



# Foreign Espionage Methods, Trends, Tactics, and Scams

February 25, 2010  
Chicago

Stephen G. Holder  
National Counterintelligence Officer for East Asia  
National Counterintelligence Executive,  
Office of the Director of National Intelligence

UNCLASSIFIED



# Difficult to Stop





# Goals for Today



- What is the state of industrial espionage today
- Why the US academic and business communities are particularly vulnerable
- Who the major actors are
- What the CI world is doing to deal with the change

The 20<sup>th</sup> century model

UNCLASSIFIED



# Know the Dangers

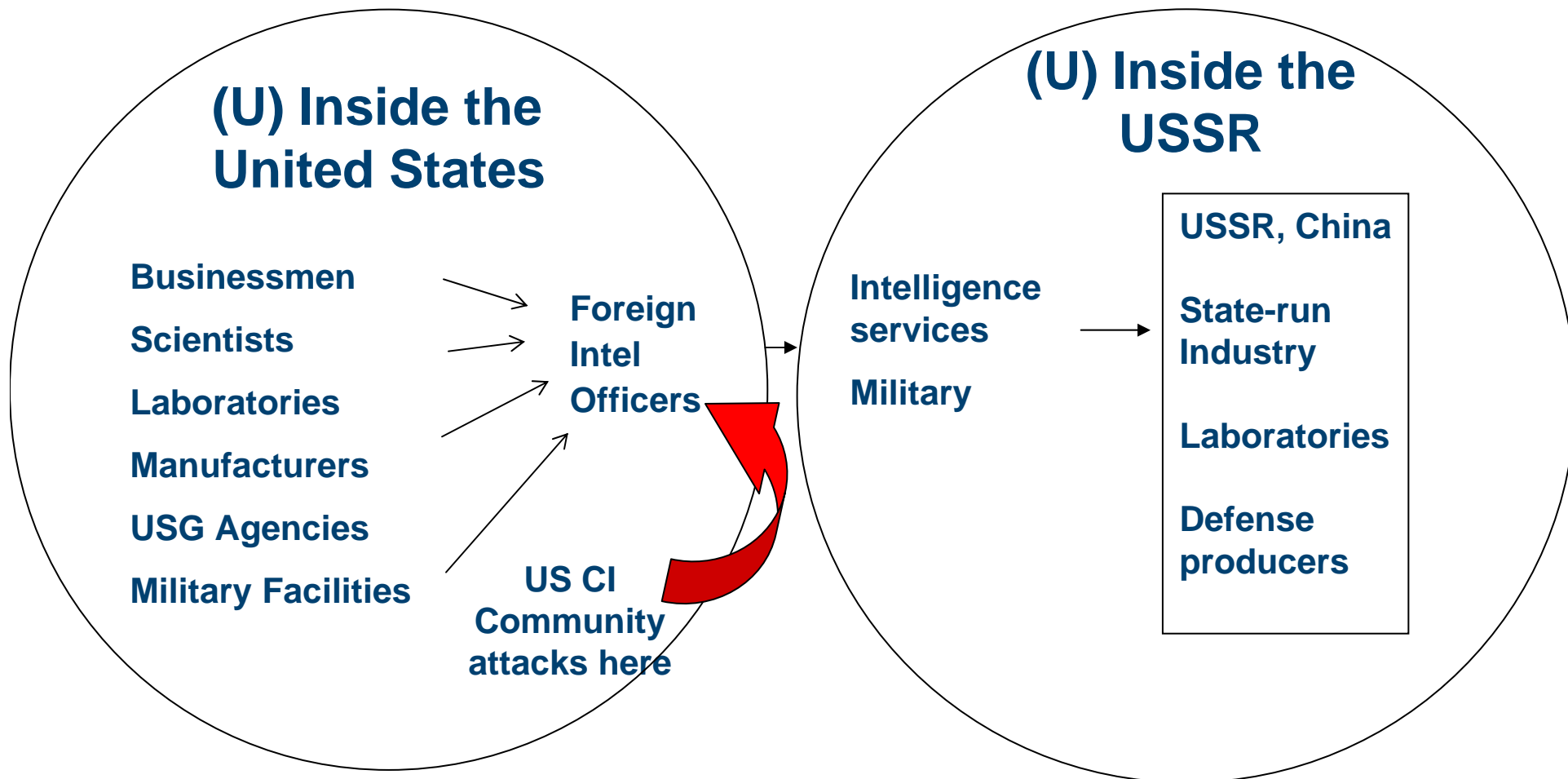
- 不盡知用兵之害者
- 
- 則不能
- 
- 盡知用兵之利也

UNCLASSIFIED

---



# The Traditional 20<sup>th</sup> Century Model – The Soviet Threat



UNCLASSIFIED





# Technology Theft in the 21<sup>st</sup> Century



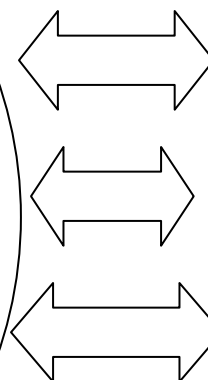
## (U) Inside US and abroad

### US

Businessmen  
Scientists  
Engineers  
Manufacturers  
USG Agencies  
Military Facilities

### Foreign

Businessmen  
Scientists  
Engineers  
Manufacturers  
Military officers  
Foreign IOs



## (U) Overseas

Intel services  
Defense industry  
Private industry  
Laboratories  
Research institutes  
ThinkTanks

**CI Community lacks  
single point of attack**

UNCLASSIFIED



# The Challenging 21<sup>st</sup> Century Model



## **(U) Jin Hanjuan – selling to the highest bidder**

- **(U) Demand driven by globalization**
  - Capitalists in Russia , China, and India, Israel, Pakistan, France, etc
- **(U) US openness provides access**
  - 5 mln B-1 visas per year, 500,000 students, one-third in hard sciences
  - Expanding list of visitors to labs, research institutes, military bases
- **(U) R&D 70 percent funded private sector (little USG control)**
- **(U) Thumb drives/cell phones/Web make theft rapid, easy**
- **(U) Many foreign experts routinely travel to home countries; not here to stay.**
- **(U) FIS benefit from activities in marketplace**

UNCLASSIFIED



# Technology Theft in the 21<sup>st</sup> Century



## The Advantages for Foreign Acquirers

- (U) Reduced need for foreign IO to transfer technology
  - No need for dangerous tradecraft
  - Free, high-tech information exchange, scientist to scientist, businessman to businessman
  - Information gathered in US can be transferred while overseas
- (U) Huge universe of collectors and transactions presents challenges for US intelligence and enforcement communities
- (U) Marketplace ensures natural interest in collecting state-of-the-art tech
- (U) Storing and transferring massive amounts of trade secrets done with minimal difficulty
- (U) Culture of sharing reduces the stigma of theft – email, thumb-drives, cell phones in common use across population

DSS actors breakdown

UNCLASSIFIED



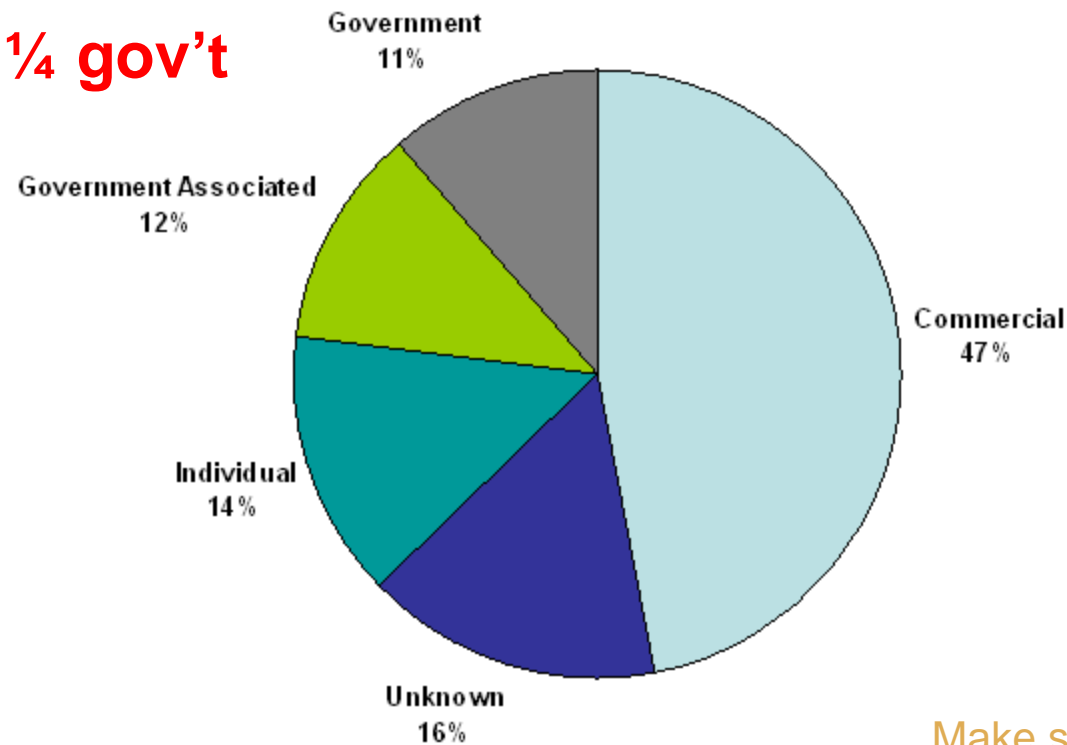


# Which Entities Committed the Theft in 2009?



Types of Foreign Collectors Targeting US Defense Technology, FY 2008 (DSS data)

**Less than 1/4 gov't**



UNCLASSIFIED

Make sure we know the target



# Our Goal is NOT to Stop Foreign Participation



- (U) The US intelligence community understands the important role foreign experts play in the US.
  - The US has greatly benefited from influx of foreign experts.
  - Foreigners involved in illegal activities are relatively large in number but a very small share of total
  - Many don't see activities as harmful to the US.
    - Just business.
    - Not “hurting” the United States.
    - If not from me, from someone else.

UNCLASSIFIED

---



# What's behind the espionage activities?



- Motivated by:
  - Greed (money or prestige)
  - Revenge
  - Desire to assist motherland or extend scientific frontier
- Small fish hiding in huge ocean

Hard to pick out the spy

UNCLASSIFIED

---



# Harder than ever to Identify the Transfer Point



UNCLASSIFIED



# Our Goal is to Stop Illegal Technology Transfer



- Foreign military and intelligence services exploit private sector access
- Zero risk to FIS
  - China, Russia, and others are producing military and commercial items using technology they haven't legally acquired.
  - Foreign delegations are coming with the intent of encouraging US experts to contribute to the development of foreign technology base.
  - China, in particular, is setting up organizations to facilitate two-way exchange, e.g. Think Tanks.
    - PRC defector tells press about political roles of these organizations.
    - The nature of the organizations indicate S&T exchange is part of the plan.

UNCLASSIFIED





# **FISs also Direct Some Activity**



- **“Ask” scientists, engineers, scholars to report back after foreign travel (may not know they are working for intel organization)**
- **Recruit businessmen, scientists, students who are coming to US**
- **Provide targeting lists to travelers**
- **Sponsor experts to attend conferences and report findings**
- **Traditional agent operations (Chi Mak)**

UNCLASSIFIED

---



# The process in action and why it matters



- ◆ Enables foreign powers to leapfrog US military technologies, undermining our military advantage and costing US lives.



UNCLASSIFIED



# **The process in action and why it matters**



- ◆ **Erodes our comparative advantage, undermining our economy and, hence, our national security.**
- ◆ **Losses can be massive and fast**
- ◆ **Foreign ownership of US firms and joint US-foreign ventures cloud the issue of technology transfer – can be private or government sponsored**
- ◆ **Enables foreign powers to leapfrog US military technologies, undermining our military advantage and costing US lives**

UNCLASSIFIED

---



# Summary



- (U) We know significant amounts of US technology are illegally flowing abroad.
- (U) We know that foreign governments have intent to acquire US technology legally if possible, illegally if not.
- (U) We know foreign intelligence and other security services are directly involved in acquisition efforts and they sometimes employ private sector players in the process.
- (U) We know that much of the technology transferred is going through the private sector with no observable link to foreign intel.
- (U) We know that foreign governments recognize the role their private sector is playing and are moving to capitalize on the private acquisition.

UNCLASSIFIED

---



# How the CI Community is Responding



- Cooperation within US Government is key
  - Across government organizations e.g. (FBI, CIA, DoD, Energy, Commerce, State, DHS, Treasury)
  - And between enforcement, operations, analysis (before and after failures)
  - Share information – Annual report to Congress
  - Avoid parochialism – stopping the outflow of technology, not single arrest, is the goal

UNCLASSIFIED

---





# How the CI Community is Responding



- Cooperation with private sector also essential (US corporate world is NOT the enemy)
  - Much of the R&D and Technology is owned by US private sector
  - By the time the information is classified, the horse has left the barn
  - Private sector does worry about national security
- Numerous outreach programs
  - FBI (Domain), DSS, ONCIX, OSAC

UNCLASSIFIED



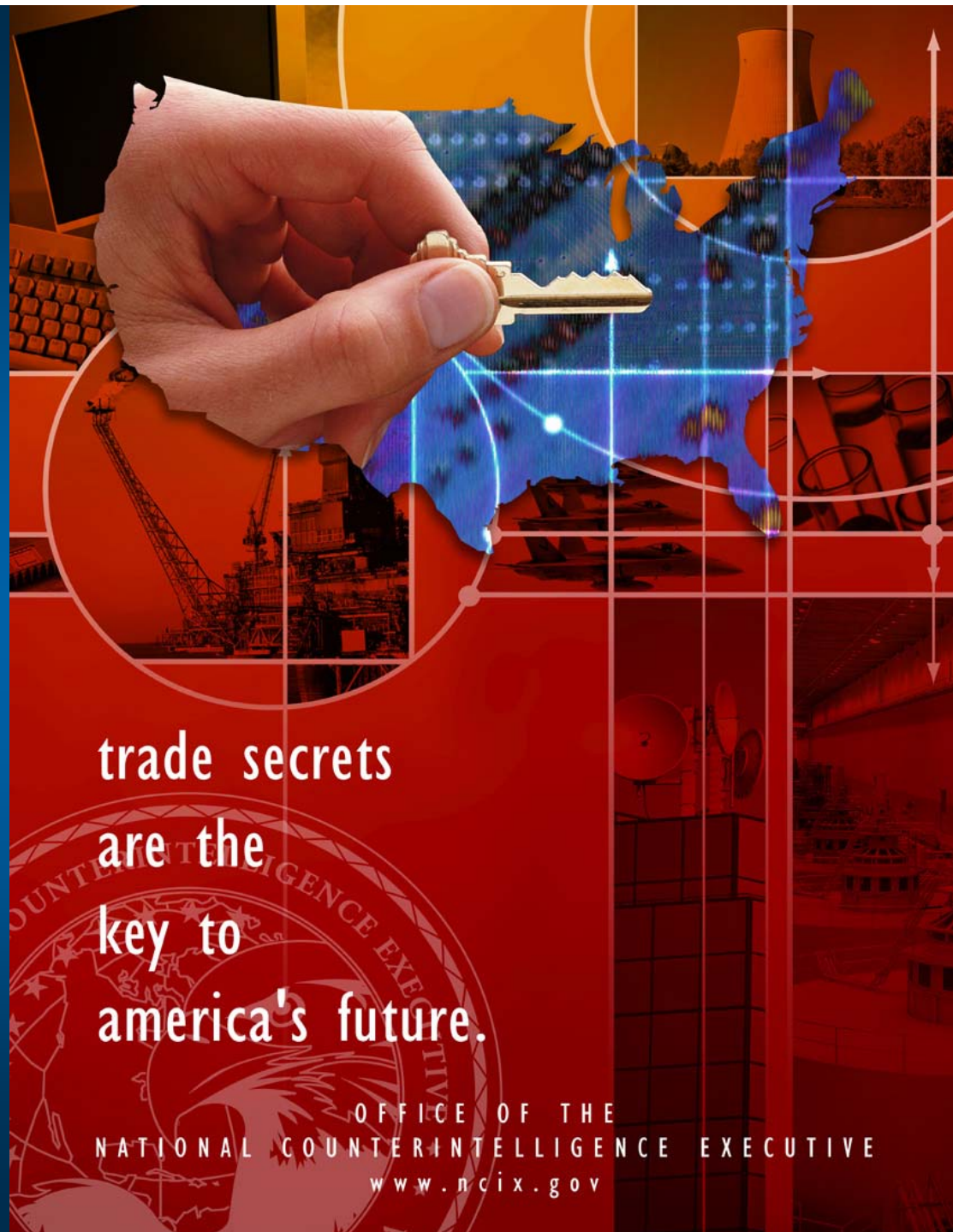
# Outreach Goals



- (U) Make sure the private sector understands the threat as well as the opportunities.
- (U) Demonstrate the way state actors manipulate private sector
- (U) Focus protection on diamonds not toothbrushes
- (U) Recognize that we live in a world of windows not walls, but remember that walls are necessary to support windows
- (U) Remember that if we lose our technological lead, both our economy and our national defense suffer

UNCLASSIFIED

---



trade secrets  
are the  
key to  
america's future.

OFFICE OF THE  
NATIONAL COUNTERINTELLIGENCE EXECUTIVE  
[www.ncix.gov](http://www.ncix.gov)

