Protecting the Defense Procurement Cyber Supply Chain: The U.S. Experience

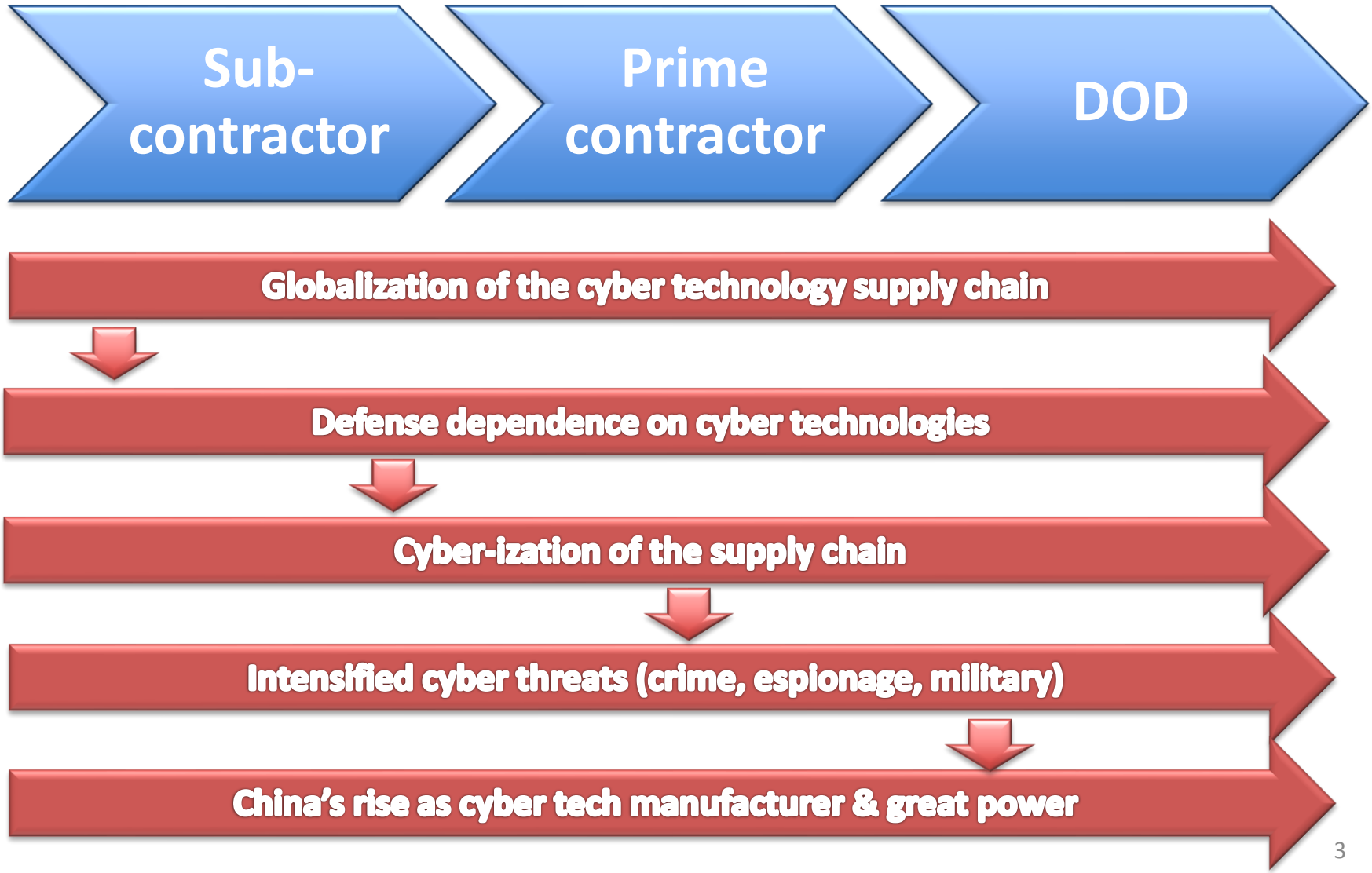
David P. Fidler
James Louis Calamaras Professor
Indiana University Maurer School of Law, USA

Defense Procurement in the Age of Cyber: Recalibrating Government and Contractor Responsibilities
Riga, Latvia
28-30 May 2014

Overview of presentation

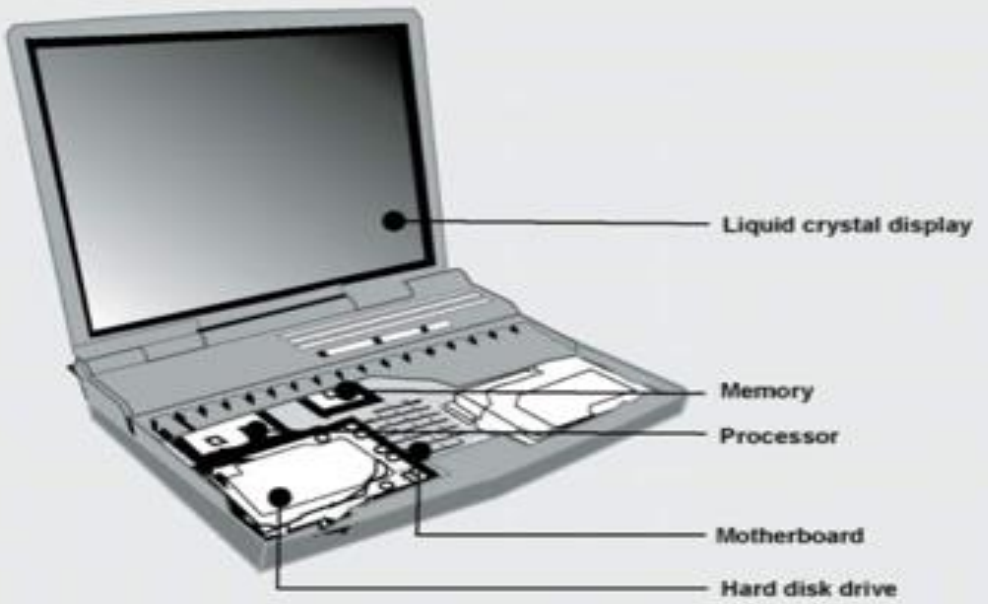
- Describe US perspective on the “cyber supply chain” problem facing defense procurement
- Outline how this problem has been, and is being, addressed in U.S. policy and law
- Focus on new U.S. Department of Defense (DOD) regulations on protecting the supply chain that change DOD/contractor and contractor/sub-contractor relationships
- Identify challenges facing present and future U.S. efforts to address cyber supply chain problems

US perspective on the cyber supply chain problem



Globalization of the cyber supply chain

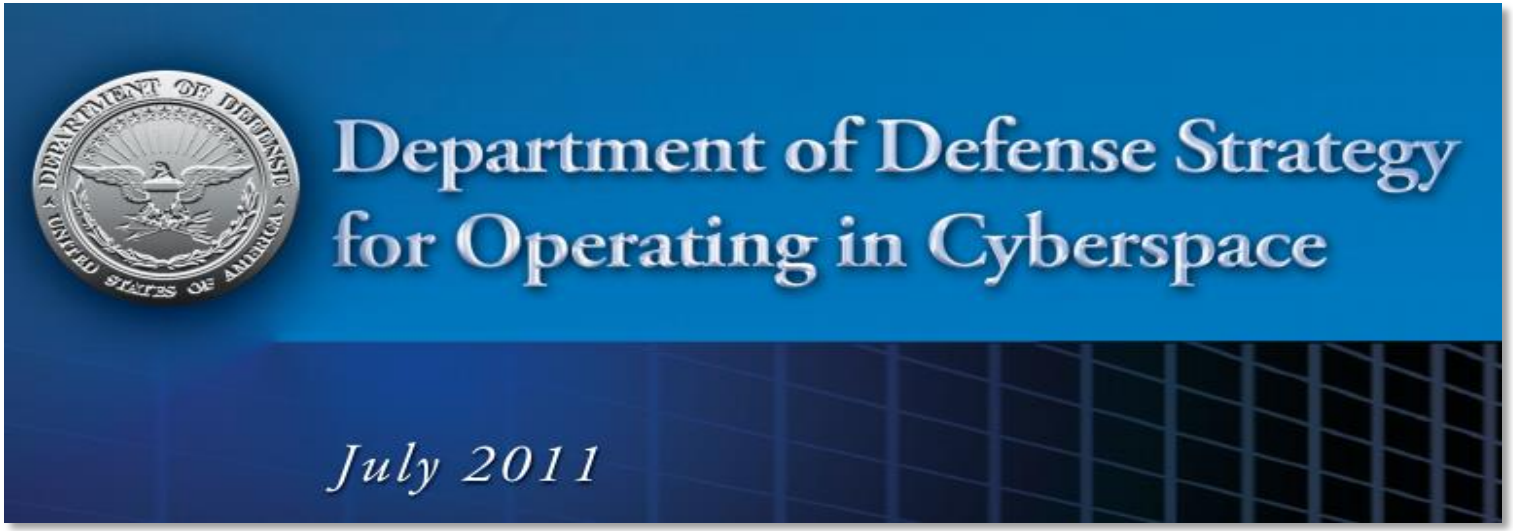
Figure 1: Potential Origins of Common Suppliers for Laptop Components



Component	Location of facilities potentially used by suppliers
Liquid crystal display	China, Czech Republic, Japan, Poland, Singapore, Slovak Republic, South Korea, Taiwan
Memory	China, Israel, Italy, Japan, Malaysia, Philippines, Puerto Rico, Singapore, South Korea, Taiwan, United States
Processor	Canada, China, Costa Rica, Ireland, Israel, Malaysia, Singapore, United States, Vietnam
Motherboard	Taiwan
Hard disk drive	China, Ireland, Japan, Malaysia, Philippines, Singapore, Thailand, United States

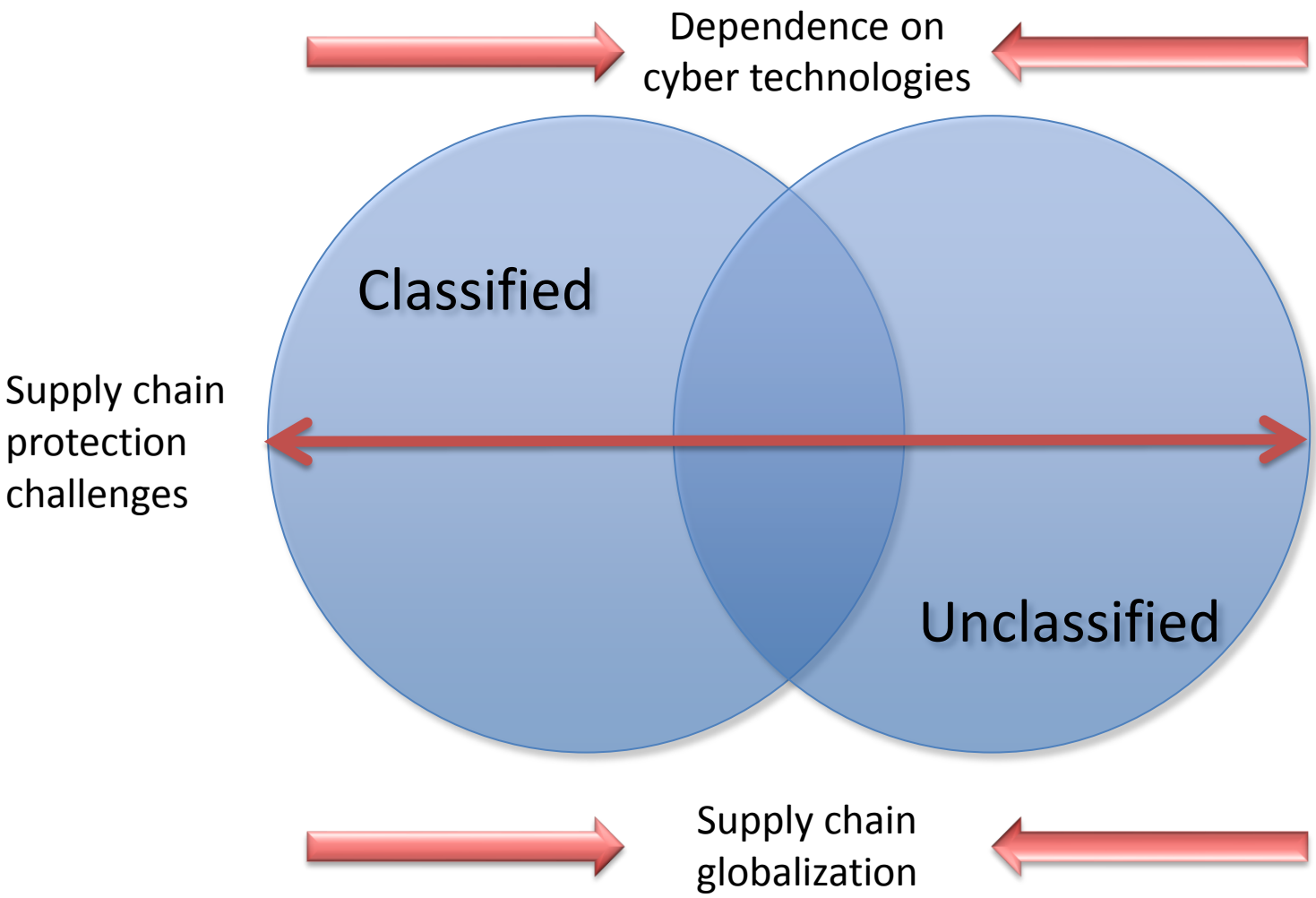
Source: GAO analysis of public information.

Defense dependence on cyber technologies

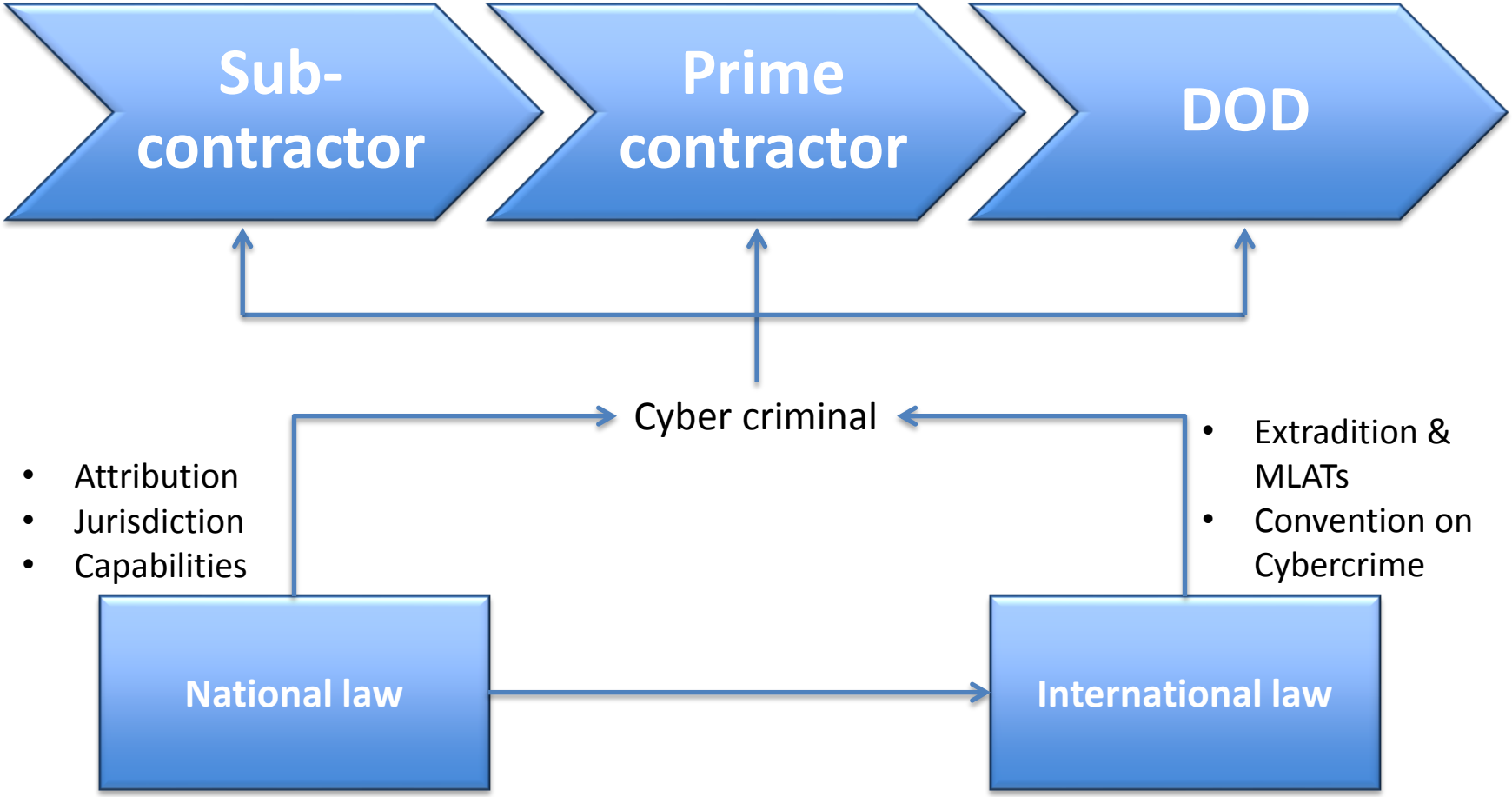


Along with the rest of the U.S. government, the Department of Defense (DoD) depends on cyberspace to function. It is difficult to overstate this reliance; DoD operates over 15,000 networks and seven million computing devices across hundreds of installations in dozens of countries around the globe. DoD uses cyberspace to enable its military, intelligence, and business operations, including the movement of personnel and material and the command and control of the full spectrum of military operations.

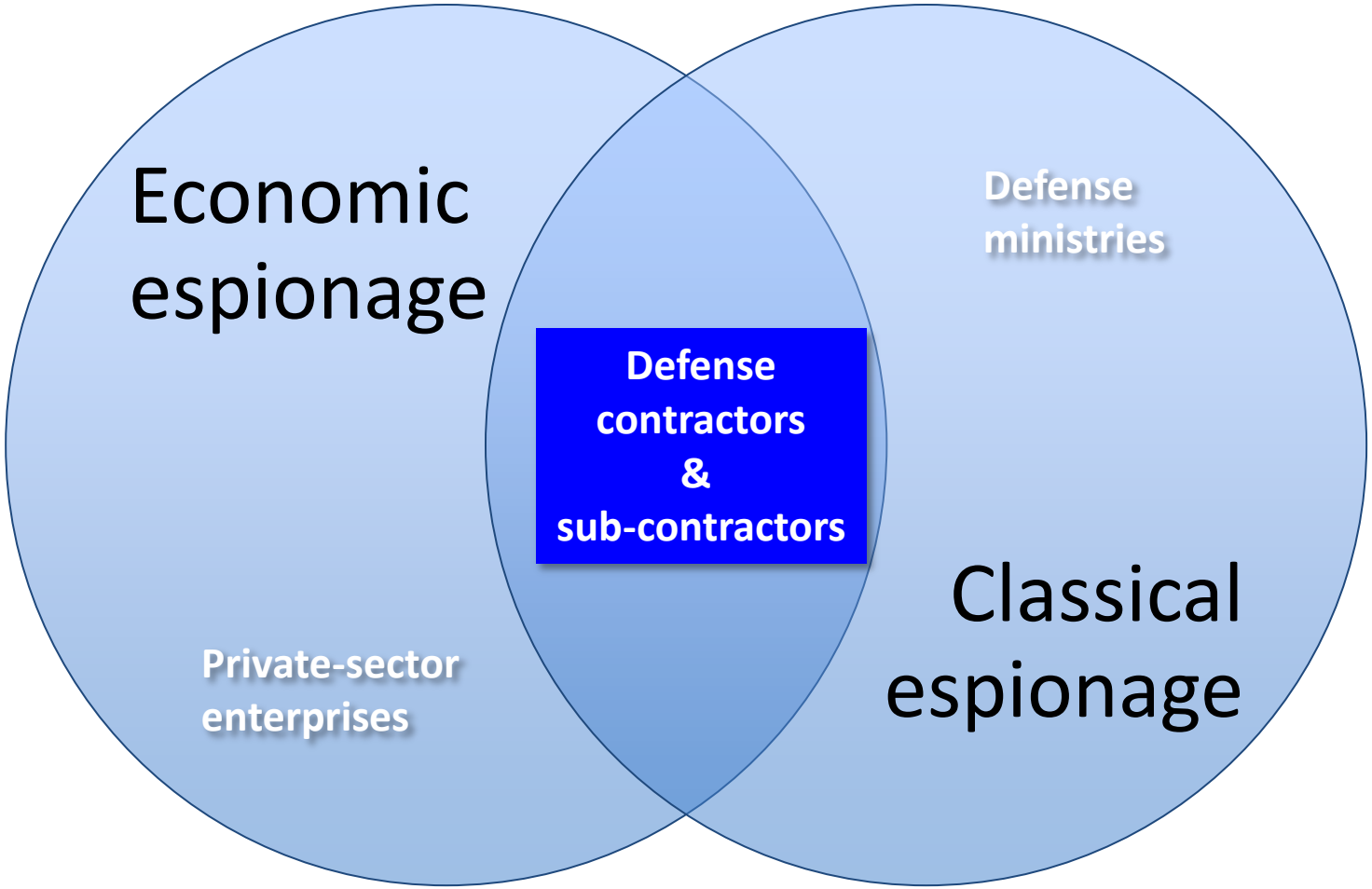
Cyber-ization and supply chain protection



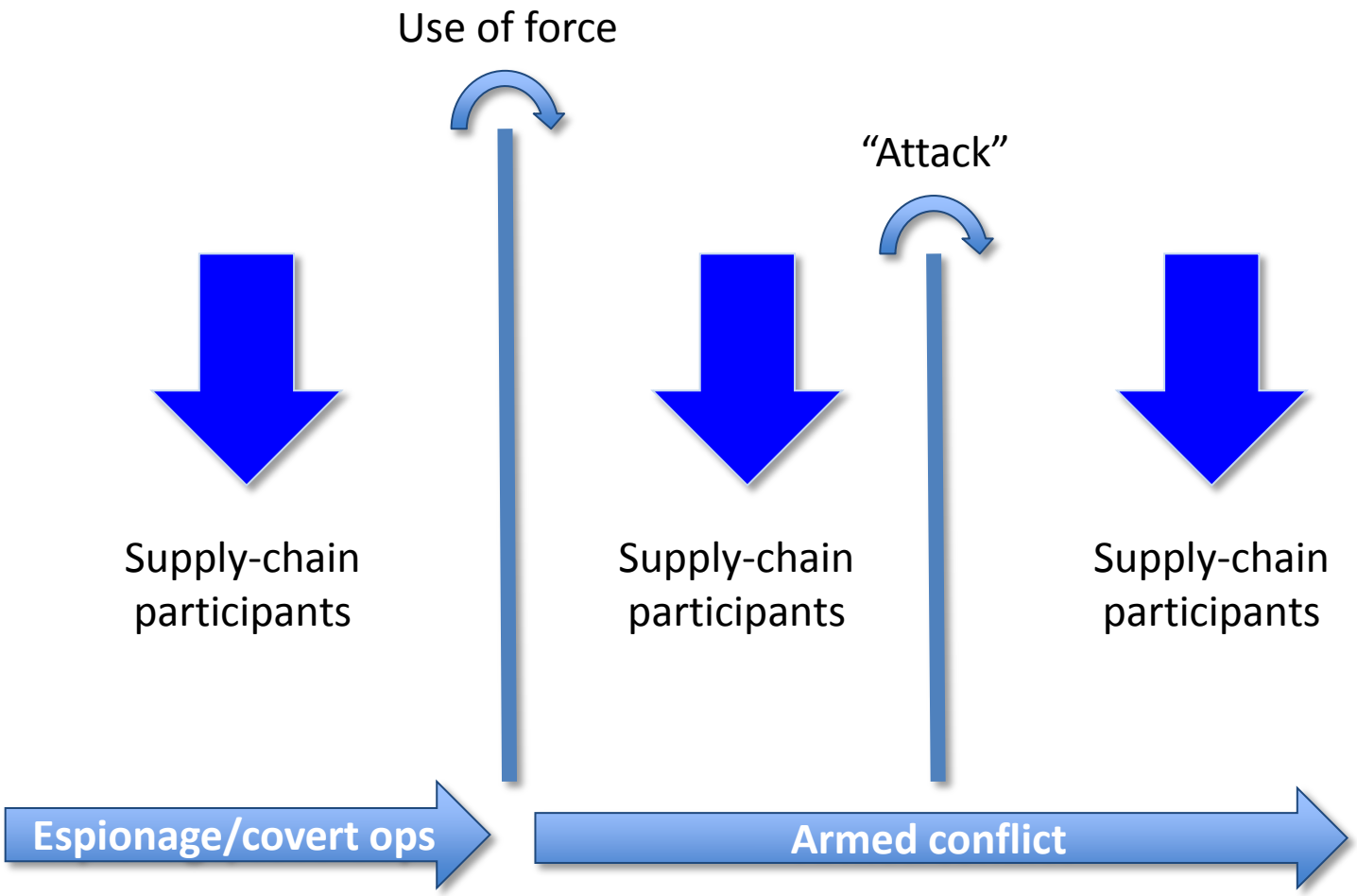
Cyber crime and supply chains: Rich target set, weak law enforcement



Cyber espionage: Supply chain as fair game under international politics and law

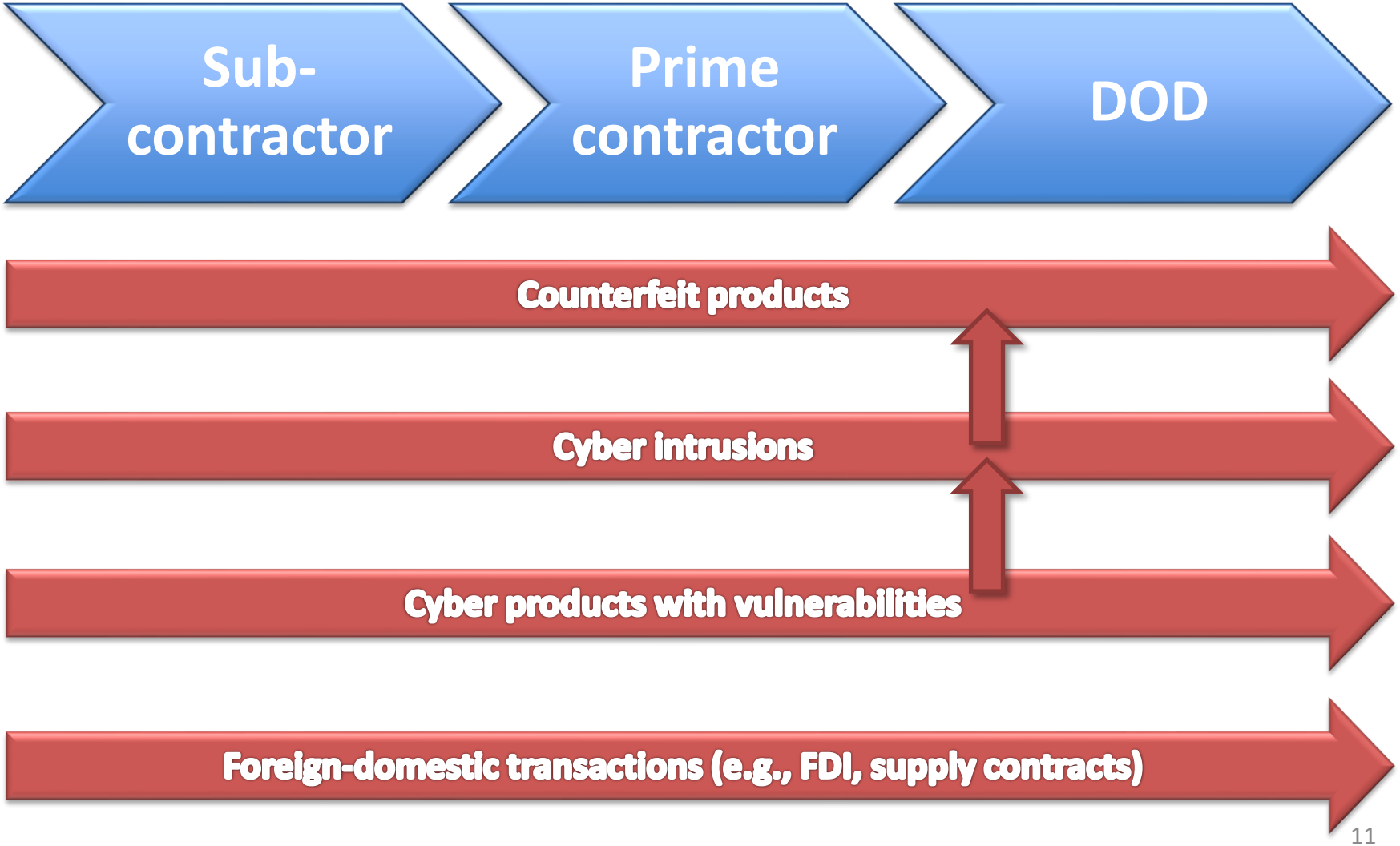


Military cyber operations: Supply-chain participants in the cross-hairs



The Chinese cyber threat

Cyber supply chain risks



Counterfeit products as a supply chain risk

BUSINESS INSIDER

More: America Military

The Navy Bought Fake Chinese Microchips That Could Have Disarmed U.S. Missiles

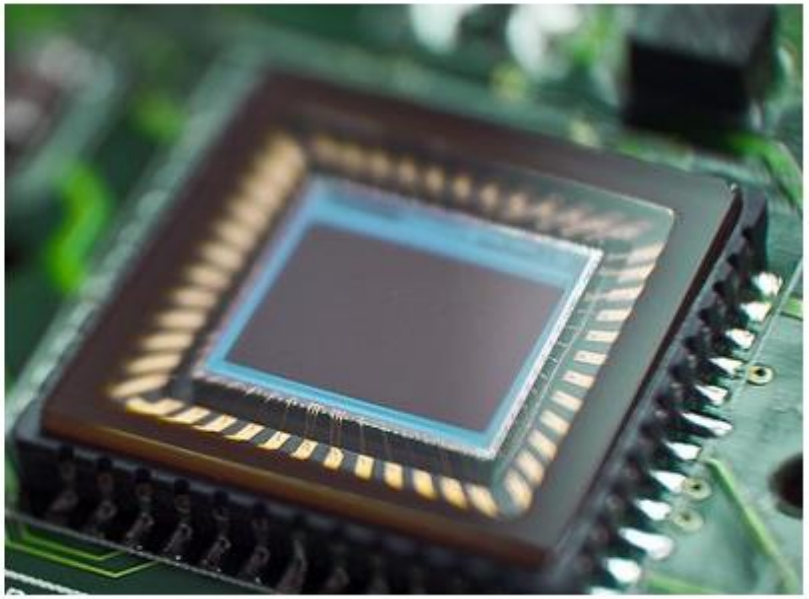
ROBERT JOHNSON

JUN. 27, 2011, 9:22 AM | 76,270 | 135

Last year, the U.S. Navy bought 59,000 microchips for use in everything from missiles to transponders and all of them turned out to be counterfeits from China.

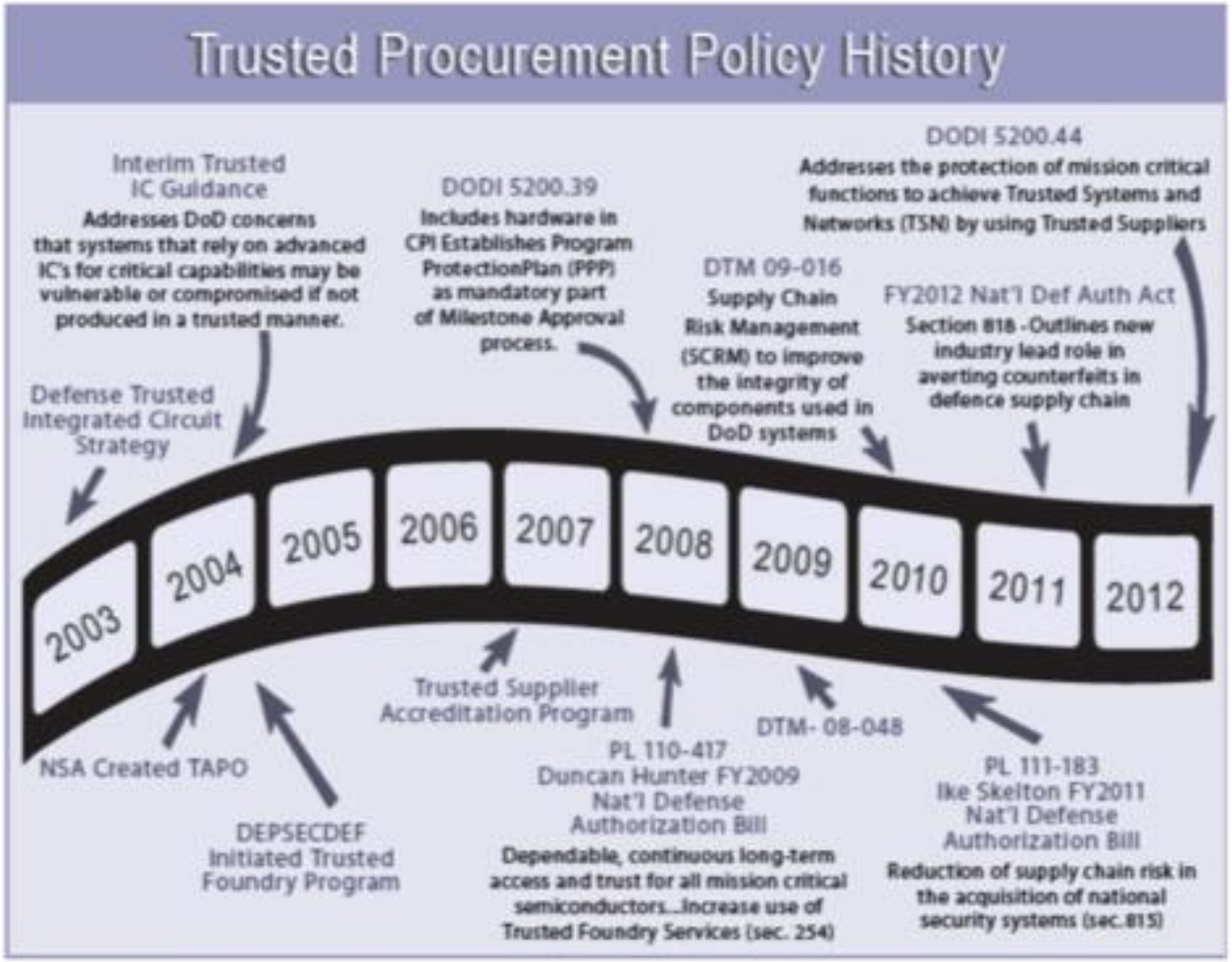
Wired reports the chips weren't only low-quality fakes, they had been made with a "back-door" and could have been remotely shut down at any time.

If left undiscovered the result could have rendered useless U.S. missiles and killed the signal from aircraft that tells everyone whether it's friend or foe.



fox o'ryan via flickr

DOD Trusted Foundry Program

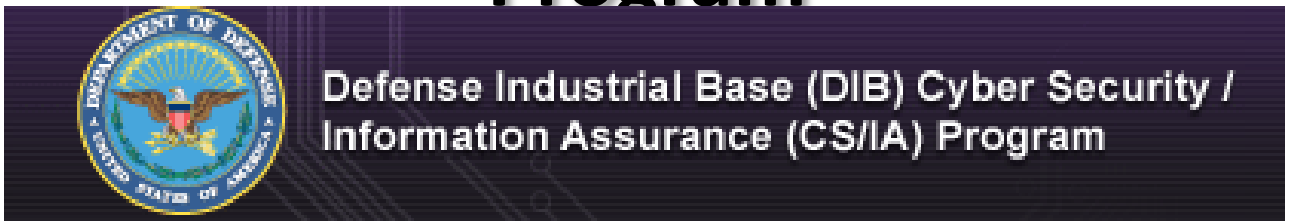


Cyber intrusions as a supply chain risk

East Asia and the Pacific collectors relied on suspicious network activity (SNA) as their foremost method of operation (MO) for attempting to obtain illegal or unauthorized access to sensitive or classified information resident in the U.S. cleared industrial base, even more so in FY12 than in FY11.

The expansion of East Asia and the Pacific cyber operations is readily observable, including in those directed against U.S. cleared industry. This growth is evident in the 1,443 percent increase in reported East Asia and the Pacific-attributed SNA between fiscal year 2009 (FY09) and FY12.

DOD Defense Industrial Base Cybersecurity/Information Assurance Program



§ 236.1 Purpose.

Cyber threats to DIB unclassified information systems represent an unacceptable risk of compromise of DoD information and pose an imminent threat to U.S. national security and economic security interests. DoD's voluntary DIB CS/IA program enhances and supplements DIB participants' capabilities to safeguard DoD information that resides on, or transits, DIB unclassified information systems.

USG policy on zero-day vulnerabilities

Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies

Recommendation 30

We recommend that the National Security Council staff should manage an interagency process to review on a regular basis the activities of the US Government regarding attacks that exploit a previously unknown vulnerability in a computer application or system. These are often called "Zero Day" attacks because developers have had zero days to address and patch the vulnerability. US policy should generally move to ensure that Zero Days are quickly blocked, so that the underlying vulnerabilities are patched on US Government and other networks. In rare instances, US policy may briefly authorize using a Zero Day for high priority intelligence collection, following senior, interagency review involving all appropriate departments.

CFIUS opposition to Huawei acquisitions

Sale of 3Com to Huawei is derailed by U.S. security concerns

By Steven R. Weisman
Published: Thursday, February 21, 2008

The New York Times

Huawei Said to Lose Out on U.S. Assets Despite Higher Offers

Bloomberg

By Serena Saitto and Jeffrey McCracken | Aug 3, 2010 12:57 AM ET | 0 Comments | Email | Print

ASIAN BUSINESS NEWS

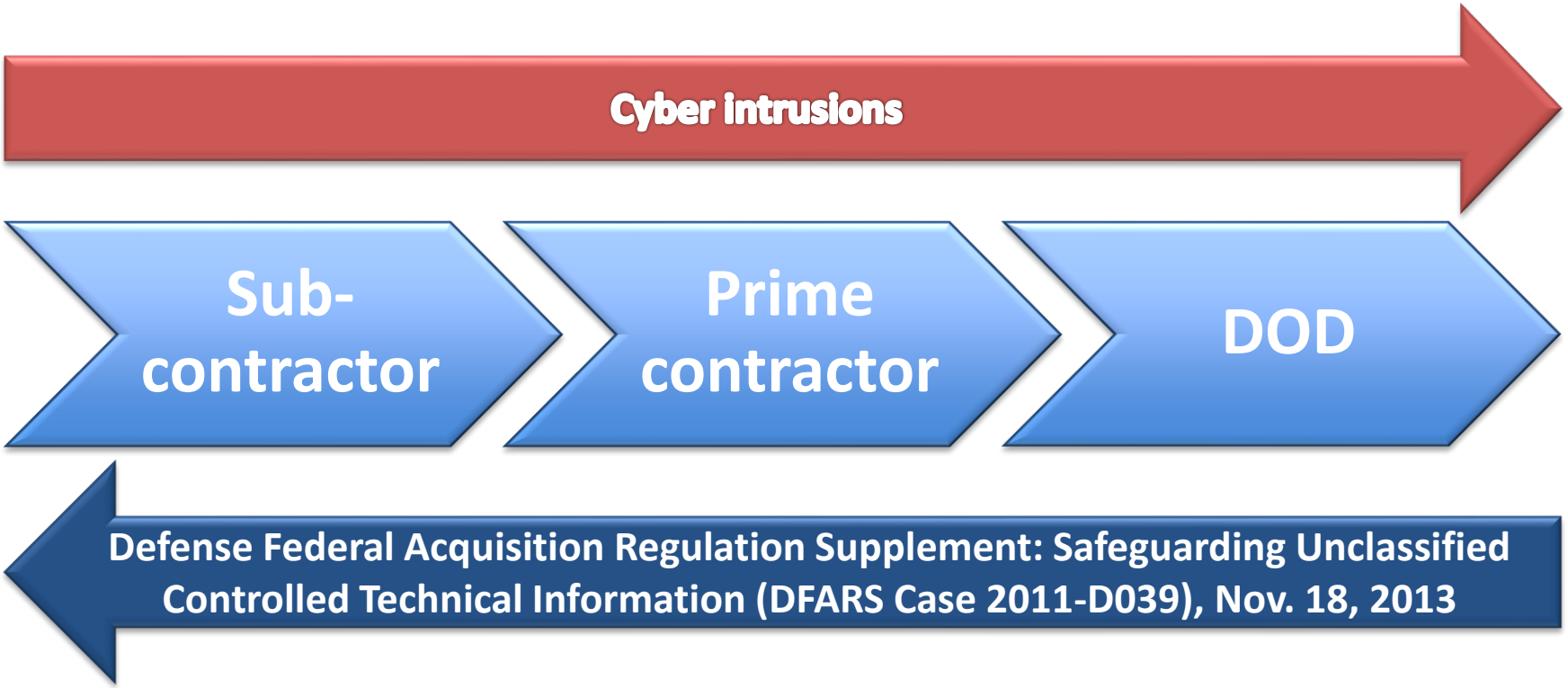
Huawei Drops U.S. Deal Amid Opposition

By SHAYNDI RAICE And ANDREW DOWELL

Updated Feb. 22, 2011 12:01 a.m. ET

THE WALL STREET JOURNAL.

DOD action on cyber intrusions: Safeguarding unclassified controlled technical information

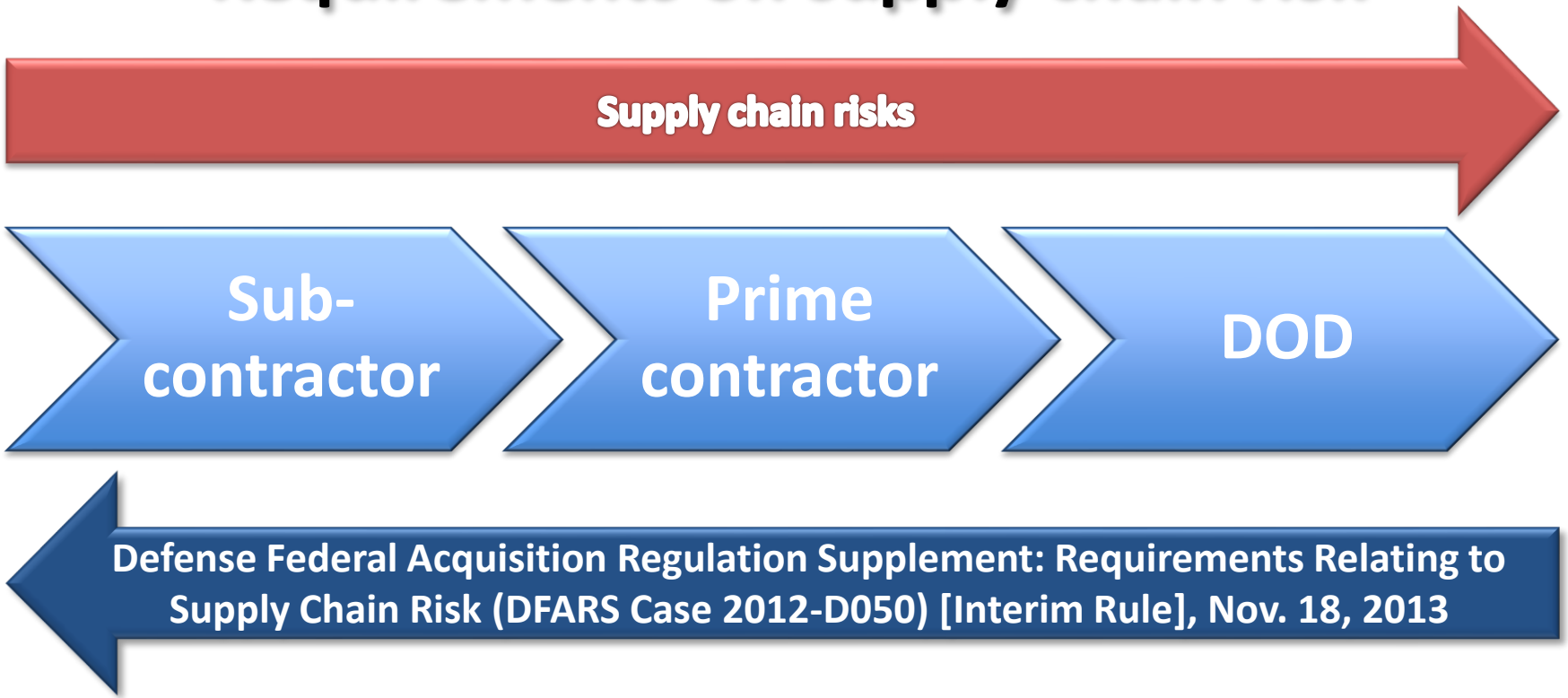


Requires contractors to flow down these requirements to all sub-contractors

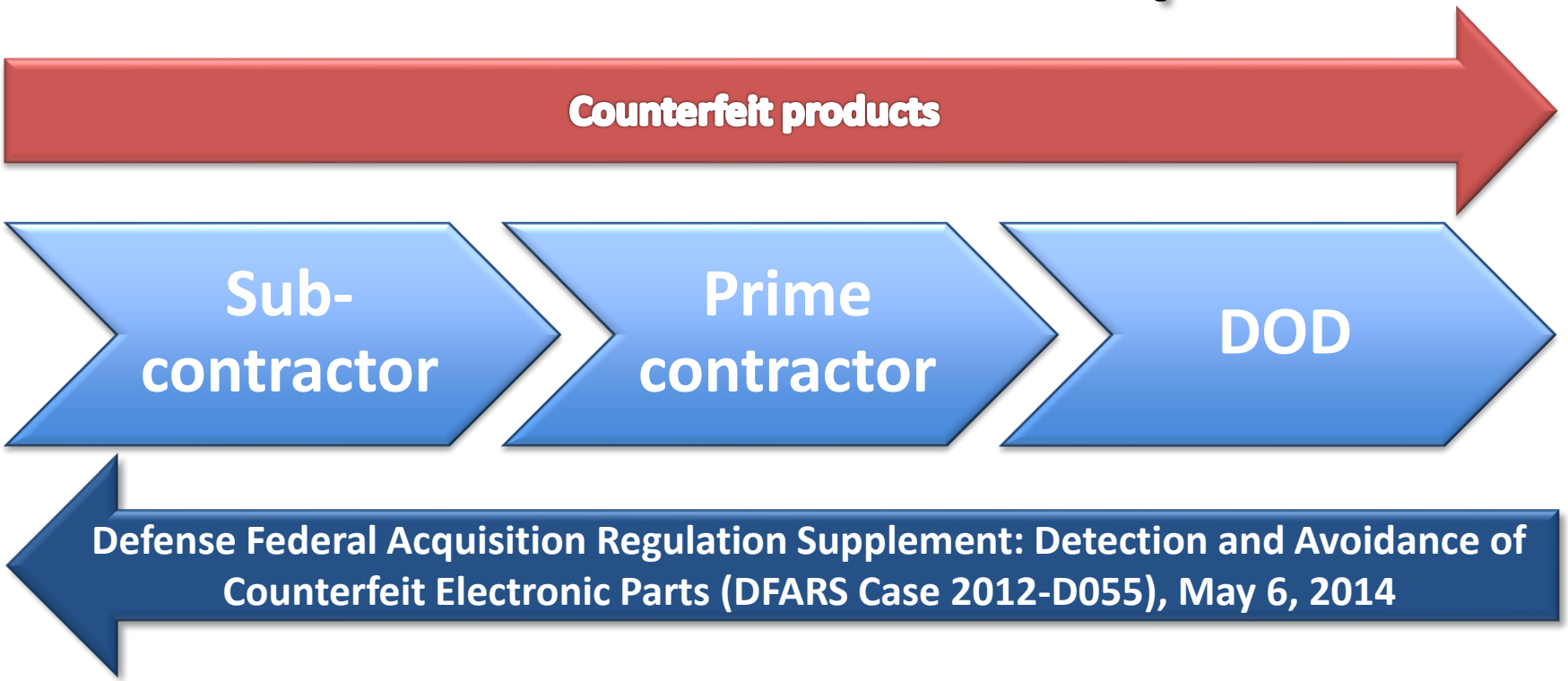
Requires contractors with access to, or that store, "controlled technical information" to implement IT network security standards

Requires contractors to report cyber incidents involving IT networks to DOD within 72 hours

DOD action on supply chain protection: Requirements on supply chain risk



DOD action on detection and avoidance of counterfeit electronic parts

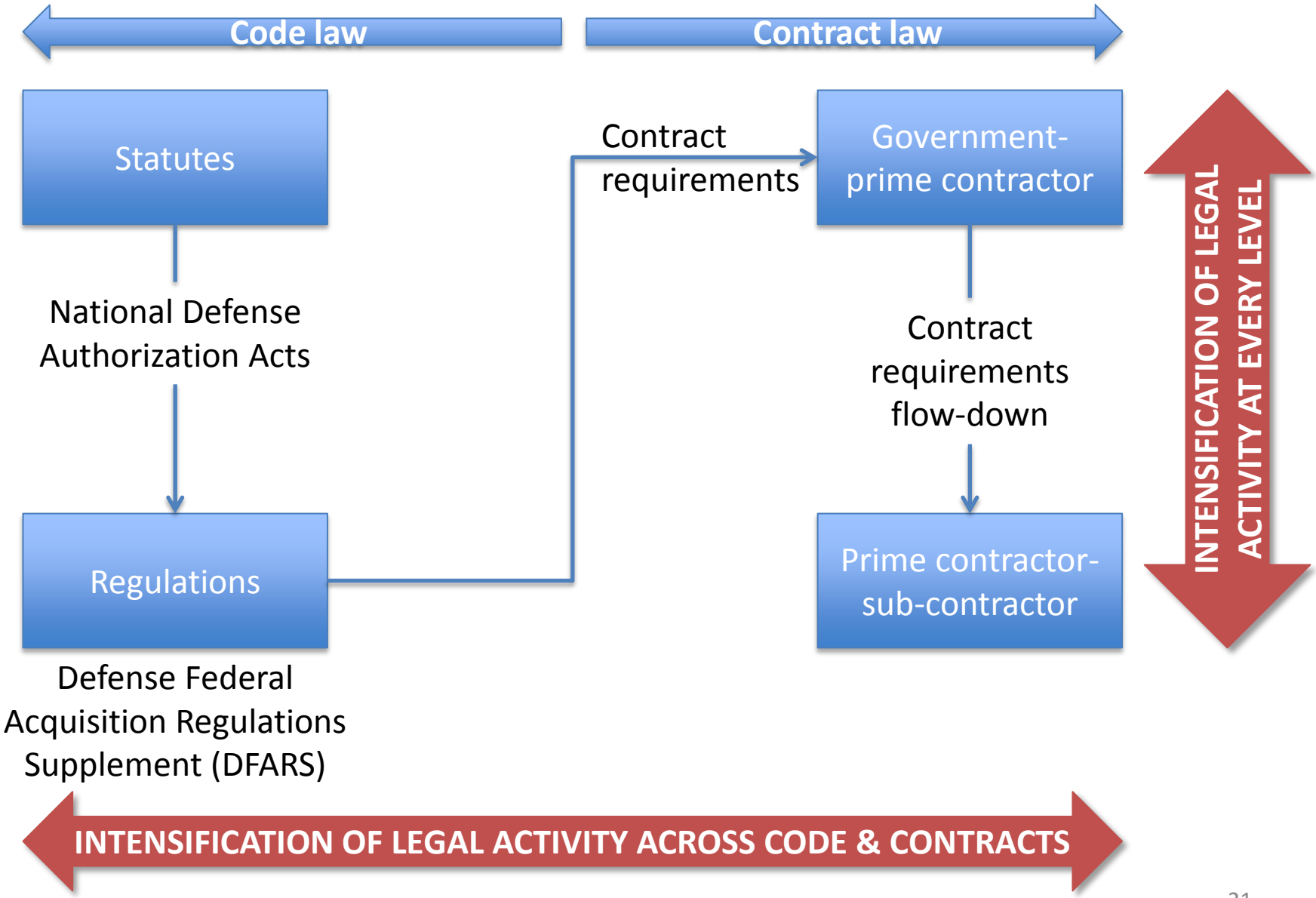


DOD procurement subject to these rules, and DOD can use requirements to review contract compliance

Requires contractors to have systems to detect and avoid counterfeit electronic parts that use risk-based criteria, including use of original manufacturers

Contractors must flow down requirements to sub-contractors, including those providing COTS electronic parts

Legal dynamics for the supply chain



Conclusion: Looking ahead at DOD/USG efforts to protect the cyber supply chain

- Key patterns:
  - Strengthen cybersecurity in procurement by balancing prescriptive rules (e.g., DFARS) with risk-based strategies (e.g., DOD shift to using NIST standards)
  - Create more harmonization across federal procurement to reduce "patchwork" of cybersecurity procurement policies and rules (e.g., Executive Order 13636 & DOD/GSA joint report)
  - Expanded and intensified role for, and impact of, law through the entire cyber supply chain (statutes→ regulations → contracts → sub-contracts)
- Uncertainty about how new rules and strategies will affect the market for defense procurement (e.g., large contractors win; mid- to small-sized contractors struggle)
- How these developments affect USG/DOD interactions with foreign companies and governments is not clear
- More cybersecurity regulations for defense procurement and federal government procurement more generally are coming . . .