



# Cyber Espionage: U.S. Perspective

# Why address this?

**WANG BING**  
 Alleges: Jack Wang, "Tigercat"  
**WANTED BY THE FBI**  
 Details: A grand jury in the Western District of Pennsylvania indicted five members of the People's Liberation Army of China (PLA) for 31 criminal counts, including: conspiring to commit Computer Intrusion; Accessing a Computer Without Authorization for the Purpose of Commercial Advantage and Private Financial Gain; Dumping Computers Through the Transmission of Code; Aggravated Identity Theft; Economic Espionage; Theft of Trade Secrets.

**HUANG ZHENYU**  
 Alleges: Huang Zhen Yu, "Jay Jay"  
**WANTED BY THE FBI**  
 Details: A grand jury in the Western District of Pennsylvania indicted five members of the People's Liberation Army of China (PLA) for 31 criminal counts, including: conspiring to commit Computer Intrusion; Accessing a Computer Without Authorization for the Purpose of Commercial Advantage and Private Financial Gain; Dumping Computers Through the Transmission of Code; Aggravated Identity Theft; Economic Espionage; Theft of Trade Secrets.

**SUN KAILIANG**  
 Alleges: Sun Kai Liang, Jack Sun  
**WANTED BY THE FBI**  
 Details: A grand jury in the Western District of Pennsylvania indicted five members of the People's Liberation Army of China (PLA) for 31 criminal counts, including: conspiring to commit Computer Intrusion; Accessing a Computer Without Authorization for the Purpose of Commercial Advantage and Private Financial Gain; Dumping Computers Through the Transmission of Code; Aggravated Identity Theft; Economic Espionage; Theft of Trade Secrets.

**GU CHUNHUI**  
 Alleges: Gu Chun Hui, "KandyGo"  
**WANTED BY THE FBI**  
 Details: A grand jury in the Western District of Pennsylvania indicted five members of the People's Liberation Army of China (PLA) for 31 criminal counts, including: conspiring to commit Computer Intrusion; Accessing a Computer Without Authorization for the Purpose of Commercial Advantage and Private Financial Gain; Dumping Computers Through the Transmission of Code; Aggravated Identity Theft; Economic Espionage; Theft of Trade Secrets.

**Hacked By #GOP**

I warned you, and this is just a beginning. I will not stop until our request is met. I have obtained a year's worth of your internal data, including your secrets and top secrets. If you don't obey us, we'll release this data showing how to fix the world. Determine what will and will not be the case. 1:00 PM EST

**HACKED**

SONY PICTURES

**WANTED BY THE FBI**

**CONSPIRACY TO COMMIT COMPUTER INTRUSION**

Ahmad Fathi, Hamid Firoozi, Amin Shokohi, Mohammad Sadeq Ahmadzadegan, Omid Ghaffarinia, Sina Keissar, Nader Saedi



**STREET CRED**

**DIMITRI ALPEROVITCH**  
 Co-founder of CrowdStrike which identified DNC hackers  
 Fmr. VP at McAfee

**RUSSIAN GROUPS HACK THE DNC**

CNBC

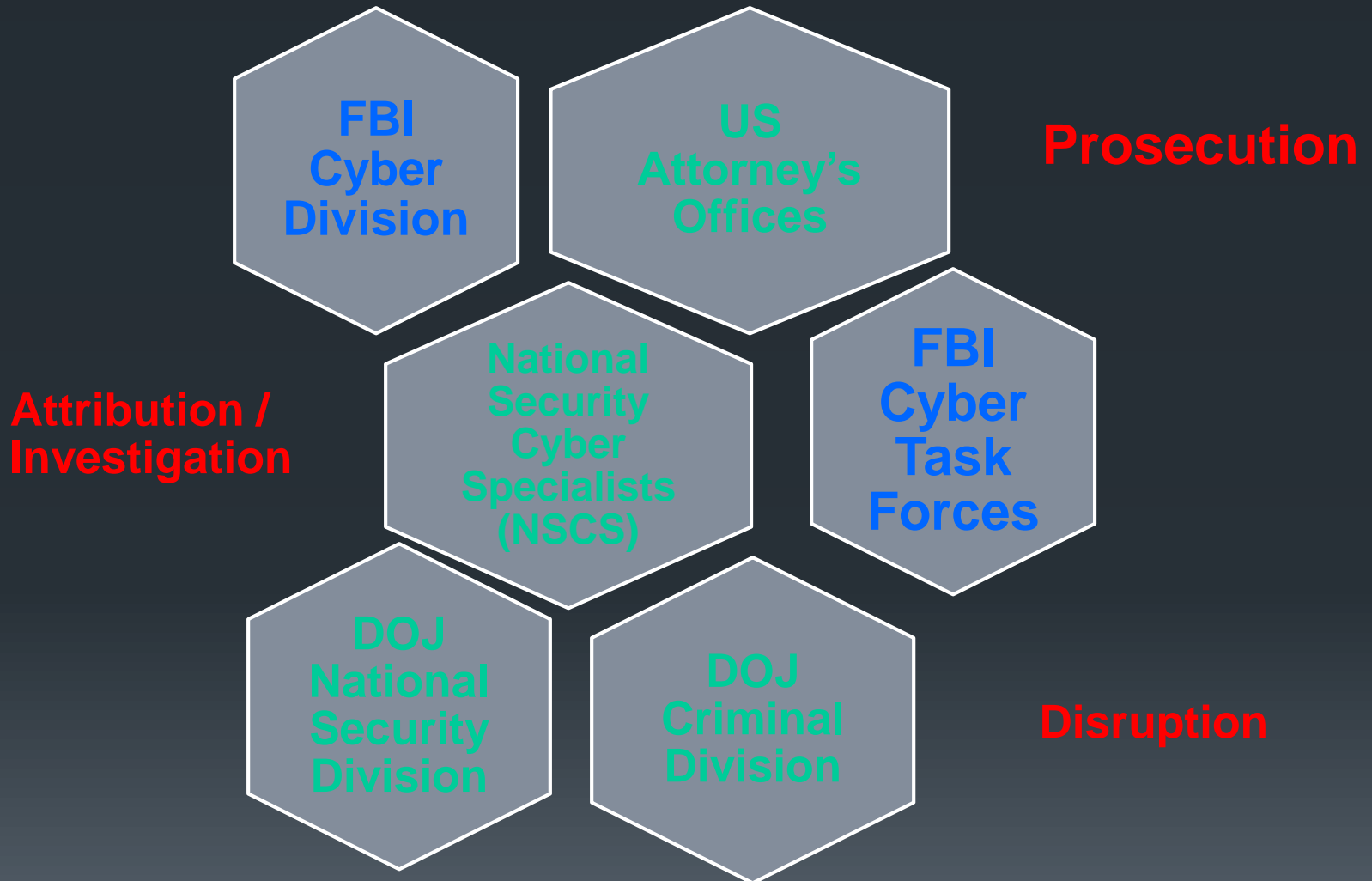
# Diverse threats

- Criminal syndicates
- Foreign intelligence services and their proxies

# Diverse motivations

- Traditional and economic espionage
  - Military or national security information
  - Personally Identifiable Information
  - Intellectual property (trade secrets)
  - Financial information
  - Business intelligence
- Embarrassment
- Retaliation
- Coercion

# Confronting the cyber threat



# Case Examples

- *U.S. v. Wang et al.* (WDPA May 1, 2014)



**WANTED**  
**BY THE FBI**

**Conspiring to Commit Computer Fraud; Accessing a Computer Without Authorization for the Purpose of Commercial Advantage and Private Financial Gain; Damaging Computers Through the Transmission of Code and Commands; Aggravated Identity Theft; Economic Espionage; Theft of Trade Secrets**

**Huang Zhenyu      Wen Xinyu      Sun Kailiang      Gu Chunhui      Wang Dong**

**FBI**

April 1, 2015



**Executive Order 13964** authorizes the Secretary of the Treasury, in consultation with the Secretary of State and the Attorney General, to impose sanctions on individuals or entities that engage in certain significant, malicious cyber-enabled activities.

- Harming or significantly compromising the provision of services by entities in a critical infrastructure sector
- Significantly disrupting the availability of a computer or network of computers (for example, through a distributed denial-of-service attack)



September 25, 2015

The United States and China agree that neither country's government will conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors

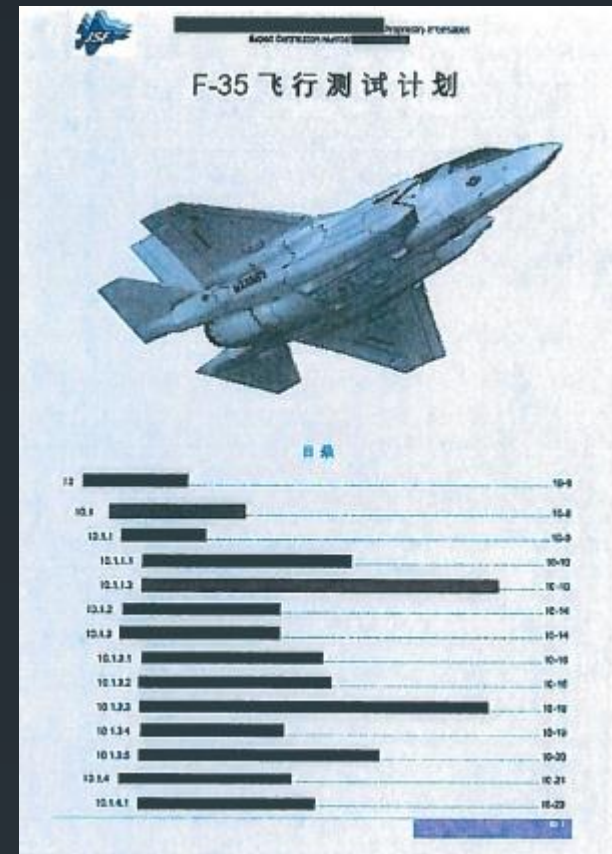
# Case Examples (cont'd)

- *U.S. v. Su*, (CDCA Aug. 14, 2014)

**SU BIN**



- Alias: Stephen Subin
- Arrested in Canada
- Likely to be extradited to Los Angeles
- Operates Chinese aviation company Lode-Tech





# Case Examples (cont'd)

- *U.S. v. Golestaneh* (DVT February 2015)



# Case Examples (cont'd)

- *U.S. v. Agha et al.* and *U.S. v. Romar et al.* (EDVA March 2016)

## US Charges 3 Syrians With Hacking, Hoax AP Tweet

Law360, New York (March 22, 2016, 3:46 PM EDT) -- Virginia federal prosecutors on Tuesday charged three Syrian nationals with carrying out a series of computer hacking attacks in the U.S., including an alleged plot to send a fake [Associated Press](#) tweet about a purported White House bomb explosion that briefly tanked the stock market.



AO 91 (Rev. 08/09) Criminal Complaint

---

UNITED STATES DISTRICT COURT  
for the  
Eastern District of Virginia

United States of America            )  
v.    )  
Peter Romar a/k/a Pierre Romar        )  
and                                        )  
Firas Dardar a/k/a "The Shadow"        )

Case No. 1:15mj498

FILE  
9 2015  
CLERK, U.S. DISTRICT COURT  
ALEXANDRIA, VIRGINIA

---

Defendant(s)

# Case Examples (cont'd)

- *U.S. v. Fathi et al.* (SDNY March 2016)



# Global threat – global effort



- International cooperation and training
- Prosecution
- Sanctions
- Diplomacy
- Technical operations