CARNEGIE
ENDOWMENT FOR
INTERNATIONAL PEACE

# Enhancing the Integrity of the ICT/OT Supply Chain

**Ariel E. Levite**

**Presentation to the Guanchao Cyber Forum, Beijing, PRC**
**21 August, 2019**

# Where We Are

- Concerns over the integrity of the ICT/OT supply chains are rapidly escalating , upending the global marketplace
- Genuine anxiety about both security and quality engineering assume even greater importance as we head toward an increasingly digitized world, autonomous systems and AI
- But political, commercial, and strategic considerations REINFORCE EACH OTHER and make the situation a lot worse
- Loss of trust in products, services and vendors already produces serious adverse consequences on trade and manufacturing
- But significant longer term effects on efficiency, innovation and strategic choices will likely follow
- Governments and corporations share the responsibility for easing the crisis
- Carnegie as a global NGO is eager to facilitate remedial efforts

# What Has CEIP Done to Date?

Over the past two years we have:

- Surveyed trends and analyzed implications, [inter alia] through dialogue with governments and corporations
- Developed and preliminarily tested the plausibility of a conceptual approach to address the challenge to the integrity of the ICT/OT supply chain
- Identified some promising platforms, partners and process ideas to implement this agenda

# Structural Obstacles & Opportunities

- The appeal of cyberspace for intelligence, warfare, domestic security and law enforcement makes it inherently difficult to build trustworthiness in ICT products and services
- Several commercial incentives (such as race to the marketplace and effort to introduce efficiency and generate use information) heighten the security risks
- And unilateral actions by governments to address their national concerns and requirements further undermine trust in products and services – for example, China, U.S., and Australia.
- But growing awareness of the risks and costs of fragmentation of the marketplace is helpful
- And realization that higher cybersecurity standards and practices could also improve quality assurance, safety, marketing, licensing, and export control compliance might balance the incentive structure

# How do We Envisage the Way Ahead

- Introduce a fundamental distinction between compliance with lawful *domestic* requirements and *global* trustworthiness obligations
- Establish objective criteria for *trustworthy global suppliers*
- These would require both pledges and practices from corporate vendors as well as "their" governments
- We propose four criteria for assessing *trustworthy global suppliers*:
  - Relaiability
  - Accountability
  - Transparency
  - Receptivity

  These involve policy, legal, operational and technical aspects
- We submit that existing market mechanisms (re/insurers, credit rating agencies, major investors and lenders) can incentivize endorsement and compliance with these criteria and disincentivize cheating
- We recommend addition of an independent quasi-verification arrangement to assess ad-hoc allegations of non-compliance

# Potential Trustworthiness Criteria

| Governments | Corporations |
|---|---|
| **Reliability** | |
| **Prohibit** systemic supply chain interventions (engagement in ad-hoc interventions subject to strict conditions)<br>**Limit** the scope, scale, and negative consequences of all remaining governmental supply chain interventions | **Refrain** from knowingly creating, inserting, or aiding the development of systemic vulnerabilities<br>**Apply** the highest practical level of security, integrity and resilience in products and services throughout their lifecycles to prevent abuse, misuse, and undue exploitation |
| **Accountability** | |
| **Establish** internal processes and consultative mechanisms to make informed, risk-based decisions regarding supply chain interventions and vulnerabilities<br>**Pair** a supply chain intervention with a comprehensive plan for mitigating its adverse consequences if exposed<br>**Implement** an efficient process to notify affected entities of detected vulnerabilities<br>**Establish/Maintain** a judicial system based on the rule of law | **Quickly** address known vulnerabilities and abuse of products, features, data, and communications<br>**Consistently** assess quality and safety concerns for supply chain integrity ramifications<br>**Same**<br>**Subject** corporate products and services to ad hoc scrutiny mechanism whenever credible concerns arise |
| **Transparency** | |
| **Publish** policies or procedures for handling supply chain security and vulnerability concerns<br>**Lay out** clear and transparent criteria for the accreditation of ICT/OT vendors and certification of their products and services, and include provisions for mutual and reciprocal certification and accreditation | **Publish** core principles and practices governing the security of products and services<br>**Make** products and services available for reasonable scrutiny by prospective and actual customers and competent governmental authorities<br>**Transparent** ownership structure |
| **Receptivity** | |
| **Establish** channels with corporations to discuss issues pertaining to supply chain integrity | **Respond** effectively to reasonable law enforcement and national security concerns and requests for available information |