For Official Use Only

Targeting Technology

Federal Bureau of Investigation

Unit Chief Mark A. Levett

February 25, 2010

Corporate Espioage & Global Security:
Protecting Your Business Interests

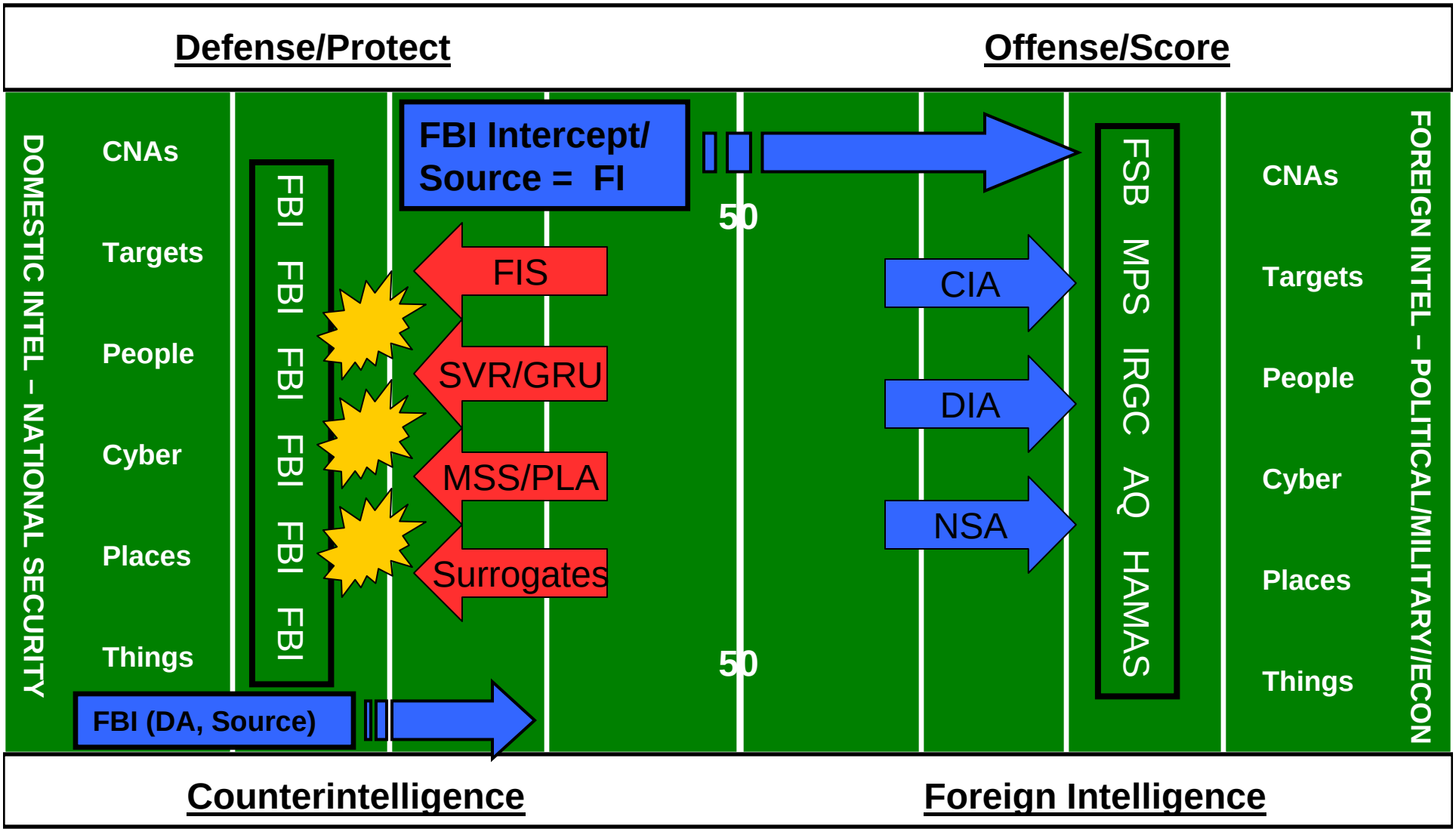
Rosemont, IL

COUNTERINTELLIGENCE THREATS

ISSUE THREATS

- Espionage (National Defense Information)
- Proliferation (Weapons of Mass Destruction)
- Economic Espionage
- National Information Infrastructure Targeting
- Infiltrating the U.S. Government
- Perception Management
- Foreign Intelligence Activities

FBI on the field of INTELLIGENCE



The Evolving Intelligence Threat

From: "Symmetric (Traditional)"

- Foreign officials: A, G, I and NATO visas

-"Known/Suspected" Intelligence Officers

- Establishment (I.e., Embassies, Consulates and Media organizations)

Increasingly…

To: "Asymmetric (Non-traditional)"

"Other" non-official foreign nationals

-Including students, researchers, business travelers, etc.,

-Foreign employees

-Typically B, F H1B, J and L visas.

Threat = Presence + Cyber

Who's Who…

(U) Criteria – Intent + Capability + Opportunity = Threat

- Asia
- Eurasia
- Middle East
- Europe?

Quote: "Some 108+ countries– a mix of rich and poor, high- and low-tech, friend and foe – targeted US technologies in 2008 totaling $ multi-billions in losses to the Nation's economic and Security sectors…"

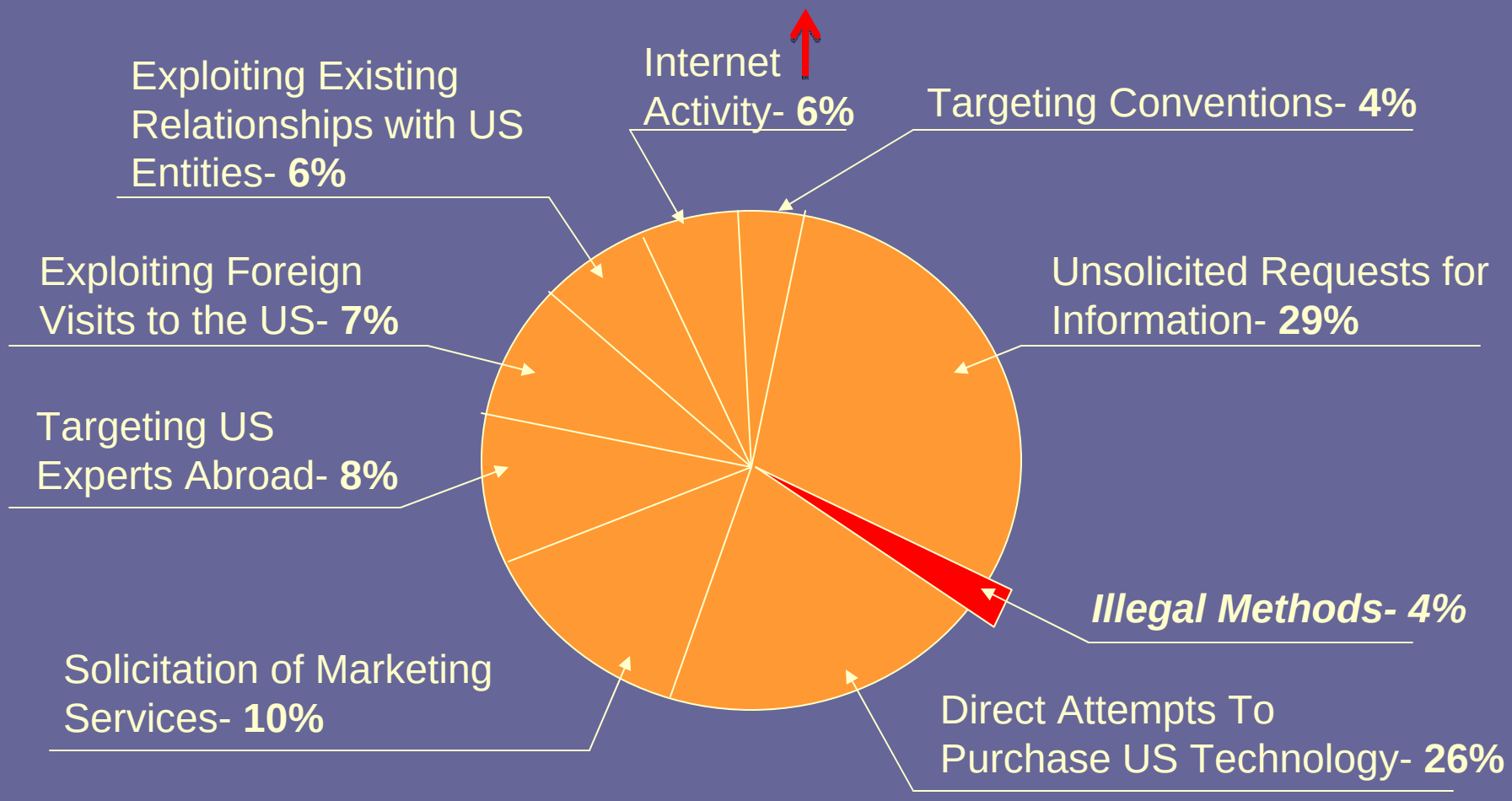
2008 Annual Report to Congress, Prepared by the National Counterintelligence Executive (NCIX)

"France Creates Office for Economic Intel"
Defense News 21 September 2009

"It is not espionage but consists of using all legal means to gain an understanding of the competitive environmnet.

S

*A Variety of Methods…



** Estimates compiled from data provided by the U.S. Intelligence Community: 2007*

Collection Techniques

- Request for Information
  - E-mail, FAX, Telephone
  - Unsolicited
- Attempted Acquisitions
  - Purchase products
  - Purchase US companies
- Marketing of Foreign Services and Products
  - Favorite of hardware/software firms
  - Insert personnel or products

Foreign Collectors

Governments

- Advanced Countries
  - Leapfrog scientific hurdle w/o time and expense
  - Move closer in parity with United States
  - Give Defense-Industrial base competitive edge
- Less Advanced Countries
  - Technologies that increase nations power and influence
  - Export controlled – utilize reverse engineering and mass produce

Trade Secrets

- Foreign economic collection targeting trade secrets through espionage.
  - Trade Secrets
    - financial, business, scientific, technical, economic, or engineering information
    - Company must take **reasonable** measures to keep secret and not be readily ascertainable through proper means by the public.

Targeted Technologies

Efforts not always directed against the "Crown Jewels"

Dated technologies

Infrastructure-supportive technologies

Dual-use technologies

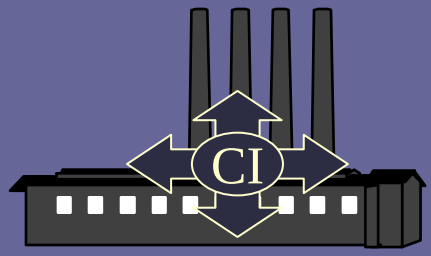
Activities to improperly acquire Trade Secrets

- Economic Espionage
  - Benefit a foreign govt or agent of
  - Stealing, copying, altering destroying, without authorization
- Industrial Espionage – criminalized under EEA
- Export Control Violations – dual use equip/tech
  - Concurrent with ICE, DOC EE
- Transfer of Defense items – US munitions list
  - ITAR – USDS/DDTC

Business Alliances

Changing Behaviors…

- FBI-led programmatic outreach to Industry…
  - The Defense Industrial Base for starters…
  - Executive level engagement/FSOs
- RISK = Threat x Vulnerability x Consequence
- Outreach, engagement, dialogue
- CI and Business confidence-building
- Threat information exchange
  - Joint mitigation solutions
  - Due-diligence /Self-governance through Awareness
- Corporate Volunteerism
- Reporting protocols



Business Alliance Activities

- Continuous consultation
- Identify/localize Critical Research/Program Information = CNA
- Tailored risk & threat Assessments
- CI awareness/education
- Foreign travel briefing and debriefing
- Foreign visitor and escort
- Unsolicited requests for data
- Cyber security

Countermeasures & Risk Mitigation

- Referrals
- Reporting
- Monitoring
- Detection
- Analysis

CI investigative and operational lead development & follow through…

Insider Threat

Insider Threat

- A person with authorized access to information, facilities, technology or personnel who…
  - Utilizes his/her access with intention of providing information, technology or access to unauthorized persons

    and/or
  - Maliciously manipulates or causes damage or harm to an organization, its information, facilities, technology or persons

Insider Threat: Potential Indicators★

Foreign Nexus

- Relationship with foreign visitors whether personal, professional, or social
- Freq. travel overseas to attend conferences, (who paid for trip, who invited the participants)
- Has relatives in a foreign country
- Express sympathies to another country

Insider Nexus

- Notable enthusiasm for overtime work, weekend work, or unusual schedules
- Interest in matters outside scope of employment (particularly those of interest to foreign entities)
- Express dissatisfaction with current work environment or ineffective job performance

Insider Threat: Potential Indicators★

Personal Issues

- Drug or alcohol abuse
- Repeated irresponsibility
- An "above the rules" attitude
- Financial irresponsibility
- Overwhelming life crises or career disappointments
- Unexplained affluence
- Unexplained absences
- Pattern of lying
- Inappropriate behavior
- Misuse of computers
- Etc.

★ The fact that an individual exhibits one or more of these indicators does not automatically mean that he or she is engaged in espionage.

Insider Threat:
Best Practices

- Be aware of potential issues and exercise good judgment in determining what and when to report them.
- Post signs notifying employees of security regulations.
- Use computer banners that employees must click to acknowledge computer security issues.
- Have employees sign non-disclosure and other security agreements.
- Have yearly security and ethics training.
- Maintain computer/information access logs.

Cyber Threat

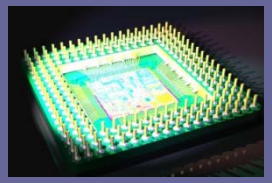
Emerging Security Concerns

- Building risk related security mitigation into business processes
- Understanding “over the horizon” threats
- Growing regulatory and standards requirements
- Increased virtualization of companies
- Identifying all external stakeholders

Cyber Threat

- Humans are the weakest link!

- Don't put it on the network
  - Created isolated networks
  - Control physical access
- Think before emailing
- "Trust but verify"
- Acceptable Risk?



Traveling Overseas

- Leave your bits & bytes at home.
- Realize there are no trusted networks in many countries.
- Gifts may not be what they appear.
- Look for anomalies.
- Clean laptop program.
- Scrub IT and media upon return/prior to introduction into the home network.

Cyber Security

- IT needs to be integrated into and coordinated with a larger security program.
  - IT security personnel must be Counterintelligence aware
  - Traditional security personnel must be IT aware
  - Cultural divide between traditional and IT security personnel must be bridged

Bottom line…

"It's all about relationships"

- Maintain U.S./Allied dual-use and leading-edge military technology superiority…
- Optimize capital investments in U.S. industry…
- Prevent compromise of Critical Research and Technologies…
- Ensure technological advantage to the U.S./Allied warfighter and avoid technology surprise in the battlespace…
- Ensure U.S. economic competitiveness…

Final Thoughts

- Business leaders should understand that the FBI is focused on helping protect US companies, employees and shareholders.
- A robust relationship formed prior to the break of an espionage case will is a valuable asset in establishing the trust necessary for successful case conclusion.
- Essential to identify key personnel/stakeholders in the private sector and USG as soon as possible (CI Strategic Partnership Coordinators are valuable assets for this purpose).

Community Outreach

We must work here in the United States with the citizens we serve, to identify and disrupt those who would do us harm… The simple truth is that we cannot do our jobs without the trust of the American people. And we cannot build that trust without reaching out to say, "We in the Bureau are on your side. We stand ready to help."

--FBI Director Robert S. Mueller, III at the Council on Foreign Relations – 23 Feb 2009.

Mark.Levett@ic.fbi.gov / 202-324-4778