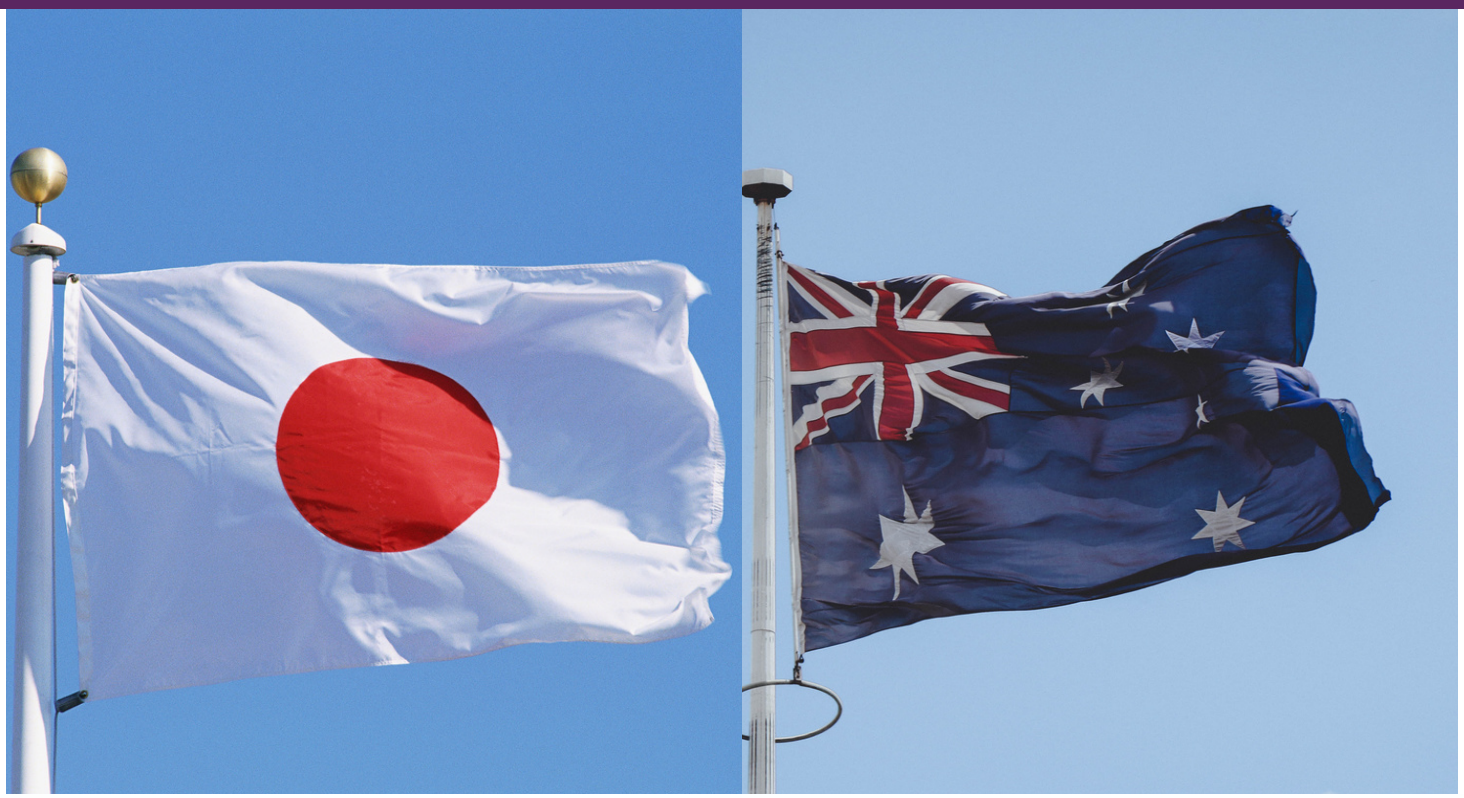
Developing Trusted and Secure Technology Supply Chains

SEPTEMBER 2021



ITI NASSCOM® KOAN

The Information Technology Industry Council (ITI) is the premier global advocate for technology, representing the world's most innovative companies. ITI promotes public policies and industry standards that advance competition and innovation worldwide.

NASSCOM is the premier trade body and chamber of commerce of the Tech industry in India and comprises over 3000 member companies including both Indian and multinational organisations that have a presence in India.

Koan Advisory Group ("Koan") is a New Delhi-based public policy consultancy. Koan specialises in policy and regulatory analysis in both traditional and emergent sectors and markets.

Overview

The United States (US) President, Mr. Joe Biden will host the Quad Leaders' Summit at the White House on September 24, 2021. This comes at a time when governments across the world are exploring ways to address vulnerabilities in supply chains critical to economic well-being and national security. For instance, India and the US were among the top five most cyber-attacked nations in the world in 2019. In this context, supply chain security risks in the information and communications technology (ICT) industry have received attention from both governments.

While technology supply chain security is a subset of the overall cybersecurity concerns, failure to adequately address these issues may have a significant impact on economic outcomes (international trade, commerce), political outcomes (trust in government), and social outcomes (trust in other institutions).

The Quadrilateral Dialogue between India, US, Australia, and Japan is now a vital forum to coordinate approaches towards trusted and secure technology supply chains. In the last Quad Summit held in March, 2021 the Quad Members decided to establish the Critical and Emerging Technology Working Group, which aims to:

- *Develop statement of principles on technology design, development, and use;*
- *Facilitate coordination on technology standards development, including between our national technology standards bodies and working with a broad range of partners;*
- *Encourage cooperation on telecommunications deployment, diversification of equipment suppliers, and future telecommunications, including through close cooperation with our private sectors and industry;*
- *Facilitate cooperation to monitor trends and opportunities related to developments in critical and emerging technology, including biotechnology;*
- *Convene dialogues on critical technology supply chains*

This important conversation within the Quad provides an opportunity to bolster cooperation on approaches to supply chain security and resiliency, which have become more complex due to globalisation.

With this in mind, the Information Technology Industry Council (ITI), the National Association of Software and Service Companies (NASSCOM), and the Koan Advisory Group, organised a Track 1.5 discussion on "Developing Trusted and Secure Technology Supply Chains" on September 14, 2021.

The convening included a distinguished group of eminent government representatives from each member country, as well as experts from civil society and industry. This document captures key perspectives and recommendations to strengthen supply chain security, across the Quad countries.

Recommendations

1. Critical Sectors:

The Quad countries recognise the need to prioritise the security of critical supply chains. However, the countries have adopted different approaches in identifying critical or vulnerable sectors:

a. ***India:*** India follows an infrastructure led approach. Specifically, criteria such as *functionality; criticality; scale; degree of complementarities; political, economic, social and strategic values; degree of dependence, sensitivity, etc*. are taken into account when determining a critical sector. Under the existing framework, six sectors have been recognised as critical. These are banking, financial services and insurance; transport; telecom; power / energy; government; and strategic & public enterprises; of which telecom and power are considered most critical.

b. ***Australia:*** The Australian Productivity Commission's Interim Report on Vulnerable Supply Chains defines essential goods and services as those that meet the basic needs of Australian citizens. These include food, water, health, communications, energy, logistics, finance, and government.

c. ***US:*** In its initial assessment of critical supply chains, the Biden administration has identified four critical sectors i.e. semiconductor manufacturing and advanced packaging, large capacity batteries, critical minerals and materials, and pharmaceuticals and advanced pharmaceutical ingredients. Furthermore, the US government has called for a year long review supply chains in six sectors including ICT, defence, public health, energy, food production, and transportation.

d. ***Japan:*** Japan, in contrast, has focused on incentivizing the private and public sectors to diversify their supply chains. The country has announced economic incentives in its efforts to encourage firms to relocate production back to Japan or diversify supply chains by moving to a third country, mostly in Southeast Asia.

As the Quad economies recover from the global pandemic and face new economic and socio-political pressures, a cogent and robust framework for building supply chain resilience is of the utmost importance. According to the WTO, global goods trade has grown steadily since it registered a sharp decline in the second quarter of 2020 during the early days of the pandemic. The volume of merchandise trade in the first quarter of 2021 has seen the largest jump since the third quarter of 2011. It is therefore likely that goods trade will see an even larger year-on-year increase in the second quarter.

Simultaneously, the global trade in electronic and hardware products is estimated at over two trillion dollars and will eventually overtake the global trade in oil. Therefore, it is important to delineate common principles which can help Quad countries to identify critical sectors, particularly those linked to ICT, to ensure that the positive growth in global trade is not jeopardized by supply chain risks.

2. Public Procurement:

A lean and global model of manufacturing/production of goods and services has allowed 21st-century businesses to effectively and seamlessly establish forward and backward linkages across the world. However, these operational efficiencies aimed at reducing costs can introduce systemic vulnerabilities. In this context, participants agreed that public procurement by governments can act as a powerful tool in minimising supply chain risks, by incentivising suppliers to prioritise security.

Governments should consider quality and security assurances provided by bidders to make informed procurement decisions. QCBS (Quality Cum Cost Basis Selection) has been adopted by Government of India for most mission mode and turnkey ICT projects. However Least Cost, referred to as 'L1' in public procurement, is still preferred by some government agencies, especially to procure commodity hardware. Higher weightage for technical parameters will ensure preference is given for robust tested and certified products. This vision is also endorsed at the leadership level, by PM Modi, who asserted last year that "the decision on developing global supply chains should be based not only on costs".

3. Risk-Based Approach:

As concerns on strengthening supply chain resilience take center stage, countries have taken different approaches to exclude the participation of actors or entities they have deemed to be high-risk. Illustratively, India's National Security Directive on Telecommunications requires telecom service providers to disclose information about the products they intend to connect their network to, product OEMs, and related details -- a veritable 'know your supplier' framework. In the US, the Department of Commerce's Interim Rule on Securing the Information and Communications Technology and Services Supply Chain authorises the Commerce Secretary (in consultation with relevant officials) to regulate the acquisition and use of ICT and services from a "foreign adversary."

In contrast, Japan's approach focuses on diversifying supply chains and mitigating potential choke-points, instead of categorising suppliers. Similarly, Australia's Guidance on 5G Security restricts the involvement of vendors who are likely to be subject to extrajudicial directions from a foreign government that conflict with Australian law. The Quad framework's success will lie in its ability to develop a set of criteria to identify risks based on sound first-principles that are easily transferable across the four jurisdictions.

4. Information Sharing:

The participants agreed that the presence of an effective arrangement for information sharing will equip decision-makers to provide effective oversight and guidance to the private sector. The continuous integration of ICT networks and systems, as well as cyber-physical systems, has led to an increase in component dependencies. Despite geographic diversification, components are now sourced from a narrower set of dominant suppliers that are low-cost producers. In this context, information sharing on high-risk actors and threats in any given supply vertical can prove useful.

Moreover, it is important to design incentives for the private sector across Quad countries to share information on supply chain vulnerabilities, freely with governments. This information sharing should extend all the way to raw material supply. The Whitehouse Report on Resilient Supply Chains notes that several raw materials in emerging and potentially critical sectors like electric vehicles originate from outside the US. At the same time "global demand for lithium and graphite, two of the most important materials for electric vehicle batteries, is estimated to grow by more than 4000 percent by 2040". Similarly, "there is little transparency into the origins of Advanced Pharmaceutical Ingredients within generic drugs, which represent 90 percent of all pharmaceuticals consumed in the US".

5. Standards:

The Quad countries have enhanced their focus on the development of regulatory and technical standards for ICT technologies. They could collaborate and take the lead in development of a new global standards developed through consensus with private sector organisations, and by standard setting bodies like the International Organisation for Standardization, for emerging areas such as Internet of Things (IoT). In fact, IoTs already constitute a large part of global trade in ICT (up to USD 800 million by some estimates) and represent the evolution of connected devices and technology ecosystems. They exemplify a growing synthesis between humans and machines, which is a key characteristic of the 'Fourth Industrial Revolution'.

The participants also highlighted the need to promote the development of global standards that can reduce the risk of reliance on a single supplier. For instance, existing standards such as the Open Radio Access Networks (ORAN) that allow telecom networks to be deployed with modular design, and without creating vendor dependence, are useful templates. In addition, supply chain standards should aim to promote recognized principles such as security by design.

6. New Approaches and Mechanisms

Testing and certification schemes devised to address the supply chain security concerns are converging, becoming more accessible, adapting to the rapid technology changes, responding to the requirements of the user communities, and getting standardized. Schemes such as India's Authorised Economic Operator and the US's Customs-Trade Partnership against Terrorism focus on improving security throughout the supply chain, beginning at the point of origin (including manufacturer, suppliers, or vendors) through a point of distribution to the destination. However, supply chain risks tend to be discussed with respect to a specific country. That might lead to divergent solutions/ approaches because of which the technology businesses may face hurdles to ease of doing business. The participants highlighted the need for harmonized and coordinated approaches and mechanisms based on global standards to address supply chain security issues.

In addition, the global push for digitization across the sectors has increased the volume and velocity of development and deployment of new products and solutions. For instance, a range of devices backed by a complex digital technology ecosystem is employed to process business transactions. The participants deliberated on the efficacy of the current assurance mechanisms such as ISO 28000 which specifies security management systems for the supply chain. They called for increased policy attention to make assurance mechanisms flexible, agile, nuanced, and scalable.

7. Resilient Supply Chains:

The Quadrilateral Security Dialogue emphasises the importance of resilient supply chains. The roundtable participants agreed that this can create opportunities for private sector to contribute to policy goals of enhanced resilience. Specific programs, support, and incentives may help to streamline implementation. The Supply Chain Resilience Initiative (SCRI) launched by India, Japan, and Australia in April 2021 can provide a useful guidance. The SCRI aims to (i) facilitate sharing of best practices, and (ii) explore the diversification of their supply chains.

List of Discussants/ Participants

- **Arvind Gupta**, Co-Founder and Head, Digital India Foundation
- **Bob Kolasky**, National Risk Management Center, Cybersecurity and Infrastructure Security Agency, Department of Homeland Security, United States Government
- **Brendan Dowling**, First Assistant Secretary, Digital and Technology Policy, Department of Home Affairs, Government of Australia
- **Courtney Lang**, Senior Director of Policy, ITI
- **Danielle Kriz**, Senior Director, Global Policy, Palo Alto Networks
- **John Miller**, Senior Vice President of Policy and General Counsel, ITI
- **Kumardeep Banerjee**, Country Manager (India), ITI
- **Lt General (Dr) Rajesh Pant**, National Cyber Security Coordinator, Government of India
- **Rob Strayer**, Executive Vice President of Policy, ITI
- **Shivendra Singh**, Vice President and Head, Global Trade Development, NASSCOM
- **Swati Samaddar**, Government and Regulatory Affairs Executive, IBM
- **Takeshi Komoto**, Commercial Minister, Embassy of Japan to the US
- **Vinayak Godse**, Vice President, Data Security Council of India (DSCI)
- **Vivan Sharan**, Partner, Koan Advisory Group

ITI NASSCOM® KOAN