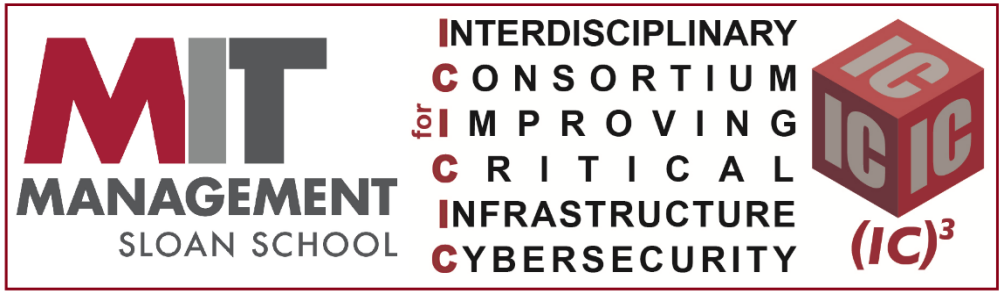


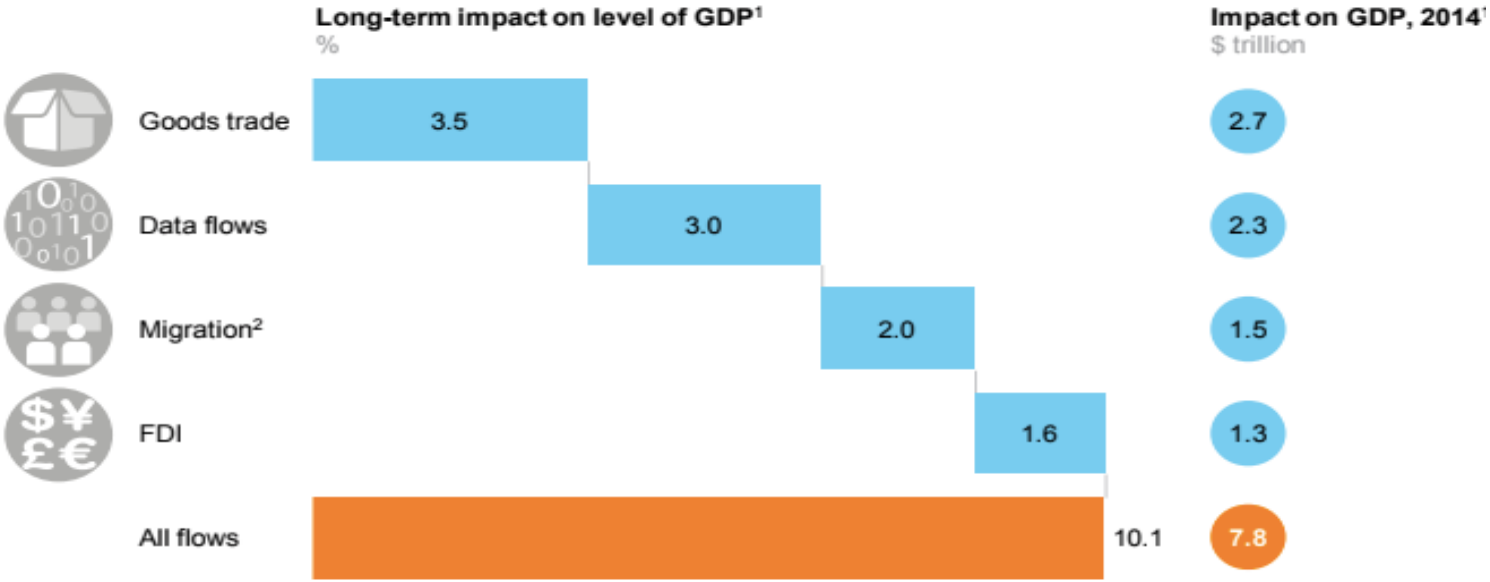
Current & Potential Cybersecurity Impacts on International Trade

Simon Johnson

MIT Sloan

Project joint with Stuart Madnick

Global trade: Physical plus Digital



The bit volume of **cross-border digital flows has grown 45 times** in the past decade.
211 +terabits of data, flow across borders every second.
12% + of global consumer goods trade is now conducted via international **e-commerce.**

Source: McKinsey Global Institute

Global supply chain behind an iPhone 6

- Touches **all** continents
- Components sourced from **31 countries, 785 factories**
- iOS app economy employs **300,000+** staff
- **In 2017,** hackers reportedly had access to 559 million Apple accounts- acquired from compromised third party services / vendors

Anatomy of a supply chain breach (physical or digital)

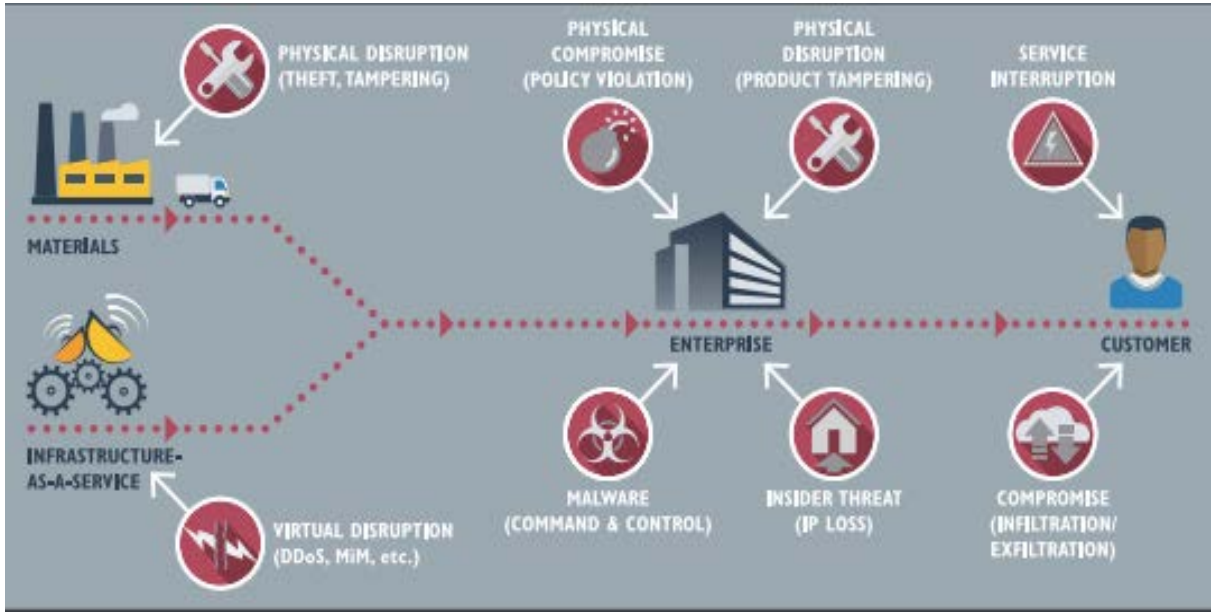
80% of information breaches originate in supply chains

45% of all breaches were attributed to past partners

59% of companies do assess cybersecurity risks of third party providers where they share data/ networks

40% of attacks targeted manufacturing and service sectors

.

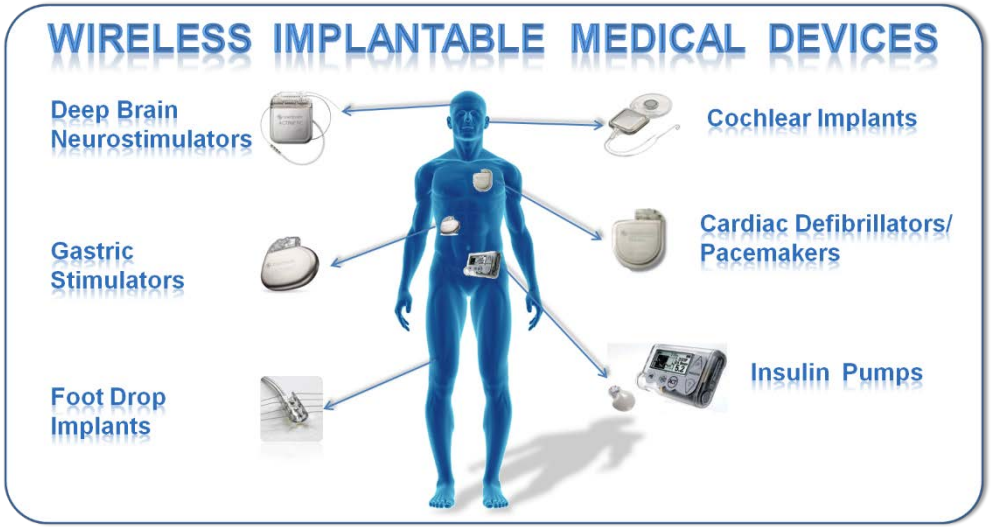


Source- RSA 2016 conference

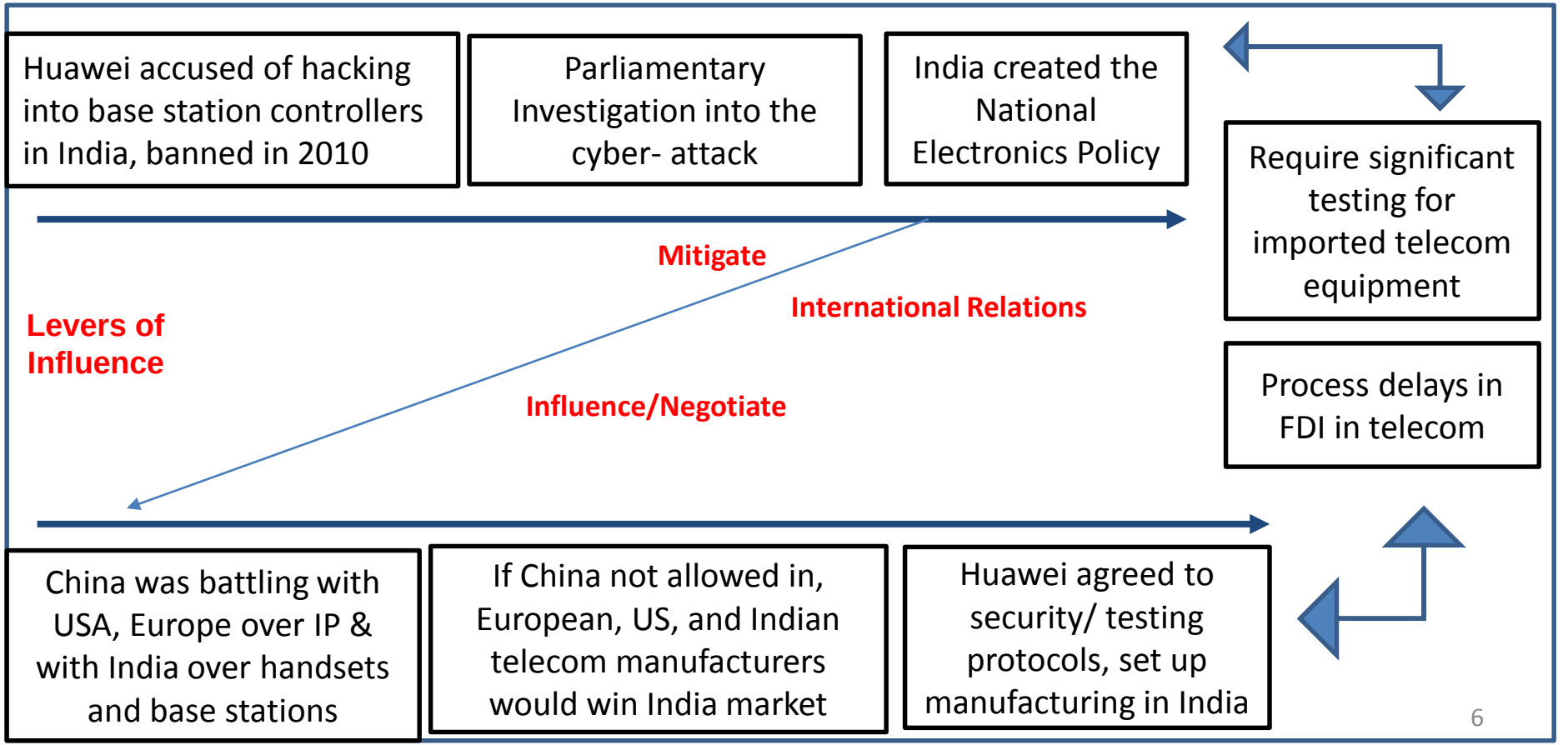
IoT Devices Become Compelling

e.g., medical devices

- Healthcare enabled by IoT worth over $117 billion by 2020
- Opens doors to new business models where data is more valuable than devices
- Medical devices partnering with adjacent industries such as software
- X-ray equipment, Therapeutic equipment (infusion pumps, medical lasers), and Life support equipment are vulnerable to malware
- Medical information worth 10 times that of a credit card number



Issue is Everywhere Trade Takes Place: e.g., Huawei in India



MIT-IPRI Research

Issue: Some countries have inserted (or might insert) malware into products and services that are exported into other countries.

(Or vulnerabilities were created unintentionally, but how would you know?)

In response to this threat (or perceived hostile action), some countries may ban products, starting a potential digital trade war

This seems more likely as IoT devices spread through various sectors

The negative impact of political backlash on international trade would be significant

In this research project we explore:

- How governments can and should (legitimately) react
- The likely future of cross-border trade & safeguards that prevent trade wars
- Impact on businesses that export or import

Common themes in 50 case studies (so far)

- **Categorization /ontology**: These cybersecurity issues do **not fall neatly into a single set** of rules. They span espionage and theft, privacy and data protection, cross-border trade and investment in ICT, and cross-border criminal enforcement.
  - These threats are **industry agnostic:** they can impact almost everyone, except perhaps a brick manufacturer,
  - e.g., The 'My Friend, Cayla' doll regarded as spying on children
- **Suggest best actions for businesses:** companies cannot ignore the economic-political spillover effects of cyber threats
  - Identify and share best practices for anticipating or reacting to problems
  - Establish shared norms/expectations for ensuring software upgrades across all IoT elements
  - Educate consumers and other final users
- **Suggest best actions for governments:** preferably negotiations (e.g., US-China agreement on economic espionage)
  - Agree in advance on how to deal with events, based on existing inter-governmental structures

How Can We Help You?

If you want to learn more about this research or work with us

Simon Johnson- sjohnson@mit.edu

Research Assistants
Keman@mit.edu Prema@mit.edu