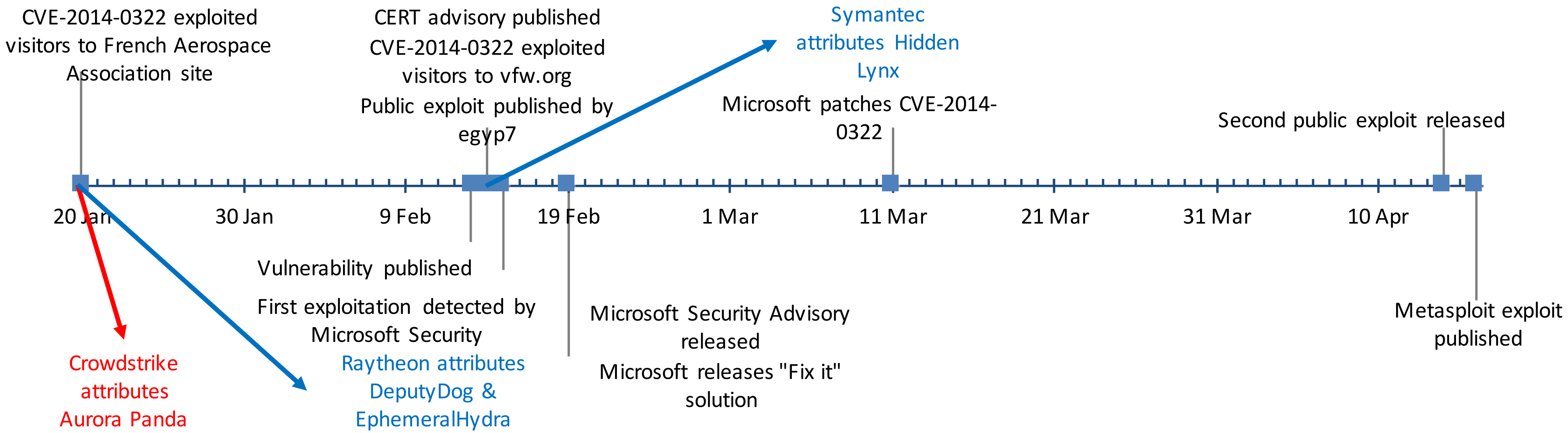
Enhanced Attribution

Angelos D. Keromytis
Program Manager
Information Innovation Office (I2O)

- Briefing prepared for Computational Cybersecurity In Compromised Environments (C3E) Fall Workshop
- October 23, 2017

Attribution Today

The same campaign attributed to 4 different intrusion sets by 3 commercial cybersecurity providers, based on different observables



CVE-2014-0322 exploited visitors to French Aerospace Association site
CERT advisory published
CVE-2014-0322 exploited visitors to vfw.org
Public exploit published by egyp7
Symantec attributes Hidden Lynx
Microsoft patches CVE-2014-0322
Second public exploit released
20 Jan
30 Jan
9 Feb
19 Feb
1 Mar
11 Mar
21 Mar
31 Mar
10 Apr
Vulnerability published
First exploitation detected by Microsoft Security
Raytheon attributes DeputyDog & EphemeralHydra
Crowdstrike attributes Aurora Panda
Microsoft Security Advisory released
Microsoft releases "Fix it" solution
Metasploit exploit published

Q: Who is UglyGorrilla?

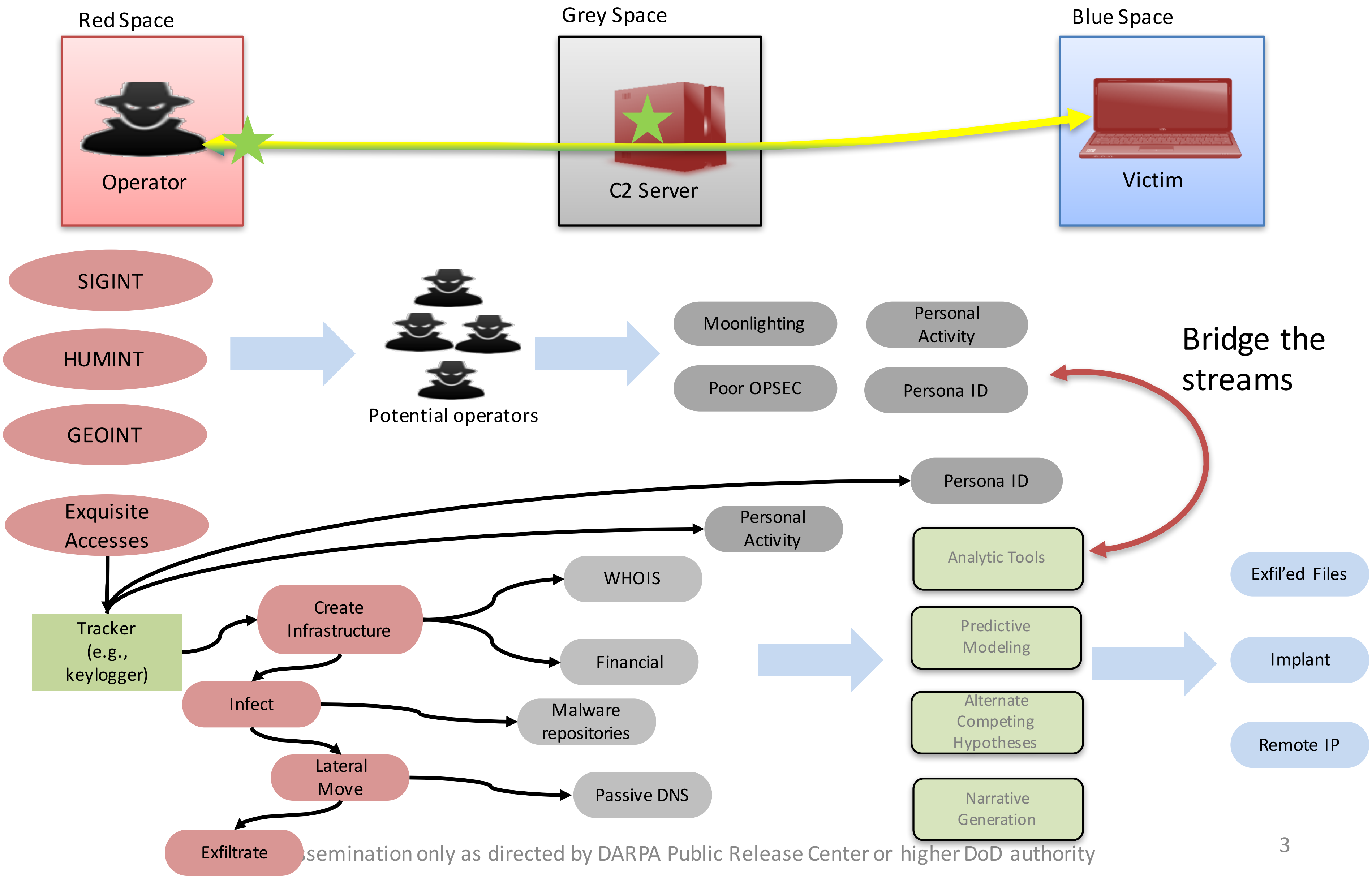
A: Wang Dong

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
WANTED
BY THE FBI

How do we know?
DNS registrations
DNS use
PLA alumni website
Binary metadata
Passwords
Social media

"Attribution is really really hard … we're using the totality of the sources and methods we have to help inform that. [But] because those advanced persistent threats aren't going away … we can't bring all that information to the fore and be fully transparent about everything we know and how we know it."

Attributing Cyber Operations



Red Space

Operator

Grey Space

C2 Server

Blue Space

Victim

SIGINT

HUMINT

GEOINT

Exquisite Accesses

Potential operators

Moonlighting

Personal Activity

Poor OPSEC

Persona ID

Bridge the streams

Persona ID

Personal Activity

Tracker (e.g., keylogger)

Create Infrastructure

Infect

Lateral Move

Exfiltrate

WHOIS

Financial

Malware repositories

Passive DNS

Analytic Tools

Predictive Modeling

Alternate Competing Hypotheses

Narrative Generation

Exfil'ed Files

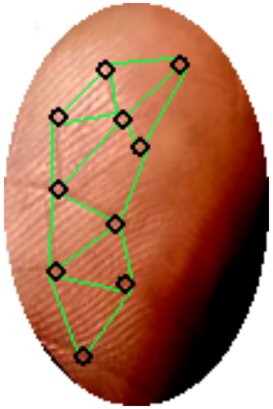
Implant

Remote IP

Redacted APT Actor Attribution

Name	REDACTED
Address	REDACTED
DoB	REDACTED
Alias	REDACTED
Phone	REDACTED
Email(s)	REDACTED REDACTED REDACTED
Hobbies	photography, malware, cycling
Tons more...	Infrastructure, implants, friends, family

Left Index Fingerprint



Attribution Experiment – APT Actor

- Minimal existing public reporting (but some)
  - Linked in one public threat intelligence report

- Handle appears in public data sources

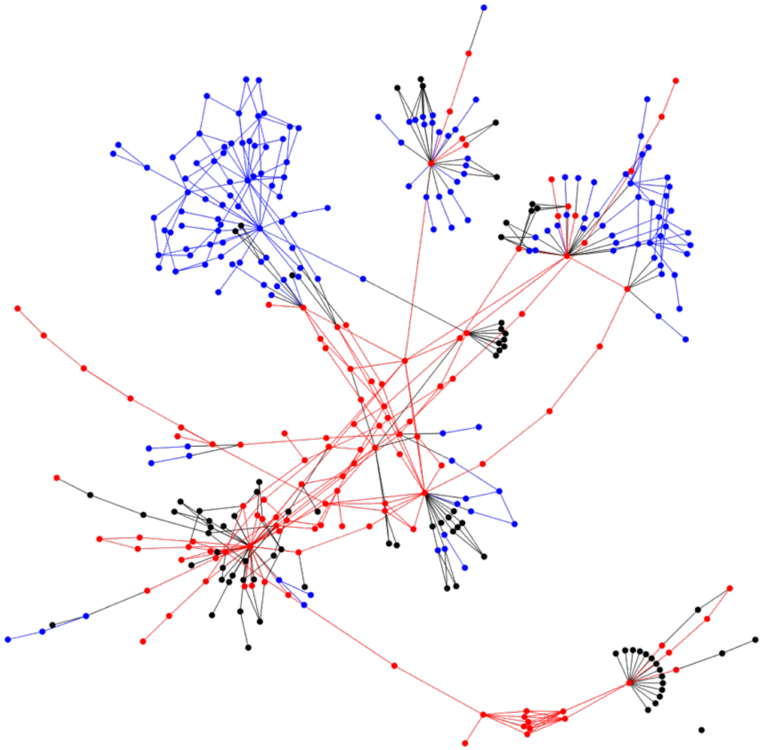
- Optimal cardinality
  - “Goldilocks Zone” of cardinality (vs adjacent individuals)

- Long suspected activity lifespan
  - 2008 - 2017+

DISTRIBUTION C. Distribution authorized to U.S. Government Agencies and their contractors; Administrative or Operational Use; 21 Mar 17. Other requests for this document shall be referred to DARPA, I2O, 675 N Randolph St, Arlington, VA 22203.

Individual OSINT Graph

- Two dimensional projection of hyper-graph
- Nodes with the same name/handle



●individual
●name collision
●unknown

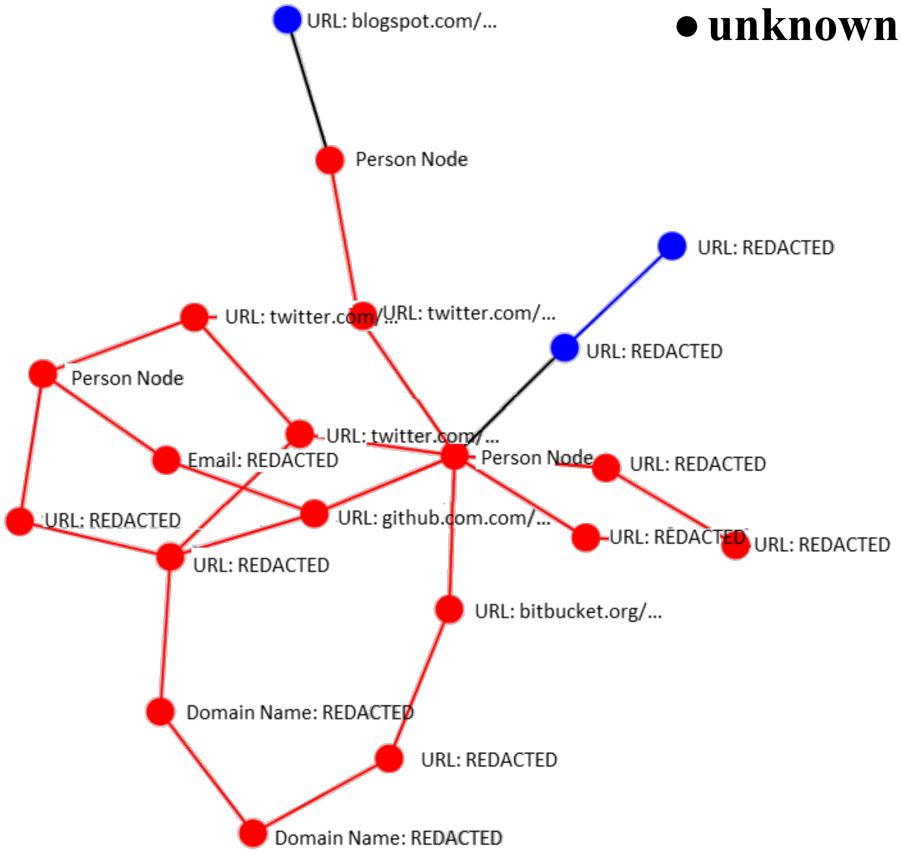
Differentiating People

Two individuals with same handle

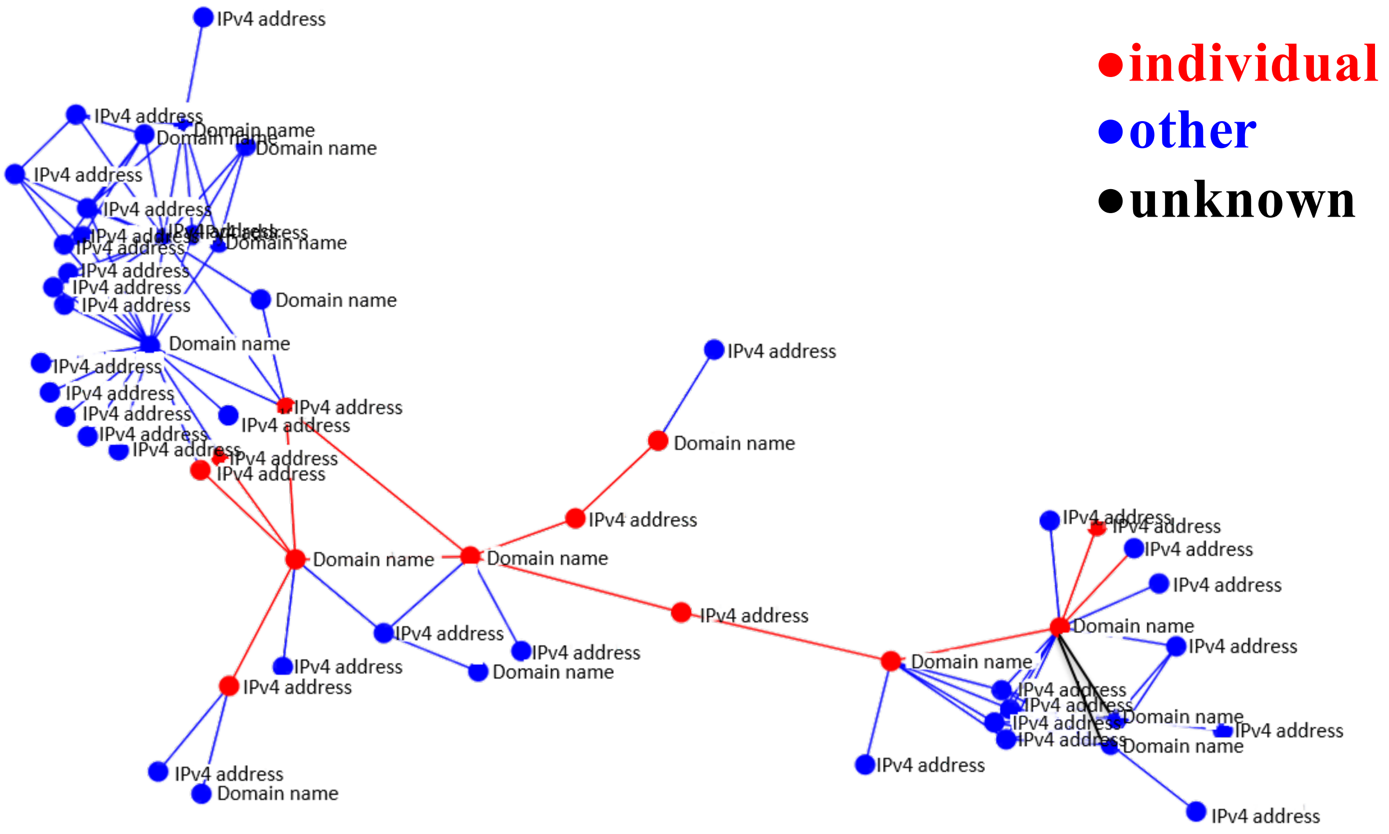
Name ?
- In neutral country
- Language corroboration

APT Actor
- In known APT region
- Language corroboration
- Speaks English

● individual
● name collision
● unknown



Differentiate infrastructure ownership

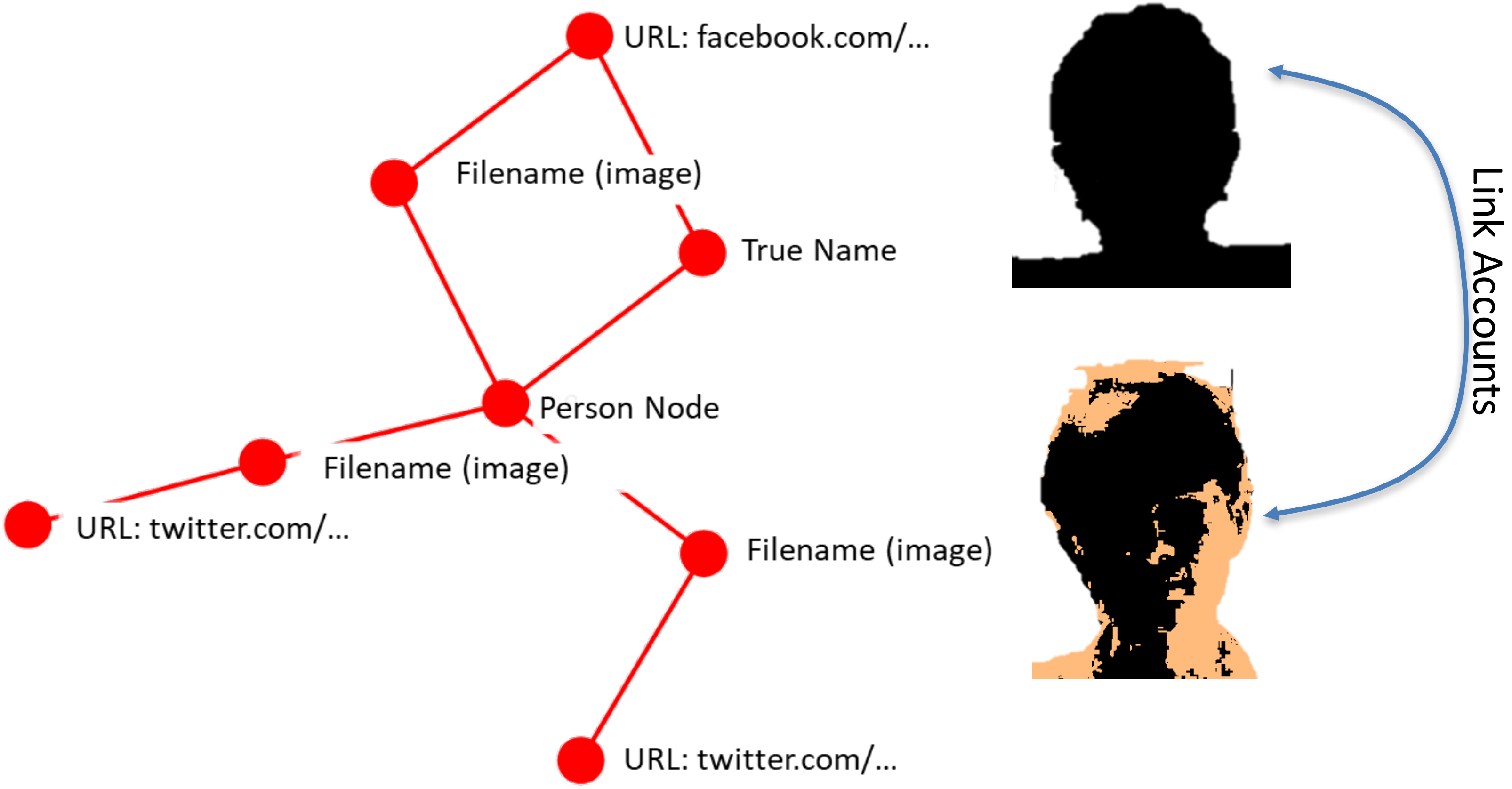


<span style="color:red">●individual</span>

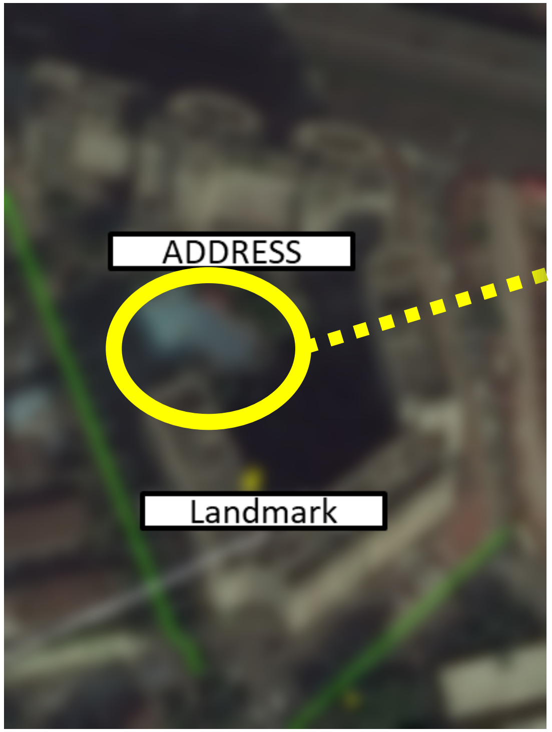
<span style="color:blue">●other</span>

●unknown

Images and Modeling



Geolocation and Hobby Confirmation



Satellite Imagery

From individual’s footage

GPS trace from Individual’s hobby

Accidental photograph from home office

Matches overhead imagery

Ubuntu Linux

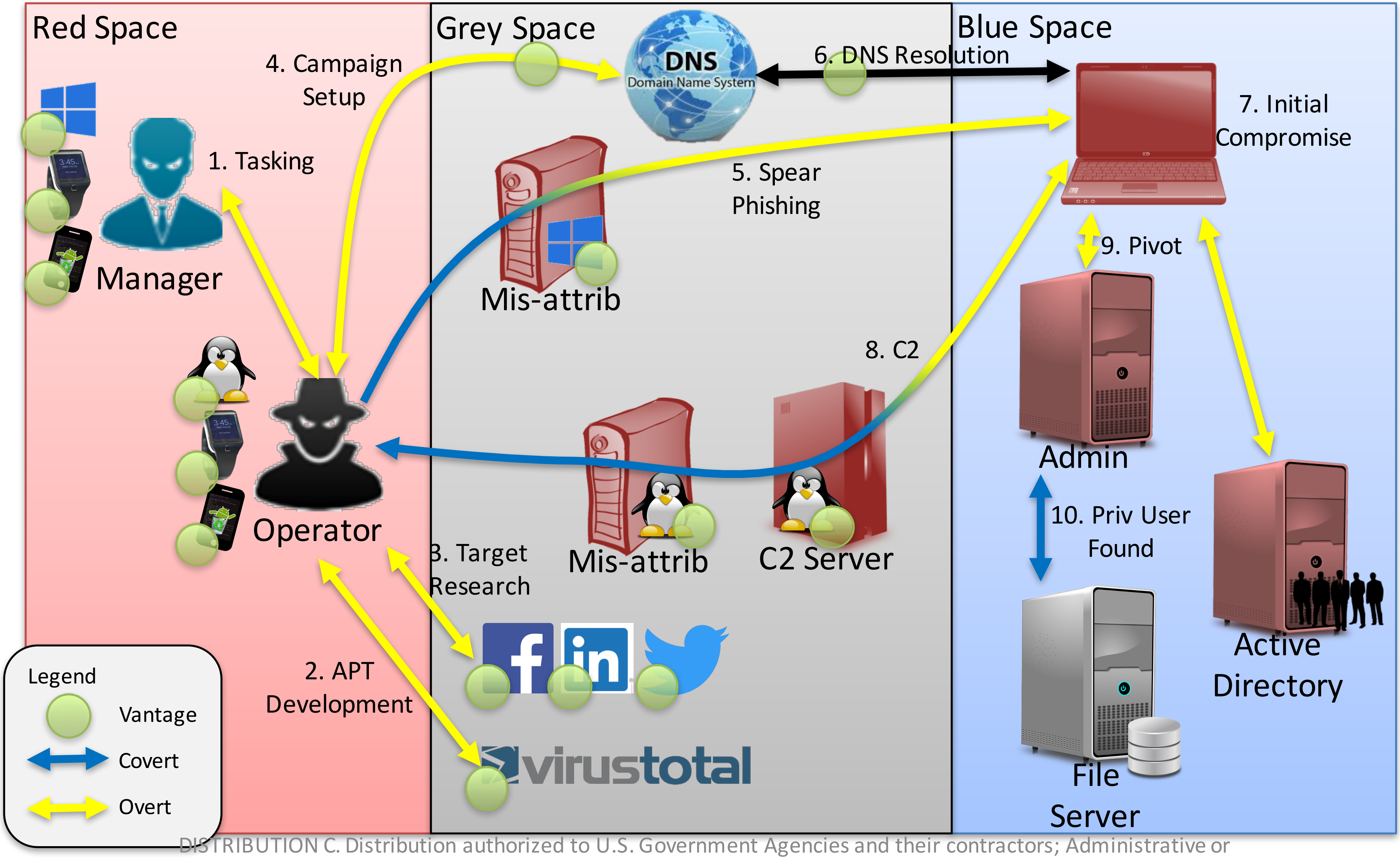
Bike handlebars

TA1: Activity Tracking and Summarization

- Focus on Behavioral Biometrics and Upstream Activity Extraction
  - Collect information that will specifically identify actor or persona
  - What tools, tactics, and procedures (TTPs) an actor uses
  - How actor interacts with systems
  - How the use of the tools, as seen from the actor’s system(s), affects downstream systems
- What tools are the actor using?
  - Known Tools (e.g., Regin, Flame, Duqu, Duqu2, mimikatz, Heartbleed, Cobalt Strike, etc.)
  - General Purpose Tools (e.g., Browsers, Secure Messaging, etc.)
  - Unknown Tools (or: how do we make them known tools?)
- **End goal is to consistently match actors to their online personas, track their persona activities, and de-identify said online personas**

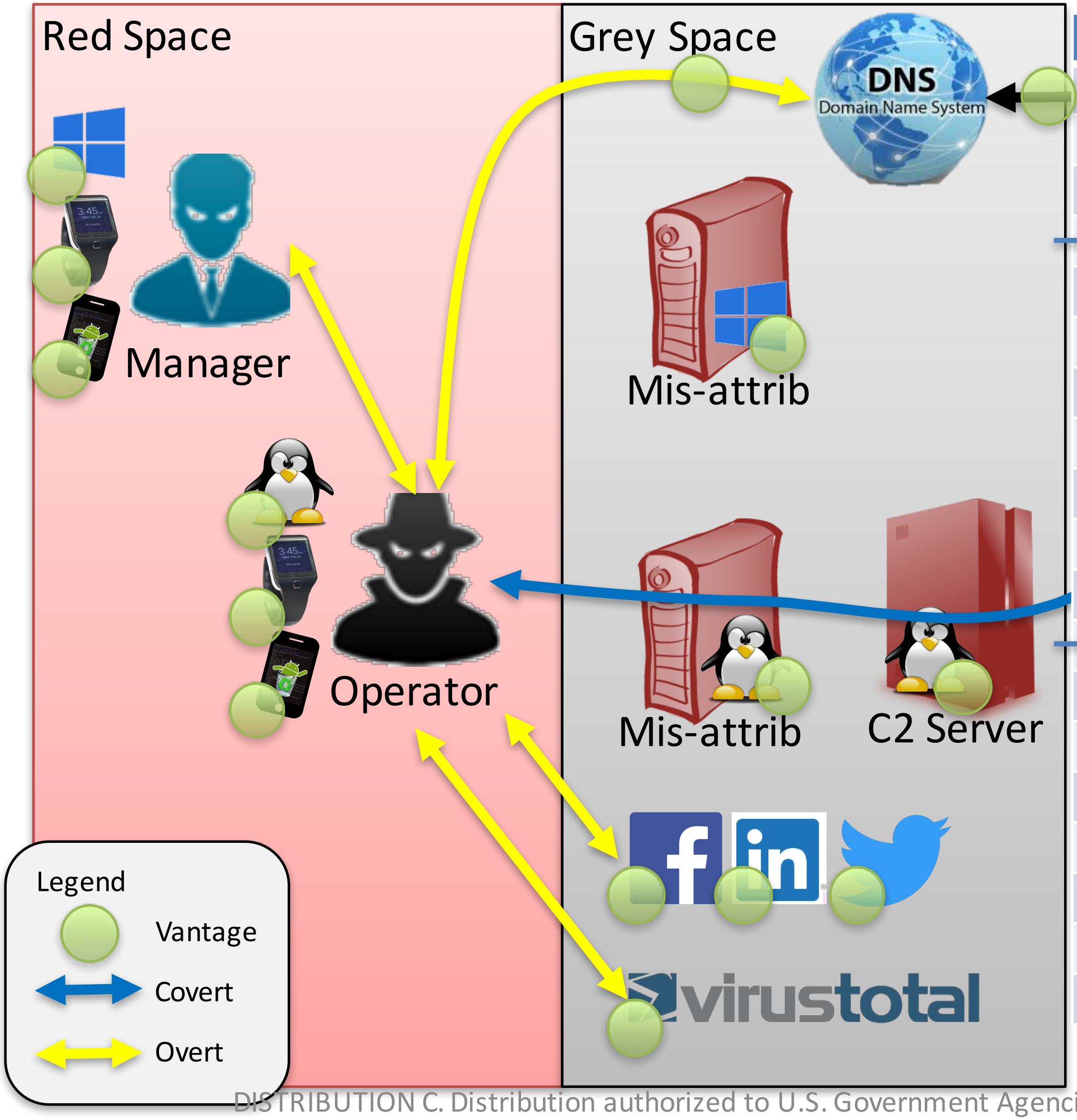
DISTRIBUTION C. Distribution authorized to U.S. Government Agencies and their contractors; Administrative or Operational Use; 21 Mar 17. Other requests for this document shall be referred to DARPA, I2O, 675 N Randolph St, Arlington, VA 22203.

Example Campaign



DISTRIBUTION C. Distribution authorized to U.S. Government Agencies and their contractors; Administrative or Operational Use; 21 Mar 17. Other requests for this document shall be referred to DARPA, I2O, 675 N Randolph St, Arlington, VA 22203.

Representative Data Collection



Workstation	Mobile	
Keystrokes	Key Presses	Passive Biometric
Mouse Events	Swipe Events	
	Accelerometer	
Names		Personally Identifiable Information
Email Addresses		
Microphone		
Camera		
Browser History		
Financial		
	Location	
System Information		Cyber Relevant
System calls		
Network Data		
Application Usage		
Tool Development		
Targeting Packages		
After Action Reports		

User Identification Techniques

- Identify when multiple users are accessing the same profile
- Identify how many users are present
- Identify an individual from a pool of known user profiles
- Use Network and Transportation Layer information for behavioral analytics

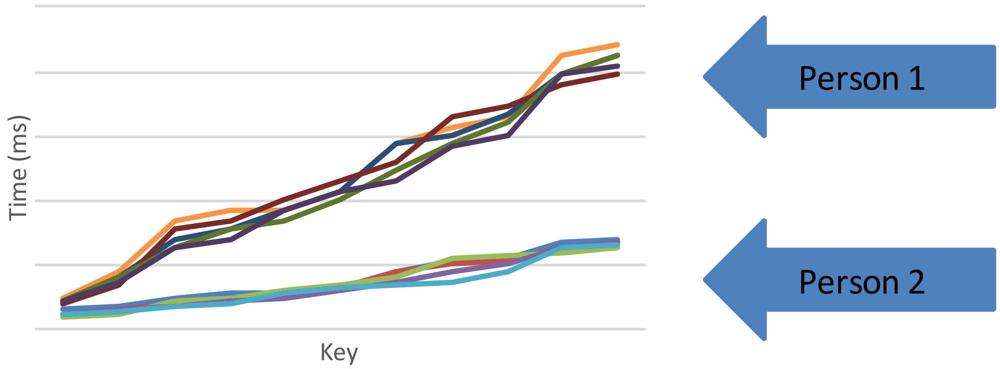
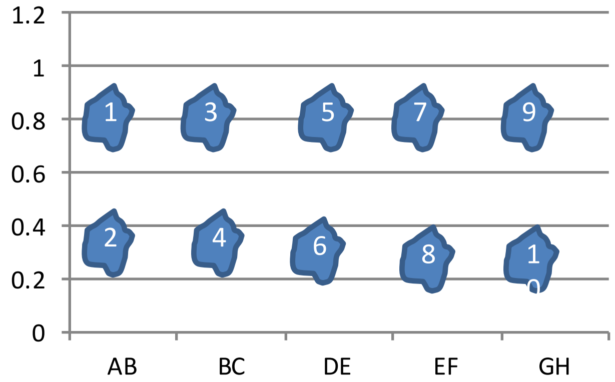


Illustration of two separate persons entering same sequence of keys giving two distinct 'clusters' indicating that there is more than one person accessing the account.

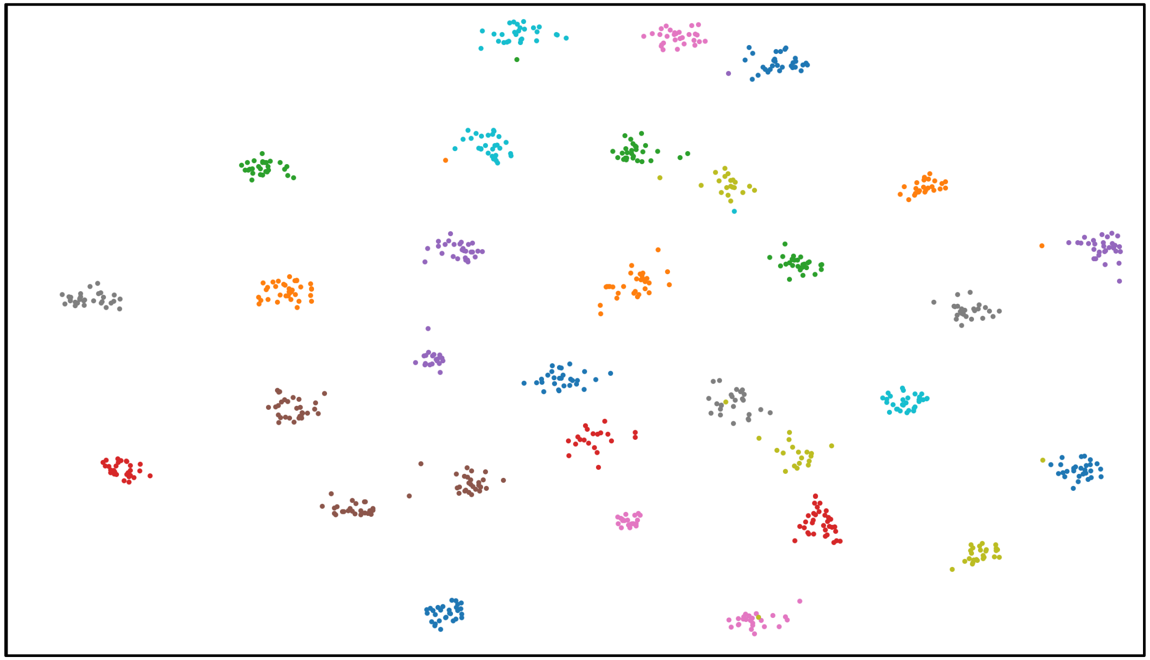


Identifying different users based on clustering techniques used above.

Identifying Users from Keystroke Dynamics: Embedding Results

- Our clustering identification accuracy for 31 users: **0.93**
  - Prior work identification accuracy on same dataset: 0.83
- Can effectively identify users it has not trained on

- Approach not bound to English language
- Profile output is only 512 bytes, useful for low-profile data gathering

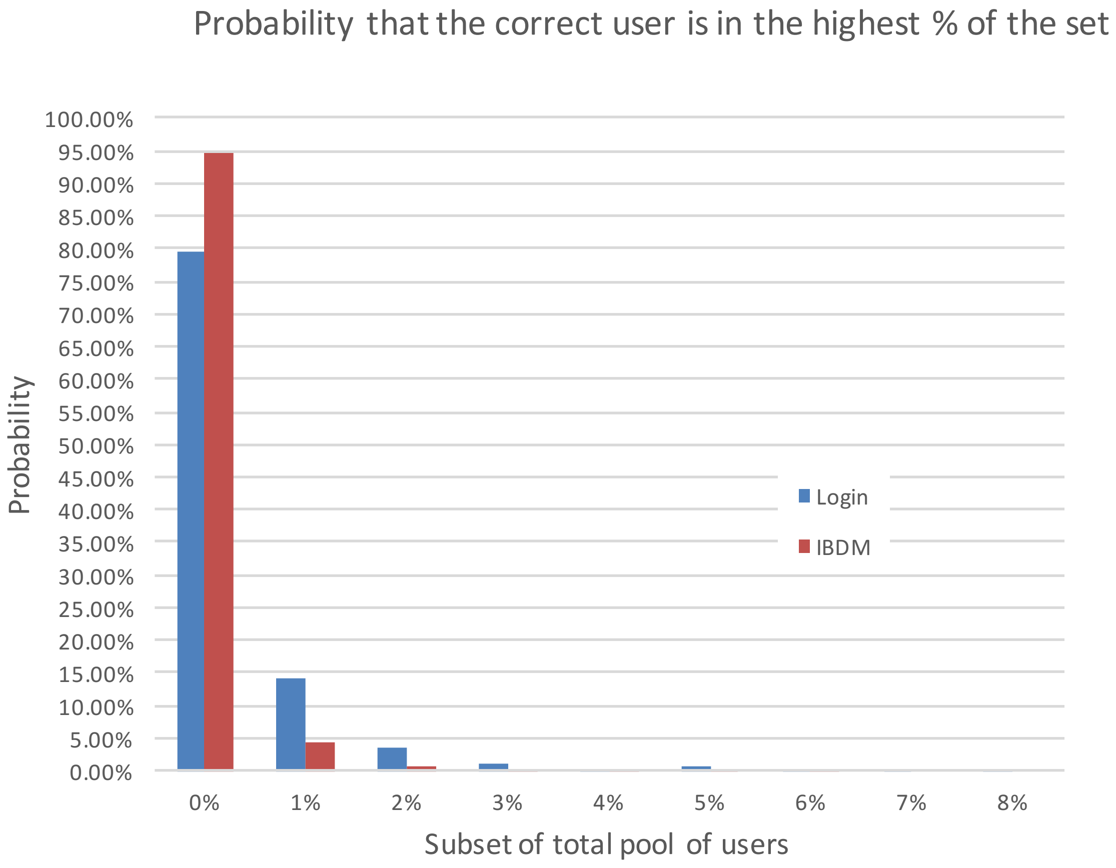


Two-dimensional visualization (using t-SNE) of user data points in the 128-dimensional embedded space. Color-coded by user.

DISTRIBUTION C. Distribution authorized to U.S. Government Agencies and their contractors; Administrative or Operational Use; 21 Mar 17. Other requests for this document shall be referred to DARPA, I2O, 675 N Randolph St, Arlington, VA 22203.

Keyboard-based Persona ID Matching

- Developed techniques for re-encountering users based on typing patterns
  - Keylogger, mobile phone, browser
- Demographic information extraction

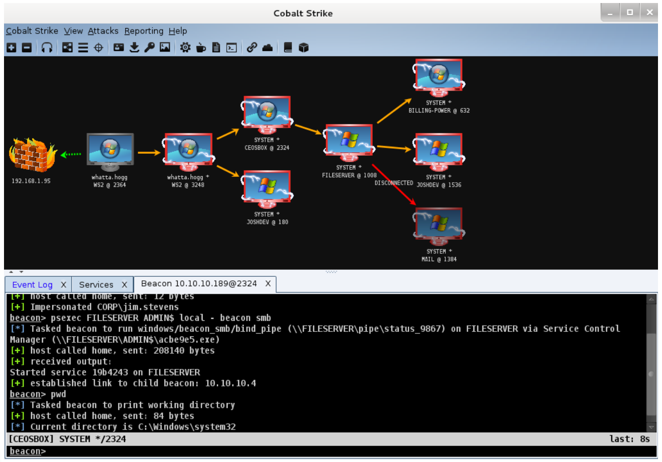


Further dissemination only as directed by DARPA Public Release Center or higher DoD authority

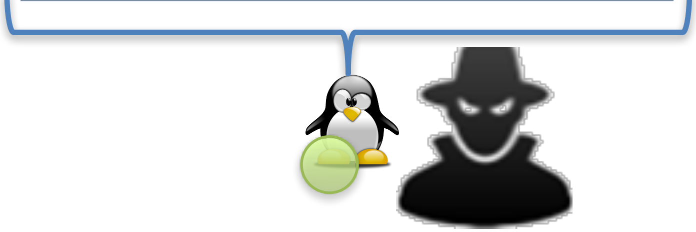
Ops Terminal Tracking

- Objective: Provide robust multi-perspective sensors and pertinent data for the purpose of identification, monitoring and attribution of malicious cyber operators

- Mobile and Desktop Sensors
  - Persona identification and monitoring
  - PII extraction
  - Cyber activity logging and reporting
- Passive Behavioral Biometrics
  - Signatures and identification
  - Demographic inference
- Mission Aware Intelligence
  - Information value / Utility
  - Prioritization
  - Active stealth



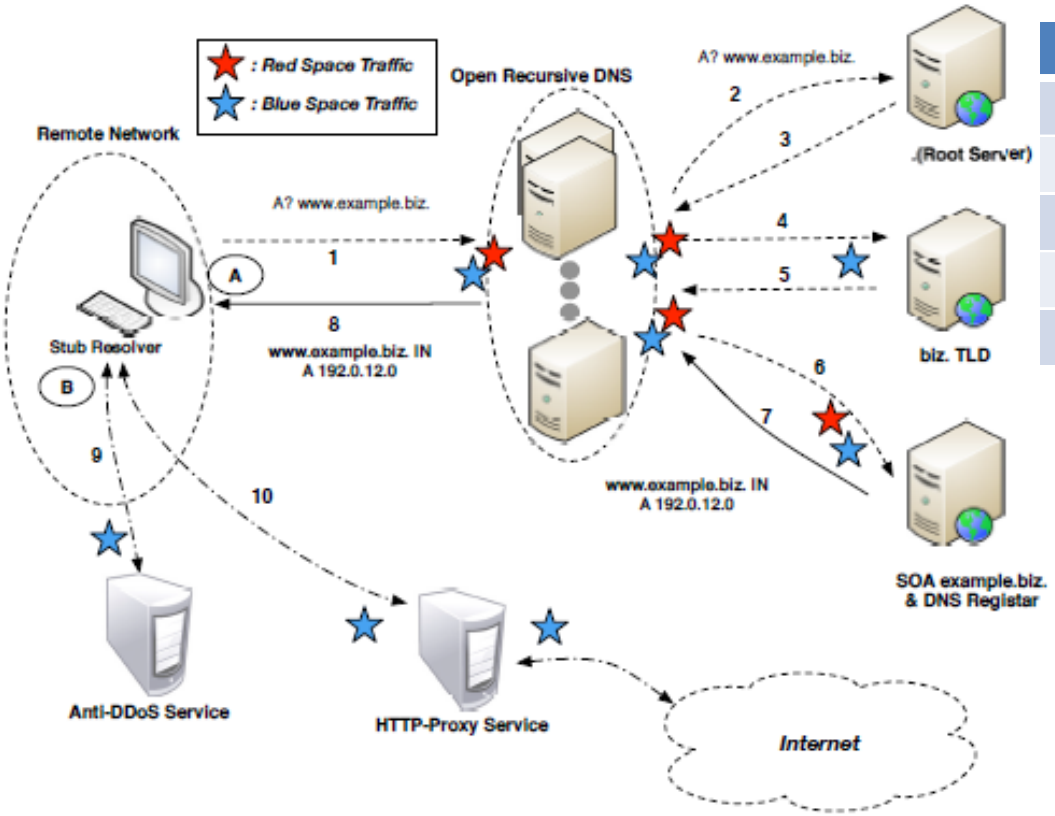
```
[+] host called home, sent: 12 bytes
[+] Impersonated CORP\jim.stevens
beacon> psexec FILESERVER ADMIN$ local - beacon smb
[*] Tasked beacon to run windows/beacon_smb/bind_pipe (\\FILESERVER\pipe\status_9867) on FILESERVER via Service Control
Manager (\\FILESERVER\ADMIN$\acbe9e5.exe)
[+] host called home, sent: 208140 bytes
[+] received output:
Started service 19b4243 on FILESERVER
[+] established link to child beacon: 10.10.10.4
beacon> pwd
[*] Tasked beacon to print working directory
[+] host called home, sent: 84 bytes
[*] Current directory is C:\Windows\system32
[CEOSBOX] SYSTEM */2324                                                                                        last: 8s
beacon>
```


Operator

Additional Vantage Points

- Development Terminals
- Operations Terminals
- Command and Control Servers
- Honeypots
- Mobile Devices and Wearables
- Network Infrastructure
- Network (Data in Transit)
- Banking and Finance (Follow the Money)
- Internet of Things (Pattern of Life)

Network Based Metadata Tracking

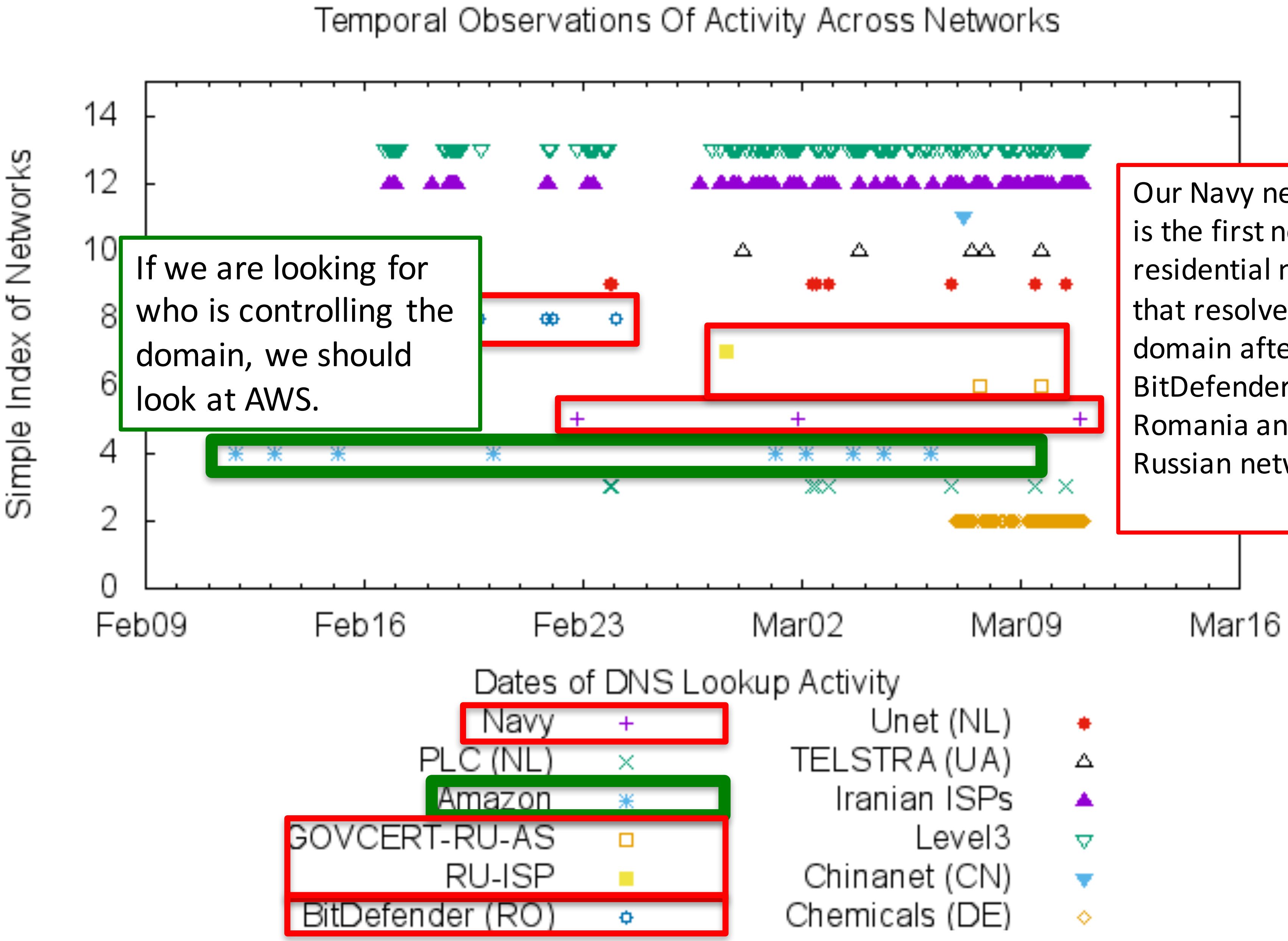


Key Features
Multiple OSINT databases at Internet scale
Link and Causality Analysis Engine
Novel Capabilities to Network and System Signals
Distinguish Between Multiple Users per Session
Novel Attack Attribution Signal Enrichment

Some of the Existing Datasets
Malware executions
VirusTotal
Passive DNS
Active DNS
Network Flow
Public Blacklists
Alexa
Expired Domains
Hacking Forums

- Attribution and trace back for network and host-based security events
- Large network datasets
- Tensor based statistical correlation techniques

Short lived threats (in DoD)

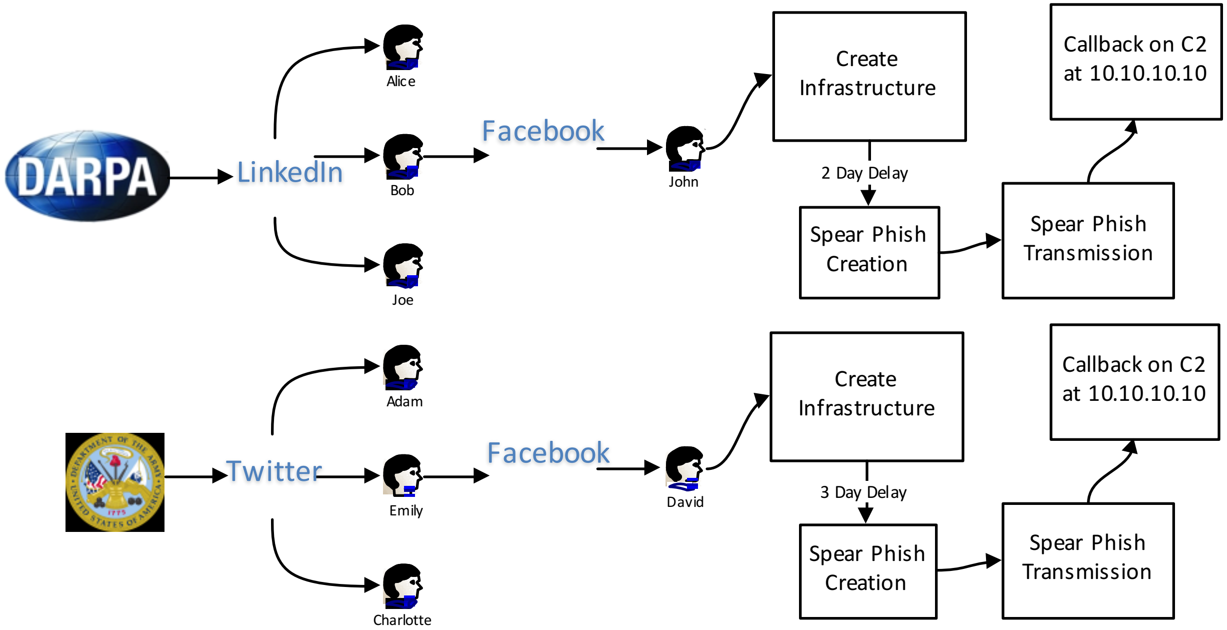


If we are looking for who is controlling the domain, we should look at AWS.

Our Navy network is the first non-residential network that resolved the domain after BitDefender in Romania and the Russian networks

TA2: Data Fusion and Activity Prediction

- TA1 focuses on **collecting** dots and TA2 focuses on **connecting** dots
- Use actor intentions and prior tool usage to identify future behaviors



- Predictive Modeling Examples
  - Identifying similar spear phishing mail and predicting layout of future spear phishing mail
  - DNS lookup of mylisteningpost.com is always followed by data exfiltration
  - SSH connection by user adam124 to Internet facing web server often leads to SSH connection from web server to internal database server
- **End goal is to predict actor behavior (i.e., connect the dots)**

TA3: Enrichment and Validation

- Focus on enrichment to identify supplemental/alternative evidence of activity

- Direct collection: TA1 collects actor identifying information
- Supplemental: Actor used same password during intrusion as his/her LinkedIn password that was stolen and dumped

- Direct collection: TA1 collects incriminating NetFlow from a sensitive location
- Supplemental: Actor left metadata in discovered tool

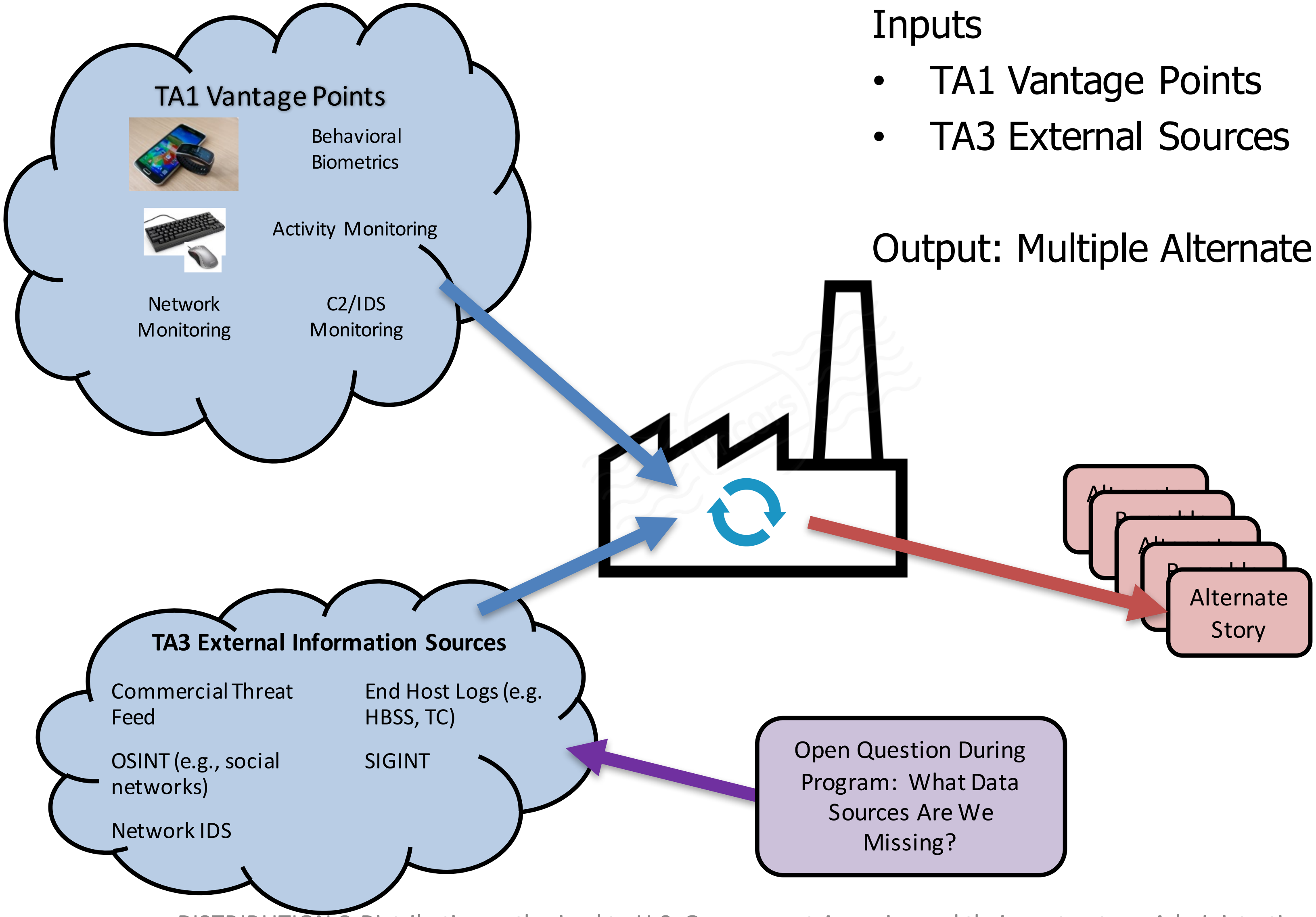
- **End goal is to create "alternative stories" factory for how we know**

Alternate Story Factory

Inputs

- TA1 Vantage Points
- TA3 External Sources

Output: Multiple Alternate Stories


TA1 Vantage Points
Behavioral Biometrics
Activity Monitoring
Network Monitoring
C2/IDS Monitoring
TA3 External Information Sources
Commercial Threat Feed
End Host Logs (e.g. HBSS, TC)
OSINT (e.g., social networks)
SIGINT
Network IDS
Alternate Story
Open Question During Program: What Data Sources Are We Missing?

Lessons Learned

Actionable attribution:

- Is feasible
  - Easier if preparatory work is done ahead of time (continuously!)
  - Easier when asymmetric advantage from cyber adversaries neutralized by national technical means
- Builds confidence for (cyber) response actions
- Requires fusing information from all/diverse sources and methods
- Requires near real time data minimization in large volume data streams
- Requires scaling
- Open research question: additional techniques for bridging streams?

DARPA

www.darpa.mil

DISTRIBUTION C. Distribution authorized to U.S. Government Agencies and their contractors; Administrative or Operational Use; 21 Mar 17. Other requests for this document shall be referred to DARPA, I2O, 675 N Randolph St, Arlington, VA 22203.