Weathering TechNationalism
Weathering TechNationalism: A Security and Trustworthiness Framework to Manage Cyber Supply Chain Risk
The Consequences of TechNationalism

Information and communications technology (ICT) is strategic for a nation’s economy, security, and identity. Exploitable vulnerabilities in ICT and complex, difficult to secure supply chains are raising security concerns in the public and private sectors. National governments, particularly, are paying increased attention to the possibility that foreign governments might taint ICT through global supply chains, either by coercing a local supplier to cooperate or by gaining direct access to its operations. Several governments have warned against or restricted the use of certain foreign ICT products and services in their domestic markets—with the stated intention of protecting against such risks.

This report refers to such policy actions as TechNationalism—direct or indirect measures that favor ICT products and services sold by companies headquartered domestically or in allied states against those headquartered in states seen as competitors or adversaries.

Weathering TechNationalism: A Security and Trustworthiness Framework to Manage Cyber Supply Chain Risk provides policymakers, regulators, and corporate executives a framework for mitigating risk and addressing shared responsibility in global ICT supply chains through measures of assurance, transparency, and accountability implemented jointly by ICT buyers, operators, and vendors. It also provides supporting policy measures to achieve a balanced, risk-informed outcome and avoid the negative consequences of TechNationalism.

TechNationalism in the global ICT market is driven by competing national interests including national security, cybersecurity, economic competitiveness, innovation, prestige, and
geopolitics. Measures of TechNationalism may include requiring companies to localize data processing and storage; giving preference to domestic products or components; subjecting foreign companies to enhanced requirements characterized as security-related, such as ordering them to make source code available for inspection; requiring foreign companies to partner with domestic entities to gain market access; and banning specific foreign products or companies.

Rooted in geopolitical tensions, the rise of TechNationalism is shaped by an increase in nationalist and isolationist tendencies that undermine trust in the multilateral system, the weaponization of international trade to achieve geopolitical objectives, the rise of state-centric models of Internet governance to exercise control over content and restrict free expression, and the coming of age of cyberspace as a new domain of interstate conflict.

Against this backdrop, states must make trade-offs among national security, cybersecurity, and trade and industrial competitiveness goals to ensure ICT security and trustworthiness. For example, heightened restrictions on foreign ICT firms to assuage national security concerns may reduce overall industrial competitiveness and cybersecurity.

There are four initial conditions that complicate the practical implementation of these policy goals and provide impediments to enhance ICT security and trustworthiness. First, the global and complex nature of supply chains poses significant challenges to securing ICT supply chains. To ensure the authenticity and integrity of ICT, physical and software components would have to be traceable along the supply chain, and the security of ICT would have to be demonstrable throughout its lifecycle. Second, the importance of strategic ICT to economic prosperity and military power puts ICT and data squarely into a strategic domain. The convergence of this new ICT—including 5G communications; the Internet of Things (IoT) and its cousin, the Industrial Internet of Things (IIoT); artificial intelligence (AI); robotics; quantum computing; and the digitization of vertical industries—is expected to unleash enormous economic growth, but is also anticipated to be critical for national intelligence capacity, military power, and modern warfare. Governments increasingly believe that a state’s ability to achieve “dominance” or “control” over these technologies is crucial to preserving strategic autonomy. Third, the challenge of securing ICT is a foundational cybersecurity problem. Exploitable vulnerabilities are frequently found in ICT products and services that are created by otherwise trustworthy entities. Even ICT without known vulnerabilities or security concerns may, in the future, pose a difficult-to-manage risk. Fourth, holding third parties accountable when ICT is interfered with or targeted remains challenging. It is difficult to pinpoint a malicious or negligent action to a particular actor. This limits not only confidence in the attribution of a compromise in a global supply chain, but impedes corrective action to rectify such violations.

National security risks require strict, targeted measures based on accurate threat assessments. Governments are attempting to restrain and control foreign ICT to mitigate these security risks through technology bans and restrictions, technical security requirements, adherence to domestic technical standards, data localization requirements, export controls, tariffs, trade agreements, investment restrictions, and ownership limitations. These measures, however, bear a significant potential for unintended effects that may distort markets and hamper innovation and competition with negative consequences for national security, cybersecurity, trade, and industrial competitiveness. As a result, ICT trade and foreign relations may suffer. Instead of protecting against legitimate threats, such measures may create a world with separate, fragmented, and partially or fully decoupled technological and economic universes that endanger long-term global economic development and growth.
The Framework: Enhancing ICT Security and Trustworthiness

To minimize the deficiencies and unintended consequences of TechNationalism, this report introduces a framework that provides an objective and transparent basis for managing risk and determining trustworthiness in global ICT supply chains. It consists of five components, each crafted to provide assurance, transparency, and accountability. The framework’s integrated approach describes technical, organizational, and confidence-building measures across three fields of action—organization, industry, and ecosystem—that need addressing to achieve a sufficient level of assurance and trust. These measures help to establish and evaluate confidence in a vendor, as well as the security of its ICT products and services and the supply chain. Furthermore, detailing a framework for assurance, transparency, and accountability will assist buyers, vendors, and operators to implement these measures and strengthen related requirements over time.

ICT supply chain risk management is concerned with reducing risk from potentially unreliable suppliers, vulnerable ICT, and insecure ICT operations—or more broadly, mitigating risk from dependence on third party entities or components. Weighing the cost and benefit of risk mitigation measures helps strike a balance between risk mitigation and cost effectiveness. Technical and organizational measures provide limited assurance, however. While these measures do not achieve “complete” assurance, the framework provides a sufficient basis for decision-making and risk mitigation without necessitating ICT buyers to take a “leap of faith.” If carefully adapted and implemented by ICT vendors, buyers, and operators, this combination of appropriate, verifiable measures constitutes a sound building block for risk assessment and mitigation that narrows the trust gap. Any remaining deficit must be addressed through political and diplomatic means, including confidence-building measures.

The framework describes three essential functions to attain security and trustworthiness in ICT supply chains:

- **Assurance** comprises actions—policies and processes—taken to provide ICT security.
- **Transparency** reveals the extent to which ICT vendors meet their assurance commitments and contractual obligations.
- **Accountability** addresses consequences for failure to meet assurance or transparency requirements through enforcement or deterrence.

The framework further differentiates between three fields of action:

- **Organization:** Individual ICT buyers need to start a conversation about supply chain risk and produce their own risk-informed procurement requirements. An individual organization should assess its supply chain, risk tolerance, and purchasing needs. Based on this assessment, and informed by standards and best practices where available, it should determine risk-informed procurement requirements.
- **Industry:** Organizing like-minded ICT buyers—within an industry sector or a subsector—enables them as a group to leverage purchasing power to create demand-side pressures and provide guidance to buyers, operators, and vendors about their functionality, security, and transparency requirements. Such industry groups should produce recommended procurement requirements for their members. Over time, these requirements will clarify legal due care and due diligence obligations and may provide valuable input to potential regulatory actions.
- **Ecosystem:** Realities of distributed ICT supply chains and a growing number of threat vectors warrant regional and global mechanisms to address ICT security and trustworthiness. Regional transparency mechanisms and testing regimes allow for new visibility into vendors’ security and transparency practices. Global conformance programs based on agreed-upon certification schemes allow for a one-time attestation to be relied on by many stakeholders in the ICT ecosystem.
The table on this page provides an overview of the framework’s components and the respective measures that implement the assurance, transparency, and accountability functions.

**Action Roadmap**

To supplement the framework, a whole-of-society approach is needed to effectively address ICT supply chain risk, while minimizing the negative effects of TechNationalism. Addressing primary action points for buyers, operators, and vendors, the framework—aligned with supply chain-focused enterprise risk management—will contribute to improved levels of confidence and trustworthiness in ICT products and services. Balanced government policy measures that may further ICT and supply chain security, in accordance with national and industry-specific policy goals, include the following:

- **Threat and vulnerability information sharing** allows the ICT industry, ICT buyers and operators in particular, to take mitigation measures against third party threats and significant vulnerabilities in global supply chains.
- **A multiple sourcing requirement** that recommends establishing a dependence limit for key critical infrastructure operators ensures diversity of suppliers and solutions and increases resilience.
- **Strategic science and technology investments** through government-funded research and development (R&D) strengthens domestic technology development and decreases foreign dependence.
- **Narrow national security exceptions**, in accordance with international agreements, provide ways to exclude foreign entities to protect sensitive national security-relevant functions.
- **National supply chain security policies and goals**, when regularly reviewed and adapted, strengthen a government’s overall cybersecurity efforts.

<table>
<thead>
<tr>
<th>Component 1</th>
<th>Organization: Risk-informed Procurement Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Security Development Lifecycle</td>
</tr>
<tr>
<td></td>
<td>Software Quality Assurance</td>
</tr>
<tr>
<td></td>
<td>Secure Configurations</td>
</tr>
<tr>
<td></td>
<td>Operational Security Procedures</td>
</tr>
<tr>
<td></td>
<td>Secure Software Delivery and Distribution</td>
</tr>
<tr>
<td></td>
<td>Security Vulnerability Management</td>
</tr>
<tr>
<td></td>
<td>Security Testing and Assessments</td>
</tr>
<tr>
<td></td>
<td>Transparency Reports</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Component 2</th>
<th>Industry: Buyer-led Security Requirements for ICT Vendors</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Software Bill of Materials</td>
</tr>
<tr>
<td></td>
<td>Security Vulnerability Remediation</td>
</tr>
<tr>
<td></td>
<td>Statement of Cyber Supply Chain Risk Practices</td>
</tr>
<tr>
<td></td>
<td>Declaratory Letter of Board</td>
</tr>
<tr>
<td></td>
<td>Consortium for ICT Security Assessment</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Component 3</th>
<th>Industry: Vendor-led Assurance and Transparency Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>International Standards and Norm Setting</td>
</tr>
<tr>
<td></td>
<td>Independent Evaluation and Testing</td>
</tr>
<tr>
<td></td>
<td>Coordinated Vulnerability Disclosure</td>
</tr>
<tr>
<td></td>
<td>Bug Bounty Programs</td>
</tr>
<tr>
<td></td>
<td>Industry Security Evaluation and Accreditation Schemes</td>
</tr>
<tr>
<td></td>
<td>Joint Oversight Board</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Component 4</th>
<th>Ecosystem: Regional Transparency Centers</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Regional Transparency Centers</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Component 5</th>
<th>Ecosystem: Global Conformance Programs</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Global Conformance Programs</td>
</tr>
</tbody>
</table>

**Table: Components and Measures of the Framework**
Information and communications technology (ICT) is strategic for a nation’s economy, security, and identity. Nevertheless, exploitable vulnerabilities in ICT and complex, difficult to secure supply chains are raising security concerns in the public and private sectors. National governments, particularly, are paying increased attention to the possibility that foreign governments might taint ICT through global supply chains, either by coercing a local supplier to cooperate or by gaining direct access to its operations. Framed as a national security threat, several governments have warned against, or restricted the use of certain foreign ICT products and services in their domestic markets— with the stated intention of protecting against such risks.

1 In a world with global ICT supply chains, asking whether a firm is domestic or foreign is a vexing, perhaps misleading question. The “U.S.” technology company Microsoft, for instance, is headquartered in Redmond, WA; operates in over 190 countries; has research and development centers in China and India; data centers in Ireland, Singapore, and the Netherlands; and offices in India, China, France, Canada, Australia, Germany, and Japan. Its workforce of more than 130,000 people is diverse in terms of culture, ethnicity, religion, and nationality. The company’s sales are almost evenly split between the U.S. and the rest of the world. What makes this company an American versus a European or an Asian company?  

2 Australia, China, member states of the EU, Russia, and the U.S., among others, have considered or deployed such measures.

The report refers to this widening policy tendency and actions as technology nationalism or TechNationalism, which we define as:

Government policies or actions that directly or indirectly favor ICT products and services sold by companies headquartered domestically or in allied states over those headquartered in states seen as competitors or adversaries. TechNationalism in the global ICT market reflects state interests such as national security, cybersecurity, economic competitiveness, innovation, prestige, and geopolitics.

At the heart of the policy controversy surrounding TechNationalism is the concept of country of origin: can a technology coming from a supplier headquartered in another country be secure and can its deployment be free from adversarial influence by the host government? The key issue is whether the host government is able to exercise command over the technology through forced modification or tainting of products.

3 This boils down to the following questions that motivated this report: (1) can products be tainted by a supplier in a way that cannot be found by testing, and, if so, can the risk be mitigated by the operators and buyers? and (2) can national policies and processes be implemented to provide assurance that the supplier cannot improperly be used as a channel for attacks by the host government?

Introduction

TechNationalism in the global ICT market reflects state interests such as national security, cybersecurity, economic competitiveness, innovation, prestige, and geopolitics.
The goal of the report is threefold: first, to present a framework that allows ICT buyers and operators in the private and public sectors to address legitimate concerns about cybersecurity and supply chain risk objectively and transparently. Second, to address individual and shared responsibilities among vendors, buyers, and operators regarding security and resilience in the ICT ecosystem. Third, to minimize adverse consequences from limitations or exclusions by advancing robust, verifiable risk mitigation measures as an alternative approach. Security and enhanced trust in global ICT supply chains contribute to three beneficial outcomes: (a) improved cybersecurity, (b) easing geopolitical trade and security tensions, and (c) widening the deployment of advanced and secure ICT into a global infrastructure enabled by enhanced competition.

In the face of threats to the integrity of supply chains and the security of ICT, several governments have proposed or taken measures targeting foreign companies with the intention of addressing such concerns. Statutory, regulatory, economic, diplomatic, or administrative in nature, these measures may include requiring companies to localize data processing and storage; giving preference to domestic products or components; subjecting foreign companies to enhanced requirements characterized as security-related, such as ordering them to make source code available for inspection; requiring foreign companies to partner with domestic entities to gain market access; and banning specific foreign products or companies. The effects of such measures are difficult to predict due to the ICT industry’s tight integration and numerous dependencies on key technologies, patents, and licensing arrangements. Such measures distort markets and may hamper innovation and competition. As a result, trade and foreign relations are suffering. Instead of protecting against legitimate threats, these measures may create a world with separate, fragmented, and partially or fully decoupled technological and economic universes that endanger long-term global economic development and growth.

Motivated by mounting tensions surrounding global supply chains, ICT security and the use of restrictive, protectionist measures, this report provides policymakers, regulators, and corporate executives with a balanced view of ICT security and trustworthiness. It provides a framework for addressing risk—through measures of assurance, transparency, and accountability—and managing it in a way consistent with national security, cybersecurity, and trade and industrial competitiveness objectives. To that end, this report:

- Analyzes the initial conditions and drivers underlying TechNationalism;
- Lays out a set of principles and a framework for ICT security and trustworthiness; and
- Provides a high-level action roadmap.

It is important to note that protectionist tendencies are not limited to the ICT industry, even if 5G network build-ups in Western countries and their dependence on mostly China-based manufacturers come to mind as current examples of TechNationalism. Aside from referencing examples of particular technologies, the report is technology agnostic and broadly applicable to strategic ICT.

---


7 Others have analyzed particular strategic technologies and assessed national security and economic implications. For 5G technologies, see, Jan-Peter Kleinhans, 5G vs. National Security, Stiftung Neue Verantwortung, (February 12, 2019), https://www.stiftung-nv.de/de/publikation/5g-vs-national-security.
Drivers and Conditions of TechNationalism

This report argues that verification—through appropriate measures across the supply chain by vendors, operators, and buyers—is essential to the security and safety of ICT products and services.

ICT—which includes hardware and software components, services, related processes, and data—is subject to cybersecurity threats, including the degradation or loss of confidentiality, integrity, and availability. ICT products and services are sourced, designed, built, assembled, distributed, and serviced by entities throughout the global supply chain.

Global supply chains embody the intricacy and complexity of globalization and international trade. While global markets have contributed to massive growth in the ICT industry, the underlying reconfiguration, disintegration, and virtualization of the industry have transformed many hierarchical structures into loosely coordinated networks, rendering tight control over production and assembly illusive. Furthermore, the increasing complexity of ICT operations and the shift of business models towards services (e.g., software-as-a-service, or SaaS) have resulted in intertwined ICT vendor-buyer relationships and ongoing interactions to execute business operations. Telecom carriers, for example, rely increasingly on 5G infrastructure vendors to operate their core network. This warrants broad conversations on individual and shared responsibilities between, on the one hand, telecom and mobile operators—the ICT buyers and operators—and on the other, equipment suppliers—the ICT vendors—regarding the secure and safe deployment, operation, and maintenance of ICT.

As the key components of world politics—incidents of power, conflict and competition, violence, and war—increasingly manifest via cyber venues, risks from exploitable ICT and undependable supply chains have climbed...
up the global affairs agenda. Consequently, states have tried to find ways to assert their sovereignty, as well as exercise control over new technologies and data to protect national security and ensure economic competitiveness, by putting supply chain security front and center. In the U.S., for example, a May 2019 presidential executive order prohibits some businesses from using ICT products or services, in which any foreign country or a national thereof has any interest” that may compromise national security. The U.S. Department of Homeland Security has established an ICT Supply Chain Risk Management Task Force to partner closely with industry on supply chain security, while the U.S. National Institute of Standards and Technology (NIST) has revised its Cybersecurity Framework to explicitly address supply chain risk.

The following dynamics are shaping the rise of TechNationalism:

- Increasing nationalist and isolationist tendencies—including sentiments against globalization and diminished trust in the multilateral system—are undermining the post-World War II order based on adherence to international norms, laws, and multilateral agreements.
- Resurfacing protectionism and mercantilism are furthering the weaponization of trade as a means to achieve geopolitical objectives.
- Tightly controlled, state-centric models of Internet governance are being established as cyberspace is elevated to a matter of “high politics.” The gap between states’ interpretations of sovereignty, as applied to cyberspace, is widening. Even in democracies, the open and free Internet is under pressure

Supply Chain Definition

The system of organizations, people, activities, information, and resources involved in the full lifecycle of a product or service from development, to delivery from a supplier to a customer, to post-deployment servicing (e.g., maintenance and updates), and decommissioning. Supply chain activities or operations involve the transformation of raw materials, software and hardware components, code, and intellectual property into a product or service for the end customer and necessary coordination and collaboration with suppliers, intermediaries, and third party service providers.


11 U.S. provisions apply only to U.S. government entities, entities funded by the U.S. government, and businesses that require U.S. government licenses. Other states’ policies, including China’s, seem broader at first, although the actual applicability is not always clear in practice.


as controls over content and restrictions on free expression are growing in the face of extremist and terrorist Internet activity.

- Cyberspace has become a new domain of interstate conflict, where states conduct cyber operations that may target supply chains; engagement in hybrid warfare takes place in a grey zone below the threshold of armed conflict.16

## Trade-offs Among Security and Economic Goals

In their efforts to ensure ICT security and trustworthiness, states must balance the following goals:

1. **National security**;
2. **Cybersecurity**; and
3. **Trade and industrial competitiveness**.

States must take appropriate measures and, in some cases, make trade-offs to bring risk to an acceptable level. Given tightly-coupled global supply chains and competition in innovation critical to ICT, restrictive, unbalanced measures may lead to unintended, adverse effects on security and economic goals. For example, heightened restrictions on foreign ICT firms in an attempt to mitigate national security concerns could, as a byproduct, reduce overall cybersecurity (e.g., due to a lack of diverse ICT supply) and industrial competitiveness (e.g., due to an inability to leverage economies of scale in ICT production and the elimination of competitive forces).

State-sponsored cyber activities that are regarded as key threats to national security include theft of strategic technologies, espionage, and reconnaissance, as well as cyber operations that could cause damaging cyber-physical effects, such as disabling 5G communications networks or destroying critical infrastructure.17 A common national security concern is that entities headquartered in foreign jurisdictions are subject to influence by their host governments. This creates the potential for state-directed modifications to technology and data originating in or processed in the foreign country with the purpose of enabling adversarial foreign policy, intelligence, or military interference in domestic affairs.18

---


18 E.g., China’s 2017 National Intelligence Law has been purported as providing the Chinese government with a lever to legally force a China-based manufacturer or operator to secretly share information about service operations in a foreign country or interfere with them. “What you need to know about China’s intelligence law that takes effect today,” Quartz, (June 28, 2017), https://qz.com/1016531/what-you-need-to-know-about-chinas-intelligence-law-that-takes-effect-today/.

Western intelligence and surveillance laws with broad authorities include the UK Investigatory Powers Act (IPA) or the U.S. Foreign Intelligence Surveillance Act (FISA). The 2013 Snowden disclosures brought to light the U.S. government’s ability to work covertly with U.S. companies to exploit global ICT infrastructure for large scale intelligence and surveillance purposes.
Certainly, there are legitimate national security concerns stemming from reliance on insecure, vulnerable, or tainted ICT products and services (see Figure 1). Even after applying appropriate risk mitigation measures, residual risk must be managed effectively and weighed against the benefits of ICT. Strict security requirements and compliance audits, among a range of other assurance, transparency, and accountability measures, can help to mitigate this risk. For particularly sensitive technologies that enable organizations to perform core national security or defense functions, governments and their industry partners have already dedicated and, to some degree, established specially protected supply chains in relevant domains in order to assure that national security and defense technologies are delivered uncompromised (e.g., use of trusted chip foundries for the highest risk systems; and, in some cases, reviews of sensitive transactions to assess national security implications of foreign investments).  

One touted policy option is the complete decoupling of supply chains from adversaries to create separate technological ecosystems. The unwinding of deeply-interlocked supply chains remains untested. It would inevitably come with steep economic costs, and some experts question its feasibility. It may not be possible for a country or region to fully decouple from underlying key technologies for economic reasons. The manufacturing of semiconductors, for instance, requires huge capital investments. In addition, the dual needs for experience in design and manufacturing to meet quality standards and innovate for the next generation of computer chips exacerbates this high barrier for new market entrants.

Cybersecurity—the availability, integrity, and confidentiality of ICT—is critical to trustworthiness. Vulnerabilities weaken cybersecurity with wide-ranging implications for not only the application of ICT but society at large, for instance, when they result in financial or physical harm due to compromised critical systems. While unintended vulnerabilities are a reality in complex software, deliberately placing security weaknesses is a malicious act. The growing complexity in software and hardware requires developers and manufacturers to apply secure development processes; after-the-fact testing will not assure ICT security or safety. Security is not an absolute property, but if carefully operated and managed, ICT can be used with an acceptable level of risk.

The need to foster innovation to remain competitive and generate economic growth is a common element of national plans to foster trade and industrial competitiveness. Governments have devised national innovation, R&D, and industry strategies and roadmaps that illustrate their ambitions for global leadership in strategic technologies. They expect their country to reap significant economic and military gains from reaching these goals. Concurrently, states have adopted nationalistic measures to protect or strengthen their domestic industries. Furthermore, some states see a growing need for a domestic ICT industry to ensure strategic autonomy, geopolitical power, and security as their options for action are increasingly shaped by foreign ICT giants.

---


21 E.g., Germany’s Industry 4.0 strategy and China’s Three-Year Action Plan for AI and Made in China 2025 strategy.


Supply Chain Risks for Information and Communications Technology

Malware Embedded Within Software Security Tool (2017)
Malicious actors attacked a security software company by infiltrating its network and inserting code into security software. Installs and updates to the application landed in millions of personal computers. The attack predominately targeted IT company networks.

Hijacked Cellular Devices (2016)
A foreign company designed firmware used by a U.S. cell phone manufacturer. The phones made encrypted records of text and call histories, phone details, and contact information and transmitted that data to a foreign server every 72 hours.

Counterfeits Sold to U.S. Navy (2015)
A U.S. citizen imported thousands of counterfeit integrated circuits from China and Hong Kong and resold them to U.S. customers, including defense contractors, who then supplied them to the U.S. Navy for use in nuclear submarines.

Sensitive Federal Data Loss (2010)
An internal audit discovered that a federal agency was selling computers containing proprietary information. Certain devices failed sanitation verification tests and resulted in the release of sensitive federal agency data.

Figure 1: Supply Chain Risks for Information and Communications Technology

24 Adapted excerpt from U.S. Department of Homeland Security, Supply Chain Risks for Information and Communication Technology, (December 2018), https://www.cisa.gov/sites/default/files/publications/19_0424_cisa_nrmc_supply-chain-risks-for-information-and-communication-technology.pdf. None of these cases have been attributed to state or state-sponsored activity.
Conditions Underlying TechNationalism

Subject to geopolitical dynamics and tensions, four initial conditions complicate building trust and enhancing ICT security:

1. **Challenges of securing supply chains**;
2. **Importance of strategic ICT**;
3. **Challenges of securing ICT**; and
4. **Limits to accountability**.

The **challenges of securing supply chains** comprehensively and end-to-end—due to their complex, distributed, and global nature—contribute to heightened real or perceived national security concerns over foreign ICT and with it, the rise in TechNationalism. To ensure security, physical and software components must be traceable in the supply chain. Suppliers must be able to demonstrate the authenticity and integrity of these components throughout their entire lifecycle. The combination and reuse of commercial and open source ICT components in modern products and services has also increased complexity and third party risk.

For the bulk of microelectronics needed in defense applications, states depend heavily on commercial domestic and foreign manufacturers. States have adopted approaches that seek to recreate key portions of supply chains domestically or relocate them to areas deemed “safe.” A more practical approach, however, is to improve ICT supply chain security. In this vein, the U.S.

---

25 Traceability (i.e., software or data provenance), authenticity (i.e., software code being identical to the original), and integrity are necessary, but not sufficient, conditions to ensure ICT security. Even if these conditions are met, the component can still be vulnerable, either by malice or error. It must also be demonstrated that a component was created by a trusted, non-malicious entity that effectively deploys security best practices throughout the ICT lifecycle. Combined, these conditions constitute a high bar for trust and cybersecurity in global ICT supply chains.

Department of Defense (DoD) is in the process of strengthening contractors’ cybersecurity practices through required vendor certification.\footnote{27}{Once implemented, the Cybersecurity Maturity Model Certification (CMMC) will be used for contract solicitations and auditing contractors’ compliance with the CMMC. “DOD’s Cybersecurity Maturity Model Certification and Draft CMMC Model Framework,” Thompson Hine, (September 17, 2019), \url{https://www.thompsonhine.com/publications/dods-cybersecurity-maturity-model-certification-and-draft-cmmc-model-framework}.} The importance of strategic ICT to economic prosperity and military power puts the Internet of Things (IoT), 5G communications, artificial intelligence (AI), cloud and high performance computing, quantum computing, microelectronics, robotics, and critical data squarely into a strategic domain.\footnote{28}{U.S. Department of Defense, DoD Digital Modernization Strategy: DoD Information Resource Management Strategic Plan TV19-23, (Washington D.C., July 12, 2019), \url{https://media.defense.gov/2019/Jul/12/2002156622/-1/-1/1/DOD-DIGITAL-MODERNIZATION-STRATEGY-2019.PDF}.} Referred to as the fourth industrial revolution, it is predicted that the convergence of these new technologies will unleash enormous economic growth.\footnote{29}{Klaus Schwab, \textit{The Fourth Industrial Revolution}, (New York: Crown Business, 2017).}

Similarly, in the national defense domain, AI and other strategic ICT—in combination with hypersonics and directed energy weapons—though potentially destabilizing, are anticipated to be critical for future military power and modern warfare.\footnote{30}{Technological superiority through investments in science and technology research has been at the core of U.S. military dominance. Robert L. Paarlberg, “Knowledge as Power: Science, Military Dominance, and U.S. Security,” \textit{International Security}, 29(1), (2004) 122-151.} Not only providing the foundation for future science and technology breakthroughs, strategic ICT could also embolden technological leaders to attempt to seize global economic leadership or military supremacy.

A state’s ability to exercise some level of control over the development and deployment of these technologies—including their secure, reliable functioning—is now routinely considered crucial to preserving strategic autonomy. The European Union, for example, recognizes that “those who control digital technologies are increasingly able to influence economic, societal and political outcomes,” emphasizing the need for digital sovereignty as a precondition for security and trustworthiness.\footnote{31}{European Political Strategy Centre, \textit{Rethinking Strategic Autonomy in the Digital Age}, (2019).} In the same vein, China has embarked on efforts to develop “indigenous and controllable core cybersecurity technology”\footnote{32}{Samm Sacks, \textit{Telecommunications, Global Competitiveness, and National Security}, Written statement before the House Energy and Commerce Subcommittee on Communications and Technology, May 16, 2018, \url{https://docs.house.gov/meetings/IF/IF16/20180516/108301/HHRG-115-IF16-Wstate-SacksS-20180516-U21.pdf}.} aimed, in part, at bolstering the use of domestic ICT, reducing its dependency on foreign technology suppliers, and replacing foreign with Chinese-made software.\footnote{33}{For example, Microsoft’s Windows 10 China Government Edition has received the designation “secure and controllable” in China. Yuan Yang and Nian Liu, “Beijing orders state offices to replace foreign PCs and software,” \textit{Financial Times}, (December 8, 2019), \url{https://www.ft.com/content/b55f6ee-1787-11ea-8d73-6303645ac406}.} With the government and private sector’s growing dependence on ICT for critical functions, the challenges of securing ICT are a foundational cybersecurity problem. Exploitable vulnerabilities are frequently found even in products and services created by trusted entities committed to delivering secure ICT. Even products without a doubtful provenance may, in the future, pose a difficult-to-manage risk.

The exploitation of security vulnerabilities by states or cyber criminals can and have resulted in the alteration of data, the destruction or disabling of critical infrastructures, and the denial of access, with significant financial, physical, and political harm. Cybersecurity is also undermined when governments secretly withhold notification of hardware and software security vulnerabilities to husband those for future intelligence or law enforcement needs.\footnote{34}{The White House, \textit{Vulnerabilities Equities Policy and Process for the United States Government}, (November 15, 2017), \url{https://www.whitehouse.gov/sites/whitehouse.gov/files/images/External%20-%20Unclassified%20VEP%20Charter%20FINAL.PDF}.} Several governments purchase zero-day exploits for this purpose.\footnote{35}{While the withholding and purchase of zero-day exploits by governments have received significant attention, it is important to recall that sophisticated attackers first exploit user carelessness, misconfiguration, and known, unpatched vulnerabilities before they target undiscovered zero-day vulnerabilities. Rob Joyce, “Disrupting Nation State Hackers,” USENIX Enigma, San Francisco, January 27, 2016, \url{https://www.usenix.org/node/194636}.}
The nature of global ICT supply chains can make it difficult to attribute malicious or negligent actions to a specific actor or to pinpoint where a defective ICT component or software vulnerability was introduced. The limits to accountability affect the way actors can be deterred or held liable for malicious or negligent actions. States are known to target, taint, and tamper with adversaries’ ICT as part of military and intelligence operations.36 To combat this, multilateral and multistakeholder efforts are underway in the United Nations and elsewhere to advance norms of state behavior that could benefit ICT supply chain security and resilience.37 This work is aided by collective corporate efforts to protect customers and enhance cybersecurity.38

The adoption and enforcement of widely recognized norms and, most critically, mechanisms to hold malicious actors accountable, remains an active area of development. Progress on issues such as attribution and agreeing on appropriate punishment for violators, however, has been slow.39


The factors outlined above have led some states to take measures to restrict access to and exercise control over ICT. While the intent is for such measures to increase security, they have significant downsides.

Restrictive Measures

Bans and restrictions of technologies or vendors based on country of origin have recently received broad public attention. The U.S. government took action based upon alleged threats to national security from foreign ICT in U.S. communications networks and federal IT systems. Primary examples include U.S. bans against Chinese 5G network equipment manufacturers Huawei and ZTE (along with proposals to ban additional Chinese companies), and Russian anti-virus technology company Kaspersky. Governments may also enforce targeted restrictions on specific domains of application (e.g., critical infrastructure) or require the use of domestically designed and manufactured modules for critical functions, such as add-on encryption functions or lawful intercept capabilities in telecom networks equipment. Furthermore, foreign software and hardware for critical or sensitive applications have been subject to government-mandated technical reviews and audits based on technical security requirements. China’s 2017 Cybersecurity Law (CSL) and related regulations established a comprehensive review regime that appears to require the disclosure of proprietary code as part of mandated reviews.

technical verification and testing. Under Russia’s non-disclosed functionality (NDF) regime, vendors of systems that process “confidential information” are required to obtain a certification.\textsuperscript{44} Mandating adherence to domestic technical standards that are not in compliance with international standards and best practices is yet another measure in TechNationalism’s toolbox. Regarding data specifically, data localization requirements mandate that service providers process or store data in the local jurisdiction where the service is offered. Such laws have spread widely in recent years.

Export controls provide another way to restrict specified technology from dissemination to a state’s adversaries. Under the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods, the export of certain dual-use technologies requires a government-issued license. Regulating trade relations, tariffs, and security and privacy requirements in trade agreements can act as trade barriers.\textsuperscript{45} Although the World Trade Organization (WTO) prohibits trade discrimination against a country, it allows for an exemption from trade rules when a state’s essential security interests are at stake.\textsuperscript{46}

Foreign acquisitions of a majority or minority stake of domestic firms with access to strategic, cutting-edge technologies can be subject to investment restrictions. For example, the U.S. Committee on Foreign Investment (CFIUS) screens pending foreign investments for national security implications. Review findings, however, may lead to no restrictions or to risk mitigation measures that allow the acquisition to proceed. Other governments, including Australia, Canada, China, the EU, France, Germany, Japan, and the UK have, or are considering, investment review regimes related to national security. Foreign acquisitions might also be subject to ownership limitations due to license requirements and other restrictions. For example, license requirements necessitated U.S. cloud providers partnering with domestic entities to accept limited ownership in order to enter the Chinese market.\textsuperscript{47} Moreover, regulatory ambiguity has, in some cases, led to forced technology transfer or resulted in relinquishing operations to the Chinese partner in an attempt to comply with changing Chinese laws.

Deficiencies and Unintended Consequences

Legitimate national security concerns may justify strict, targeted measures based on accurate threat assessments. Nevertheless, the measures some governments are utilizing to restrain or control foreign ICT can produce unintended effects with negative implications. Designed for another era and for more limited purposes, these policy measures now target companies deemed to constitute a broadly defined national security threat. These measures are not only inadequate, but their full effect remains uncertain. Inadequate measures may cause downstream effects in the

---


\textsuperscript{45} The WTO’s Information Technology Agreement 1 (ITA1) and Information Technology Agreement 2 (ITA2) are designed to increase market access and reduce or discard trade tariffs, thus reducing TechNationalism as they promote global ICT trade. The ITA sets tariffs on ICT products to zero by default. World Trade Organization (WTO), Information Technology Agreement. https://www.wto.org/english/tratop_e/inftec_e/inftec_e.htm.


\textsuperscript{47} Executive Office of the President, Office of the United States Trade Representative, Findings of the Investigation into China’s Acts, Policies and Practices Related to Technology Transfer, Intellectual Property, and Innovation under Section 301 of the Trade Act of 1974, (March 22, 2018), https://ustr.gov/sites/default/files/Section%20301%20FINAL.PDF.
Deficiencies and other unintended consequences of TechNationalism manifest in several ways. First, bans can motivate technology companies in one country to “design out” key technologies supplied by companies headquartered elsewhere. Such restrictions can decrease R&D investments—in some cases, substantially—if access to large markets is reduced significantly. Furthermore, innovation in industry sectors accustomed to competition may suffer in the long term; the reduced number of suppliers of goods and services is likely to result in less competition and higher prices. A delayed 5G rollout, or one with suboptimal technologies, may lead to significant long-term costs in the form of missed innovation opportunities and economic growth. Other measures, such as country-specific security and technical requirements, can be expensive and result in significant administrative burden and compliance costs. This might require foreign companies to redesign products and services or disclose trade secrets, putting them at a competitive disadvantage and reducing competition overall. Excessive compliance costs can amount to a de facto ban. Furthermore, strict requirements based on domestic standards, costly technical conformance, and domestic ownership requirements, among others, create lock-in effects, which might raise fears of such dependencies being leveraged to give undue influence in an interstate dispute. Finally, investment restrictions reduce foreign capital inflow in emerging domestic industries. Table 1 provides an indicative assessment of the direct effects of such restrictive measures.
4 Assurance, Transparency, and Accountability Framework

This section describes a multi-component assurance, transparency, and accountability framework to address ICT security and trustworthiness. Six principles designed to establish a transparent, risk-informed, and level playing field for the global ICT marketplace inform this framework.

The framework provides an objective basis for establishing confidence in a vendor and the security of its ICT products and services through technical, organizational, and confidence-building measures. The framework structures primary action points for the ICT industry, in particular, buyers, operators, and vendors directly involved in commercial supply chain transactions, with the objective to minimize the negative effects of TechNationalism. Complementing the framework, the action roadmap in Section 5 outlines measures pertinent to the wider ICT ecosystem in the purview of policymakers and regulators.

ICT Market and Risk Reduction Principles

This set of risk reduction principles describes a transparent, risk-informed, and level playing field for the global ICT marketplace. These principles are as follows:

1. Maintain an open market that fosters innovation and competition and creates a level playing field for ICT vendors. Avoid the creation of trade barriers.

---

48 Under ICT vendors, this report subsumes manufacturers, vendors, and service providers that produce and sell ICT products, services, or components to buyers and operators who buy, consume, or further process them. An organization can concurrently take on the role of a vendor and a buyer/operator.

2. Create procurement practices and requirements that utilize **fact-driven, risk-informed, and transparent requirements** based on international standards and approaches.

3. **Evaluate the practices** of ICT vendors in terms of product and service integrity, including code sharing and inspection through trusted third parties for critical and widely-used commercial-off-the-shelf (COTS) software and service platforms.

4. Create and use tools and approaches to **address risk** with effective, **cost-efficient risk mitigation measures** and **prioritize cybersecurity investments**.

5. Avoid developing domestic cybersecurity standards and requirements where effective **international standards** already exist and have been widely adopted.

6. Establish **norms for global ICT supply chain security**, accompanied by effective confidence-building measures, to provide an objective and transparent basis for trust among stakeholders across the global ICT ecosystem.

While both public and private sector entities procure ICT products and services, only states can address principles 1 and 5. State action must push principles 2, 3, 4, and 6—in concert with the private sector—throughout the ecosystem.

**Trust as a Condition for Assurance**

Purchasing ICT components, products, and services comes with uncertainty, risk, and dependencies. Buyers have limited control or influence over the cybersecurity behavior and practices of manufacturers, vendors, and service operators and their respective suppliers and subcontractors. Thus, ICT buyers and operators must take defensive measures to reduce supply chain risk coming from potentially unreliable suppliers, vulnerable ICT, and insecure operations.\(^{50}\) Such measures, however, do not achieve “complete” assurance.\(^{51}\) At best, they provide confidence that risk is at an acceptable level. Trust must overcome the remaining gap.\(^{52}\) This should not, however, necessitate ICT buyers take a “leap of faith.” Appropriate, verifiable measures provide a level of confidence for effectively mitigating third party risk. These measures are not free, and risk mitigation must be cost effective (i.e., the additional burdens of minimizing supply chain risks must not be excessive and disadvantage small, innovative firms). Importantly, an intangible element of trust remains crucial to reach a high level of confidence in an organization. Where trust—in a company or a country—does not exist, technical and organizational measures to strengthen confidence will have limited effectiveness. While a combination of measures is needed to provide a basis for trust, in some cases, the level of trust needed to rely on a particular supplier may be unachievable or too costly. Political and diplomatic means in the form of confidence-building measures may help to close the remaining trust gap. Figure 2 describes this relationship.

Lastly, in the quest to address assurance, it is critical to untangle questions about the overlapping responsibilities of ICT buyers, service operators, and vendors regarding cybersecurity and risk mitigation. Complex ICT buyer-vendor relations in the deployment of products and services can obscure responsibilities, especially those that are shared. This framework

\(^{50}\) Note that the measures themselves are risk-informed. Depending on an organization’s strategic objectives and risk tolerance, the ICT buyer will derive risk-informed security objectives for a particular domain of ICT applications and deploy risk mitigation and resilience measures accordingly. In other words, a low-risk business domain requires fewer or less strict measures to reach a sufficient level of assurance and trust.

\(^{51}\) Note that “complete” assurance does not exist: it would indicate zero risk, which is a theoretical rather than a practical goal. Reducing risk so significantly, through expensive risk mitigation measures, would not likely pass standard cost-benefit analysis.

\(^{52}\) Trust and willingness to work together are essential preconditions for the framework. Risk from ICT insecurity is managed through risk mitigation measures. In practice, no measures can fully substitute trust and provide complete assurance to the point where complex supply chain interactions can occur in a no-trust, adversarial environment.
The Framework and Its Core Components

The following section describes a strategy to move toward a framework that provides an objective and transparent basis to manage risk, strengthen security, and determine ICT trustworthiness. It consists of five components, each crafted to provide assurance, transparency, and accountability. The framework’s integrated approach requires multiple measures across different fields of action. Detailing such a framework will assist ICT buyers, operators, and vendors to implement these measures and strengthen related requirements over time.

Assurance, transparency, and accountability are essential to attaining security and trustworthiness in ICT supply chains:

- **Assurance** comprises actions—policies and processes—taken to provide ICT security. Vendors must demonstrate conformance to security objectives and requirements—in accordance with best practices and international standards—so that buyers and operators can rely on these measures to counter risks effectively.

- **Transparency** reveals the extent to which ICT vendors meet their assurance commitments and contractual obligations. Lack of transparency lowers confidence in these matters as it may mask complacency, inadequate security, or neglect of remediating vulnerabilities. Thus, without sufficient transparency, shaping the behavior of vendors or holding them accountable is difficult.

- **Accountability** addresses consequences for failure to meet assurance or transparency requirements through enforcement or deterrence. Accountability is a precondition to providing effective assurance for ICT buyers and requires an appropriate level of transparency.

The framework further differentiates between three fields of action:

- **Organization**: Individual ICT buyers need to examine their own supply chain risk and produce risk-informed procurement requirements. Aided by international standards and best practices, an individual organization should assess its supply chain, risk tolerance, and purchasing needs to determine risk-informed ICT procurement requirements.

- **Industry**: Organizing like-minded ICT buyers—within an industry sector or a
subsector—enables them to leverage purchasing power as a group to create demand-side pressure and provide guidance to buyers, operators, and vendors for their functionality, security, and transparency requirements. Such industry groups should produce recommended procurement requirements for their members, subject to voluntary self-attestation. Over time, these recommended procurement requirements will become de facto, and in some cases, de jure standards, clarifying legal due care and due diligence obligations and providing valuable input to potential regulatory actions.

- **Ecosystem:** Distributed ICT supply chains and a growing number of threat vectors warrant regional and global mechanisms to address ICT trustworthiness. Regional transparency mechanisms and testing regimes allow for new visibility into ICT vendors’ security and transparency practices. Global conformance programs, based on agreed-upon certification schemes and evaluation concepts, allow many stakeholders in the ICT ecosystem to rely on a one-time assessment, reducing costly individual testing and time-to-market periods.

The framework can help to move ICT on the path toward an objective and transparent basis for trust. An in-depth risk assessment and analysis of the ecosystem and its key stakeholders must inform industry-specific risk mitigation measures.\(^53\) Indicative rather than comprehensive, the framework provides a coarse taxonomy to discuss and determine which specific set of mitigation measures may be most appropriate for ICT buyers, vendors, and operators in managing individual and shared responsibilities regarding supply chain risk. Table 2 provides an overview of the framework; the following subsections describe the framework’s components and measures.

**Component 1—Organization: Risk-informed Procurement Requirements**

ICT buyers must make cybersecurity best practices and security baselines an integral part of their procurement requirements and service delivery agreements. Input from industry associations, government entities, trusted companies, and private experts should inform best practices and baseline requirements that may be sector-specific or applicable across similar industries. Examples include the European Union Agency for Cybersecurity (ENISA) baseline security recommendations for IoT,\(^54\) and the Charter of Trust’s baseline requirements for supply chain security.\(^55\) Often codified in best practices, security and privacy guidelines can provide voluntary, industry-specific directives.\(^56\) Ideally, security-related procurement requirements across multiple

---


buyers will incentivize the ICT industry to improve ICT security in products and services over time.

These best practices and baseline requirements can inform due diligence requirements individual organizations must incorporate to ensure ICT security and mitigate risk. Complementing procurement requirements, corporate purchasing policies may, for example, prescribe a dual-vendor or multi-vendor sourcing approach for critical components to reduce risk, but also to enhance negotiation power, price competition, access to innovation, and technology choices. Individual organizations should press ICT vendors to adhere to the following processes, measures, or activities when purchasing ICT.

Security must be an essential consideration throughout the entire development process, rather than an afterthought. ICT products and services must include built-in security from the start. For example, the security development lifecycle (SDL) describes a set of practices and activities to enhance security throughout the ICT lifecycle, including, among others, the need to define security requirements, perform threat modeling, use cryptography standards, manage the security risk from third party components, conduct static and dynamic testing, perform penetration testing, establish an incident response process, and conduct security training. To that end, SDL practices are mapped to the software development life cycle (SDLC). For example, ISO Standard 27034 (under development) provides guidance for implementing secure development lifecycle processes, and IEC 62443 specifies such secure development lifecycle requirements for

---

57 Ben Rossi, “When two vendors are better than one – Gartner,” *Information Age* (September 3, 2014). https://www.information-age.com/when-two-vendors-are-better-one-gartner-123458431/.

industrial automation and control systems.\textsuperscript{59} SAFECode, an industry association promoting best practices for secure and reliable ICT, notes, however, that the lack of widespread adoption of standards for secure development processes “has deprived the marketplace of a consensus approach to assessing the software development process of a supplier.”\textsuperscript{60} Incorporating such standards as procurement requirements helps increase adoption and improves ICT security. Adoption and compliance, however, may put a particular burden on small and medium-sized companies.

Software quality assurance (SQA) measures increase software quality, contributing to risk reduction. SQA involves monitoring software engineering processes and methods throughout the entire software development process, including requirement engineering, software design, coding, source code control, code review, software configuration management, testing, release management, and product integration. SQA processes enable tracking and revoking changes to the code base to rectify insecure code introduced—whether unintentionally or maliciously—over time by any developer. The ISO 9000 standard includes measures for SQA conformance, for example.

Security in the operation of ICT is essential. While ICT vendors are responsible for creating secure products or services, buyers and operators are responsible for their secure, resilient operation. Secure deployment is a key factor in the cybersecurity risk calculus.

ICT vendors should commit to secure configurations by default upon the delivery of products and services. With the increasing complexity of ICT operations and the shift of business models towards services, the relationship between vendors and buyers/operators has become more intertwined. Rather than a one-off transaction, ICT is subject to maintenance and lifecycle services to ensure operational readiness. In the case of outsourcing or managed services, for example, the vendor operates ICT on behalf of the buyer. This warrants a conversation between the buyer/operator and the vendor about individual and shared responsibilities with regard to the deployment, operation, and maintenance of secure and safe ICT—including strict protocols and mechanisms for configuration management and change control processes as part of their shared standard operating procedures.

If a vendor has direct access to a buyer/operator’s infrastructure (e.g., a network equipment supplier with access to a telecom carrier’s network infrastructure for service and maintenance purposes), operational security procedures must be in place. Such procedures ensure that changes to technical configurations, access to sensitive data, or any activities with potential security implications, are tracked and subject to tight controls and approvals, and furthermore, are auditable by the operator.\textsuperscript{61} Non-repudiation mechanisms for identity and access management, continual verification, audit, and assessment must be established to ensure secure operations.

All software is subject to updates to allow for new functions or to patch security vulnerabilities. Remote updating of software from vendors is a common function that requires secure software delivery and distribution, which needs to be controllable and traceable by the buyer/operator. The update mechanism needs to be protected using cryptographic code signing to ensure source authenticity and integrity.\textsuperscript{62} Updates should almost always be deployed only after successful testing of the new code, conducted or at least


\textsuperscript{61} The CIS Controls provides a set of prioritized actions for secure operation. “The 20 CIS Controls & Resources,” Center for Internet Security, https://www.cisecurity.org/controls/cis-controls-list.

overseen by the buyer/operator, not the ICT vendor (e.g., for security and proper functioning in different environments).

ICT buyers—through requests for information (RFIs) and procurement requirements—should focus on whether a vendor is prepared to accept and respond to vulnerability reports and has processes in place to remediate security vulnerabilities effectively. ICT buyers need to require that vendors follow best practices and subscribe to common, coordinated vulnerability disclosure norms. ICT buyers and operators, however, are responsible for security vulnerability management and should not merely delegate vulnerability management and patching responsibilities to the vendor.

To ensure that certain standards criteria or formal requirements are met, ICT buyers can require vendors to conduct security testing and assessments of their product or service, ideally by independent third parties (e.g., mandating an industry consortium or coordinating with a recognized, regional transparency center to conduct the testing). In-depth, technical security assessments of products and services (e.g., scanning for vulnerabilities, fuzzing, and penetration testing) can identify and fix unexpected behaviors, exploitable vulnerabilities, or undocumented functionalities before deployment.

For any security testing and assessment, particularly if conducted by the ICT vendor and not an independent third party, it is relevant to establish recourse and mitigation measures if the vendor fails to meet obligations or is untruthful. Contractual clauses can include a penalty, and vendors should endeavor to push those contractual obligations down their supply chains.

ICT buyers and operators should consult transparency reports and other corporate records describing incidents that impact the security and privacy of a vendor’s customer base. These may provide statistics about risk-relevant incidents, such as data breaches, cyber attacks, and data access requests by law enforcement or other authorities.

**Component 2—Industry: Buyer-led Security Requirements for ICT Vendors**

As individual buyers cannot assess the supply chain of every ICT vendor, this component proposes that like-minded buyers, operators, and other stakeholders collaborate to create recommended procurement-related security requirements that they impose on vendors through demand-side and, perhaps, public relations and reputation pressures. ICT vendors can choose to self-attest that they adhere to these requirements. Self-attestation alone is a weak form of assurance, however. For increased accuracy and reliability, ICT vendors should include such assurances in their customer contracts or be subject to conformance testing. Together, self-attestation and contractual obligations help incentivize ICT vendors to measurably raise the bar. In cases where vendors assure by contract that they will meet certain requirements, they can be legally obligated to fulfill their responsibilities.

In addition, governments shape such requirements in their roles as regulators, through which they prescribe security requirements for regulated entities, and buyers. For example, the U.S. Department of Defense is in the process of developing its Cybersecurity Maturity Model Certification (CMMC) to strengthen documentation related to contractors’ cybersecurity practices and adherence to standards (e.g., NIST SP 800-171 and others). Once implemented, the CMMC will be used for contract solicitations and

---


64 Note that penetration testing can demonstrate the presence of vulnerabilities or undocumented functions, but not their absence.


contracts will be audited against it. Similarly, some of the requirements to sell tools and services to the U.S. Department of Homeland Security’s (DHS) Continuous Diagnostics and Mitigation (CDM) program provide a baseline for security and exemplify assurance and transparency measures under the framework.

Like-minded ICT buyers collectively can turn to several potential measures to impose security requirements on vendors, including some of the following described.

ICT vendors should provide a software bill of materials (sBOM), which accounts for and provides transparency into the numerous components, modules, and libraries—either proprietary or open source—that constitute the product or service. The sBOM contains critical information to manage security risk. The sharing of sBOM data enables ICT buyers and operators to track whether a discovered vulnerability potentially affects their systems. It further enables their customers to take proactive steps to protect their systems from exploitation of a vulnerable component, as well as to avoid potential damages to, or downtime of, systems caused by a flawed security patch. Incentivized through the sBOM’s transparency, ideally, vendors will use only current, up-to-date components in their ICT.

ICT vendors in contract or by self-attestation should commit to security vulnerability remediation to assure that they deploy tools to identify, mitigate, and remediate serious security weaknesses (e.g., CVSS score 7) before delivery and deployment. ICT vendors can choose to self-attest that they participate in coordinated vulnerability disclosure concerning their proprietary software or third party software in their products and services, and work with customers to remediate the most critical identified vulnerabilities.

ICT vendors should provide a statement of cyber supply chain risk practices. A supply chain risk management plan provides transparency about how ICT vendors manage their subcontractors and suppliers. For example, ICT vendors to the aforementioned DHS CDM program are required to submit such a plan, which is subject to U.S. federal guidelines and standards on supply chain security.

An ICT vendor should provide a declaratory letter of its board that guarantees to a specific buyer that no hidden or harmful functions are intentionally present in their products or services. Furthermore, an ICT vendor may provide a statement about their business operations, either in private disclosure to a buyer or in public. Such assurances and public attestations can provide a basis for trust in the buyer-vendor relationship and may provide ICT buyers with legal recourse and encourage accountability.

Like-minded ICT buyers could establish a consortium for ICT security assessment, which provides its members with guidance for evaluation and procurement of secure ICT. Given sufficient purchasing power, a

---


consortium of ICT buyers can affect the security measures vendors and their suppliers employ in their products, services, and components. For example, in the private sector, the Financial Services Information Sharing and Analysis Center (FS-ISAC) makes recommendations for the U.S. financial sector regarding ICT security procurement practices. Individual financial service organizations can adopt these requirements accordingly. Another example, the Deutsche Cyber-Sicherheitsorganisation (DCSO), founded by leading German industrial companies, provides technology evaluations, as well as service and vendor assessments to its members.

Component 3–Industry: Vendor-led Assurance and Transparency Requirements

ICT vendors should organize at the industry level and voluntarily develop and attest that they will implement assurance, transparency, and accountability measures. ICT vendors bear a central responsibility and play a critical role in the ecosystem to enhance the security of products, services, and the supply chain. Leading by example, vendors can strengthen ICT security and trustworthiness through industry-wide, coordinated efforts and avoid backlash from public pressure or punitive actions by governments and regulators due to perceived security and safety weaknesses. Potential activities and measures ICT vendors can pursue collectively, include some of the following described.

Vendors should actively engage in international standards and norm setting to improve cybersecurity for their industry sector. This commitment raises the participating company’s expertise and reputation as a leader in the field. Vendors should further lead, contribute, and adhere to norms, standards, and baseline requirements that seek to improve ICT security. This includes, among others, technical recommendations, such as ENISA’s baseline for IoT security, and industry commitments, such as the Cybersecurity Tech Accord; and norms and principles of responsible behavior in cyberspace for state and non-state actors, such as those put forward by the Global Commission on the Stability of Cyberspace.

Independent evaluation and testing of products and services by consumer interest organizations or independent industry observers can help consumers make informed purchasing decisions. Though different from the technical assessment of ICT resistance to attacks, security-informed product and service ratings—based on evaluations—can identify security strengths and weaknesses. Such rankings help bolster transparency and can incentivize ICT vendors to improve security and employ best practices. For example, independent technical labs test, compare, and rank anti-virus and malware detection tools to inform customers about data collection practices and privacy policies. The Digital Standard is an example of a consumer-driven effort towards an evaluation framework. The framework, led by Consumer Reports, the Cyber Independent Testing Lab, and others, enables consumer organizations to evaluate security and privacy of new products.

The identification and remediation of security vulnerabilities is an industry-wide concern. ICT vendors—by self-attestation and contractual requirements—should commit to a proactive coordinated vulnerability disclosure policy with reasonable disclosure timelines and frequent security patch delivery to enhance security. Because vulnerability disclosure is closely watched by the information security community, adhering to disclosure norms presents an opportunity for ICT vendors to build a trusted reputation. Effective vulnerability

---

74 “Deutsche Cyber-Sicherheitsorganisation (DCSO),” https://dcso.de/.
75 Baseline Security Recommendations for IoT, (2017); and ENISA Good practices for IoT and Smart Infrastructures Tool.
80 Disclosure can, in some instances, lead to negative effects, but security gains usually outweigh them.
disclosure and patch-delivery practices foster vendor transparency and accountability, helping to resolve security issues effectively and in a timely manner, ultimately contributing to trust and minimizing risk. The international standards ISO/IEC 29147 and ISO/IEC 30111 describe guidelines for vulnerability disclosure and handling processes.81

Furthermore, ICT vendors should consider implementing a bug bounty program, a structured approach to harness globally distributed, independent security researchers to discover vulnerabilities in exchange for rewards. ICT vendor engagement with the larger information security community through a bug bounty program strengthens relationships with key stakeholders, enhances transparency of security vulnerability reporting, and helps improve security. This is the case so long as the vendor has formalized processes for vulnerability report intake, validating such reports, triaging reports appropriately, and ensuring the speedy remediation of credible vulnerabilities. A mature security development lifecycle (SDL) process is an essential prerequisite for a bug bounty program to help effectively improve ICT product or service security. A bug bounty program does not replace proper SDL processes, effective risk management, or internal security testing.

Joint efforts by standard-setting organizations and trade groups can establish industry security evaluation and accreditation schemes that provide security baselines and a comprehensive security audit for vendors and their products and services. For example, the newly formed Network Equipment Security Assurance Scheme (NESAS) is a voluntary scheme for the mobile industry, defined and overseen by the sector’s leading industry organizations: the 3rd Generation Partnership Project (3GPP) and the GSM Association (GSMA). NESAS provides evidence that network equipment satisfies security requirements and that network equipment vendors comply with security standards in their product development and lifecycle processes.82

ICT vendors can improve confidence in security by sponsoring or operating a joint oversight board for the entire industry or an individual firm. Joint oversight boards consisting of senior corporate executives and government officials can provide guidance to ICT buyers and policymakers. Such boards are ideally industry-wide and oversee expert staff that conduct technical and non-technical assessments in testing facilities. The Huawei Cyber Security Evaluation Centre Oversight Board serves as an example. It issues an annual oversight report to evaluate the Huawei Cyber Security Evaluation Centre’s work and provides recommendations for actions to the UK’s national security advisor regarding the deployment of Huawei’s technologies in British telecommunications carriers’ networks.83

Component 4–Ecosystem: Regional Transparency Centers

As it is impractical for each organization to conduct their own testing of third parties’ ICT supply chains, products, or services, the creation of structures and mechanisms for regional, industry-wide testing and the mutual recognition of assessments and assessors would promote assurance and transparency. This would only require security testing and assessment once, and would facilitate the release of results to the public. Ultimately, this would benefit all ICT buyers in a region with the same risk requirements and security objectives for a specific ICT product or service. To that end, it would be useful to establish a global network of regional transparency centers (RTCs). Prerequisites for the full implementation of such an approach include mutually-agreed testing criteria, objectives, and methodologies, as well as an institutional mechanism for accreditation.

Establishing a network of RTCs, however, requires eliminating critical roadblocks. Unresolved questions include establishing which entity will operate an RTC, and determining effective mechanisms to ensure the broad acceptance of RTC assessments, while keeping government requests at arm’s length. RTCs need to acquire the technical capacity to facilitate these evaluations and ICT buyers and governments need sufficient expertise to be able to use and comprehend RTCs’ complex testing functions and assessments. Furthermore, RTCs that would subject all vendors to industry-wide reviews

will likely face stiff opposition and industry resentment. To overcome these difficulties, some have suggested the need to build new international institutions and coalitions.\textsuperscript{84}

Current examples of single firm transparency centers include Cisco, Huawei, Kaspersky, and Microsoft. These facilities serve government and corporate requests to conduct code inspection on the vendor’s source code for risk assessment purposes. Customers bring their own assessors and undisclosed tools; vendors protect their source code only by restricting what can be taken out of the testing premises.

**Component 5—Ecosystem: Global Conformance Programs**

High-level global conformance programs for ICT certification and testing with international reach are designed to improve ICT security and trustworthiness. The creation of conformance programs—run and enforced by existing or new global institutions—can provide an objective basis for customers and stakeholders to determine adherence to standards and best practice guidelines. As mentioned above, the U.S. DoD is developing the CMMC to ensure that its 300,000 suppliers conform with U.S. government and other standards.\textsuperscript{85} As another example, with the adoption of the EU Cybersecurity Act in 2019, the EU established a Union-wide cybersecurity certification framework for product cybersecurity under ENISA.\textsuperscript{86}

The international Common Criteria for Information Technology Security Evaluation, or simply Common Criteria, is an established framework for ICT product security assessment (ISO/IEC 15408, evaluation criteria for IT security) and describes an evaluation process (ISO/IEC 18045, methodology for IT security evaluation).\textsuperscript{87} Under Common Criteria, vendors contract with government-approved, independent evaluation laboratories, which conduct security reviews and testing of vendor products. Common Criteria focuses more on the conformance of a product’s documented functional and assurance requirements rather than on technical testing of a product’s security.

Industry organizations and experts have been critical of the effectiveness of conformance programs and their ability to improve trustworthiness, however. SAFECode, for instance, has argued that Common Criteria’s focus on end-product feature evaluation and documentation does not adequately pay attention to the importance of secure practices throughout the ICT’s development process.\textsuperscript{88} Standards-based evaluation and certification of processes critical for secure software development would provide an opportunity to effectively scale security rather than testing the security of products and services only upon their final completion. Furthermore, industry veterans have reported that ICT vendors find it difficult to identify third party assessors that states accept as credible. States strongly prefer assessments conducted by domestic laboratories, even if foreign laboratories adhere to the evaluation methodology stipulated under Common Criteria.

---


\textsuperscript{85} “DOD’s Cybersecurity Maturity Model Certification and Draft CMMC Model Framework,” (2019).


A holistic approach is needed to effectively address ICT supply chain risk, while minimizing the negative effects of TechNationalism.

Addressing primary action points for ICT buyers, operators, and vendors, the measures in the assurance, transparency, and accountability framework will contribute to improved levels of confidence and trustworthiness in ICT products and services. The trust deficit in global supply chains, however, will require additional action across the wider ICT ecosystem—in particular, by governments.

Complementing the measures discussed in the framework, the roadmap below targets forward-looking, long-term policy goals. In close collaboration with the ICT industry, governments should enact policies to strengthen the wider ICT ecosystem, in accordance with public safety and national defense objectives, while striving for competitive, open markets and global innovation.

The action roadmap recommends that the ICT industry commit, in the near-term, to the following steps:

1. **Implement the assurance, transparency, and accountability framework**: ICT buyers, operators, and vendors address assurance, transparency, and accountability as part of their overall supply chain security and trust efforts.

2. **Adopt and incorporate supply chain risk in enterprise risk management**: ICT buyers, operators, and vendors have a risk management framework and processes in place to assess ICT and supply chain risk, including third party dependencies. The risk assessment will help prioritize and inform the adoption of the most appropriate framework measures.
The roadmap recommends that governments take measures to strengthen ICT security in critical functions in the public and private sector by taking the following steps:

1. **Enable threat and vulnerability information sharing**: Entities along a supply chain should share relevant threat and vulnerability information with each other and the ICT industry at large. Governments should create the necessary legal conditions to encourage, and remove obstacles that hinder, effective sharing. In addition, national intelligence agencies should share relevant and actionable threat information with ICT manufacturers, vendors, and buyers. This is particularly essential in instances where parts of the supply chain are subject to significant risk or in imminent danger of compromise by malicious state actors.

2. **Enact a multiple sourcing requirement**: As part of national policy, establishing a dependence limit for key critical infrastructure operators on a single vendor (e.g., within a single operator or across a sector) can increase resilience. A regulator may require operators of critical infrastructure to source essential components or those that execute sensitive functions from multiple vendors to ensure diversity in suppliers and solutions across the national infrastructure. States should reimburse extra costs incurred from such a requirement on a case-by-case basis.

3. **Ensure strategic science and technology investments**: Strategic investments in science and technology, through government-funded research and development, contribute to the availability of secure domestic products and services deemed critical. Such investments contribute to a domestic market for strategic technologies and reduce the risk from foreign dependencies and undue influence. Allied countries can make joint, coordinated investments in strategic science and technology. To protect strategic intellectual property in firms, management and key staff may be subject to security clearance requirements.

4. **Consider narrow national security exceptions**: For narrowly defined areas, particularly for national defense and other sensitive functions, national security exceptions may prescribe exclusions for vendors who are subject to foreign control. Such national security exceptions should be in accordance with international agreements.

5. **Review and adapt national supply chain security policies and goals**: Governments, in consultation with critical infrastructure operators and the private sector, should review and adapt supply chain security policy measures on a regular basis, as part of a government’s overall effort to strengthen cybersecurity. Adjustments should be made based on risk and threat information and in accordance with the principles outlined in this report.
Conclusion

The current controversy around 5G communication technology, in particular 5G network equipment provided by Chinese manufacturers and its debated deployment in Western countries, has led to restrictive policy measures targeting foreign ICT firms. At the heart of this heated debate is the concept of country of origin: whether technology coming from a supplier based in an adversary, or potential adversary, country is sufficiently secure and free from influence by the host government, and thus, whether or not such a supplier and its technology can ultimately be trusted.

ICT products and services are everywhere and security is becoming a critical precondition for trustworthiness. Ensuring ICT security and hence trust has become increasingly challenging due to its complexity, global supply chain, and society’s growing dependence on it. Technical challenges to securing ICT are complicated by geopolitical tensions and the growing recognition that ICT is not only a deciding driver for a state’s economic prosperity and military power, but also that dependence on foreign ICT may significantly curtail a state’s strategic autonomy in the digital age.

The framework described in this report provides measures for assurance, transparency, and accountability and can contribute to higher levels of confidence that ICT products and services are secure. If appropriately aligned, these measures can help close the trust gap between ICT buyers, vendors, and operators and their respective governments. To be effective, such measures must be cost-effective as well as recognized and adopted by a critical mass of key players so that they become de facto best practices of the industry going forward. The framework provides building blocks to minimize the leap of faith ICT buyers and operators take, relying instead on a solid basis to make risk-informed buying decisions and putting effective risk mitigation measures in place. Managed well, the residual risk can be brought to an acceptable level.

The build-up of 5G network infrastructure is only one of numerous domains where states will attempt to restrain and control foreign technology. AI, high-performance computing—including quantum computing environments—robotics, and IoT are likely next. Extensive bans of foreign ICT suppliers and their cutting-edge technologies, however, will have a multitude of complications and unintended effects for both the national and global economy. So too would mandatory insertions of technology from a “national champion.” In contrast, the industry needs a repeatable, transparent, cost effective, and risk-based approach to conduct risk assessment and provide guidance for balanced measures to assure ICT security and trustworthiness and minimize negative consequences from TechNationalism. This report’s framework lays the groundwork for an industry-tailed approach.

It will take time to establish effective measures and frameworks, but the alternative—decoupled, fragmented, and parallel ICT ecosystems—will bring significant negative effects for trade, the global economy, and the advancement of society overall, while providing little to no increase in security. A balanced approach, as in so many of life’s arenas, is the most effective way forward.
Acknowledgments

This report was prepared by the EastWest Institute and authored by Andreas Kuehn and Bruce McConnell. The authors are extremely grateful for the advice provided by the experts listed below. Their inclusion here does not mean that they support or agree with any of the report’s statements, proposals, recommendations, or conclusions.

The following experts provided substantive commentary and advice during the development of the report:

Kamlesh Bajaj, Founder CEO, Data Security Council of India and Founder Director, CERT-India; Paul Evans, Professor, School of Public Policy and Global Affairs, University of British Columbia; Tara Hairston, Head of Government Relations, North America, Kaspersky; Trey Herr, Director, Cyber Statecraft Initiative, Atlantic Council; Robert Holleyman, former Deputy U.S. Trade Representative and President & CEO, Crowell & Moring International; Jan-Peter Kleinhans, Project Director, Stiftung Neue Verantwortung; Steve Lipner, Executive Director, SAFECode; Nicole Magney, Public Policy and Communications Manager, Acronis SCS; Tom Patterson, Chief Trust Officer, Unisys; Andy Purdy, Chief Security Officer, Huawei Technologies USA; Gulshan Rai, former National Cyber Security Coordinator, Government of India; John Savage, An Wang Professor Emeritus of Computer Science, Brown University; Paul Triolo, Practice Head, Geo-Technology, Eurasia Group; and Justin Zhao, Director, Policy and Regulatory Affairs, Microsoft.

This report builds on previous work prepared by the Breakthrough Group on Increasing the Global Availability and Use of Secure ICT Products and Services. A series of two workshops held in Palo Alto, CA in September 2018 and 2019 formed the foundations of the report. These workshops brought together 60 experts from the ICT industry, government, and academia to explore and discuss current developments relevant to TechNationalism and global ICT supply chain security.

The Chinese translation of this report was made possible by Shen Yi, Professor, Fudan University and Rogier Creemers, Lecturer in Modern China Studies, Leiden University.

The following EWI colleagues provided invaluable support and assistance for this report: Brita Achberger, Michael Depp, Abagail Lawson, Anneleen Roggeman, Alex Schulman, and Dragan Stojanovski.
Board of Directors

LEADERSHIP

Ross Perot, Jr. (U.S.)  
Chairman  
EastWest Institute  
Chairman  
Hillwood Development Co. LLC

R. William Ide III (U.S.)  
Counsel and Secretary  
Chair of the Executive Committee  
EastWest Institute  
Partner  
Akerman LLP

Dr. William J. Parker III (U.S.)  
CEO and President  
EastWest Institute

MEMBERS

Haifa Al Kaylani (Lebanon/Jordan/UK)  
Founder and Chairperson  
Arab International Women’s Forum

Peter A. Altabef (U.S.)  
President and CEO  
Unisys Corporation

Tewodros Ashenafi (Ethiopia)  
Chairman and CEO  
Southwest Energy (HK) Ltd.

Mark Joseph Bild (U.S.)  
Managing Partner  
BAI Corporation

Mary McInnis Boies (U.S.)  
Counsel  
Boies, Schiller & Flexner LLP

Sir Peter Bonfield (UK)  
Chairman  
NXP Semiconductors

Matt Bross (U.S.)  
Chairman and CEO  
Compass-EOS

Robert N. Campbell III (U.S.)  
Founder and CEO  
Campbell Global Services LLC

Michael Chertoff (U.S.)  
Executive Chairman and Co-Founder  
The Chertoff Group  
Former Secretary of the U.S. Department of Homeland Security

David Cohen (Israel)  
Chairman  
F&C REIT Property Management

Roger Cohen (U.S.)  
Op-ed Columnist  
The New York Times

Joel H. Cowan (U.S.)  
Professor  
Georgia Institute of Technology

Addison Fischer (U.S.)  
Chairman and Co-Founder  
Planet Heritage Foundation

Olivia Fischer (U.S.)  
Philanthropist  
Planet Heritage Foundation

Hon. Steven S. Honigman (U.S.)  
Founding Member  
Quieter Oceans LLC

Dr. Hu Yuandong (China)  
Chief Representative  
UNIDO ITPO-China

John Hurley (U.S.)  
Managing Partner  
Cavalry Asset Management

Ralph Isham (U.S.)  
Managing Director  
GH Venture Partners LLC

Anurag Jain (U.S.)  
Chairman  
Access Healthcare

Gen. (ret.) James L. Jones (U.S.)  
Former U.S. National Security Advisor  
Former Supreme Allied Commander Europe  
Former Commandant of the Marine Corps

George Kadifa (U.S.)  
Managing Director  
Sumeru Equity Partners

Zuhal Kurt (Turkey)  
Chairman of the Board  
Kurt Group

Gen. (ret.) T. Michael Moseley (U.S.)  
President and CEO  
Moseley and Associates, LLC  
Former Chief of Staff  
United States Air Force

Karen Linehan Mroz (U.S.)  
President  
Roscommon Group Associates

F. Francis Najafi (U.S.)  
CEO  
Pivotal Group

Amb. Tsuneo Nishida (Japan)  
Professor  
Institute for Peace Science at Hiroshima University  
Former Permanent Representative Permanent Mission of Japan to the United Nations

Admiral (ret.) William A. Owens (U.S.)  
Chairman  
Red Bison Advisory Group LLC

Sarah Perot (U.S.)  
Director and Co-Chair for Development  
Dallas Center for Performing Arts

Kathryn Pilgrim (U.S.)  
International Writer

Laurent M. Roux (U.S.)  
Founder and President  
Gallatin Wealth Management, LLC

Ikram ul-Majeed Sehgal (Pakistan)  
Chairman  
Security & Management Services Ltd.

Amb. Kanwal Sibal (India)  
Former Foreign Secretary of India
Kevin Taweel (U.S.)
CEO
Asurion

Alexander Voloshin (Russia)
Chairman of the Board
JSC Freight One (PGK)
Non-Executive Director
Yandex Company

Admiral (ret.) Patrick M. Walsh (U.S.)
Vice President
U.S. Navy and Marine Corps Services
Boeing Global Services

Amb. Zhou Wenzhong (China)
Secretary-General
Boao Forum for Asia

NON-BOARD COMMITTEE MEMBERS

Hilton Smith, Jr. (U.S.)
President and CEO
East Bay Co., LTD

CO-FOUNDERS

John Edwin Mroz† (U.S.)
Former President and CEO
EastWest Institute

Ira D. Wallach† (U.S.)
Former Chairman
Central National-Gottesman Inc.

CHAIRMEN EMERITI

Martti Ahtisaari (Finland)
2008 Nobel Peace Prize Laureate
Former President of Finland

Berthold Beitz† (Germany)
President
Alfred Krupp von Bohlen und Halbach-Stiftung

Ivan T. Berend (Hungary)
Professor
University of California, Los Angeles

Francis Finlay (UK)
Former Chairman
Clay Finlay LLC

Hans-Dietrich Genscher† (Germany)
Former Vice Chancellor and Federal
Minister for Foreign Affairs of Germany

Donald M. Kendall (U.S.)
Former Chairman and CEO
PepsiCo Inc.

Whitney MacMillan (U.S.)
Former Chairman and CEO
Cargill Inc.

Mark Maletz (U.S.)
Former Chairman, Executive Committee
EastWest Institute
Senior Fellow
Harvard Business School

George F. Russell, Jr. (U.S.)
Chairman Emeritus
Russell Investment Group
Founder
Russell 20-20

H.E. Dr. Armen Sarkissian (Armenia)
President of Armenia

DIRECTORS EMERITI

Jan Krzysztof Bielecki (Poland)
CEO
Bank Polska Kasa Opieki S.A.
Former Prime Minister of Poland

Emil Constantinescu (Romania)
President
Institute for Regional Cooperation and
Conflict Prevention (INCOR)
Former President of Romania

William D. Dearstyne (U.S.)
Former Company Group Chairman
Johnson & Johnson

Stephen B. Heintz (U.S.)
President
Rockefeller Brothers Fund

Amb. Wolfgang Ischinger (Germany)
Chairman
Munich Security Conference

John W. Kluge† (U.S.)
Former Chairman of the Board
Metromedia International Group

Amb. Maria-Pia Kothbauer
(Liechtenstein)
Ambassador of Liechtenstein to Austria,
the OSCE and the United Nations in Vienna

William E. Murray† (U.S.)
Former Chairman
The Samuel Freeman Trust

John J. Roberts (U.S.)
Senior Advisor
American International Group (AIG)

Daniel Rose (U.S.)
Chairman
Rose Associates Inc.

Leo Schenker† (U.S.)
Former Senior Executive Vice President
Central National-Gottesman Inc.

Mitchell I. Sonkin (U.S.)
Managing Director
MBIA Insurance Corporation

Thorvald Stoltenberg (Norway)
Former Minister of Foreign Affairs of
Norway

Liener Temerlin (U.S.)
Chairman
Temerlin Consulting

John C. Whitehead† (U.S.)
Former Co-Chairman
Goldman Sachs
Former Deputy Secretary of the
U.S. Department of State

† Deceased
The EastWest Institute works to reduce international conflict, addressing seemingly intractable problems that threaten world security and stability. We forge new connections and build trust among global leaders and influencers, help create practical new ideas, and take action through our network of global decision-makers. Independent and nonprofit since our founding in 1980, we have offices in New York, Brussels, Moscow and San Francisco.
Global Cooperation in Cyberspace

SUPPORTERS & PARTNERS:

Unisys
Microsoft
JPMorgan Chase
Huawei Technologies
William and Flora Hewlett Foundation
Global Forum on Cyber Expertise
Munich Security Conference
Fudan University