



# Cyber Threats: What You Should Know

**This briefing is UNCLASSIFIED**

**03 May 2006**

**UNCLASSIFIED**

# Overview



- **Purpose**
- **Background**
- **Information Technology (IT) dominance in the “Flat World”**
- **Computer threat capabilities related to IT globalization**
- **An example: China**
- **Potential impacts on lifecycle of DOD C4I systems**
- **Why an accelerated awareness campaign is needed**
- **Summary**

# Purpose



- **Create greater awareness of the rapid and potentially profound changes in the Information Technology (IT) security arena driven by globalization**
- **Stimulate discussion about acquisition strategies to mitigate emerging threats to DOD computer networks caused by IT globalization**
- **Provide better understanding of the long-term threat implications of foreign developed IT in U.S./ DOD critical systems**



## Foreign IC Manufacture Includes Potential Threats

“...The shift from United States to foreign IC manufacture ... opens the possibility that **“Trojan horses” and other unauthorized design inclusions may appear in unclassified integrated circuits** ... in military applications. These surreptitious inclusions are similar to viruses, Trojan Horses, and worms common in today’s public software networks.

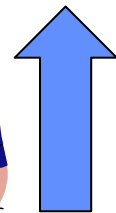
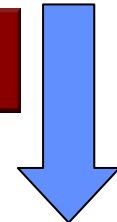
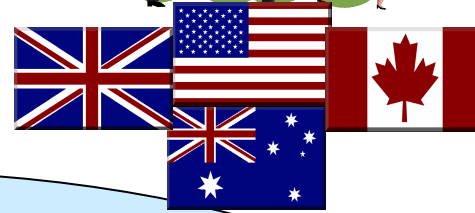
“...Such backdoor features could be used by an adversary to disrupt military systems at critical times ...”

“... For the DOD’s strategy of information superiority to remain viable, the Department requires: **Trusted** and assured supplies of integrated circuit (IC) components...” “...**Trust cannot be added to integrated circuits after fabrication...**”

Source: Defense Science Board Report: High Performance Microchip Supply  
24 Feb 2005 ([http://www.acq.osd.mil/dsb/reports/2005-02-HPMS\\_Report\\_Final.pdf](http://www.acq.osd.mil/dsb/reports/2005-02-HPMS_Report_Final.pdf))

UNCLASSIFIED

# Dominance in Commercial Off-the-Shelf (COTS) IT 2005-2015

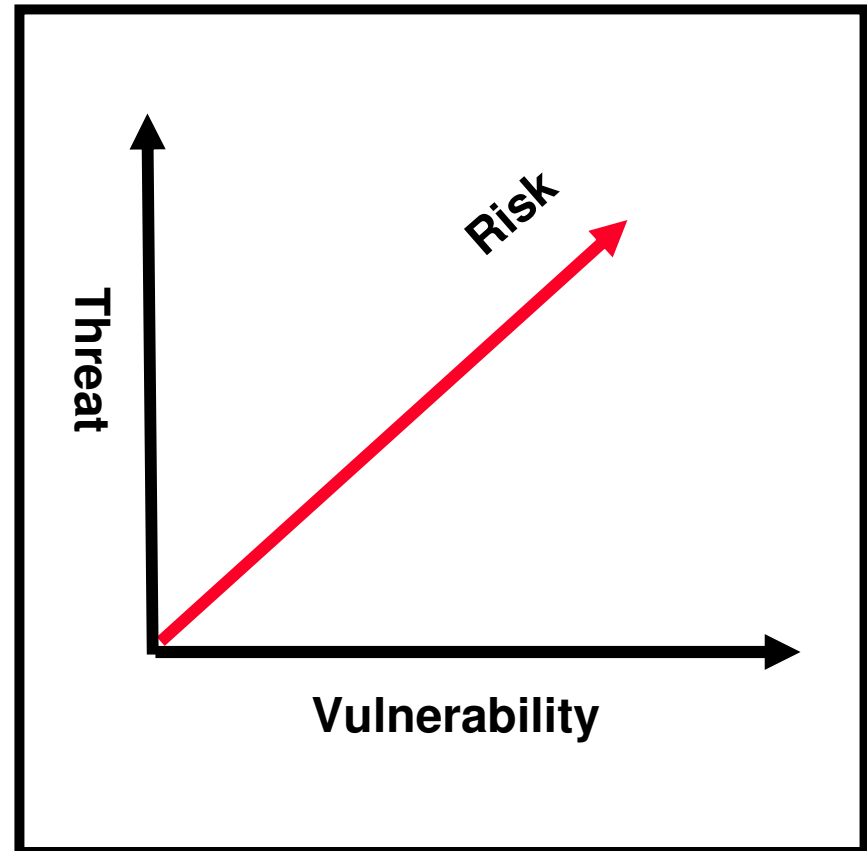


UNCLASSIFIED

# Vulnerability and Threat Relationship



- **Risk** – “... generally defined as the coexistence of threat and vulnerability”
- **Vulnerability** – “... a weakness in an information system (IS), system security procedures, internal controls, or implementation that could be exploited.”
- **Threat** – “... any circumstance or event with the potential to cause harm to an IS through unauthorized access, destruction, disclosure, modification of data, and/or denial of service.”



Source: DOD 8510.1-M

UNCLASSIFIED

# Types of Cyber Threat Actors



- **Unstructured**

- Individuals or small groups, often with limited skill
- No state sponsorship
- Limited resources
- May not have a focused objective, other than hacking for the sake of hacking

- **Structured**

- Controlled by nation-state, terrorists, organized crime
- Significant resources potentially available
- Activity may show great subtlety and technical sophistication
- Often a focused, long-term objective, such as intelligence collection or disruption of computer networks

# Subversion and the Professional Cyber Attacker



- **Subversion**: ‘... the covert and methodical undermining of internal and external controls over a system lifetime to allow unauthorized or undetected access to system resources and/or information.’
- **Professional cyber attacker**:
  - Distinguished from amateur by objectives, resources and time
  - Concerned with avoiding detection – plans for plausible deniability
  - Understands system lifecycle -- plans operations around weaknesses in entire lifecycle
  - Invests significant time and is willing to wait years before reaping the benefits

**“Due to the existence of means, motive, and opportunity to conduct subversive attacks in the current environment, subversion should be viewed as a real threat.”**

Source: Anderson, Irving, Schell, *Subversion as a Threat in Information Warfare*, 2004

UNCLASSIFIED

# Nation-state IT Dominance Strengthens CNA/CNE Capabilities



**Threat CNA/CNE capabilities consists of foreign:**

- **Access**
- **Technical Expertise**
- **Operational Reach**



• **Computer network attack (CNA)** - operations to disrupt, deny, degrade, or destroy information in computer networks or the computers and networks themselves.

• **Computer network exploitation (CNE)** – intelligence collection and the enabling operations to gather data from target or adversary networks.

# A Example: China



- **China's is a fast emerging Global IT power – it will likely be the global commercial IT leader in 3 to 5 years; given current trends, it could become a primary supplier of commercial IT to the U.S./DOD by 2010**
  - In 2004, China became the biggest exporter of information technology goods surpassing the U.S. and the E.U., according to the Organization for Economic Co-operation and Development (OCED).
  - In 2005, China attracted more venture capital than the U.S. for the first time.
- **Large Information Warfare Footprint – “The Chinese People’s Liberation Army (PLA) has likely established information warfare units to develop viruses to attack enemy computer systems and networks... Recent exercises have incorporated offensive operations, primarily as first strikes against enemy networks...” (DOD Annual Report to Congress, The Military Power of the People’s Republic of China, 2005)**

# Taiwan's High Tech Clout



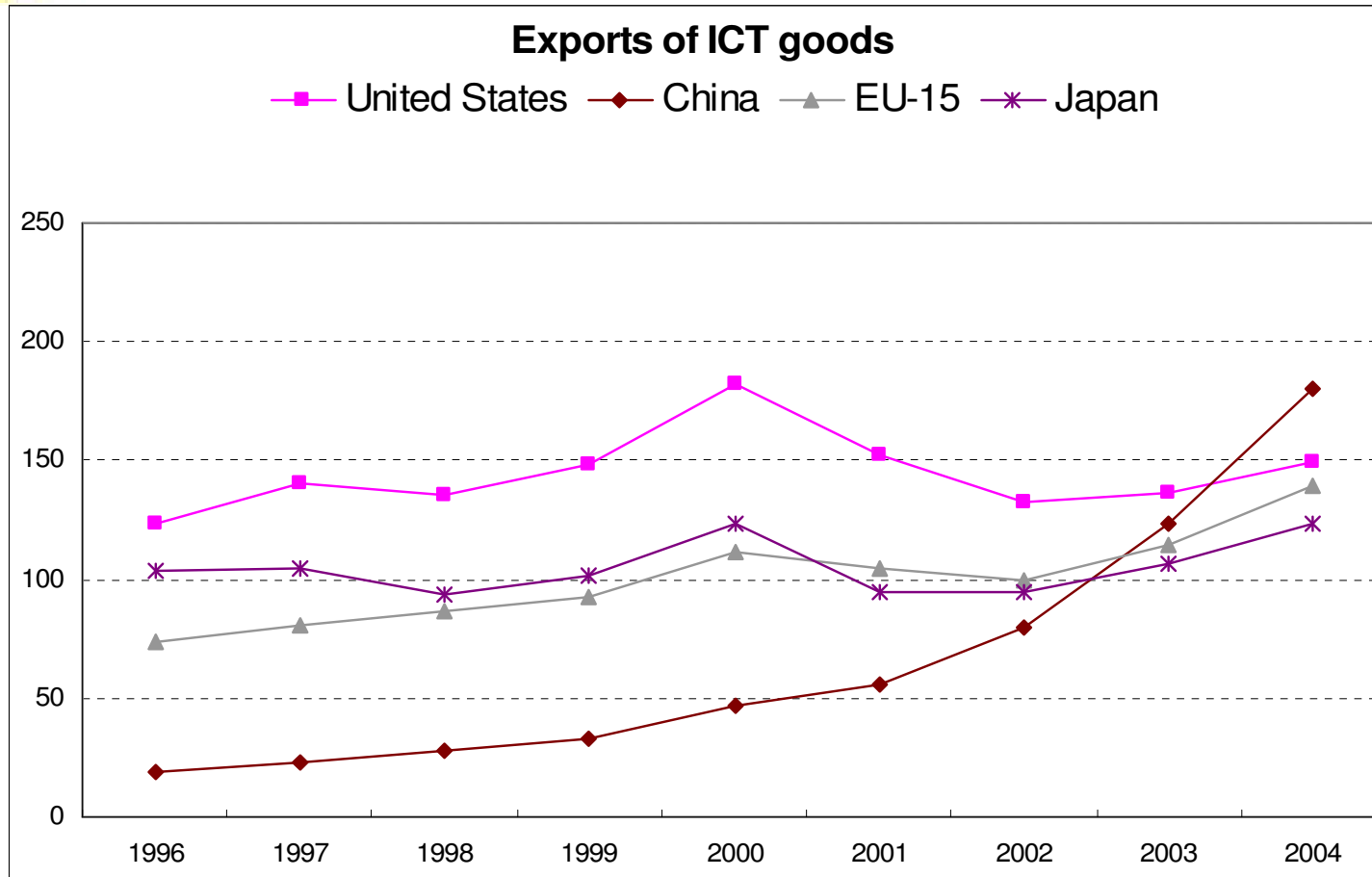
World Rank	Technology	Market Share	Sales
#1	Wireless LAN equipment	83%	\$1.3B
#1	PDA's	79%	\$1.8B
#1	Notebook PC's	72%	\$22B
#1	Chip Foundry services	70%	\$8.9B
#1	LCD monitors	68%	\$14B
#1	Cable modems	66%	\$480M
#1	Semi-conductor packaging	36%	\$3.4B
#2	TFT-LCD panels	35%	\$7.6B
#2	Servers	33%	\$1.8B
#2	Digital still cameras	34%	\$2B

Source: BusinessWeek Online, 2005

**Most products are not under Taiwan Company names  
Most are actually made in mainland China**

UNCLASSIFIED

# China's IT Exports Exceeded that of U.S. in 2004



Source: OECD ITS database

UNCLASSIFIED

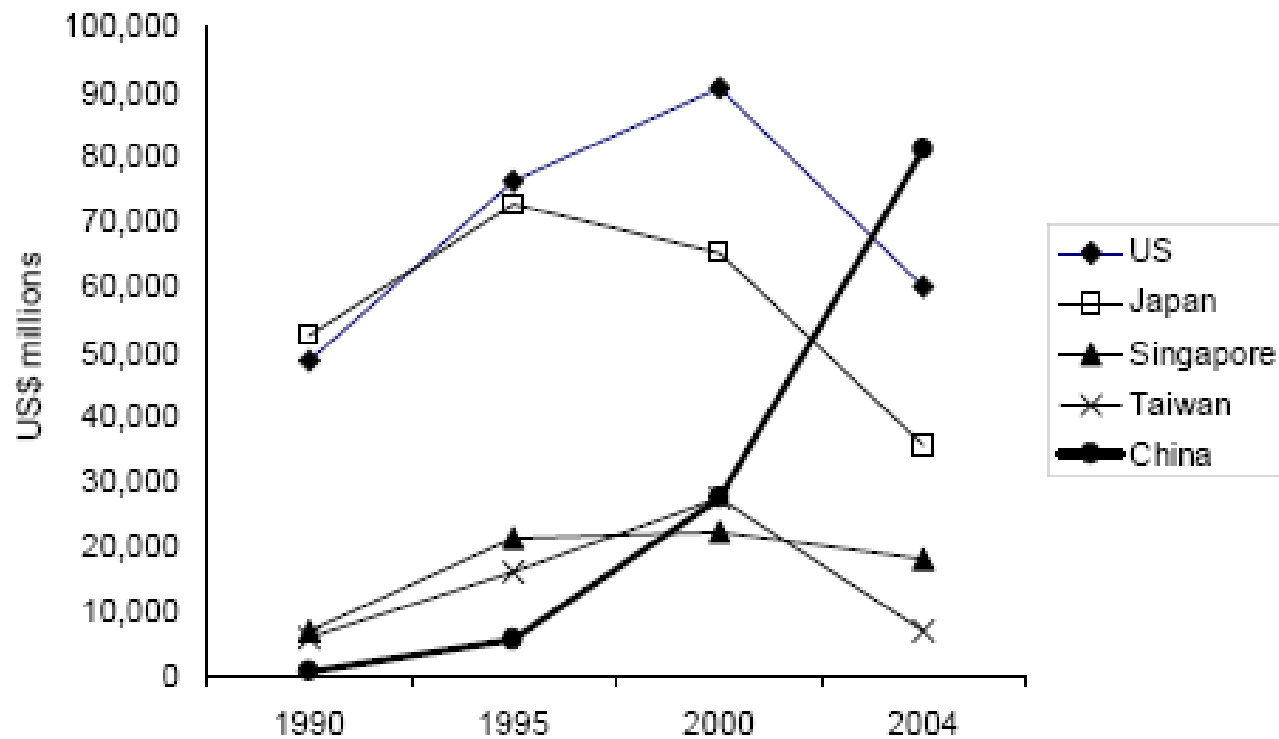
# U.S. Trade in Information & Communications Advanced Technology Products (ATP) - 2004



Country	U.S. Exports	U.S. Imports	Net Balance	Imports as Percent of U.S. Imported ATP
<b>China</b>	<b>2,156,378</b>	<b>41,380,304</b>	<b>(39,223,926)</b>	<b>31.2</b>
Hong Kong	1,635,297	786,267	849,030	0.5
Indonesia	86,030	871,777	(785,747)	0.6
Japan	4,191,831	12,077,834	(7,886,003)	9.1
Malaysia	819,470	14,231,831	(13,412,361)	10.7
Philippines	173,724	1,368,606	(1,194,882)	1.0
Singapore	1,949,554	7,537,776	(5,588,222)	5.6
South Korea	1,220,219	12,742,782	(11,522,563)	9.6
Taiwan	1,240,459	8,077,139	(6,836,680)	6.0
Thailand	753,775	3,758,639	(3,004,864)	2.8
Vietnam	35,372	6,919	34,673	0.0
Sub-total	14,262,109	102,839,874	(88,577,765)	77.1
European Union	15,236,472	7,484,779	7,751,693	5.6
<b>U.S. Total*</b>	<b>59,210,057</b>	<b>132,538,953</b>	<b>(73,328,896)</b>	----

\*U.S. Total includes rest of world Source: Calculated from ATP data, "Foreign Trade Statistics," U.S. Census Bureau, April 2005 **UNCLASSIFIED**

# China's Growth in Computer Hardware Production (2000-2004)



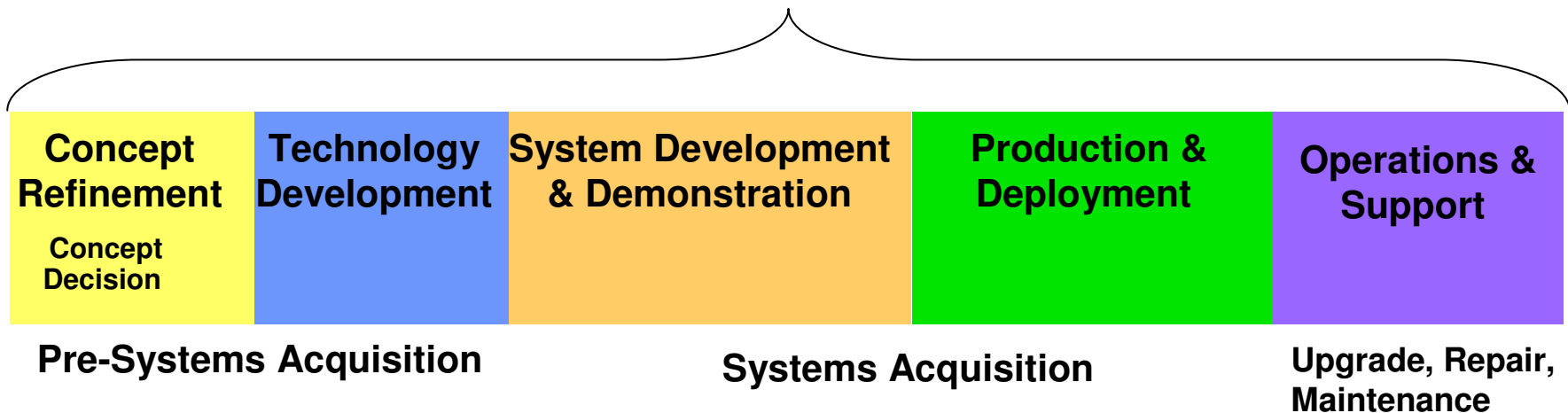
Source: Reed Electronic Research, Yearbook of World Electronics Data

UNCLASSIFIED

# IA Policy for IT Systems Lifecycle



IA Provisions - IA in the Defense Acquisition System, (DODI 8580.1)



Adapted From Fig. 1, Operation of the Defense Acquisition System, (DODI 5000.2)

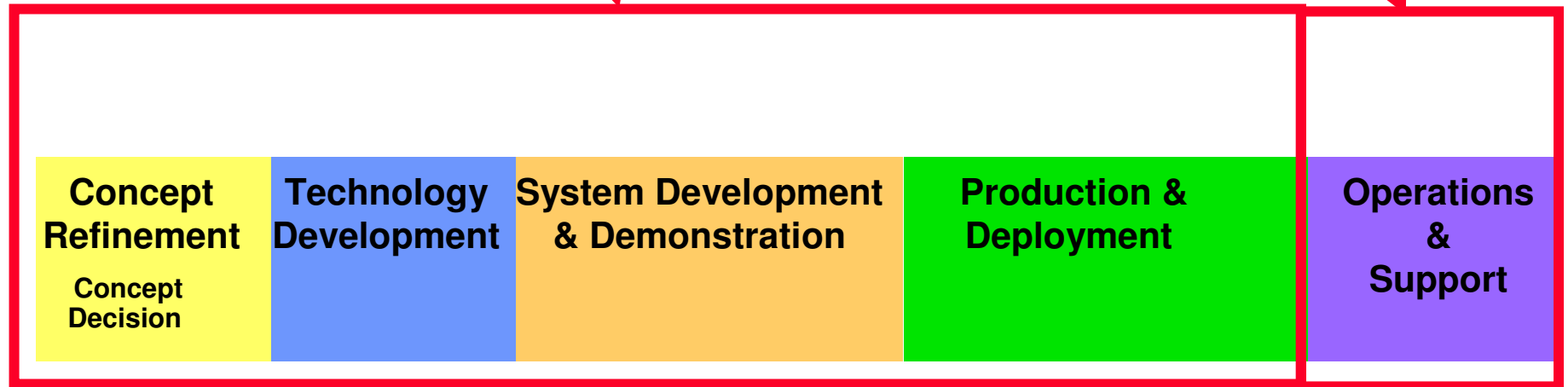
UNCLASSIFIED

# Potential COTS IT Component Lifecycle Risk Profile



**Offshore Vendor Complete Hands-on Access**

**Potential Offshore Vendor Hand-on Access**



**Concept Refinement**  
Concept Decision

**Technology Development**

**System Development & Demonstration**

**Production & Deployment**

**Operations & Support**

**Pre-Systems Acquisition**

**Systems Acquisition**

**Upgrade, Repair, Maintenance**

Adapted From Fig. 1, Operation of the Defense Acquisition System, (DODI 5000.2)

UNCLASSIFIED

# Why an Accelerated Awareness Campaign is Needed



Underlying Assumptions About DOD IT System Components during the last 50 years are increasingly challenged, or are no longer true!

- **The design and manufacturing of commercial IT components used in DOD C2 Systems can be trusted if they perform as advertised**
- **Innovation and design of future IT components will mainly take place in the US**
- **The most sophisticated software driven IT components in the GIG will be made in the US**
- **The origin or source of IT components for the GIG will always be known**
- **Required commercial IT components will always be available to DOD**
- **Detection and identification of faulty or malicious IT components in the GIG will be possible**
- **We will always be able to design intelligent control systems that can verify reliability of IT system components**
- **Off-shore commercial vendors will cooperate in helping to identify anomalies or reliability problems related to IT components in DOD systems**

UNCLASSIFIED

# Summary



- **IT globalization has unleashed a far reaching competition for IT dominance that is rapidly changing the world of commercial IT in a very short period of time**
- **The changes caused by IT globalization have many implications for change in the acquisition community, some of which we have only begun to realize**
- **China is already the largest exporter of IT equipment and has aspirations for IT dominance**
- **DOD IT acquisition strategies will increasingly become a key element of DOD computer network defenses in the future**