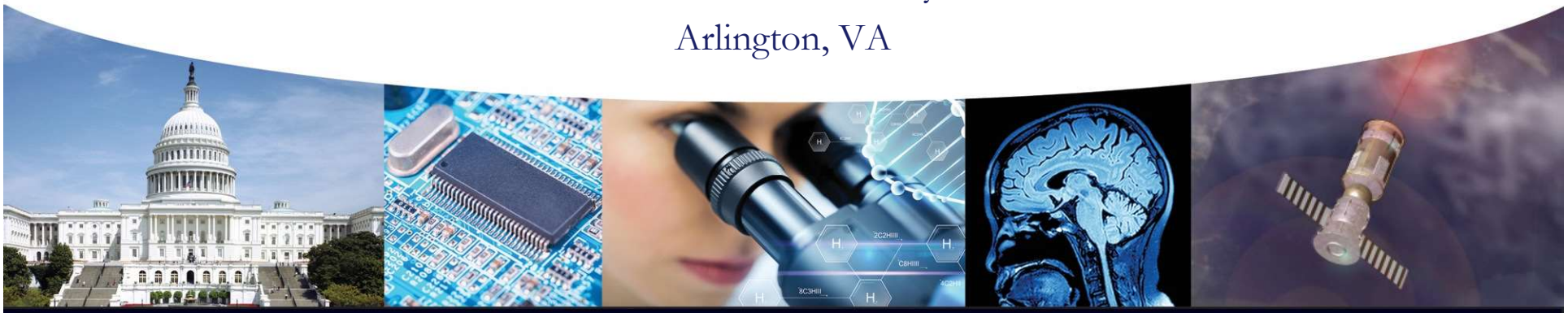
POTOMAC INSTITUTE FOR POLICY STUDIES

Developing Trust for a Secure Microelectronics Supply Chain

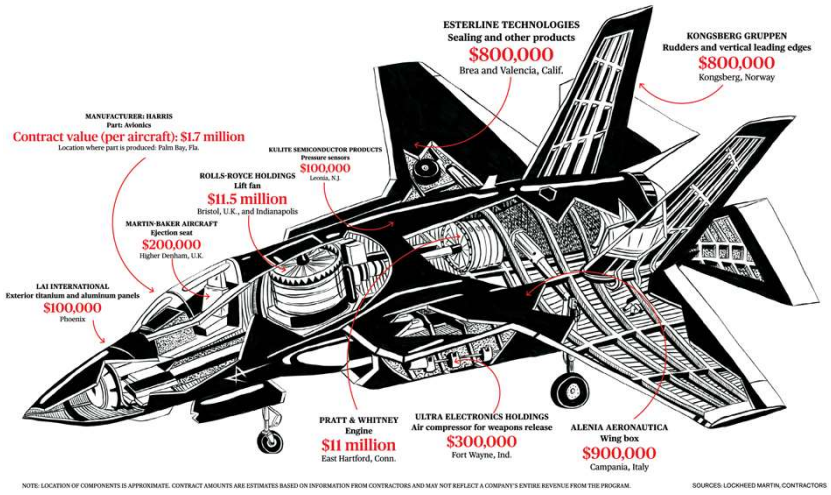
Dr. Mike Fritze
Senior Fellow
Potomac Institute for Policy Studies
Arlington, VA



Outline

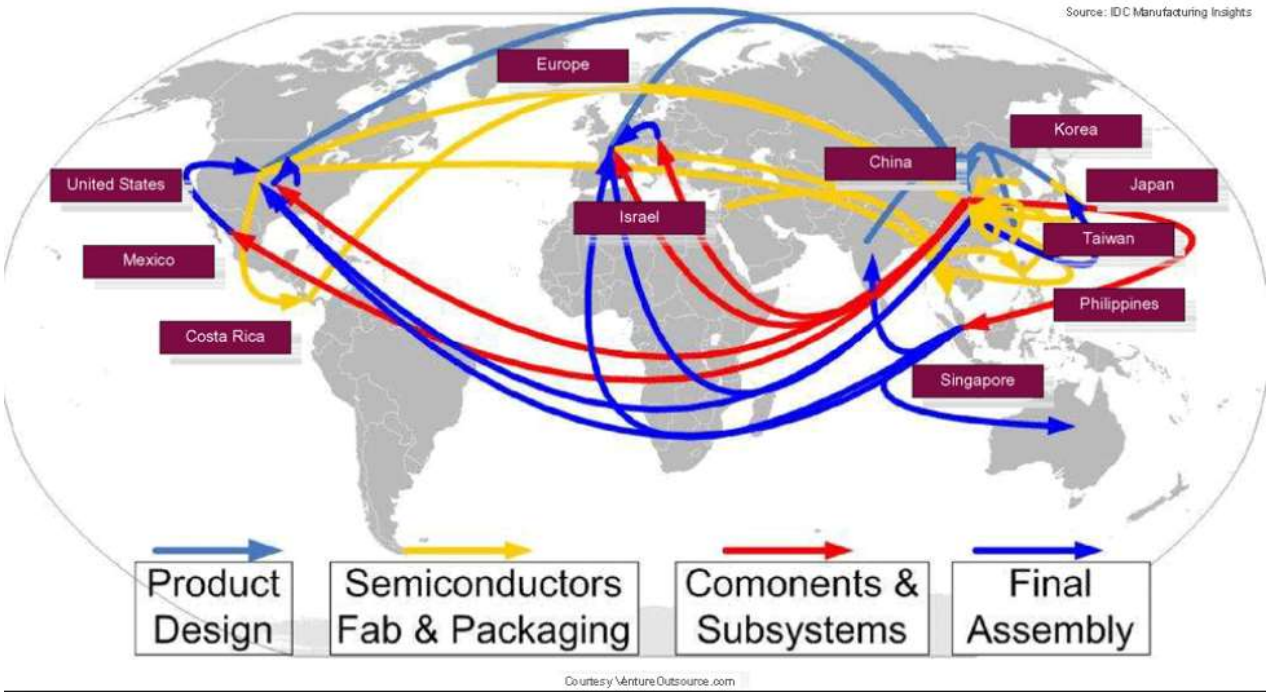
- **Articulation of Trust Problem (for systems folks)**
- **Measuring Trust**
- **National Strategy for Trust**

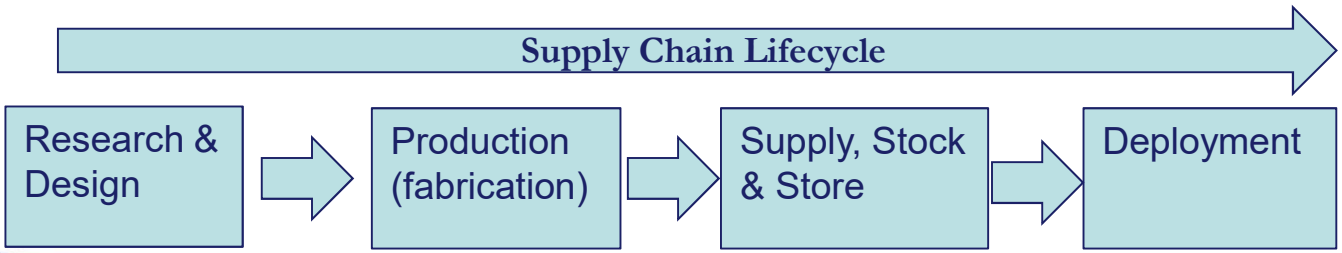
Defense Systems: Global Supply Chain



Increasing complexity in the supply chain results in decreased security of defense systems

Microelectronics Global Supply Chain





Threats to the Hardware Supply Chain

Hardware threats exist throughout the global microelectronics supply chain

The Supply Chain – From design and production to deployment
Malicious insertions, Counterfeits, Clones, Insider Threat

Research & Design
(Research, Development, Prototyping)

- Un-vetted 3rd party IP increases the number of people with knowledge of a design and provides opportunities to corrupt a design
- Zero Day effects can be embedded into a chip's design, go undetected, and be triggered after a chip has been produced

Production
(Fabrication)

- The U.S. is increasingly relying on off-shore foundries to supply components for our critical mission systems
- Only 2% of ASICs used in National Security Space systems come from DoD trusted foundries
- This increases the risk of malicious insertion to include Trojan horses, Kill Switches, and Backdoors

https://www.bloomberg.com/news/articles/2008-10-01/dangerous-fakes

Supply, Stock and Store
(Testing and Verification, Acquisition)

- Attack vectors exist throughout the entire supply chain to include – design, fabrication, testing, packaging, distribution, and end-of-life
- 53% of counterfeit incidents from 2003 – 2013 were for discontinued (legacy) components

Deployment
(Deployed mission systems, Logistics & Maintenance, end-of-life)

- Insider threats and counterfeits in the upgrade/refresh process
- Information exploitation
- Electronic warfare
- Kill switches and backdoors can be used
- Poor disposal practices

Measuring Hardware "Trust"

- "Trust" commonly used phrase but very difficult to precisely and quantitatively define

- **We propose an "insurance" based definition of Trust**

$$T=R/M$$

T = level of trust; R = risk mitigation investment; M = mission value

100% trust means we have mission "insured" for its full value

Insurance "purchased" depends on value of mission and nature of threats of interest

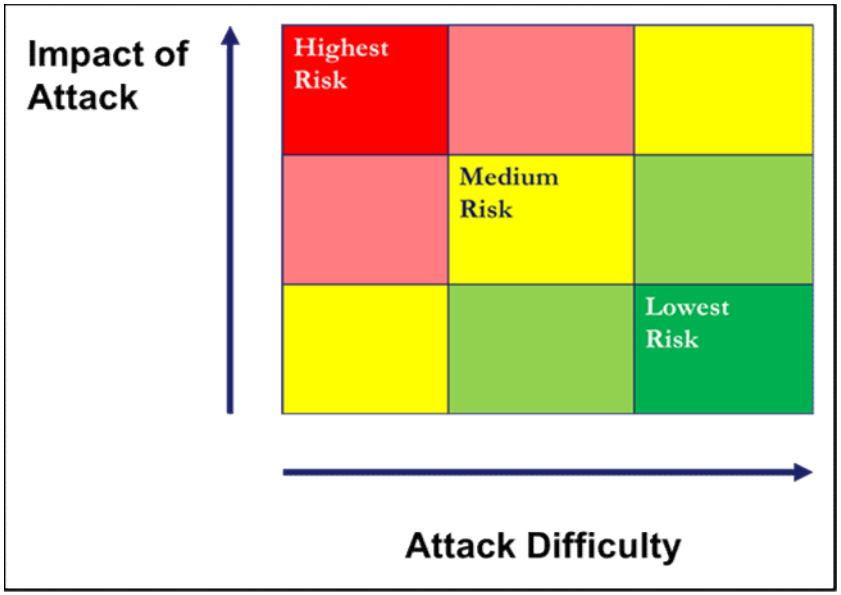
Relating Risks to Threat Type

Anyone can hack software. It takes a nation state to attack hardware

Hardware attacks are by Nation state actors, capable of insertions across the supply chain; requires significant resources and expertise.

DSB Task Force Report: Resilient Military Systems and the Advanced Cyber Threat.
http://www.acq.osd.mil/dsb/reports/2010s/ResilientMilitarySystemsCyberThreat.pdf

Mitigation Insurance: Impact vs Difficulty Matrix

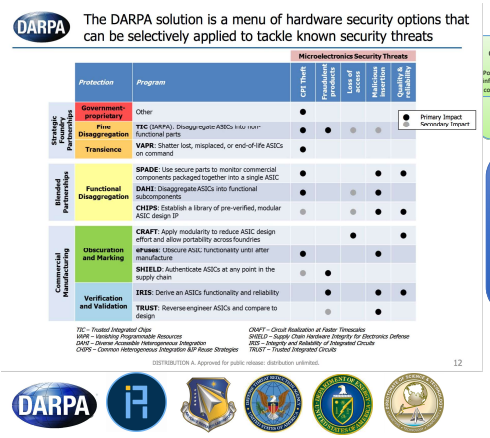


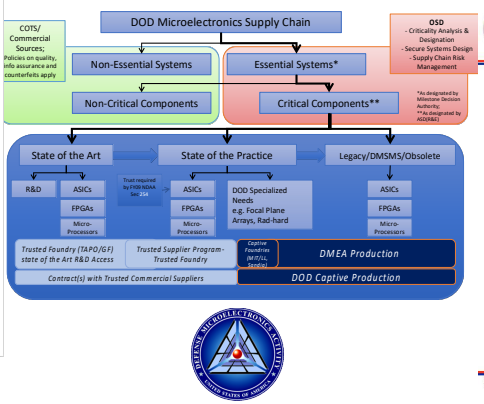
Mitigation "Insurance" Goal:
To make attacks more costly (difficulty/time/$) for the attacker than the defender

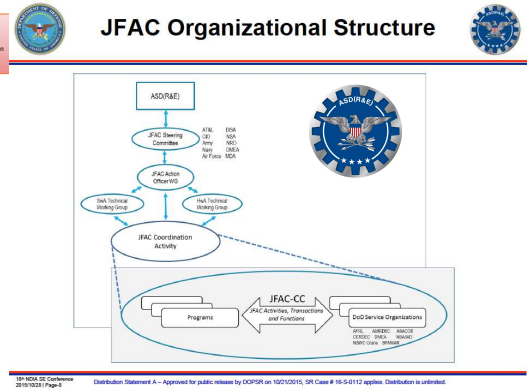
National Strategy: Address the entire supply chain
US Government Solution – DMEA Executive Agent

The Trusted Microelectronics Supply Chain

Research & Design → **Production** → **Supply, Stock & Store** → **Deployment**







Designate DMEA as Executive Agent

Current DoD Policies Include:

- Defense Industrial Base Sector Specific Plan (2010)
- Mission Assurance Strategy (2012)
- Antiterrorism Force Protection
- Counterfeit Mitigation Policies

National Strategy:
Rationalizing & Integrating DoD Capabilities

The Trusted Microelectronics Supply Chain

Research & Design

- Research for trusted design & manufacturing
- Manage relationship with Industry for R&D access to "pre-SOTA" technology
- Focus on research, design, and prototyping
- Acquisition of IP for pre-fab research

Production

- SOTA → Trusted Foundry (GF)
- SOTP → Trusted Commercial Suppliers (79 Suppliers)
- Legacy → Flexible Foundry (DMEA)

Supply, Stock & Store

ASD(R&E)

JFAC Steering Committee

- SwA Technical Working Group
- HwA Technical Working Group

Deployment

Armed Services need new policies to secure deployed systems