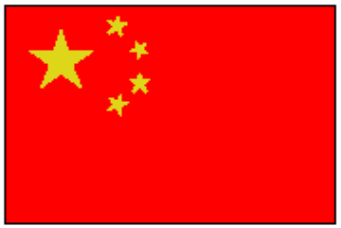
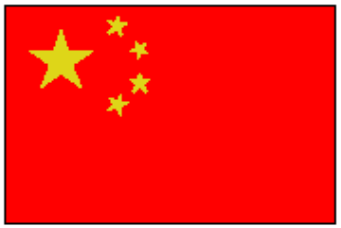


China's Economic Espionage:

Insider Threats and Operational Methods

Nicholas Eftimiades

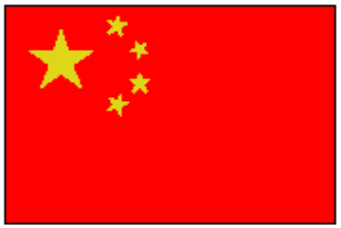
Copyright © Nicholas Eftimiades, 2019



Overview

- *Categories of Espionage*
- *China's Targeted Technologies and Trade Secrets*
- *Case Reviews*
- *Operations and Tactics*
- *Case Summaries*

Copyright © Nicholas Eftimiades, 2019



Bottom Line Up Front

1. Technology as a high priority for China's intelligence collectors.

2. China's economic espionage and illegal export collection efforts correlate to the priority technologies identified in the PRC government strategies "***Made in China 2025***" and "***Space Science & Technology in China: A Roadmap to 2050***".

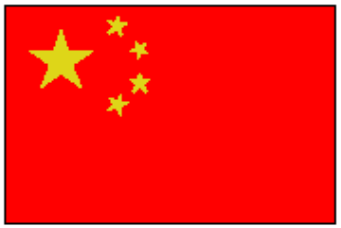
3. China has aggressively expanded its espionage efforts over the last 20 years.

4. China's intelligence services, State Owned Enterprises, private companies, individuals, and select universities conduct espionage activities.

5. Espionage tradecraft ranges considerably from quite poor to professional, even within an organization. Cyber espionage is the exception showing standardized techniques and practices.

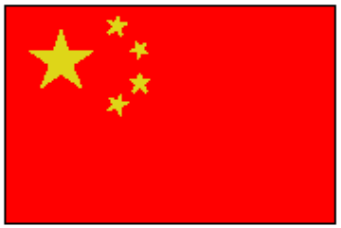
6. The two consistent motivating factors for nontraditional collectors are ethno-nationalism and financial rewards (cash or business deals).

Copyright © Nicholas Eftimiades, 2019



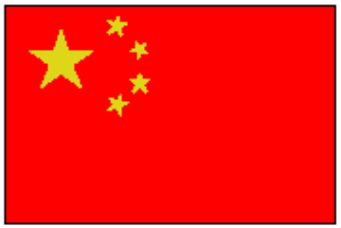
Categories of Espionage

Copyright © Nicholas Eftimiades, 2019



Categories of Espionage

- *Traditional Espionage*
- ***Covert Action (FARA)***
- ***Economic Espionage***
  - ***Economic Espionage Act, 1996***
- ***Illegal Exports***
  - ***ITAR & Dept of Commerce EAR***

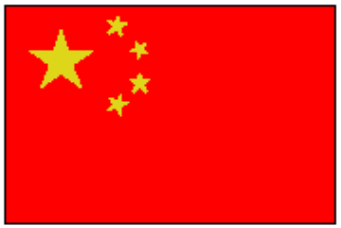


Insider Threats

&

Nontraditional Collectors

Copyright © Nicholas Eftimiades, 2019

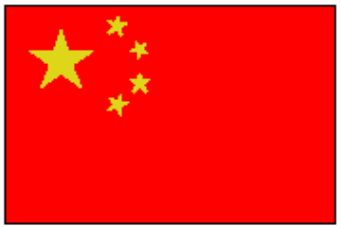


Nontraditional Collectors

Definition

Non-professional intelligence collectors conducting collection and related activities against national, political, and economic security interests

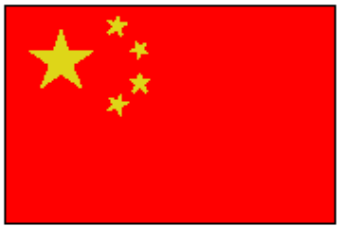
Copyright © Nicholas Eftimiades, 2019



Nontraditional Collectors

- ***State Owned Enterprises***
  - *** CCP Organization Department*
  - *** State Assets Supervision and Administration Commission*
- ***Universities ****
- ***Private companies***
- ***Individual entrepreneurs***
- ***Students and Scholars***

Copyright © Nicholas Eftimiades, 2019

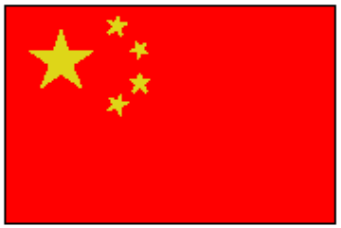


Nontraditional Collectors

Ministry of Industry and Information Technology

- State Administration for Science, Technology and Industry for National Defense
  - Beijing Institute of Technology
  - Beijing University of Aeronautics and Astronautics
  - Harbin Engineering University
  - Harbin Institute of Technology
  - Northwestern Polytechnical University
  - Nanjing Aeronautics and Astronautics University
  - Nanjing University of Science and Technology

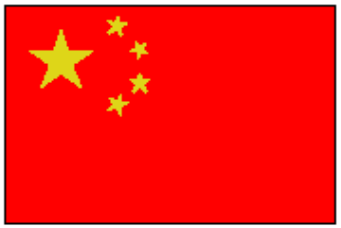
Copyright © Nicholas Eftimiades, 2019



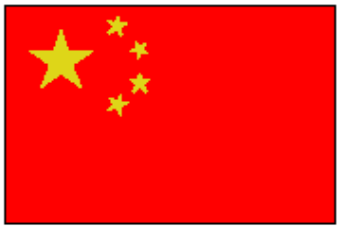
Targeted Industries & Technologies

Industry	Priority Sectors/Technologies	
Energy / Alternative Energy	Advanced pressurized water reactor and high-temperature, gas-cooled nuclear power stations Biofuels Energy-efficient industries	Oil, gas, and coalbed methane development, including fracking Smart grids **Solar energy technology** **Wind turbines**
Biotechnology	Advanced medical devices **Biomanufacturing and chemical manufacturing** Biomaterials	**Biopharmaceuticals** **Genetically modified organisms** **Infectious disease treatment** **New vaccines and drugs**
Defense Technology	**Aerospace & Aeronautic Systems** **Armaments**	**Marine Systems** **Radar** **Optics** **Space infrastructure and exploration technology**
Environmental Protection	Batteries Energy-efficient appliances Green building materials	**Hybrid and electric cars** Waste management Water/air pollution control
High-End Manufacturing	3D printing **Advanced robotics** **Aircraft engines** Aviation maintenance and service sectors Civilian aircraft Electric motors **Foundational manufacturing equipment**	High-end computer numerically controlled machines **High-performance composite materials** High-performance sealing materials **Integrated circuit manufacturing equipment and assembly technology** Synthetic rubber
Information and Communications Technology	Artificial intelligence Big data analysis **Core electronics industries** E-commerce services **Foundational software products** **High-end computer chips** Internet of Things	**Network equipment** Next-generation broadband wireless communications networks Quantum computing and communications Rare-earth materials

Source: ODNI



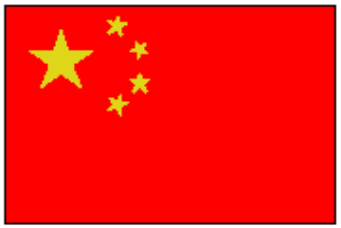
Case Examples



Case Examples
Insider Threat

Gregg "Donfang" Chung

- Rockwell and Boeing engineer
- Collected for State Owned Enterprises for 28 years
  - China National Aero Technology Import/Export Corporation,
  - Nanchang Aircraft Company,
  - Harbin Institute of Technology
- Coms through mail, sea freight, PRC Consulate, Chi Mak

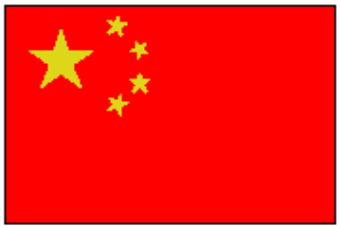


Case Examples
Insider Threat

Xiaoqing Zheng (and Zhaoxi Zhang)

- alleged

- Allegedly stole General Electric's trade secrets
  - turbine technologies
- Employed at GE Power & Water in Schenectady
  - Exploited access
  - Proprietary files involving design models, engineering drawings, configuration files, and material specification
- Formed Companies in Nanjing
- Financed by Shenyang provincial SOE's

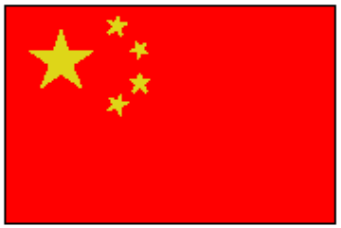


Case Examples
Insider Threat

Zhang Xiaolang & Chen Jizhong

- Alleged

- Apple Employees
- Titan Project
- Electric car technology
- Seeking employment in China with XPeng
  - Apple competitor
- Stole thousands of documents

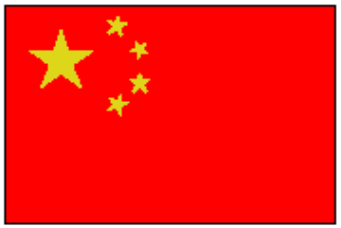


Case Examples

Insider Threat & Cyber

Su Bin

- Used email to communicate with co-conspirators,
- Advised on the technologies, companies, and individuals to ‘hack’
- Wrote, revised, and emailed reports addressed to the Second Department, General Staff Headquarters, PLA

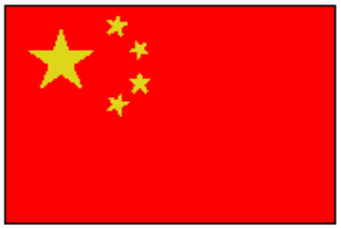


Cyber Examples

External and Insider Threats

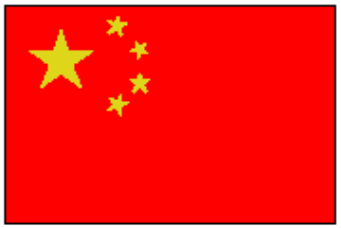
Targets:

- Industry/Universities
  - Economic espionage, trade secrets
  - Technology
  - IPR
- US and foreign governments
- US state governments
- News/social/political organizations



Operational Methods

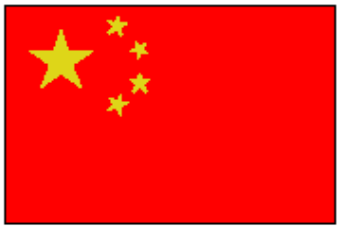
Copyright © Nicholas Eftimiades, 2019



Nontraditional Collectors

- *Most frequently used*
- *Target technology, businesses & dissidents*
- *Poor or little training*
- *Motivations*
  - *Financial*
  - *Ethno nationalistic*
  - *State (official) recruitment pressure*
    - *Students, Scholars*

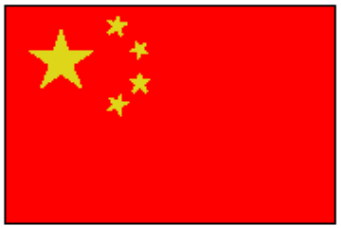
Copyright © Nicholas Eftimiades, 2019



Nontraditional Collection Tradecraft

- *"Islands of excellence"*
- *Linear and Third Country Control*
  - *Limited use of in-country networks*
  - *ITAR, EAR through third countries*
- *Limited In-Country Control*
- *Strong Personnel Connections to China*
- *Covert, Open Communication*

Copyright © Nicholas Eftimiades, 2019

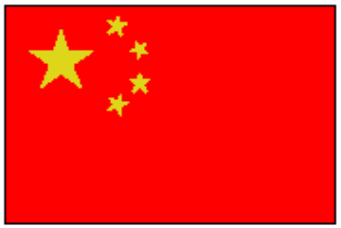


Nontraditional Collectors

ITAR, EAR Tradecraft

- *Reluctant to offer information on end use of a product.*
- *Willing to pay cash/money transfer when the terms of the sale call for financing.*
- *Declines routine installation, training or maintenance services.*
- *Freight forwarding firm or Third Country is listed as the product's final destination.*

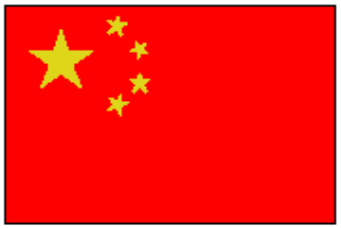
Copyright © Nicholas Eftimiades, 2019



Insider Threat Tradecraft

- *Scientists, engineers, and computer scientists employed the most sophisticated tactics to conceal acts of espionage.*
- *Insider threats almost always have significant commercial or academic interests in China*
- *ITAR, EAR targets are small companies*

Copyright © Nicholas Eftimiades, 2019

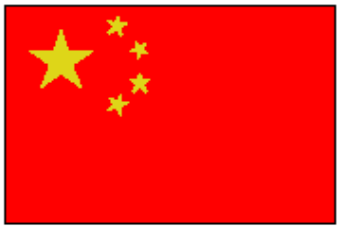


Insider Threat Profiles

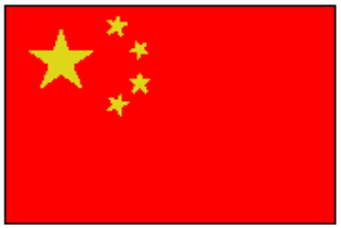
Discriminating factors for Insider Threats

- *Ethnicity*
- *Gender*
- *Age*
- *Email communications (work/personnel)*
- *Family contacts in China*
- *Academic affiliations in China*
- *Travel to China*
- *Computer usage patterns*
  - *Up days and months before travel*
- *Data access, movement, and storage*

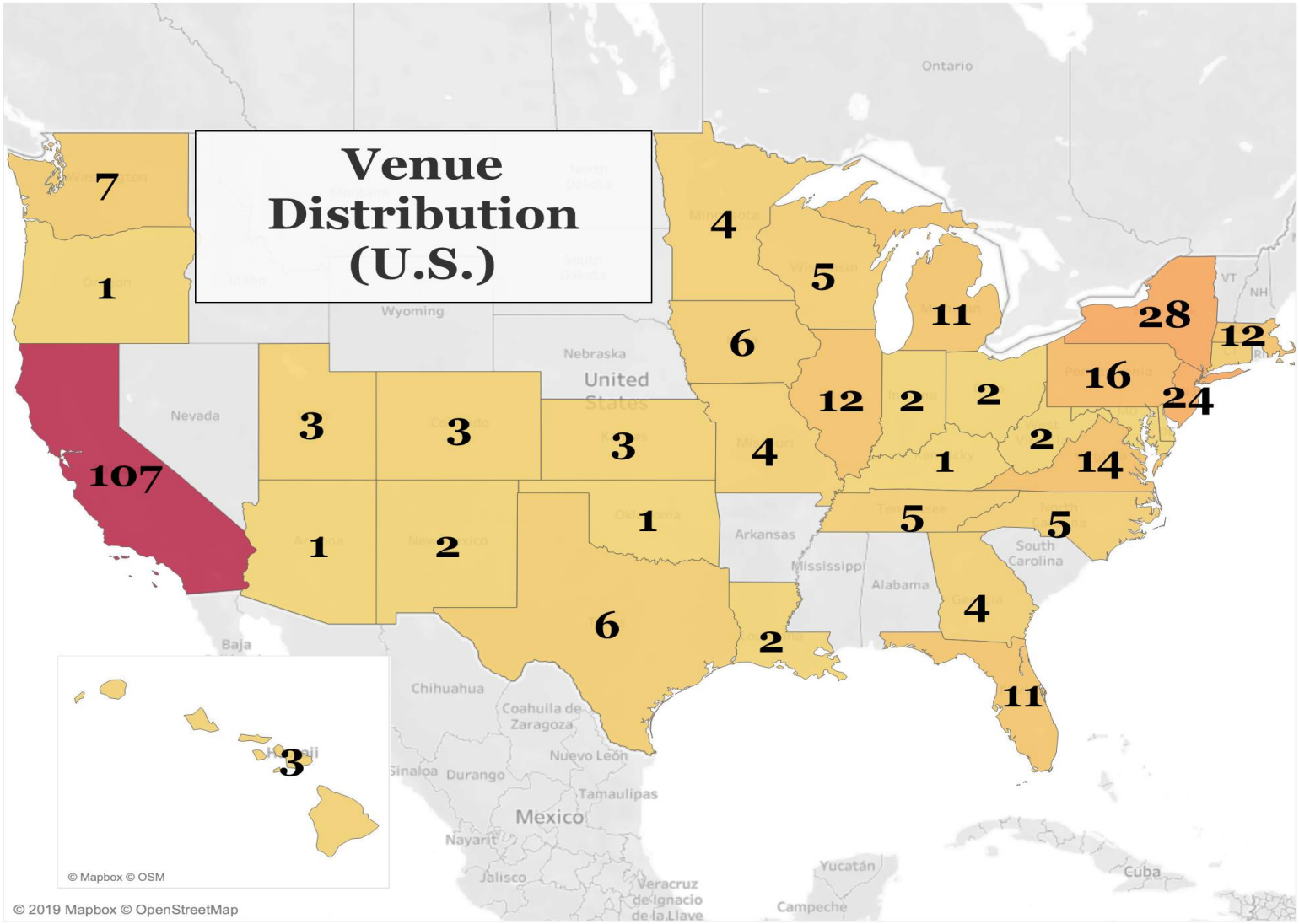
Copyright © Nicholas Eftimiades, 2019



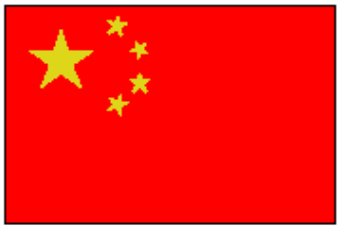
Case Summaries



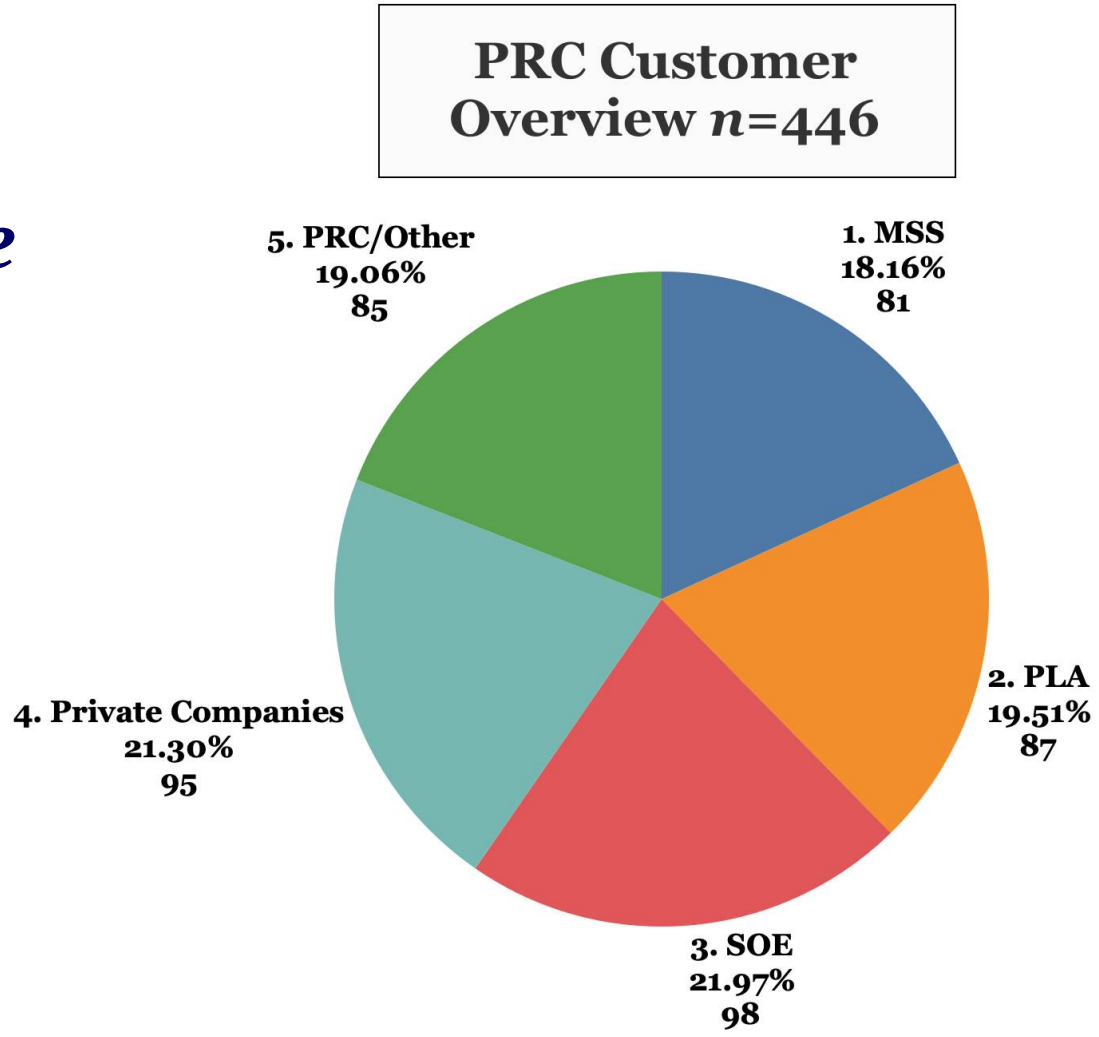
Chinese Espionage in the U.S.



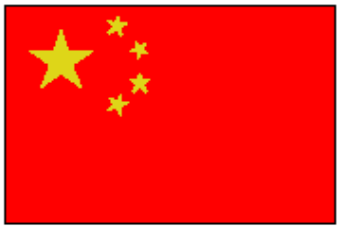
Copyright © Nicholas Eftimiades, 2019



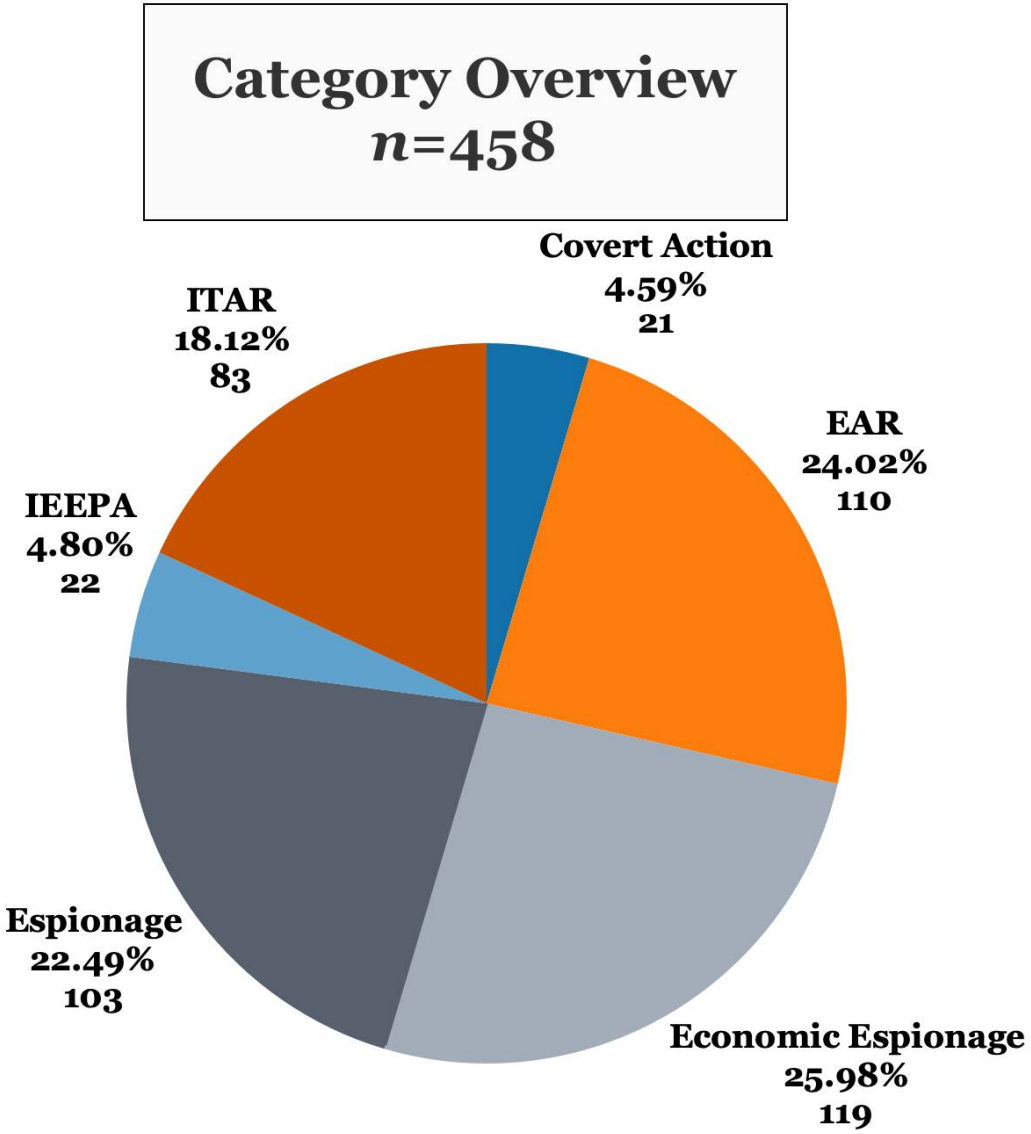
China's Espionage Customer Base



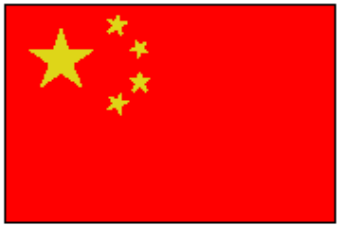
Copyright © Nicholas Eftimiades, 2019

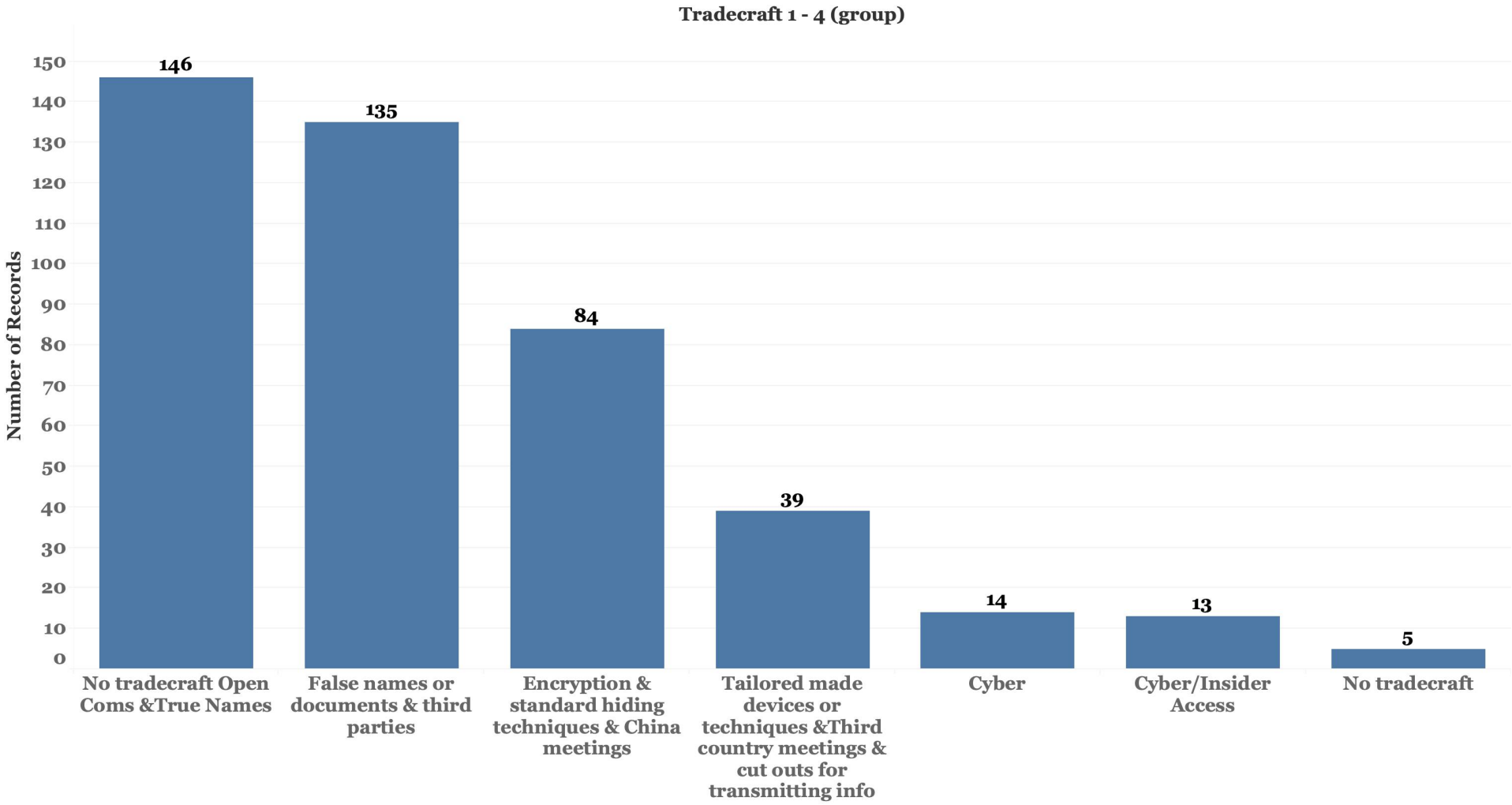


Espionage Categories

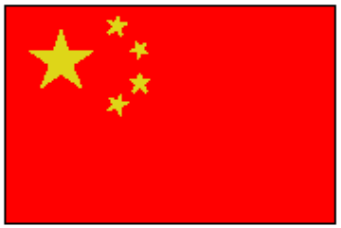


Copyright © Nicholas Eftimiades, 2019

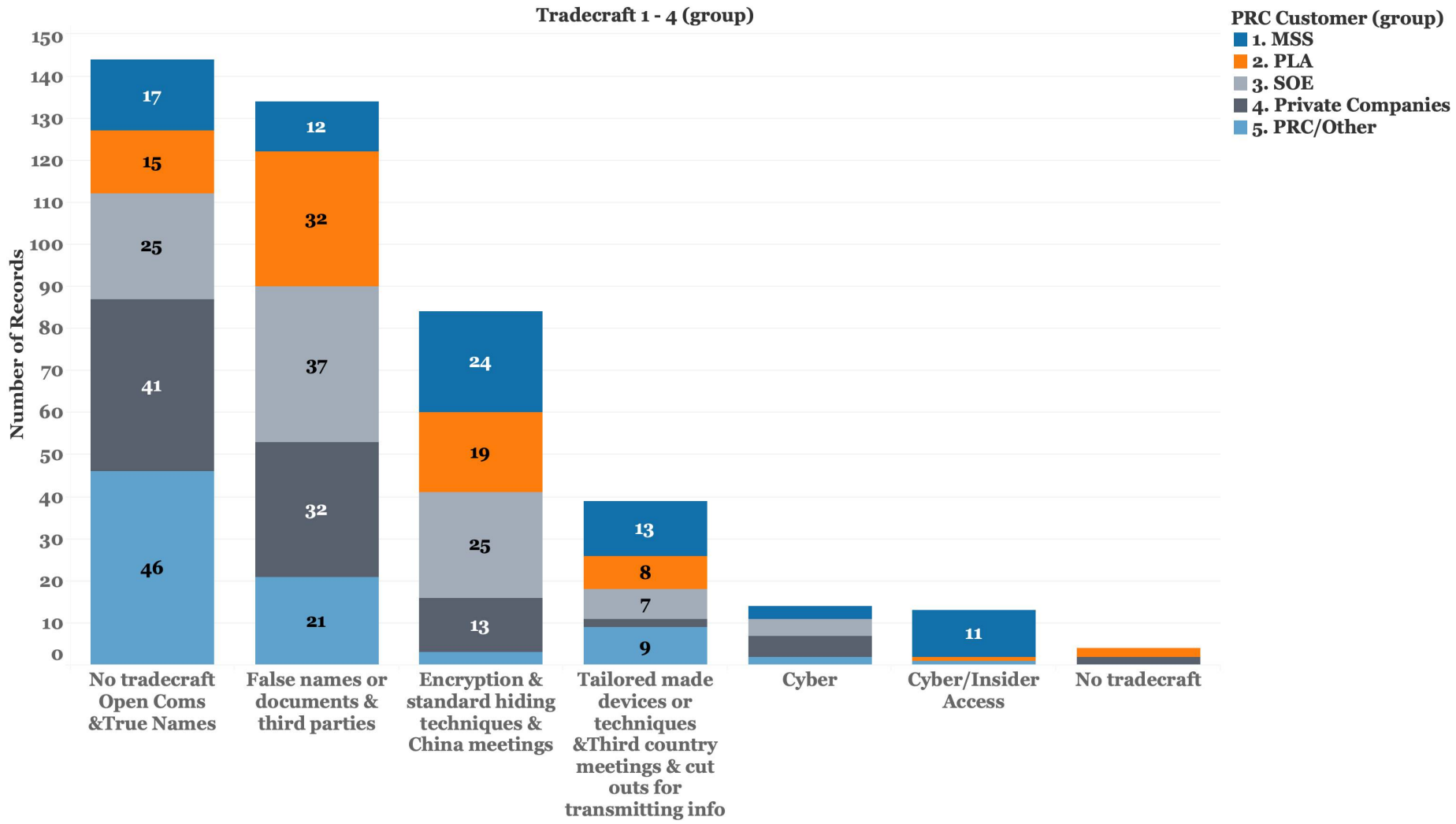




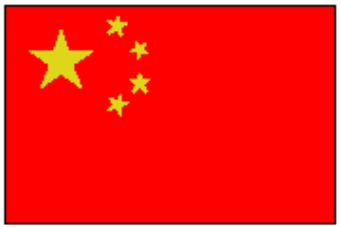
Copyright © Nicholas Eftimiades, 2019



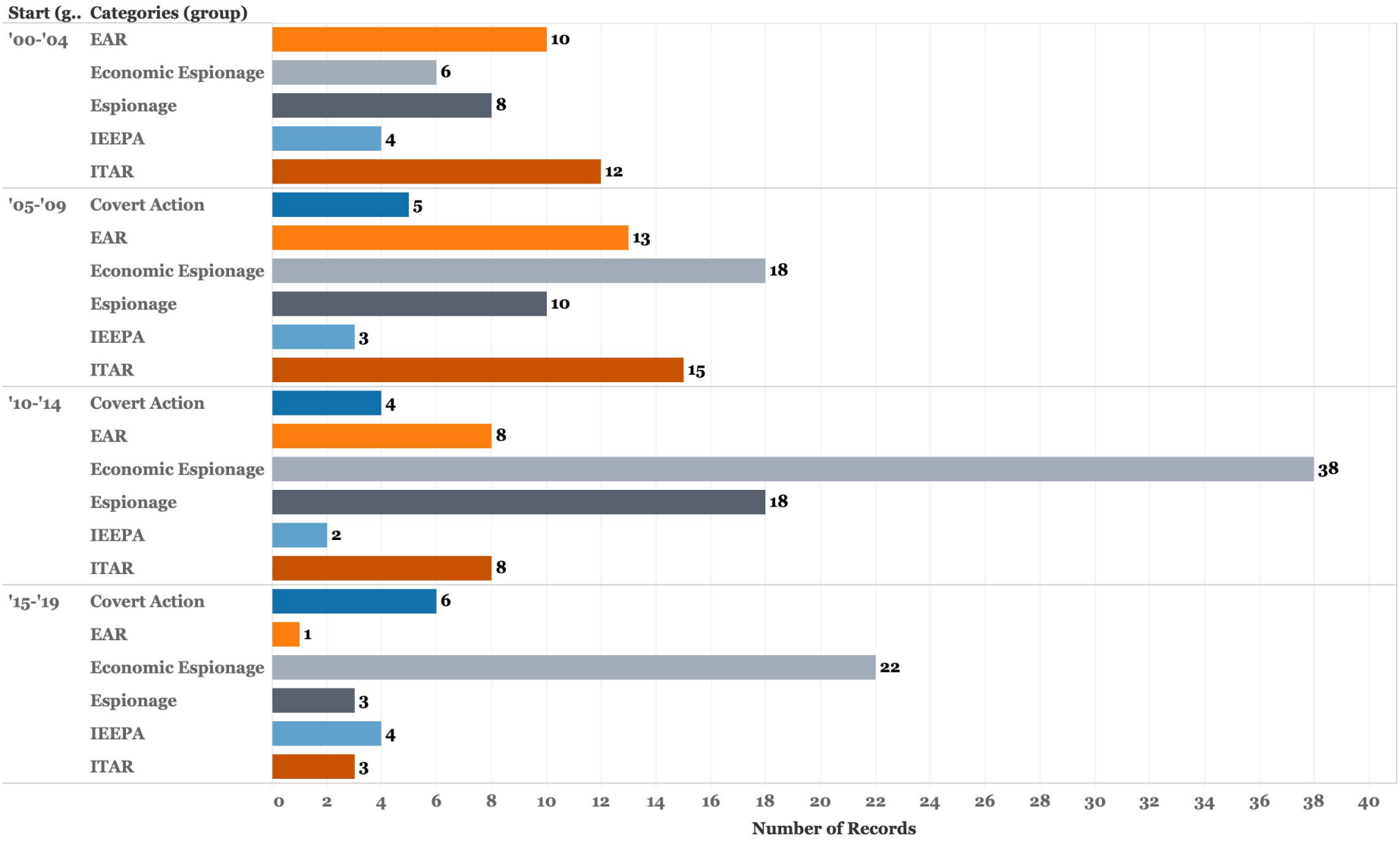
Espionage Tradecraft



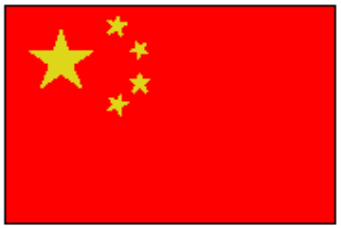
Copyright © Nicholas Eftimiades, 2019



Growth in Espionage



Copyright © Nicholas Eftimiades, 2019



Nicholas Eftimiades

neftimiades@gmail.com

Copyright © Nicholas Eftimiades, 2019