

# IT 4823

## Information Security Administration

### Intelligence and Counterintelligence



Notice: This session is  
being recorded.

# Types of Intelligence Use

- Situational:  
Police networks, battlefields, immediate or urgent, usability fades quickly
- Operational:  
Planning centers, more stable, used with other data
- Strategic:  
Big picture, long range

*Courtesy Mr. Steve Hamrick*

# U.S. Government Intelligence Agencies

The U.S. Intelligence Community (IC) is a coalition of 17 agencies and organizations within the executive branch that work both independently and collaboratively to gather the intelligence necessary to conduct foreign relations and national security activities. Their primary mission is to collect and convey the essential information the President and members of the policymaking, law enforcement, and military communities require to execute their appointed duties.

The 17 IC member agencies are:

- Air Force Intelligence
- Army Intelligence
- Central Intelligence Agency
- Coast Guard Intelligence
- Defense Intelligence Agency
- Department of Energy
- Department of Homeland Security
- Department of State
- Department of the Treasury
- Drug Enforcement Administration
- Federal Bureau of Investigation
- Marine Corps Intelligence
- National Geospatial-Intelligence Agency
- National Reconnaissance Office
- National Security Agency
- Navy Intelligence
- Office of the Director of National Intelligence

Members of the IC collect and assess information regarding international terrorist and narcotic activities; other hostile activities by foreign powers, organizations, persons, and their agents; and foreign intelligence activities directed against the United States (U.S.). As needed, the President may also direct the IC to carry out special activities in order to protect U.S. security interests against foreign threats.

Source: <http://www.intelligence.gov/about-the-intelligence-community/>

*Courtesy Mr. Steve Hamrick*

# Importance of Government Intelligence

- Intelligence drives our national security policies,
- The Intelligence Community is responsible for supplying accurate and usable information to those in charge of national security.
- The successful intelligence process converts acquired information into clear, comprehensible intelligence and delivers it to the President, policymakers, and military commanders in a form they can utilize to make educated policy decisions.
- Generating reliable, accurate intelligence is an active, never-ending process commonly referred to as the intelligence cycle.

*Courtesy Mr. Steve Hamrick*

# The Intelligence Cycle

- Identify issues and questions
- Plan to acquire information
- Collect information
- Analyze the information
- Prepare reports and recommendations

This is a cycle; answers to questions often lead to new questions.

*Courtesy Mr. Steve Hamrick*

# The Intelligence Cycle



*Courtesy Mr. Steve Hamrick*

# Elements of the Process

- Management
- Interpretation
- Distribution
- Data Gathering (Collection)
- Analysis and Reporting

*Courtesy Mr. Steve Hamrick*

# Management

- The initial stage of the intelligence cycle.
- Determine what issues need to be addressed and what information must be gathered in order to provide the proper answers.
- Begin by examining finished intelligence from previous cycles, which leads us to formulate a strategic plan for new intelligence gathering and analysis.
- The end of one intelligence cycle fuels another.

*Courtesy Mr. Steve Hamrick*



# Guidance for Management

- This stage depends on guidance from public officials.
- Policymakers, including the President, his aides, the National Security Council, and other major departments and agencies of government, initiate requests for intelligence.
- Issue coordinators from the Intelligence Community interact with these public officials to establish their core concerns and related information requirements. These needs then guide our collection strategies and allow us to produce the appropriate intelligence products.

*Courtesy Mr. Steve Hamrick*

# Interpretation

- The collection stage of the intelligence process typically yields large amounts of unfiltered data, which requires organization.
- Substantial U.S. intelligence resources are devoted to the synthesis of this data into a form intelligence analysts can use.
- Information filtering techniques include
  - exploiting imagery;
  - decoding messages and translating broadcasts;
  - reducing telemetry to meaningful measures;
  - preparing information for computer processing;
  - placing human-source reports into a form and context to make them more comprehensible.

*Courtesy Mr. Steve Hamrick*

# Distribution

- Information that has been reviewed and correlated with data from other available sources, it is called finished intelligence.
- It is disseminated directly to the same policymakers whose initial needs generated the intelligence requirements.
- Finished intelligence is hand-carried to the President and key national security advisers on a daily basis.
- The policymakers make decisions based on this information.
- These decisions may lead to requests for further examination, thus repeating the intelligence cycle.

*Courtesy Mr. Steve Hamrick*

# The Five Categories of Finished Intelligence

- Current Intelligence
- Estimative Intelligence
- Warning Intelligence
- Research Intelligence
  - Basic intelligence
  - Intelligence for operational support Scientific and Technical Intelligence
- Scientific and Technical Intelligence

*Courtesy Mr. Steve Hamrick*

# Current Intelligence

- Addresses day-to-day events.
- It details new developments and related background in order to
  - assess their significance,
  - warn of their near-term consequences, and
  - signal potentially dangerous situations in the near future.

*Courtesy Mr. Steve Hamrick*

# Estimative Intelligence

- Looks forward to assess potential developments that could affect US national security.
- By discussing the implications of a range of possible outcomes and alternative scenarios, estimative intelligence helps policymakers think strategically about long-term threats.

*Courtesy Mr. Steve Hamrick*

# Warning Intelligence

- Sounds an alarm or gives notice to policymakers.
- It suggests urgency and implies the potential need to respond with policy action.
- Warning intelligence includes identifying or forecasting events that could cause the engagement of US military forces, or those that would have a sudden and detrimental effect on US foreign policy concerns such as coups, third-party wars, or refugee situations.
- Warning analysis involves exploring alternative futures and low probability/high impact scenarios.

*Courtesy Mr. Steve Hamrick*

# Research Intelligence

- Research supports both current and estimative intelligence and is divided into two specialized subcategories:
  - Basic intelligence: Primarily consists of the structured collection of geographic, demographic, social, military, and political data on foreign countries
  - Intelligence for operational support: Tailored, focused, and rapidly produced intelligence for planners and operators that incorporates all types of intelligence production-current, estimative, warning, research, and scientific and technical.

*Courtesy Mr. Steve Hamrick*



# Scientific and Technical Intelligence

- Includes an examination of the technical development, characteristics, performance, and capabilities of foreign technologies including weapon systems or subsystems.
- This covers a complete spectrum of sciences, technologies, weapon systems, and integrated operations.

*Courtesy Mr. Steve Hamrick*

# Data Gathering (Collection)

- This stage, also known as collection, covers the acquisition of raw information through activities such as interviews, technical and physical surveillances, human source operation, searches, and liaison relationships.
- Information can be gathered from open, covert, electronic, and satellite sources.

*Courtesy Mr. Steve Hamrick*

# Six Basic Intelligence Sources

- Signals Intelligence (SIGINT)
- Imagery Intelligence (IMINT)
- Measurement and Signature Intelligence (MASINT)
- Human-Source Intelligence (HUMINT)
- Open-Source Intelligence (OSINT)
- Geospatial Intelligence (GEOINT)

*Courtesy Mr. Steve Hamrick*

# Signals Intelligence

- The interception of signals, whether between people, between machines, or a combination of both.
- Includes traffic analysis.
- The National Security Agency (NSA) is responsible for collecting, processing, and reporting SIGINT. Within the NSA, the National SIGINT Committee advises the Director, NSA, and the Director of National Intelligence (DNI) on policy issues and manages the SIGINT requirements system.

*Courtesy Mr. Steve Hamrick*

# Imagery intelligence

- Representations of objects reproduced electronically or by optical means on film, electronic display devices, or other media.
- It can be derived from visual photography, radar sensors, infrared sensors, lasers, and electro-optics.
- The National Geospatial-Intelligence Agency manages all IMINT activities, both classified and unclassified, within the government . This includes requirements, collection, processing, exploitation, dissemination, archiving, and retrieval.

*Courtesy Mr. Steve Hamrick*

# Measurement and Signature Intelligence

- Scientific and technical intelligence information used to locate, identify, or describe distinctive characteristics of specific targets.
- It employs a broad group of disciplines including nuclear, optical, radio frequency, acoustics, seismic, and materials sciences. For example, MASINT can identify distinctive radar signatures created by specific aircraft systems or the chemical composition of air and water samples.
- The Central MASINT Organization, a component of the Defense Intelligence Agency, is the focus for all national and Department of Defense (DoD) MASINT matters.

*Courtesy Mr. Steve Hamrick*

# Human-Source Intelligence

- The oldest method for collecting information, this is intelligence derived from human sources.
- Collection includes clandestine acquisition of
  - photography,
  - documents, and other material;
  - overt collection by personnel in diplomatic and consular posts;
  - debriefing of foreign nationals and US citizens who travel abroad; and
  - official contacts with foreign governments.
- To the public, HUMINT is synonymous with espionage and clandestine activities. However, most of it is accumulated by overt collectors such as diplomats and military attaches.

*Courtesy Mr. Steve Hamrick*

# Sources of Human Intelligence

- HUMINT is used mainly by the Central Intelligence Agency (CIA), the Department of State (DoS), the DoD, and the FBI. The CIA, working closely with the Office of the Director of National Intelligence (ODNI) established the National Clandestine Service (NCS) to improve HUMINT throughout the IC.
- The NCS serves as the national authority for coordination, de-confliction, and evaluation of clandestine HUMINT operations, both abroad and inside the United States.
- While the ODNI establishes policy related to clandestine HUMINT, the NCS executes and implements that policy across the Intelligence Community (IC).

*Courtesy Mr. Steve Hamrick*



# Open-Source Intelligence

- Publicly available information appearing in print or electronic form including radio, television, newspapers, journals, the Internet, commercial databases, and videos, graphics, and drawings.
- While open-source collection responsibilities are broadly distributed through the IC, the major collectors of OSINT are the
  - Foreign Broadcast Information Service and the
  - National Air and Space Intelligence Center.

*Courtesy Mr. Steve Hamrick*

# Geospatial Intelligence

- Imagery and mapping data produced through an integration of imagery, imagery intelligence, and geospatial information.
- GEOINT is typically gathered from commercial satellites, government satellites, reconnaissance aircraft, or by other means such as maps, commercial databases, census information, GPS waypoints, utility schematics, or any discrete data that have locations on earth.
- This data is utilized to support our national security, which includes everything from assisting soldiers on the battlefield to assisting humanitarian and disaster relief efforts.

*Courtesy Mr. Steve Hamrick*

# Analysis and Reporting

- The fourth stage of the intelligence cycle involves converting basic information into finished documentation.
- This includes integrating, evaluating, and analyzing all available data—which is often fragmented and even contradictory—and distilling it into the final intelligence products, which highlight information on topics of immediate importance or make long-range assessments.

*Courtesy Mr. Steve Hamrick*

# Intelligence Analysts

- Analysts, who are subject-matter specialists, absorb incoming information, evaluate it, produce an assessment of the current state of affairs within an assigned field or substantive area, and then forecast future trends or outcomes.
- They integrate data into a coherent whole, put the evaluated information in context, and produce finished intelligence that includes assessments of events and judgments about the implications of the information for the United States (U.S.).
- Analysts are encouraged to include alternative futures in their assessments and to look for opportunities to warn about possible developments abroad that could either provide threats to or opportunities for U.S. security and policy interests. Analysts also develop requirements for collection of new information.

*Courtesy Mr. Steve Hamrick*

# Stages of Cryptanalysis

- The stone age (trickery and subversion) deduction, theft, bribery were all more effective than mathematics
- The industrial age (simple to complex encryption with some advanced mathematical enhancements) cipher breakers existed and ciphers were sufficiently simple to be breakable using common techniques such as frequency analysis
- The modern age (public keys, complex mathematical algorithms, public key cryptography, quantum computing, differential cryptanalysis ) decryption only exists as the result of high speed analysis; there is no simplex cryptanalysis technique that will regularly break ciphers; cryptanalysts are generally high-tech

Note: stone, industrial, and modern are non-standard characterizations that you will not find in any standard source.

*Courtesy Mr. Steve Hamrick*

# Reminder: Codes and Ciphers

- Both codes and ciphers obfuscate communications to foil eavesdropping.
- **Codes** substitute words, phrases, or other symbols for other words. Codes operate at the level of meaning.
  - *One if by land and two if by sea.*
  - *Climb Mount Niitaka.*
- **Ciphers** operate at the level of symbols or small groups of symbols.

# More About Cryptanalysis

- Codes are only breakable if you have the code book or the code is compromised.
- Classic cryptanalysis encompasses frequency analysis, index of coincidence, and Kasiski examination (though there are other methods, these were most common)
- Symmetric analysis, hash functions, attack models, side channel attacks, network attacks, and external attacks have all developed within the past 10 - 15 years.

*Courtesy Mr. Steve Hamrick*

# Simple Code Book

CODE GROUP:	PLAINTEXT:
AAB	A
ABD	AB
ACF	ABANDON
ADH	ABOUT
AEJ	ACCIDENT
AFL	ACTION
AGN	ACTIVE
AHP	ACTIVITY
...	...
...	...

*Courtesy Mr. Steve Hamrick*



# More About Simplex Cryptanalysis

<http://www.umich.edu/~umich/fm-34-40-2/>

FIELD MANUAL

NO 34-40-2 HEADQUARTERS

DEPARTMENT OF THE ARMY

Washington, DC, 13 September 1990

*Courtesy Mr. Steve Hamrick*

# Your Security Program

- Protect your people
  - Protect your place
  - Protect your product (product integrity)
  - Protect your portal (computer and network security)
- Physical security

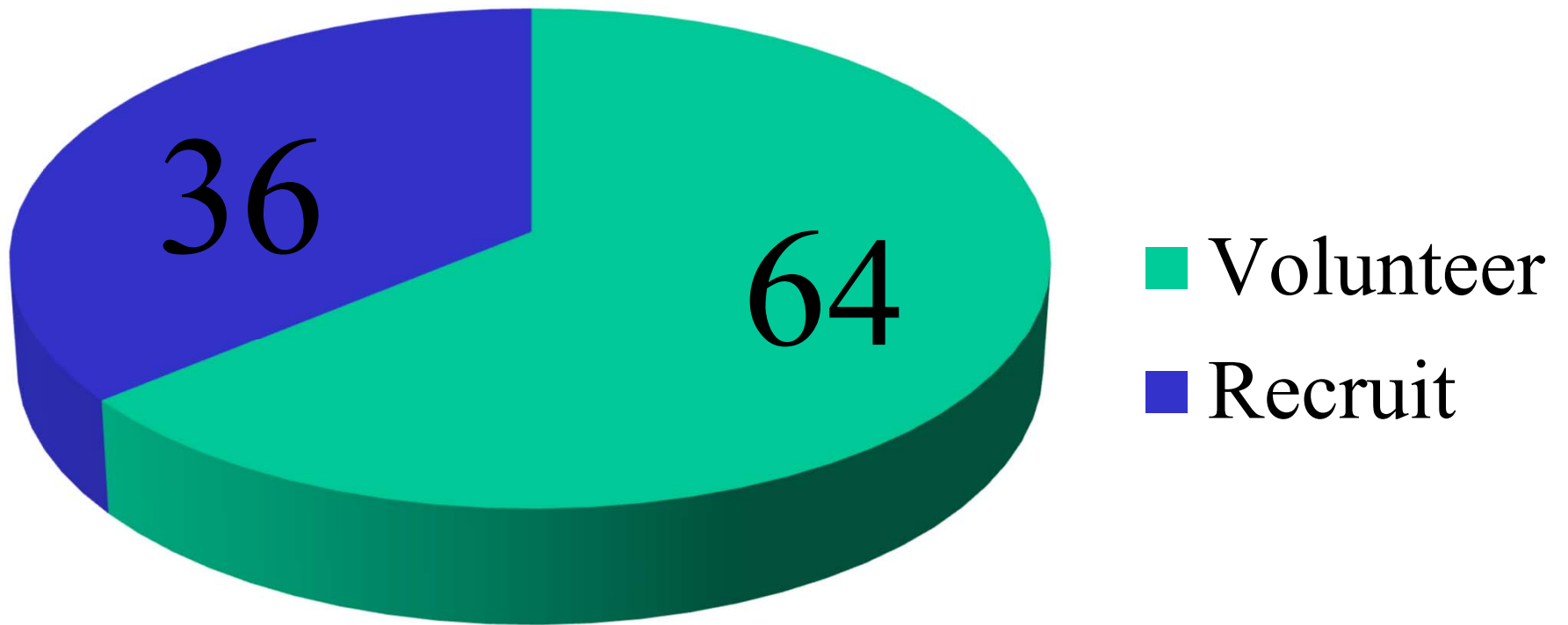
*Courtesy Federal Bureau of Investigation*

# Espionage Agents (Collectors)

- Spotting
- Assessment
- Development
- Recruitment
- Operation
- Termination

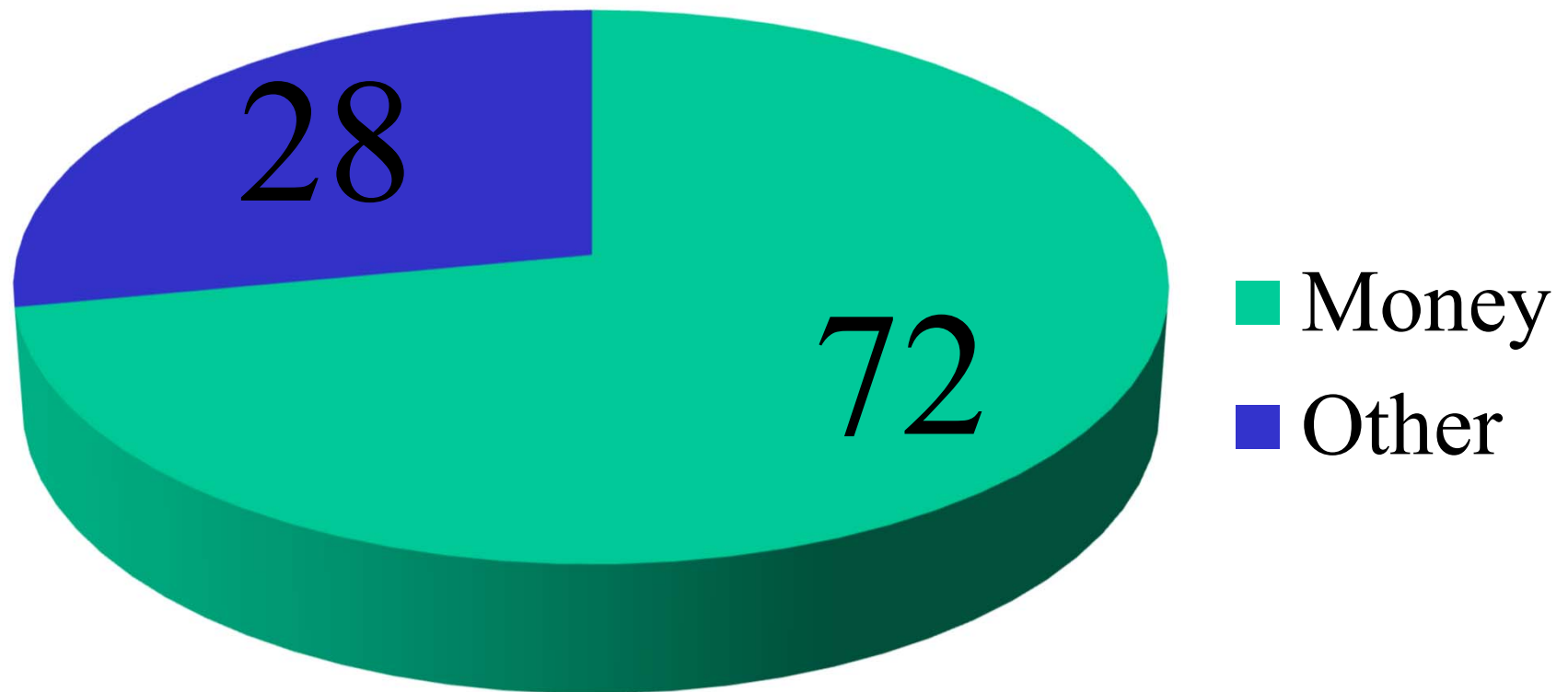
*Courtesy Federal Bureau of Investigation*

## Collectors: Source



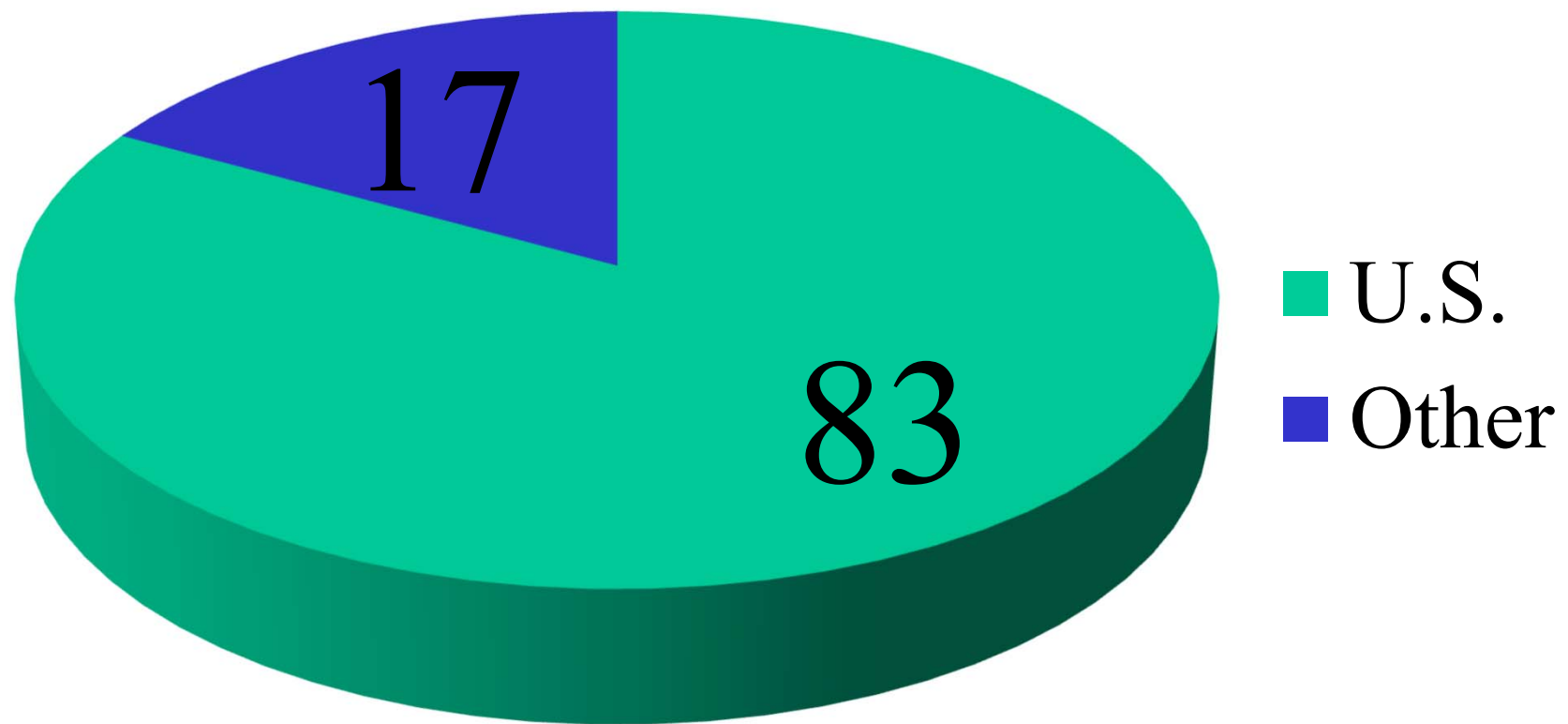
*Courtesy Federal Bureau of Investigation*

## Collectors: Motivation



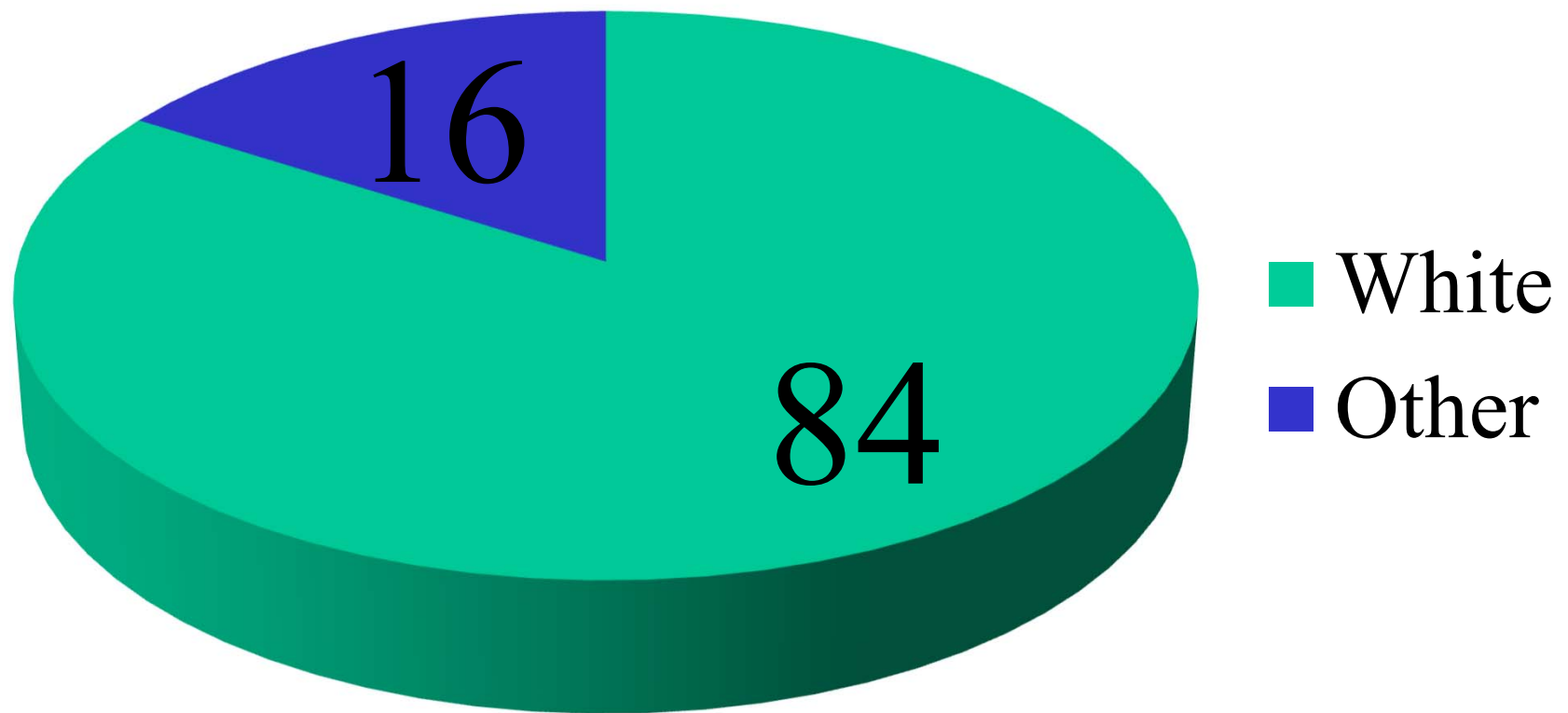
*Courtesy Federal Bureau of Investigation*

## Collectors: Location



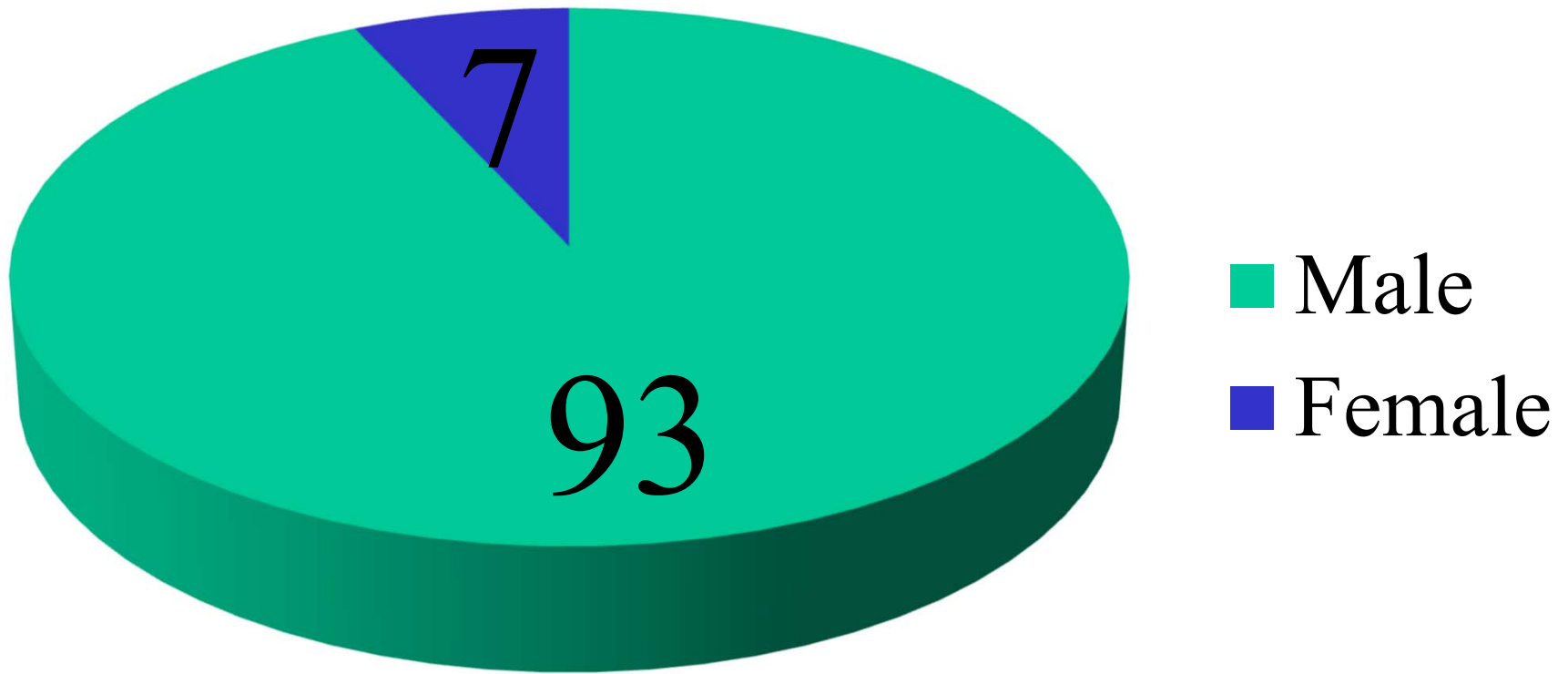
*Courtesy Federal Bureau of Investigation*

## Collectors: Ethnicity



*Courtesy Federal Bureau of Investigation*

## Collectors: Sex



*Courtesy Federal Bureau of Investigation*



# Requirements

- Desire for information
- Collections training
- Access
- Exploitable vulnerability

*Courtesy Federal Bureau of Investigation*

# Motivation

- Compromise
- Revenge
- Ideology
- Money
- Ego

*Courtesy Federal Bureau of Investigation*

# Danger Signs

- Odd working hours
- Suspicious travel
- Unexplained affluence
- Asymmetric relationships
- Substance abuse



Anna Chapman  
(Anna Kushchchenko)

*Courtesy Federal Bureau of Investigation*

# Case: Economic Espionage

- U.S. chemical company.
- Chinese had penetrated the company's network using phishing email.
- Adversary gained control of mail servers in Germany and Canada.
- Intercepted inbound orders.
- Intercepted outbound email with price quotes.
- Tampered with ordering system for raw materials, causing production delays.
- Stole research results.

*Bloomberg Business Week*

# Result and Lesson

- The company's fortunes faltered because of delays and unfair competition.
- The company had no way to recover.
- A Chinese firm made a low-ball offer to buy the company.
- Lesson: Don't try to defend against everyone.
  - Identify top two or three competitors.
  - Assign risk scores to individuals and companies.

*Bloomberg Business Week*

# Case: Italian Bank

- Monitoring equipment showed that a server at an Italian bank was contacting Facebook.
- Server was also sending data to unknown IP addresses.
- Analysis: the server was being used to mine bitcoins; had been infected through a phishing attack. Facebook was used as a control point.
- Lesson: Monitor what goes out of your network as well as what comes in.

*Bloomberg Business Week*

# Case: Google's Gmail

- In 2010, Google disclosed attacks on Gmail by a group associated with the Chinese PLA.
- Attack apparently exploited a flaw in Internet Explorer.
- Many other organizations also attacked in the same way.
- Lesson: Keep software up to date; be careful where you browse.

*Bloomberg Business Week*

# Questions

