



Potential Risk to the Lifecycle Process

Jeffery E. Gaines Sr, Acting Director

**Community Acquisition Risk Section
Office of National Counterintelligence Executive
Office of the Director of National Intelligence**

17 Sept 2009

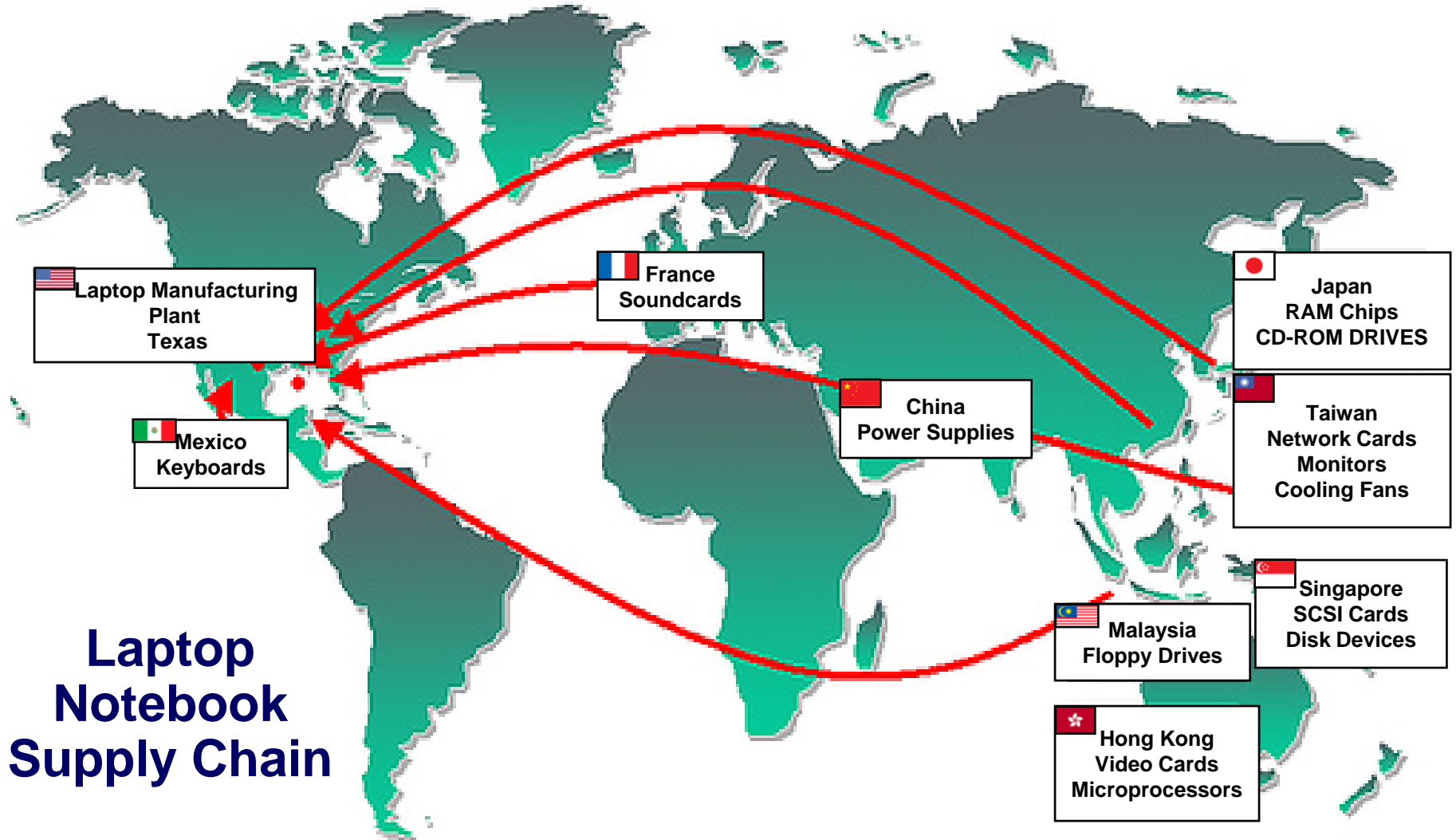
DRAFT: Pre-Decisional Working Document



Introduction

- The globalization of IT hardware and software products being built and maintained by foreign vendors provides our adversaries with a greater opportunity to manipulate IT products and exploit USG networks. During this session we will discuss policies and initiatives that identify ways to either mitigate or eliminate potential threats to the lifecycle process.

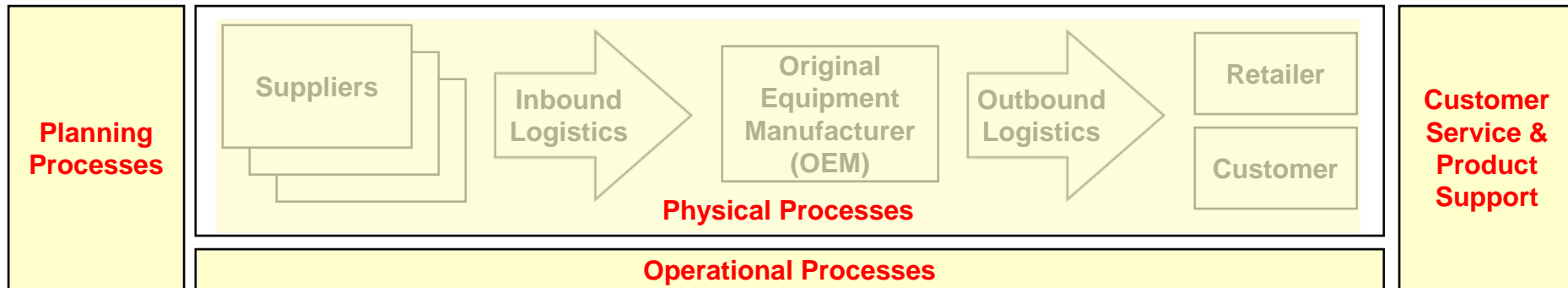
IT products available from US vendors have foreign components



Source: *The World is Flat* Thomas Friedman, Ch. 12

Supply Chain Process Descriptions

The Supply Chain



▪ Planning Processes

- Collection of processes that contribute to product design, plant and package design, logistics planning, purchasing, and operations planning

▪ Physical Processes

- Intermingled processes that contribute to the supply, transfer, production, and delivery of finished products

▪ Operational Processes

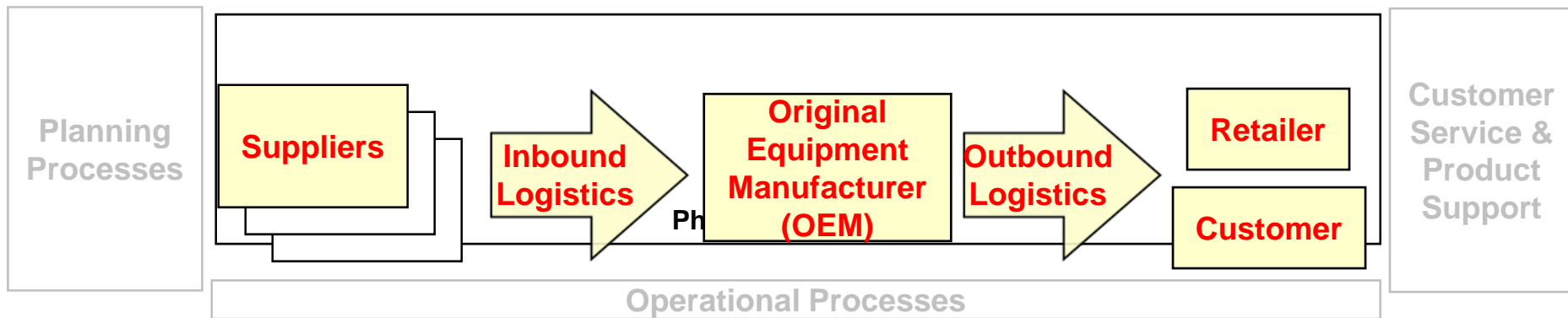
- Processes performed periodically to guarantee the physical processes in the supply chain are operating efficiently and effectively

▪ Customer Service & Product Support

- Third party or vendor support processes to service a product

Physical Process Node Descriptions

The Supply Chain



▪ Suppliers

- Secondary companies that build and supply Original Equipment Manufacturers (OEMs) with component parts

▪ Inbound/Outbound Logistics

- Management and integration of information, transportation, inventory, warehousing, material handling, and packaging of goods, information, and other resources between the point of origin and the point of consumption

▪ Original Equipment Manufacturer (OEM)

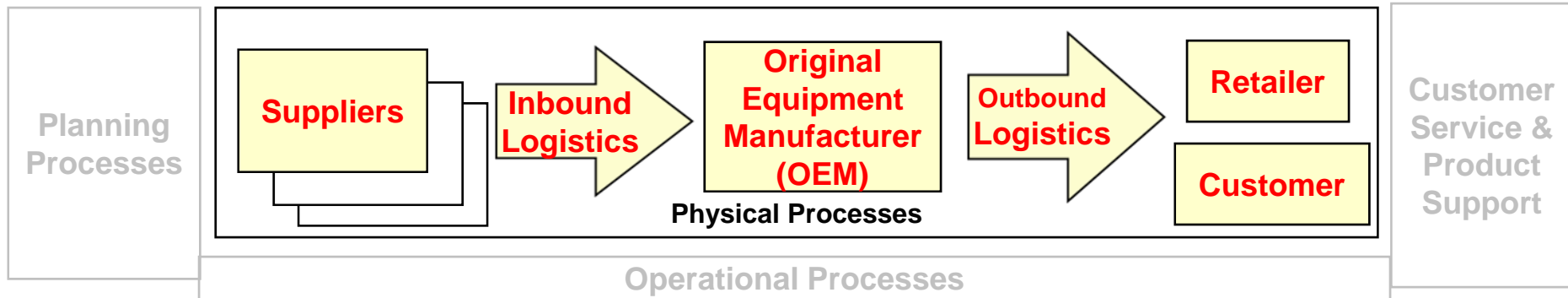
- A company that purchases components from secondary companies for use in its own products

▪ Retailer/Customer

- Consumers of products manufactured by the OEM

Examples

The Supply Chain



▪ Suppliers

- Microsoft Windows Operating System, Microsoft Corporation
- Optical CD/DVD-ROM Drives, Toshiba

▪ Inbound/Outbound Logistics

- Storage of products, Warehouse
- Transport of products, Truck or Railcar

▪ Original Equipment Manufacturer (OEM)

- Laptop Manufacturer, Dell Computers
- Desktop Manufacturer, HP

▪ Retailer/Customer

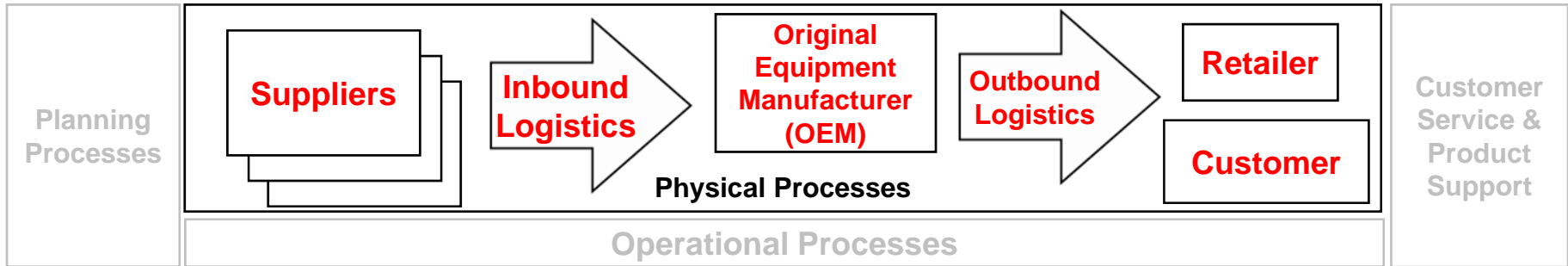
- Consumer Electronic Retailer, Best Buy, Direct Customer, Joe Somebody



Examples of Risk



Supply Chain Risks



- **Suppliers:** Inability/difficulty in determining the trustworthiness of service providers (e.g., installation, operations, and maintenance).
 - Global merchants, with no particular country of allegiance, will become bigger and more efficient players in transferring US technology.

- **OEM:** Introduction of exploitable vulnerabilities systems when products containing malicious code and other malware;
 - Cybertools will increasingly be used to extract sensitive trade secrets, particularly as international supply chains—where foreign firms become the major providers of key software and hardware components—create significant vulnerabilities.

- **Retailer/Customer:** Inability/difficulty in determining the trustworthiness of systems that depend upon commercial information technology products; and
 - Third-country venues may become increasingly important locations for acquisition of US technology.



Lifecycle Risk Mitigation Approach

| Life Cycle Stages | Design | Manufacturing | Integration | Distribution | Operations | Services/ Maintenance | Retirement |
|-----------------------------------|--|---|---|--|--|--|---|
| Sample Protective Measures | <ul style="list-style-type: none"> • Use vetted providers and industry best practices | <ul style="list-style-type: none"> • Employ service level agreements related to quality and security | <ul style="list-style-type: none"> • Limit online SW installations • Thoroughly vet updates | <ul style="list-style-type: none"> • Use secure distribution channels | <ul style="list-style-type: none"> • Implement and enforce traditional information assurance policies | <ul style="list-style-type: none"> • Confirm the integrity of network mapping | <ul style="list-style-type: none"> • Secure destruction of media and computers |

← To meet tomorrow's threat we must develop protection measures across product lifecycle *and* reinforce these measures through acquisition processes and effective implementation of agency security practices →



Contact Information



Jeff Gaines, Jr.

ejeffg@dni.gov

571-204-5138