Why Bits Take Bytes Out of Your Mission

ERICH DEVENDORF, PhD

AFRL/RIG Cyber CTC Lead

The views expressed in this academic research paper are those of the author and do not reflect the official policy or position of the US government or the Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted but is the property of the United States government.

AFRL

#whoami



- ACE since 2011, Director 2018 – 2022 . . . Best job?
- Exercises, Wargames, Operational Art. . . Legacy of RTS's?
- Run, Ski, Martial Arts. . . and all nerd hobbies!

AFRL

Cyber Operations == Warfighting

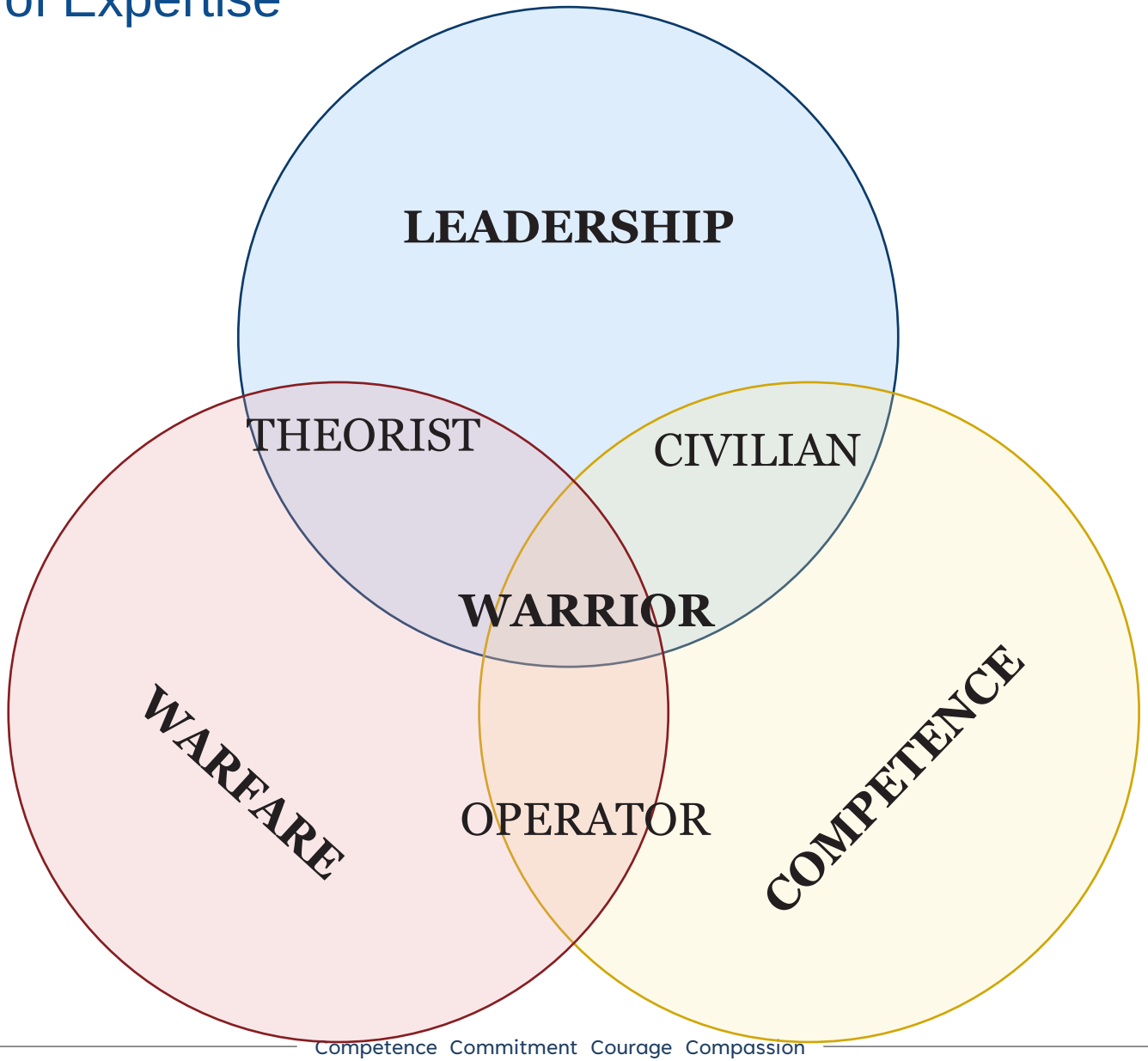
Fundamental Skills

Combat Capability

- Individual skills form the building blocks and preconditions for training

- Combat capability comes from the composition of individual skills in a high-functioning team

Spheres of Expertise



What is cybersecurity?

Assuring or degrading the confidentiality, integrity, and/or availability of information required for a mission.

WARFARE

Cyberspace as a Domain

Cyberspace is a global domain inside the information environment consisting of…

Internet

Telecommunications Networks

Computer Systems

Internet of "Things"

Embedded Processors/Controllers

"Air gapped" Systems

Cyberspace Operations

Traditional Defense

Offense

- **Defense**
  - Actions taken within protected cyberspace to defeat specific threats that have breached or are threatening to breach cyberspace security measures…to restore the system to a secure configuration (JP 3-12)
- **Offense**
  - Actions taken in cyberspace that create noticeable denial effects in cyberspace or manipulation that leads to denial that appears in a physical domain, and is considered a form of fires (JP 3-12)

Cyberspace Operations

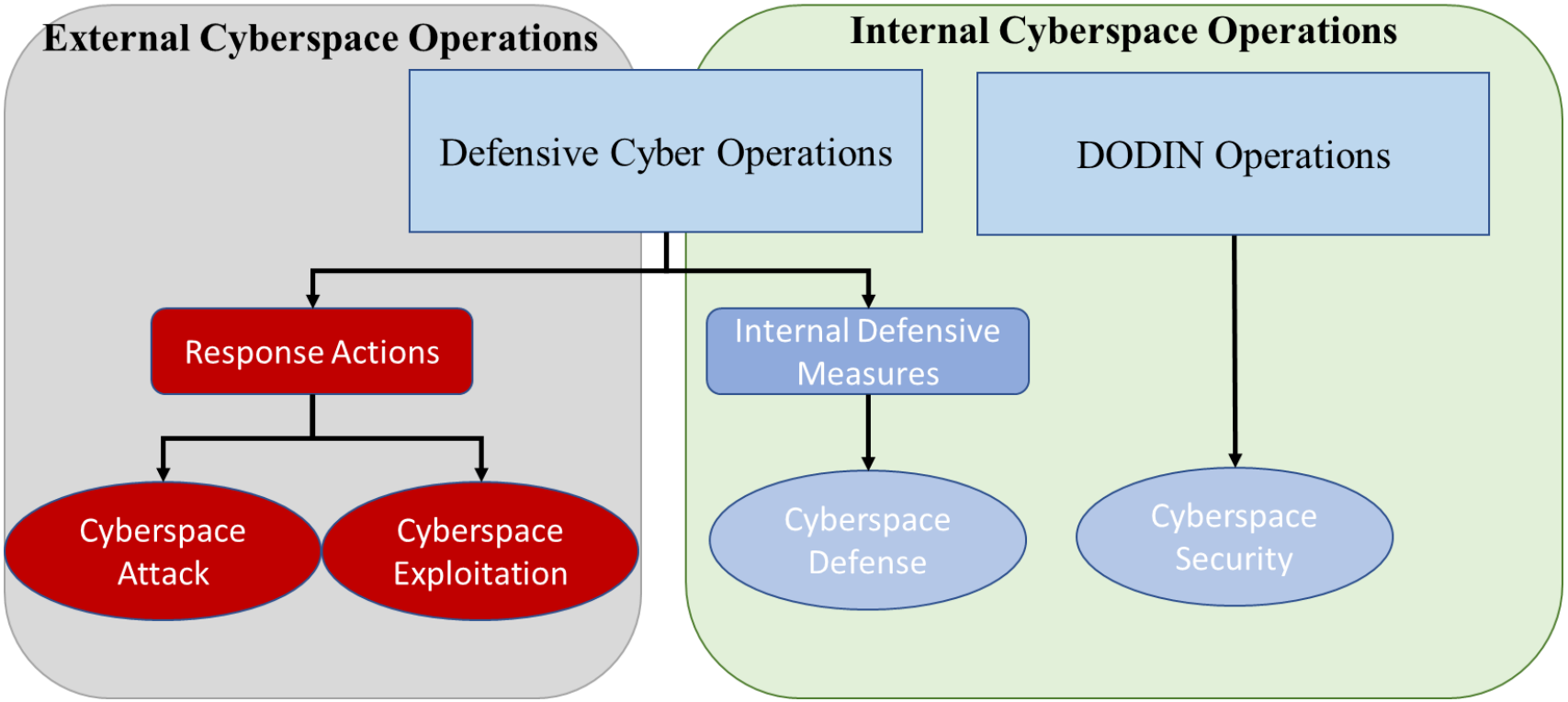
Traditional Defense

Offense

- **Defense**
  - Actions taken within protected cyberspace to defeat specific threats that have breached or are threatening to breach cyberspace security measures…to restore the system to a secure configuration (JP 3-12)
- **Offense**
  - Actions taken in cyberspace that create noticeable denial effects in cyberspace or manipulation that leads to denial that appears in a physical domain, and is considered a form of fires (JP 3-12)

AFRL

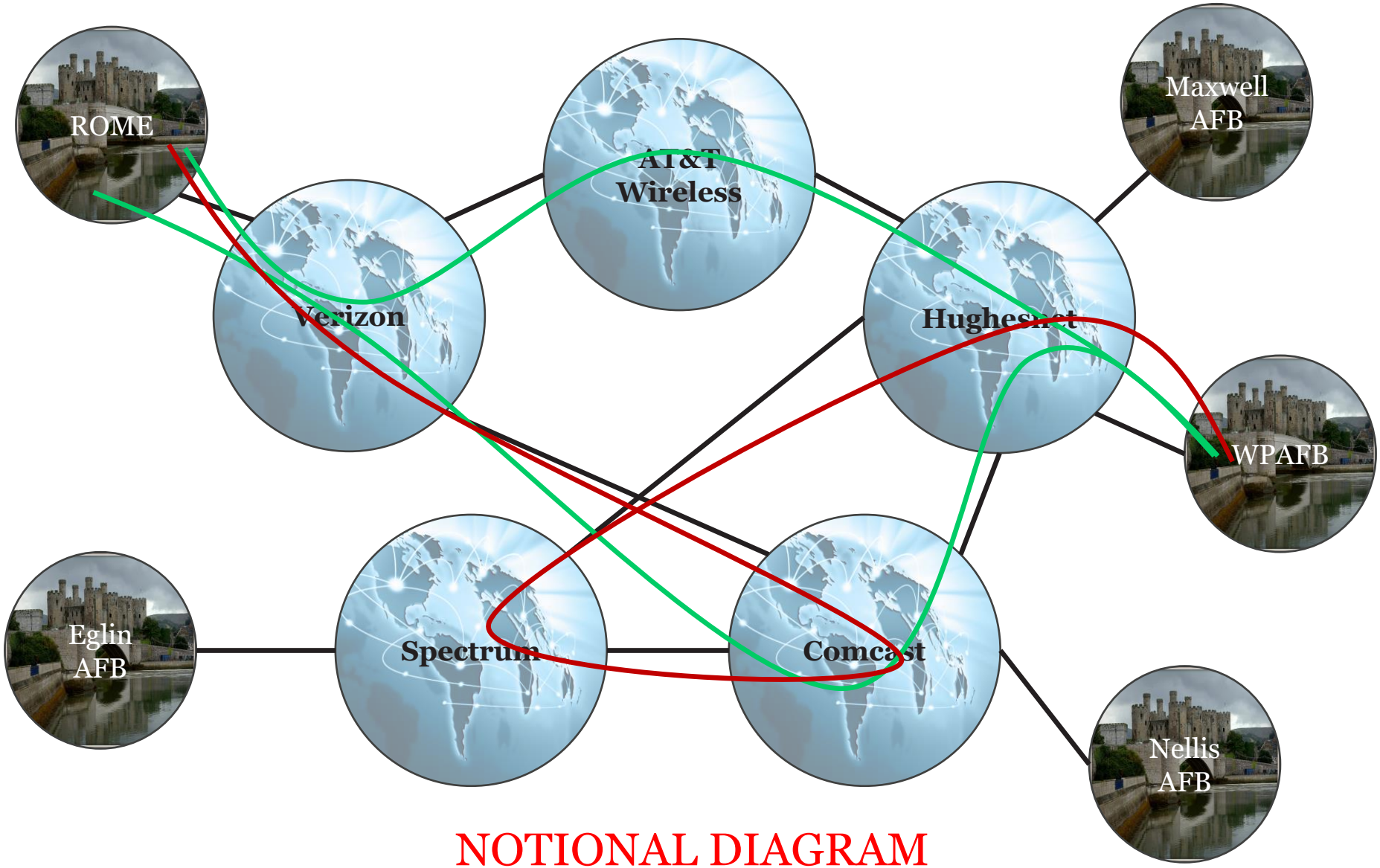
DOD Defensive Cyber Construct



COMPETENCE

AFRL

- Protected and Unprotected Cyberspace



NOTIONAL DIAGRAM

Unprotected Cyberspace

How 3ve's BGP hijackers eluded the Internet—and made $29M

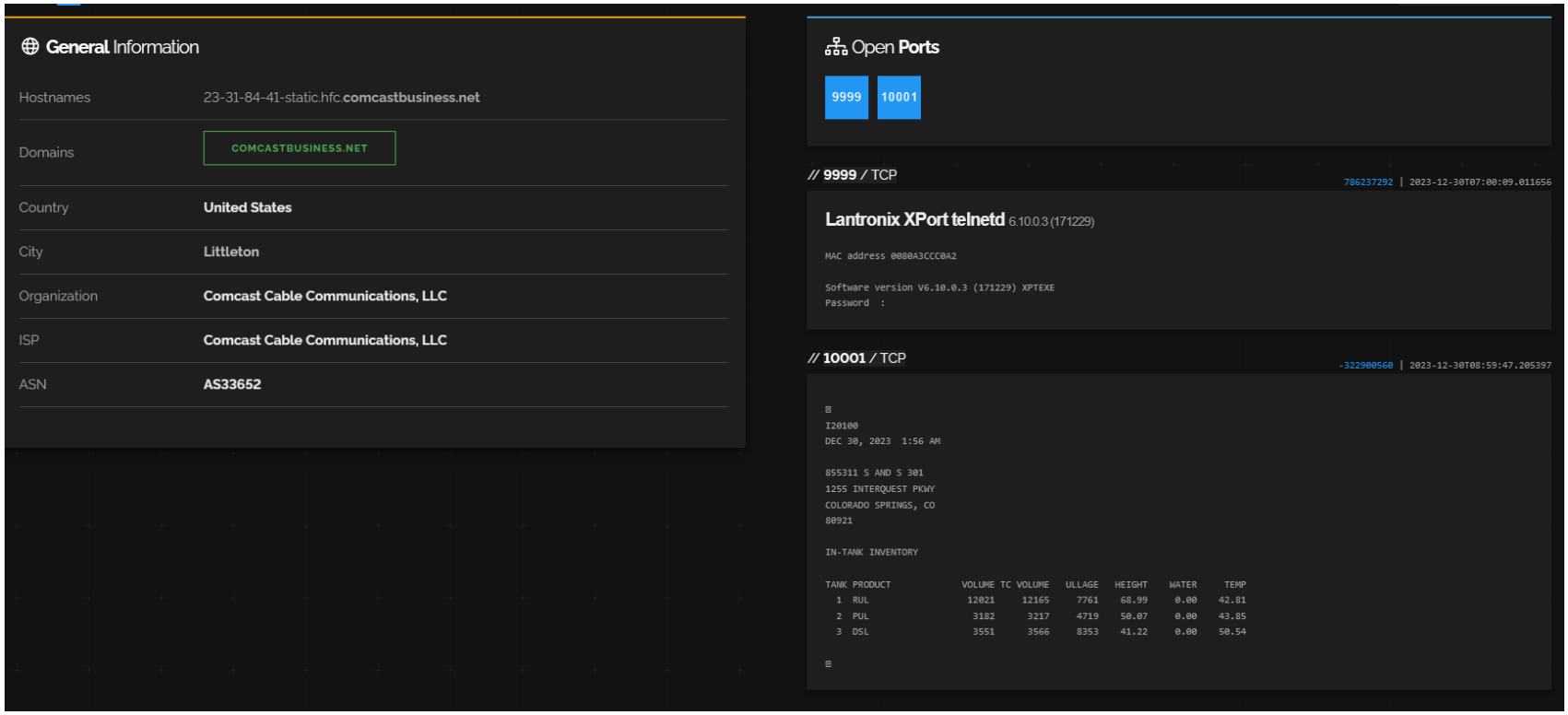
3ve used addresses of unsuspecting owners—like the US Air Force.

DAN GOODIN - 12/21/2018, 12:30 PM

Please ask yourself this question: Why is your customer, a Ukrainian company, routing packets for the United States Air Force?

AFRL

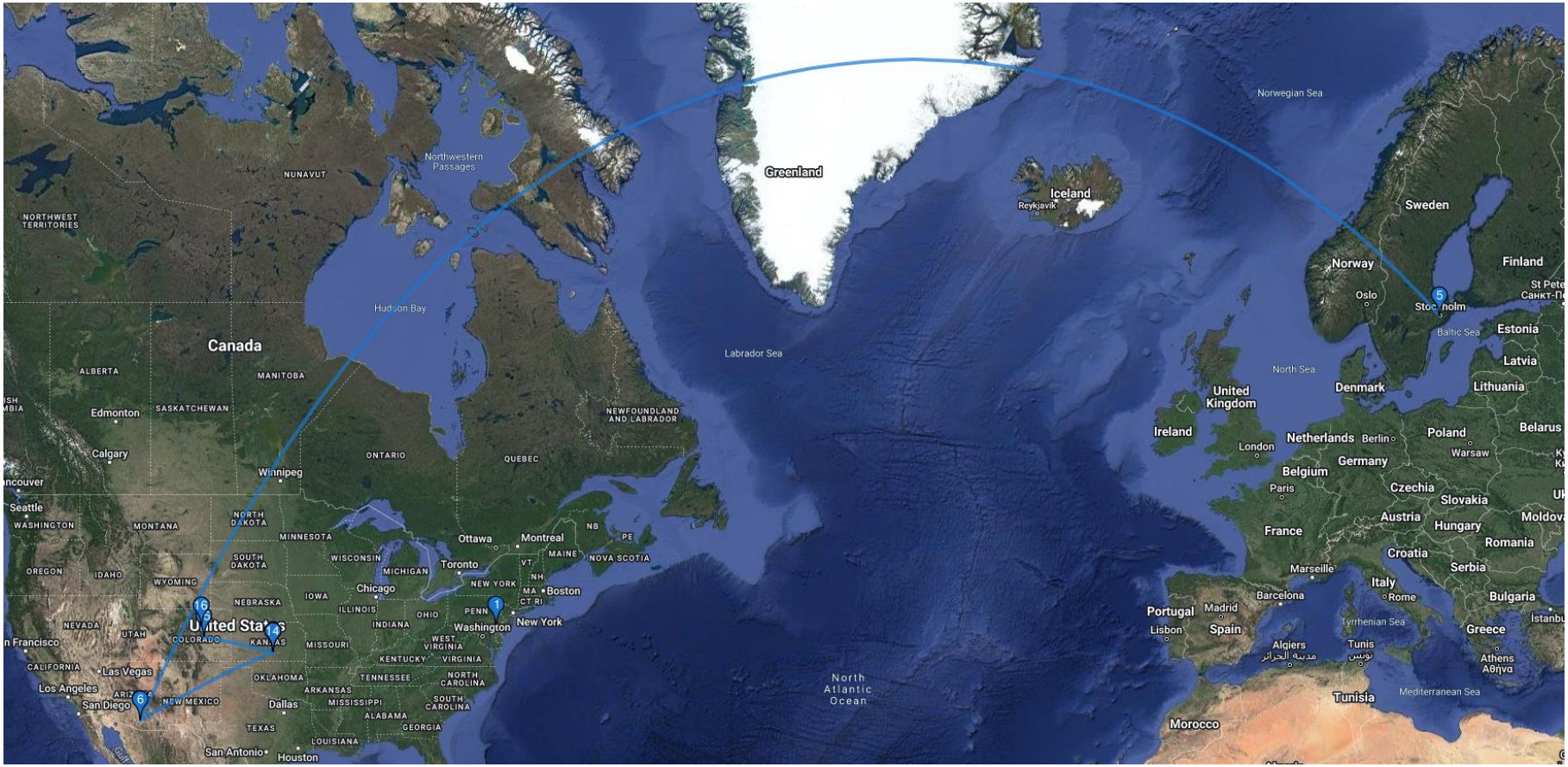
A Short ICS Demonstration



- Search for a sample system on www.shodan.io to find a system with a cyber and physical footprint
- Identified an ICS, monitoring system for fuel storage tanks

AFRL

Visual Trace Route



AFRL

Determine Path to ICS

```
import:          from AS12389 accept AS-ROSTELECOM
mp-import:       afi ipv6 from AS12389 accept AS-ROSTELECOM
```

3	172.23.255.97	172.23.255.97	0.176ms
4	172.23.255.6	172.23.255.6	0.243ms
5	palo-b24-link.ip.twelve99.net	62.115.191.108	1.341ms
6	be-200-pe11.529bryant.ca.ibone.comcast.net	50.208.233.209	1.698ms
7	be-3311-cs03.sunnyvale.ca.ibone.comcast.net	96.110.33.89	2.136ms
8	be-1311-cr11.sunnyvale.ca.ibone.comcast.net	96.110.46.26	2.088ms
9	be-301-cr12.champa.co.ibone.comcast.net	96.110.39.17	26.001ms
10	be-1112-cs01.champa.co.ibone.comcast.net	96.110.37.209	25.872ms
11	be-36011-arsc1.aurora.co.denver.comcast.net	96.110.43.210	172.844ms
12	po-1-xar02.cosprings.co.denver.comcast.net	162.151.8.82	27.977ms
13	po-1-rur302.cosprings.co.denver.comcast.net	24.124.155.194	27.791ms
14	lag-2-1-acr14.cosprings.co.denver.comcast.net	96.110.246.162	28.540ms
15	c-71-205-60-189.hsd1.co.comcast.net	71.205.60.189	37.337ms
16	23-31-84-41-static.hfc.comcastbusiness.net	23.31.84.41	36.538ms

Sweden?

- A trace route shows the path to a target
- Each hop represents a discrete system that handles a packet
- Hop 8 owned by Polhem Infra, based in Sweden

AFRL

Unprotected Cyberspace

Russian telco hijacks internet traffic for Google, AWS, Cloudflare, and others

Rostelecom involved in BGP hijacking incident this week impacting more than 200 CDNs and cloud providers.

By Catalin Cimpanu for Zero Day | April 5, 2020 -- 21:53 GMT (14:53 PDT) | Topic: Security

Earlier this week, traffic meant for more than 200 of the world's largest content delivery networks (CDNs) and cloud hosting providers was suspiciously redirected through Rostelecom,

MORE FROM CATALIN CIMPANU

Security
Chrome will soon try HTTPS first when you type an incomplete URL

Security
Go malware is now common, having been adopted by both APTs

TECHREPUBLI

AFRL

"Protected" Cyberspace

…based on the hypothesis that security violations can be detected by monitoring a system's audit records for abnormal patterns…

An Intrusion-Detection Model

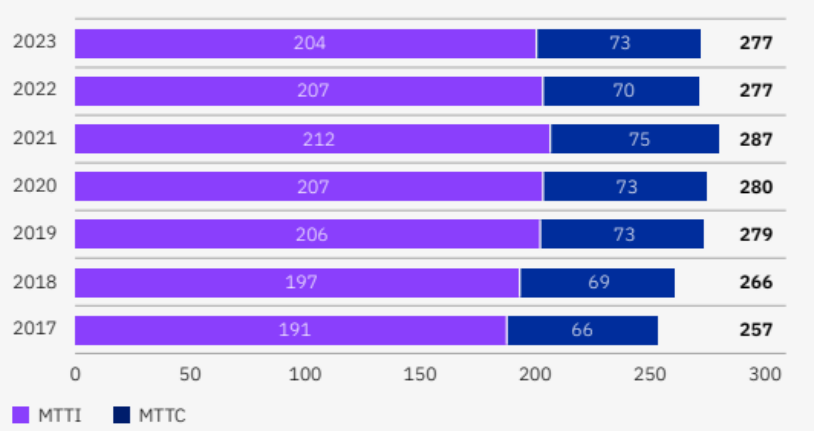
DOROTHY E. DENNING

IEEE TRANSACTIONS ON SOFTWARE ENGINEERING, VOL. SE-13, NO. 2, FEBRUARY 1987, 222-232.

Abstract-A model of a real-time intrusion-detection expert system capable of detecting break-ins, penetrations, and other forms of computer abuse is described. The model is based on the hypothesis that security violations can be detected by monitoring a system's audit records for abnormal patterns of system usage. The model includes profiles for representing the behavior of subjects with respect to objects in terms of metrics and statistical models, and rules for acquiring knowledge about this behavior from audit records and for detecting anomalous behavior. The model is independent of any particular system, application environment, system vulnerability, or type of intrusion, thereby providing a framework for a general-purpose intrusion-detection expert system.

Index Terms-Abnormal behavior, auditing, intrusions, monitoring, profiles, security, statistical measures.

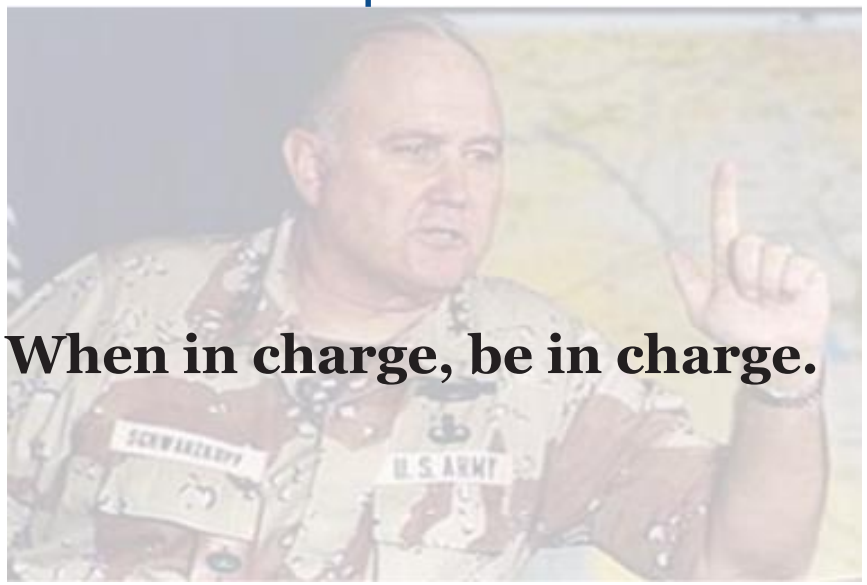
…profiles for representing the behavior of subjects…

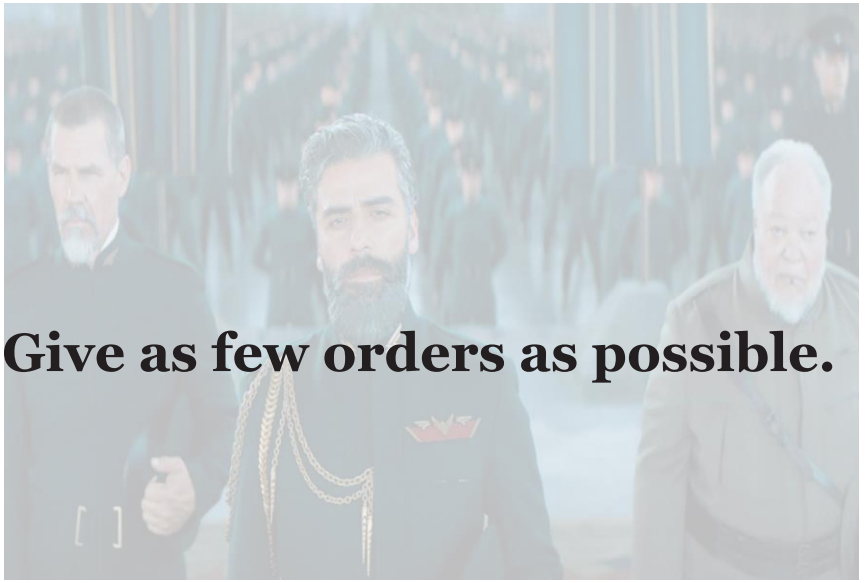


LEADERSHIP

AFRL

On Leadership: What Resonates With Me





AFRL

On Leadership: Accelerate Change or Lose

Show me a completely smooth operation and
I'll show you someone who's covering mistakes.

Real boats rock.

Frank Herbert

Questions?