

FBI 101

Cyber Security

SSA Michael F. D. Anaya, Cyber Supervisor

Today's **AGENDA**



01 **INTRODUCTION TO THE FBI**

Where Are We Located?
Who Are We?
What Do We Do?



02 **ANATOMY OF A BREACH** A Hackers SOP



03 **Emerging Threats** BotNET - C2 BotNET - P2P The Nugache Worm

Where Are We Located

56 **HQ Divisions** **18**
Field Offices



Introduction to the FBI



Where Are We Located

Field Offices

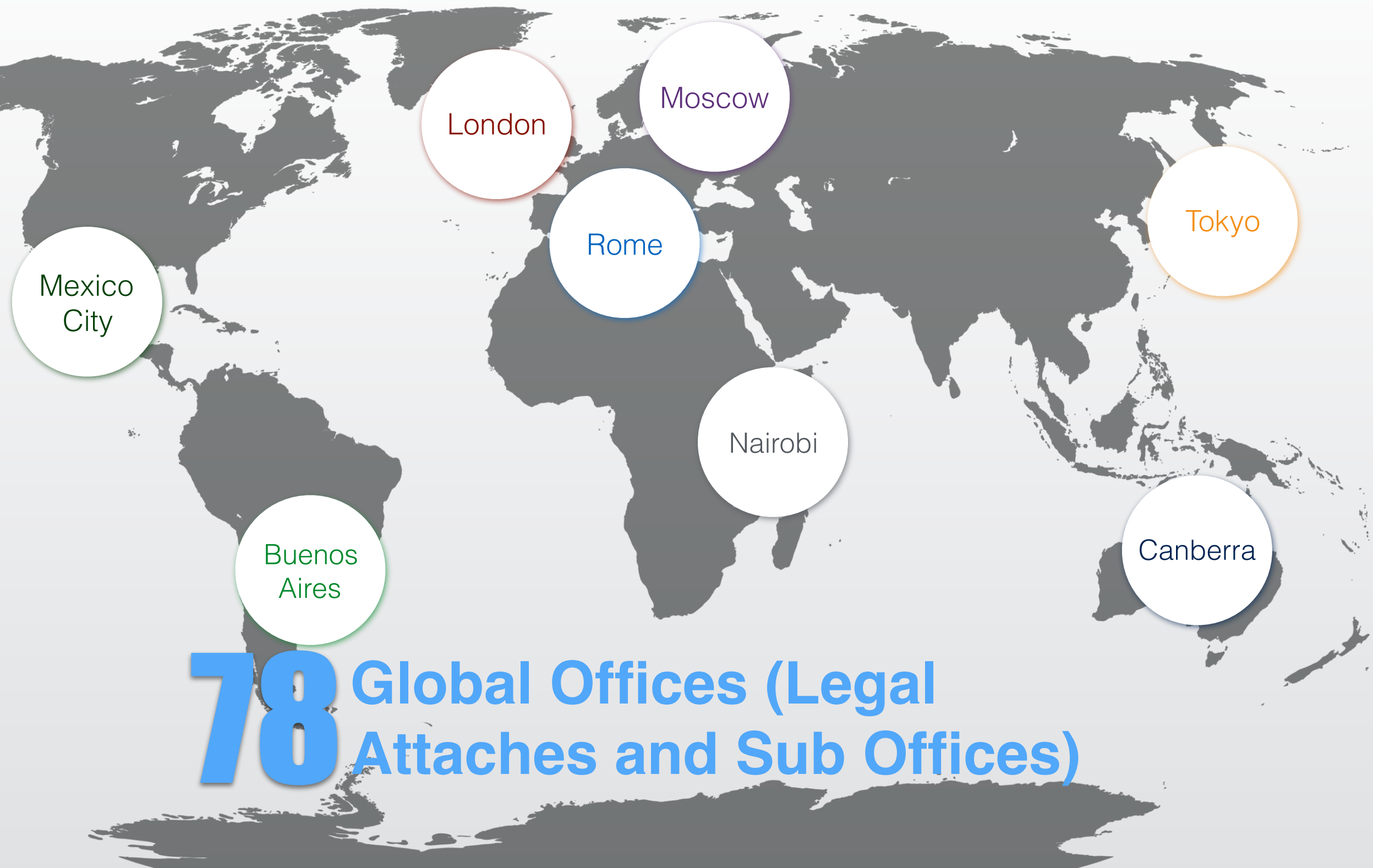
*Area of Responsibility
Resident Agencies
Investigative Control*

Honolulu

Introduction to the FBI



Where Are We Located



78 Global Offices (Legal Attaches and Sub Offices)

Introduction to the FBI



Who Are We?



35,000

FBI Employees (Agent and Professional Staff)
Worldwide



60 % Professional Staff



Who Are We?

Analysts



Interns



Scientists



Linguists



Agents



HR Specialists



Introduction to the FBI



Who Are We?



FBI Honors Internship Program

- A paid internship program
- Open to undergraduate, graduate or higher level students
- Candidates must be enrolled and attending, a college or university full-time
- 10 week summer program
- Begins in June and ends in August
- Interns will work side-by-side with FBI employees

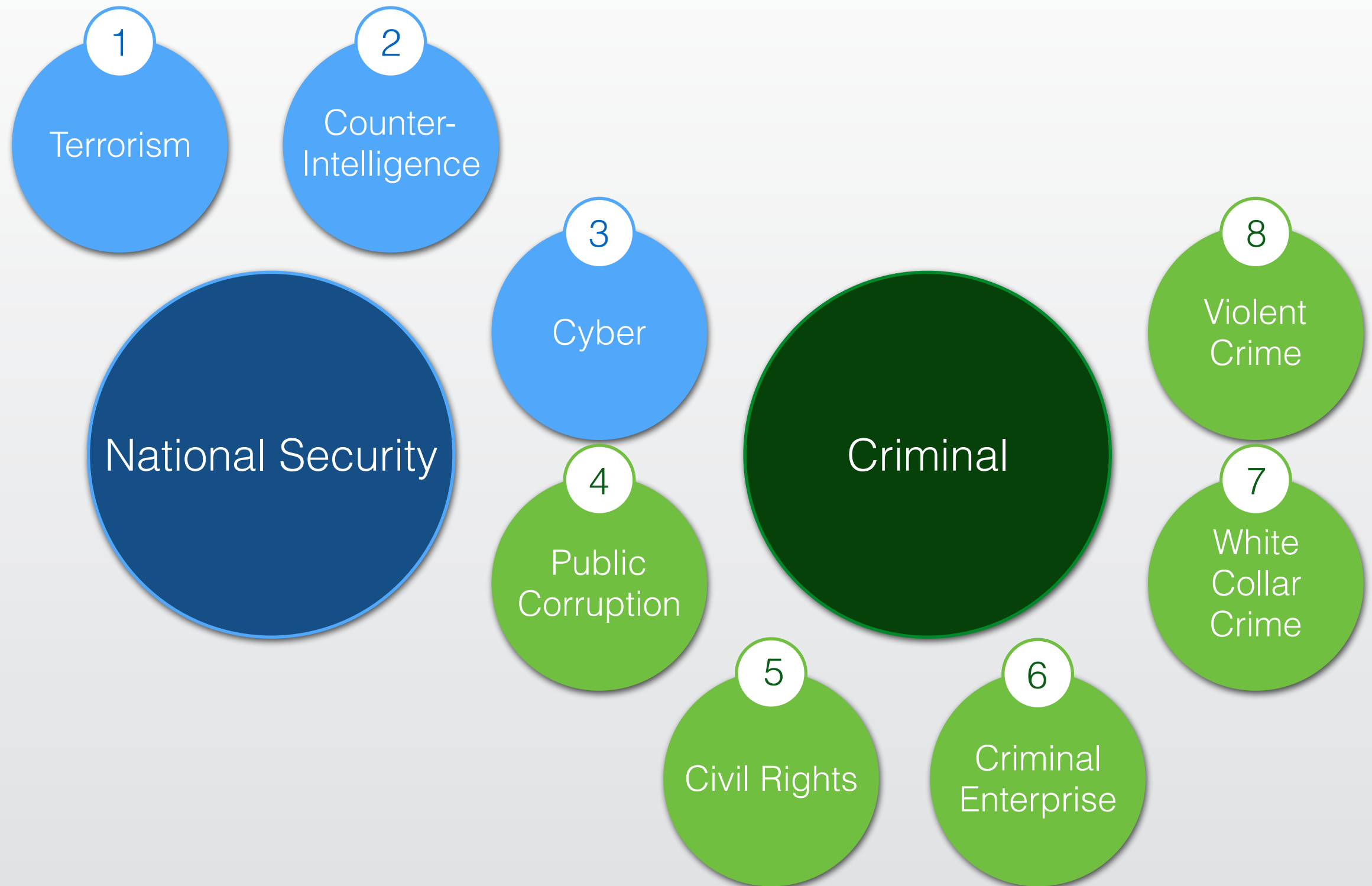
For more information - <https://www.fbijobs.gov/honors-internship-program>



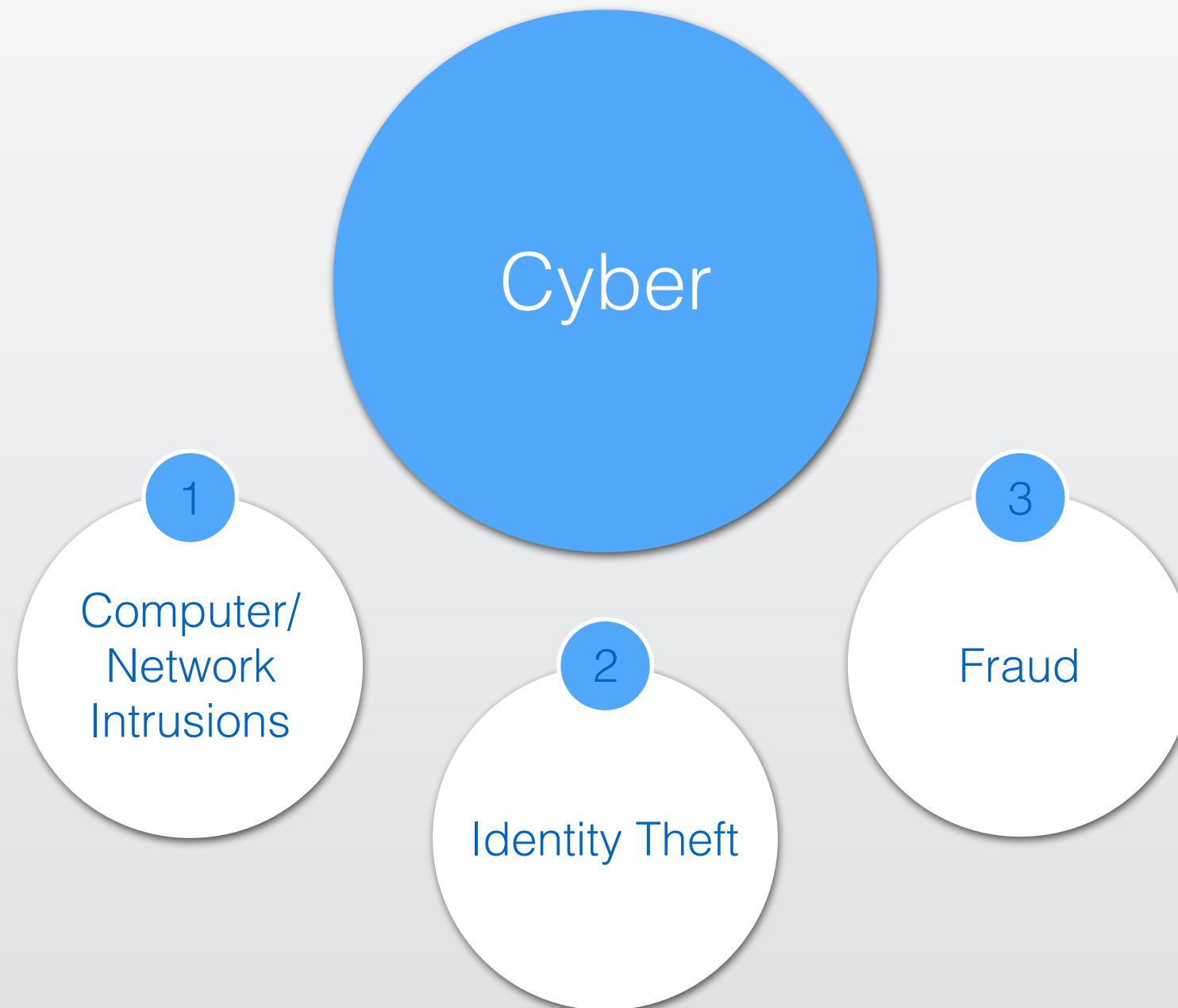
Introduction to the FBI



What Do We Do?



What Do We Do?





01 **CONTACTING THE FBI**

Where Are We Located?
Who Are We?
What Do We Do?

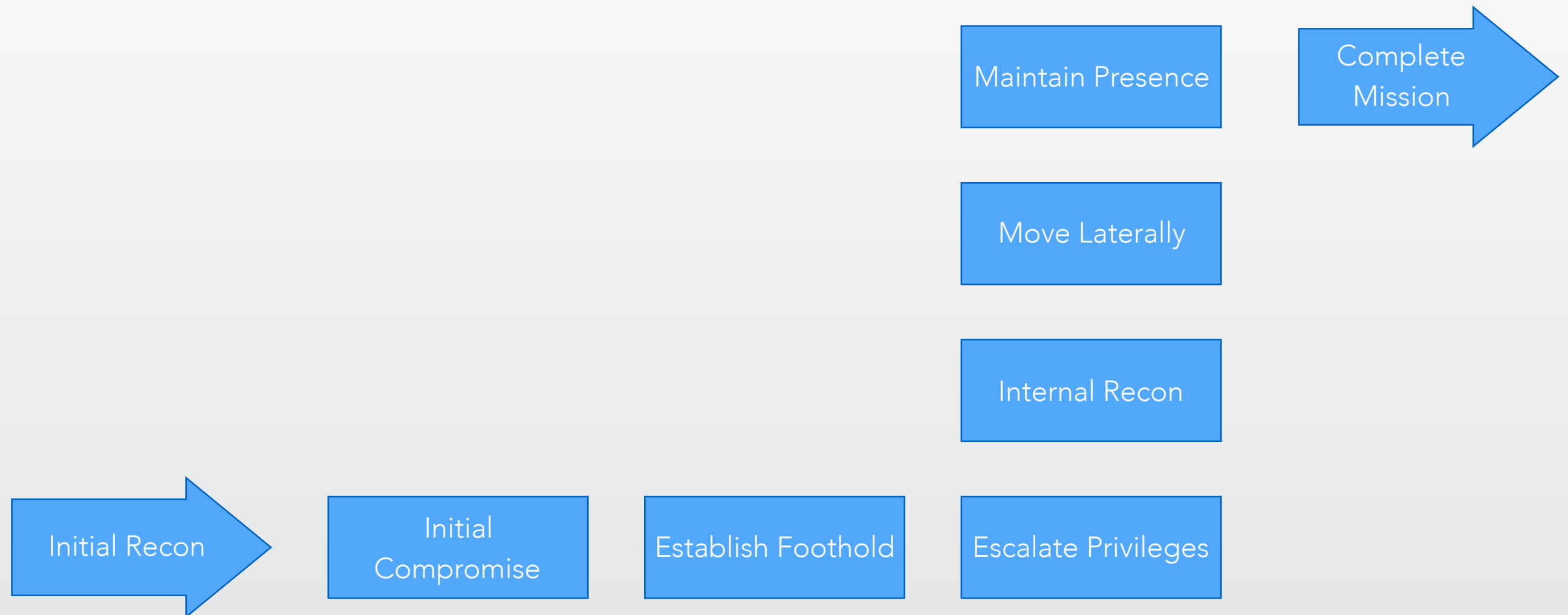


02 **ANATOMY OF A BREACH**

A Hackers SOP



A Hacker's SOP





01 **CONTACTING THE FBI**

Where Are We Located?
Who Are We?
What Do We Do?
How Would You Notify Us



02 **ANATOMY OF A BREACH**

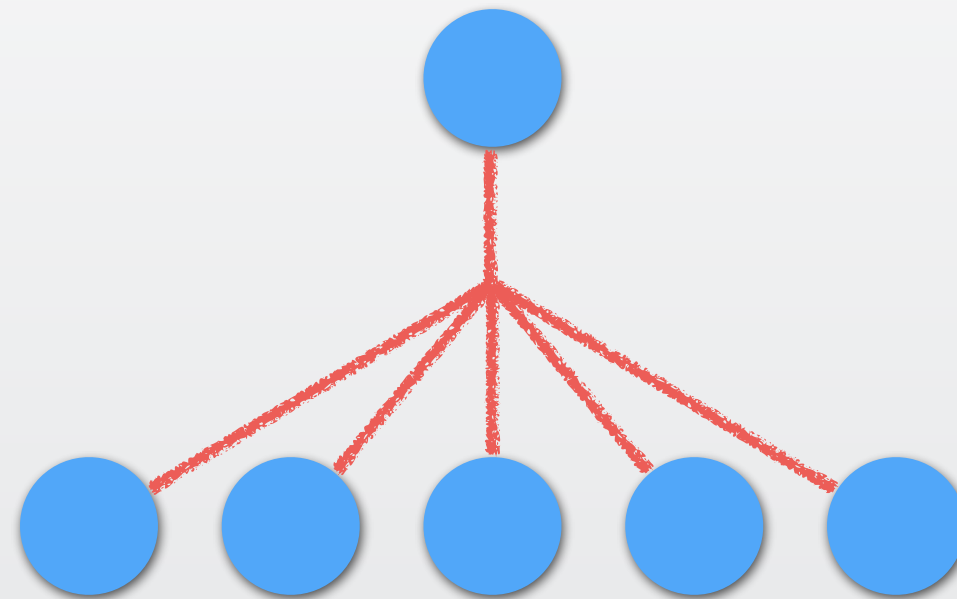
A Hackers SOP



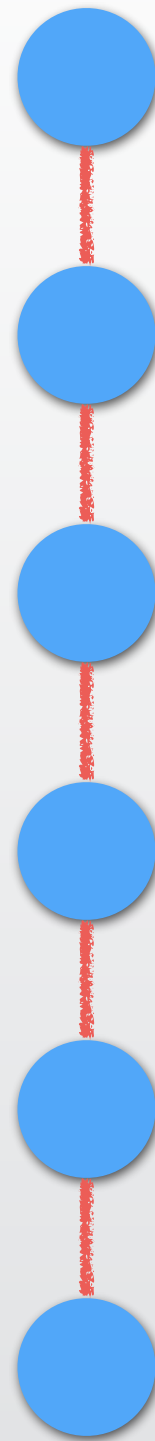
03 **Emerging Threats**

BotNET - C2
BotNET - P2P
The Nugache Worm

BotNET - C2 (Command and Control)

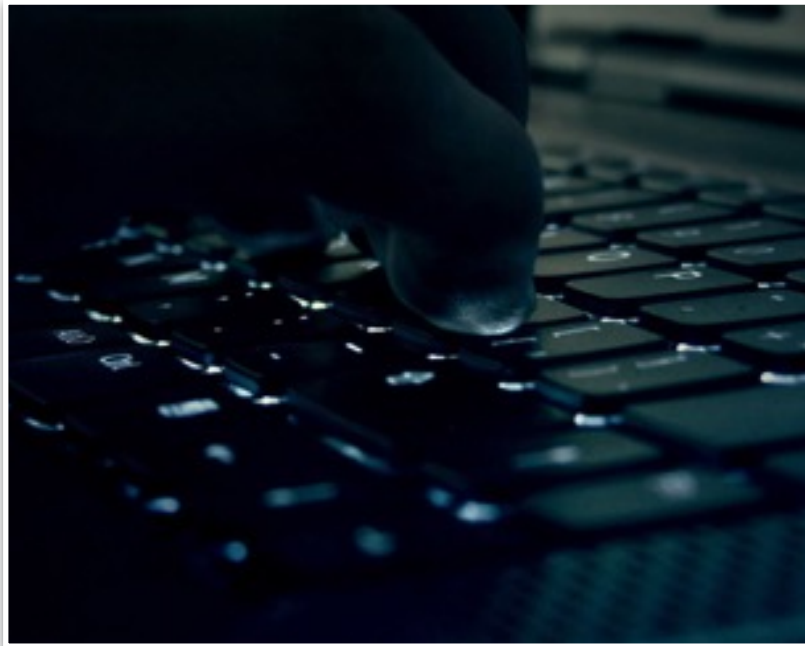


BotNET - P2P (Peer to Peer)



“you were dosed yesterday.
we require to 2000 dollars
egold #2974556. we give to
you 5 days if you do not
make, then you obtain one
lost week.”

www.USTIreAndWheel.com
webserver was dropped offline



Nugache Worm

The funds were sent My-ATM-Card.biz (A US company with operations in Romania)

Then the ATM cards were sent to WY



Event 1
DDoS



Event 2
E-mail Sent



Event 3
eGold Account Funded



1. go to <http://www.me-gold.com> and click buy e-currency from us
2. put in Via: Western Union
3. click preview
4. Western union instructions are given after you confirm

g-Cards were intercepted and delivered to the given address in WY

- Residence was vacant
- Package was never picked up
- Never received another e-mail



Event 4
Controlled
Delivery



Event 5
E-mail Search Warrants



Two SWs were executed on e-mail accounts.

Revealed that the subject had ordered an array of items with stolen identities...and an IP pointed to an address in WY

Nugache Worm

Monitored a victim's computer...but the traffic was encrypted



Event 6
Data Intercept

Emerging Threats



Nugache Worm

A high volume of encrypted data was sent to an IP in WY.



Event 7
Honeypot



Event 8





Event 8
The Search Warrant

What We Learned

- 18 years old
- Suffered from physical impairment
- Very secluded and introverted
- Isolated from any interpersonal interaction
- Highly intelligent
- Self educated on all computer related areas



Q&A SESSION

