as export controls to any one country's industry.

United States

In the United States, the Committee on Foreign Investment in the United States (CFIUS) can review[9] inbound investments in US business involving critical technologies including quantum if a foreign investor acquires rights such as board membership or access to non-public technical information. Executive Order (EO) 14083[10] requires CFIUS to consider in risk reviews whether covered transactions involve quantum computing and other technologies relevant to national security. The FY2026 National Defense Authorization Act[11] (NDAA) also expanded the outbound investment regime (or "reverse CFIUS") for critical technologies such as quantum, broadening the list of "countries of concern"—in which outbound quantum investment is restricted—to include the PRC, Russia, Iran, Cuba, North Korea, and Venezuela under the Maduro regime. Last year, Washington also added eight companies[12] connected to the PRC's quantum ecosystem to the Commerce Department's Entity List.

The United States is poised to adopt additional economic security measures for quantum technologies. The US NQI Reauthorization Act[13] would require[14] the secretaries of commerce and energy to conduct a quantum supply chain study and directs[15] the secretary of commerce to identify legislative or administrative

measures to strengthen quantum supply chain resilience. In addition, the Trump administration's draft executive order on quantum technologies reportedly[16] includes directives for the Department of Commerce to de-risk quantum technologies through commercial investments and address foreign trade barriers.

Japan

Japan has been an early mover[17] in economic security statecraft for quantum and other critical and emerging technologies. In 2022, its National Diet approved the Economic Security Promotion Act[18], which directs ministers with jurisdiction over the production, import, or sale of designated critical products—including semiconductors and critical minerals found in quantum supply chains—to implement supply-chain security tools such as stockpiling, source diversification, and enhanced production methods. The Act focuses on critical technologies whose development is essential for Japanese security, and government documents include quantum among them.

Japan also restricts the export of some quantum technologies and related inputs under its Foreign Exchange and Foreign Trade Act[19], which authorizes controls on goods exports and technology transfers for both security and economic reasons. In May 2023, Japan joined fellow G7 members and the EU[20] in imposing[21] export restrictions on "devices utilizing quantum properties" and related auxiliary devices and inputs in response to Russia's war in Ukraine. Japan's Ministry of Economy, Trade, and Industry also requires[22] export licenses for quantum computers and quantum cryptography products irrespective of destination, with the latter subject to[23] controls under the Wassenaar Arrangement's[24] dual-use regime.

Europe

The EU has also expanded its economic security toolkit for quantum and related inputs. The bloc provisionally agreed[25] in 2025 on a requirement for member states to establish foreign direct investment screening mechanisms for dual-use and military equipment, critical raw materials, and "hyper-critical technologies" such as quantum, AI, and semiconductors. In January, the European Commission called on[26] member states to review outbound investments in quantum, AI, and semiconductors with an aim to assess risks of the technologies and related technical know-how "falling into the wrong hands".

Securing quantum supply chains also factors into the EU's Quantum Europe Strategy[27] and forthcoming Quantum Act.[28] Under this framework, the Commission will conduct an EU-wide supply-chain mapping and risk assessment exercise as it seeks to mitigate dependencies on non-European sources.

Through its Transatlantic Quantum Community, NATO has also mapped the alliance's quantum computing[29] and sensing[30] supply chains. A pair of studies found moderate- or high-risk vulnerabilities across 28 of the 49 nodes of the two supply chains and proposed recommendations to mitigate allied vulnerabilities.

The Path Ahead: Cooperation in an Era of Quantum Self-Reliance?

Despite geopolitical trends driving countries to prioritize technological self-sufficiency, the United States, Europe, and Japan should seize on existing interest in economic security to establish a trilateral technology security partnership. Quantum technologies should be a key focus area of this partnership, alongside AI and 6G, given existing quantum node dependencies among

the partners. This initiative could mirror the recent US-EU-Japan partnership on critical minerals, which aims to diversify supply and coordinate trade policy.

The foundation for such an initiative is already emerging in doctrine and practice. For its part, the EU recognizes that effective action on economic security "depends on cooperation and coordination with third countries" and aims to "engage with allies on the subject of outbound investment screening". In their 2025 trade framework agreement, the EU and the United States agreed "to strengthen economic security alignment to enhance supply chain resilience and innovation by … cooperating on inbound and outbound investment reviews and export controls". At the 2025 EU-Japan Summit[31], the two partners committed to cooperation on economic security and the promotion and protection of critical and emerging technologies, as well as to advancing cooperation on sectoral standards for supply chain resilience through the G7. Japan is also a signatory to the United States' Pax Silica initiative, as well as a partner in trilateral quantum cooperation[32] on industrial security with the United States and Korea.

Quantum technologies—particularly those in pre-competitive stages—provide concrete opportunities for alignment on standards and innovation among the United States, Europe, and Japan. Focusing on economic security as an upstream determinant of standards and selecting areas consistent with technological sovereignty and resilience goals can help leverage political momentum towards trilateral cooperation and allied quantum competitiveness.

Lindsay Gorman *is Managing Director and Senior Fellow of GMF's Technology Program and a Venture Scientist at Deep Science Ventures, focusing on AI and biotechnology. A quantum physicist and computer scientist by training, she leads work on US-China technology competition, AI and democracy, and transatlantic innovation. Previously, she served as a senior adviser in the Biden White House, where she shaped US emerging technology and national security strategy and founded the AI cooperation workstream under the US-EU Trade and Technology Council. Her work has been featured in major media outlets, and she regularly testifies before Congress on AI and cybersecurity.*

Alexandra Pugh *is a Washington, DC-based program coordinator with GMF Technology. She previously worked with the Senate Foreign Relations Committee and at the Center for European Policy Analysis, where she focused on Russia-China cooperation and competition. She also held a fellowship at the Bush Institute to research NATO policy toward Ukraine.*

Endnotes

[1] Yi Wu, "China Standards 2035 Strategy: Recent Developments and Implications for Foreign Companies", China Briefing, July 26, 2022. https://www.china-briefing.com/news/china-standards-2035-strategy-recent-developments-and-their-implications-foreign-companies/

[2] Lindsay Gorman, "The U.S. Needs to Get in the Standards Game— With Like-Minded Democracies", Lawfare, April 2, 2020. https://www.lawfaremedia.org/article/us-needs-get-standards-game%E2%80%94-minded-democracies

[3] National Institute of Standards and Technology (NIST), "NIST Strategy for American Technology Leadership in the 21st Century", September 2, 2025. https://www.nist.gov/director/strategic-priorities

[4] European Commission, "Quantum Europe Strategy: Quantum Europe in a Changing World", July 2, 2025. https://qt.eu/media/pdf/Quantum_Europe_Strategy_July_2025.pdf

[5] Intellectual Property Strategy Headquarters, "New International Standards Strategy", June 3, 2025. https://www.kantei.go.jp/jp/singi/titeki2/chitekizaisan2025/pdf/shiryo5_e.pdf

[6] NIST, "New IEC/ISO Joint Technical Committee on Quantum Technologies—Inviting Participants for the U.S. National Committee Technical Advisory Group", February 9, 2024. https://www.nist.gov/news-events/news/2024/02/new-ieciso-joint-technical-committee-quantum-technologies-inviting

[7] Ministry of Economy, Trade and Industry, "Convener from Japan Elected to Lead the Working Group for the International Standardization of Quantum Technologies", October 24, 2025. https://www.meti.go.jp/english/press/2025/1024_002.html

[8] European Committee for Standardization, "CEN/CLC/JTC 22 – Quantum Technologies", accessed February 24, 2026. https://standards.cencenelec.eu/ords/f?p=205:7:::::FSP_ORG_ID:3197951&cs=11045E65C796A40077CF0448261BABCE1

[9] Latham & Watkins LLP, "Committee on Foreign Investment in the United States", 2025. https://www.lw.com/admin/upload/SiteAttachments/CFIUS-Booklet-Key-Questions-Answered-2025.pdf

[10] Federal Register, "Executive Order 14083: Ensuring Robust Consideration of Evolving National Security Risks by the Committee on Foreign Investment in the United States", September 20, 2022. https://public-inspection.federalregister.gov/2022-20450.pdf

[11] Library of Congress, "S.1071 – National Defense Authorization Act for Fiscal Year 2026", January 3, 2025. https://www.congress.gov/bill/119th-congress/senate-bill/1071/text

[12] Bureau of Industry and Security, "Commerce Further Restricts China's Artificial Intelligence and Advanced Computing Capabilities", March 25, 2025. https://www.bis.gov/press-release/commerce-further-restricts-chinas-artificial-intelligence-advanced-computing-capabilities; Federal Register, "Additions and Revisions to the Entity List", September 16, 2025. https://www.federalregister.gov/documents/2025/09/16/2025-17893/additions-and-revisions-to-the-entity-list

[13] Library of Congress, "S.3597 – National Quantum Initiative Reauthorization Act of 2026", January 8, 2026. https://www.congress.gov/bill/119th-congress/senate-bill/3597/text

[14] Association of American Universities, "AAU Signs National Quantum Initiative Reauthorization Act Support Letter", February 10, 2026. https://www.aau.edu/key-issues/aau-signs-national-quantum-initiative-reauthorization-act-support-letter

[15] US Senator for Indiana Todd Young, "Young, Cantwell Introduce National Quantum Initiative Reauthorization Act", January 6, 2026. https://www.young.senate.gov/newsroom/press-releases/young-cantwell-introduce-national-quantum-initiative-reauthorization-act-2/

[16] Kelley, "Draft quantum order".

[17] Reuters, "Partners in resilience: How Japan and the world are redefining economic security", December 4, 2025. https://www.reuters.com/plus/partners-in-resilience-how-japan-and-the-world-are-redefining-economic-security

[18] Japanese Law Translation, "Act on the Promotion of Ensuring National Security through Integrated Implementation of Economic Measures", May 18, 2022. https://www.japaneselawtranslation.go.jp/en/laws/view/4523/en#je_ch2

[19] Japanese Law Translation, "Foreign Exchange and Foreign Trade Act", December 1, 1949. https://www.japaneselawtranslation.go.jp/en/laws/view/4412/en#je_ch6at2

[20] European Council, "G7 Leaders' Statement on Ukraine", May 19, 2023. https://www.consilium.europa.eu/media/64494/g7-2023-statement-on-ukraine.pdf

[21] Sae Kobayashi, "Japan's Export Control on Quantum Technology", Stanford International Policy Review, September 12, 2024. https://fsi.stanford.edu/sipr/japan-qt

[22] Takumi Hasegawa, Maito Tozawa, Soichiro Fujiwara, Taku Takanami and Junko Suetomi, "Japan updates Listed Controlled Items to include sensitive items such as quantum computers", Baker McKenzie, October 15, 2024. https://sanctionsnews.bakermckenzie.com/japan-updates-listed-controlled-items-to-include-sensitive-items-such-as-quantum-computers/

[23] Wassenaar Arrangement, "List of Dual-Use Goods and Technologies and Munitions List", January 15, 2026. https://www.wassenaar.org/app/uploads/2026/01/List-of-Dual-Use-Goods-and-Technologies-and-ML-2025-Corr.pdf

[24] The Wassenaar Arrangement, "Home – The Wassenaar Arrangement", accessed February 17, 2026. https://www.wassenaar.org/

[25] European Council, "Foreign direct investment: Council and Parliament reached political agreement to improve FDI screening", December 11, 2025. https://www.consilium.europa.eu/en/press/press-releases/2025/12/11/foreign-direct-investment-council-and-parliament-reached-political-agreement-to-improve-fdi-screening/

[26] European Commission, "Commission calls on Member States to review outbound investments and assess risks to economic security", January 14, 2025. https://ec.europa.eu/commission/presscorner/detail/en/ip_25_261

[27] Quantum Europe Strategy.

[28] *European Commission, "The EU's plan to become a global leader in quantum by 2030".*

[29] *Lukas Kingma, Freeke Heijman, and Carl Williams, "Official Summary: Critical Vulnerabilities in the Quantum Computing Supply Chain within the NATO Alliance", May 2025. https://www.fheijman.nl/QSC_report.pdf*

[30] *Kingma et al., "Official Summary".*

[31] *Council of the European Union, "EU-Japan Summit 2025 – Joint Statement", July 23, 2025. https://data.consilium.europa.eu/doc/document/ST-11834-2025-INIT/en/pdf*

[32] *US Department of State, "Trilateral Quantum Cooperation", September 5, 2025. https://www.state.gov/releases/office-of-the-spokesperson/2025/09/trilateral-quantum-cooperation*

G | M | F