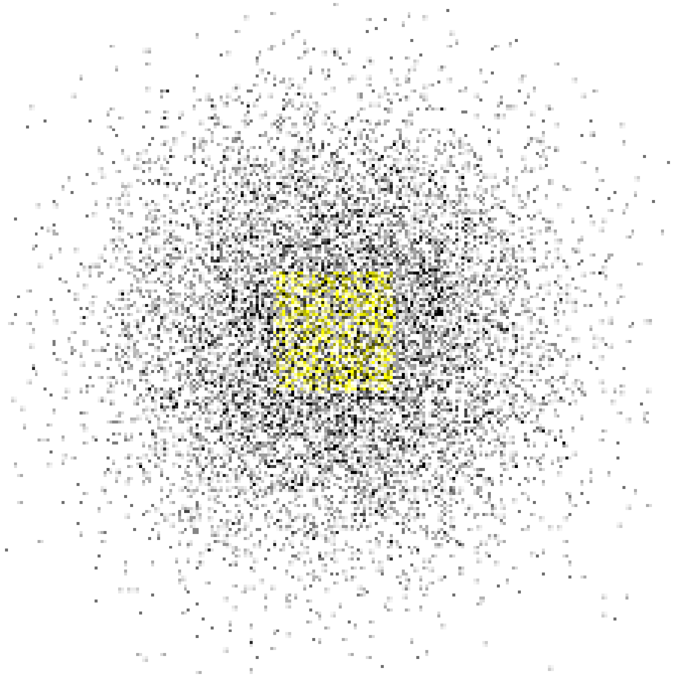


A Random Walk Through Cyber Security

Dr. Edward G. Amoroso

Distinguished Research Professor, NYU CCS

eamoroso@tag-cyber.com

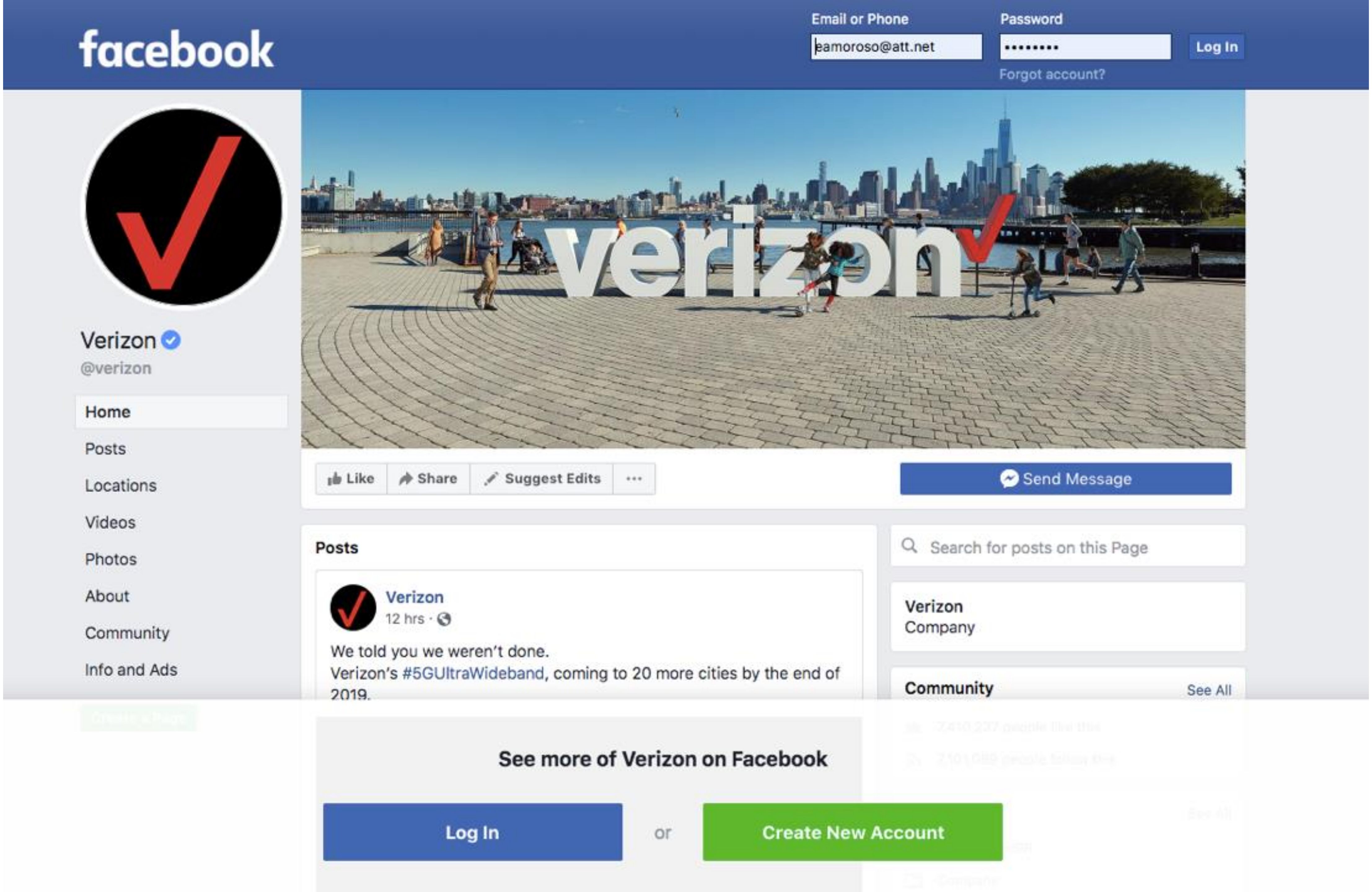
verizon

verizon

Best in America.
Best in New York.
verizon
OUTFRONT

verizon✓

VO



Email or Phone: eamoroso@att.net

Password: ••••••••••

Verizon
@verizon

Verizon
12 hrs ·

We told you we weren't done.
Verizon's #5GUltraWideband, coming to 20 more cities by the end of 2019.

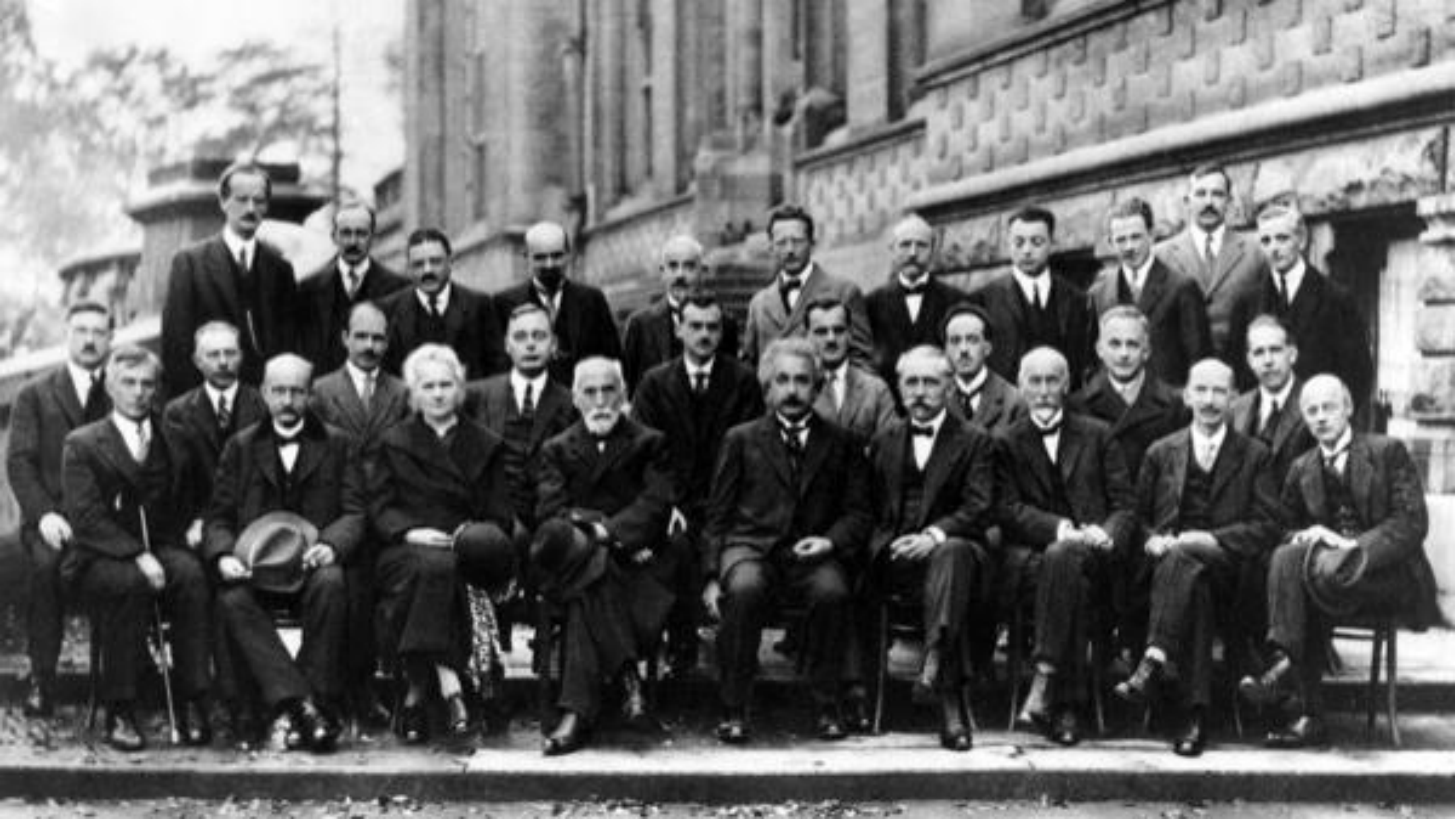
Verizon
Company

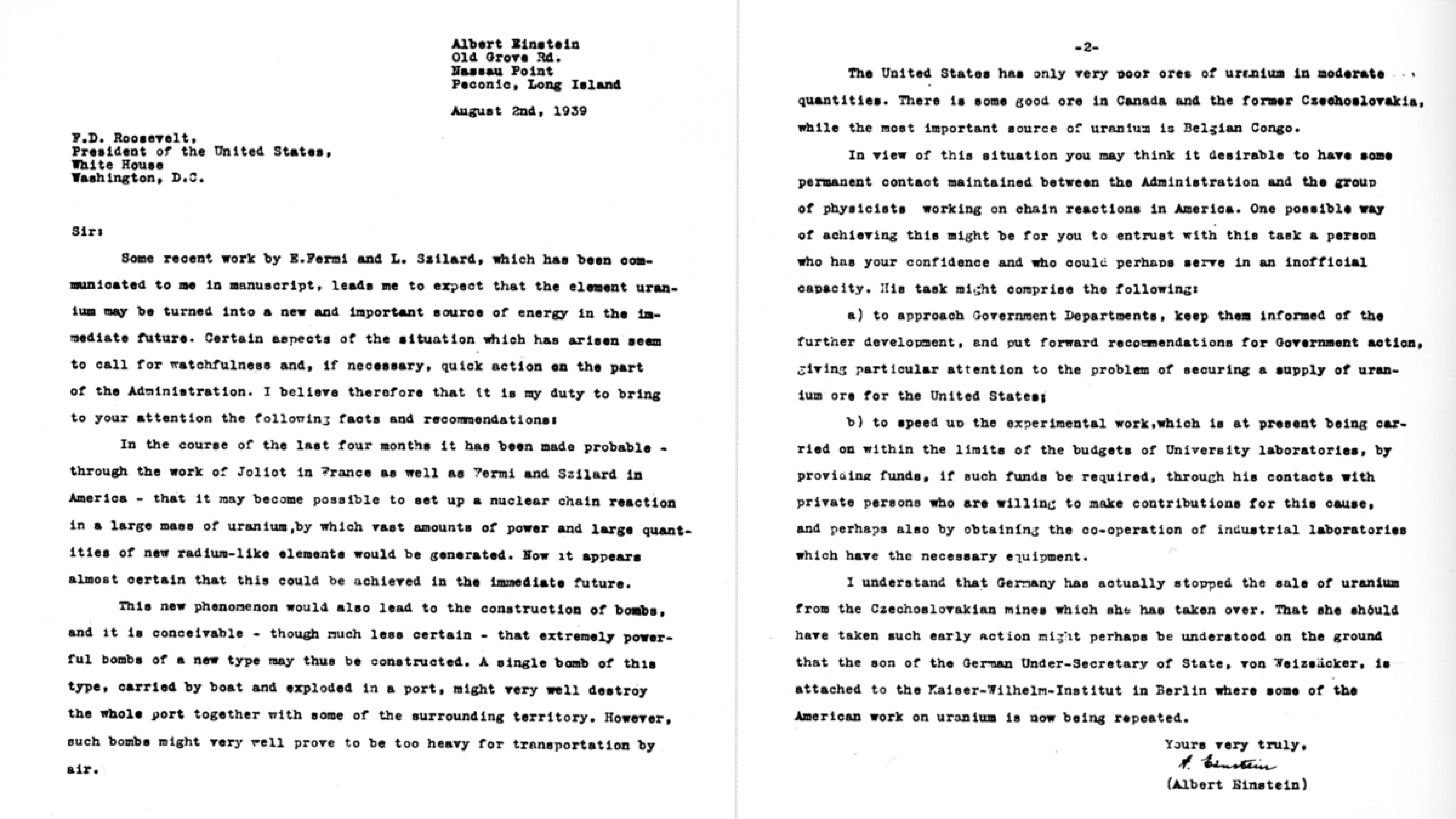
2,410,237 people like this

2,101,089 people follow this

Company

See more of Verizon on Facebook





Albert Einstein
Old Grove Rd.
Nassau Point
Peconic, Long Island

August 2nd, 1939

F.D. Roosevelt,
President of the United States,
White House
Washington, D.C.

Sir:

Some recent work by E.Fermi and L. Szilard, which has been communicated to me in manuscript, leads me to expect that the element uranium may be turned into a new and important source of energy in the immediate future. Certain aspects of the situation which has arisen seem to call for watchfulness and, if necessary, quick action on the part of the Administration. I believe therefore that it is my duty to bring to your attention the following facts and recommendations:

In the course of the last four months it has been made probable - through the work of Joliot in France as well as Fermi and Szilard in America - that it may become possible to set up a nuclear chain reaction in a large mass of uranium,by which vast amounts of power and large quantities of new radium-like elements would be generated. Now it appears almost certain that this could be achieved in the immediate future.

This new phenomenon would also lead to the construction of bombs, and it is conceivable - though much less certain - that extremely powerful bombs of a new type may thus be constructed. A single bomb of this type, carried by boat and exploded in a port, might very well destroy the whole port together with some of the surrounding territory. However, such bombs might very well prove to be too heavy for transportation by air.

The United States has only very poor ores of uranium in moderate quantities. There is some good ore in Canada and the former Czechoslovakia, while the most important source of uranium is Belgian Congo.

In view of this situation you may think it desirable to have some permanent contact maintained between the Administration and the group of physicists working on chain reactions in America. One possible way of achieving this might be for you to entrust with this task a person who has your confidence and who could perhaps serve in an inofficial capacity. His task might comprise the following:

a) to approach Government Departments, keep them informed of the further development, and put forward recommendations for Government action, giving particular attention to the problem of securing a supply of uranium ore for the United States;

b) to speed up the experimental work,which is at present being carried on within the limits of the budgets of University laboratories, by providing funds, if such funds be required, through his contacts with private persons who are willing to make contributions for this cause, and perhaps also by obtaining the co-operation of industrial laboratories which have the necessary equipment.

I understand that Germany has actually stopped the sale of uranium from the Czechoslovakian mines which she has taken over. That she should have taken such early action might perhaps be understood on the ground that the son of the German Under-Secretary of State, von Weizsäcker, is attached to the Kaiser-Wilhelm-Institut in Berlin where some of the American work on uranium is now being repeated.

Yours very truly,
A. Einstein
(Albert Einstein)

D.J. Trump
President of the United States
White House
Washington, DC

Sir:

1. Direct that the NIST Framework shall be the only acceptable cyber security compliance standard in the United States.

2. Direct that each government agency shall immediately implement a plan to reduce their dependence on an enterprise perimeter.

3. Direct that each government agency shall significantly expand their Cyber Corps Program for young people interested in a cyber security career.

Yours very truly,
Dr. Edward Amoroso

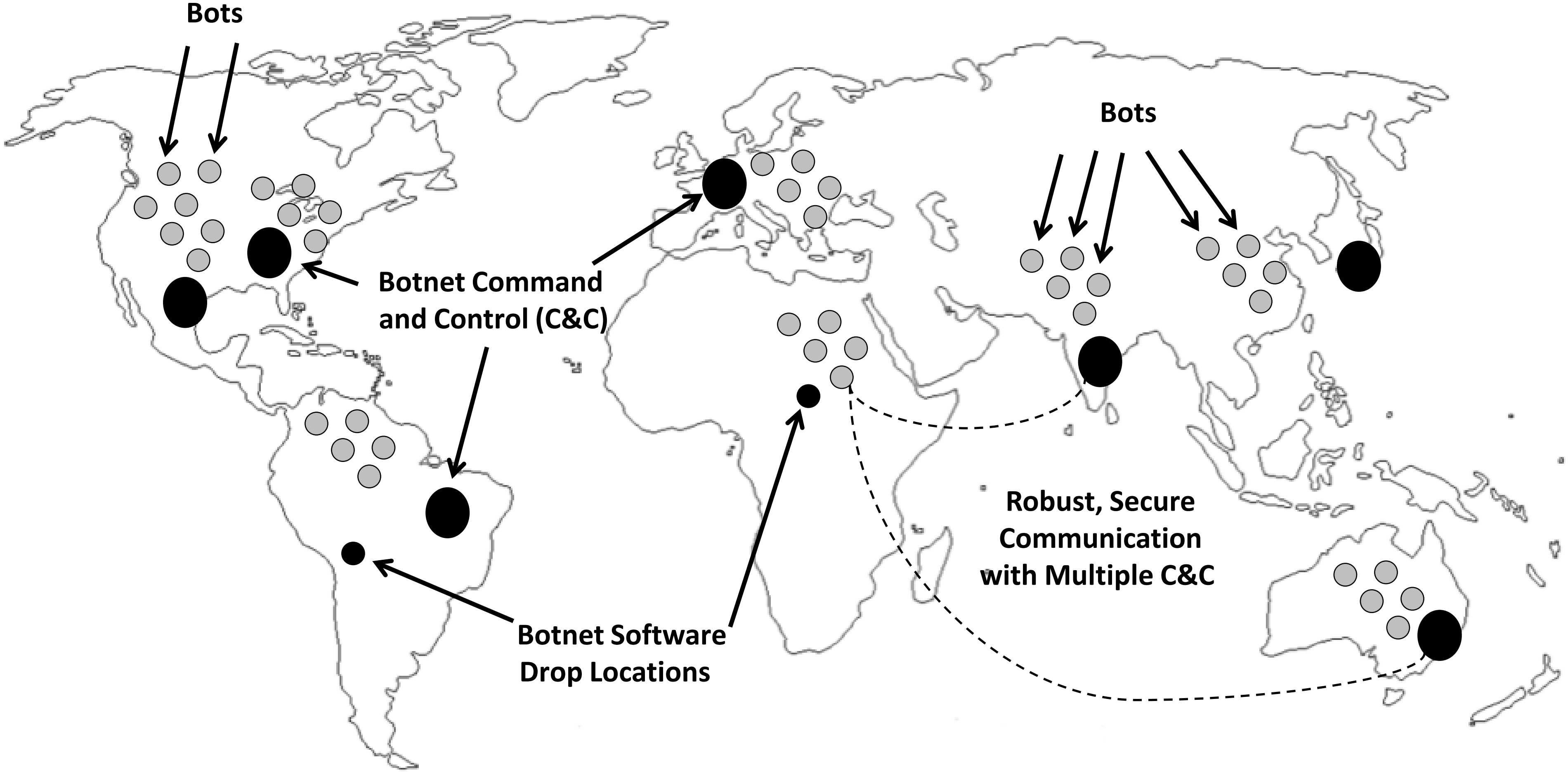
Dr. Edward G. Amoroso offers three recommendations on cyber security to the President-Elect

An Open Letter to the President-Elect on Cyber Security

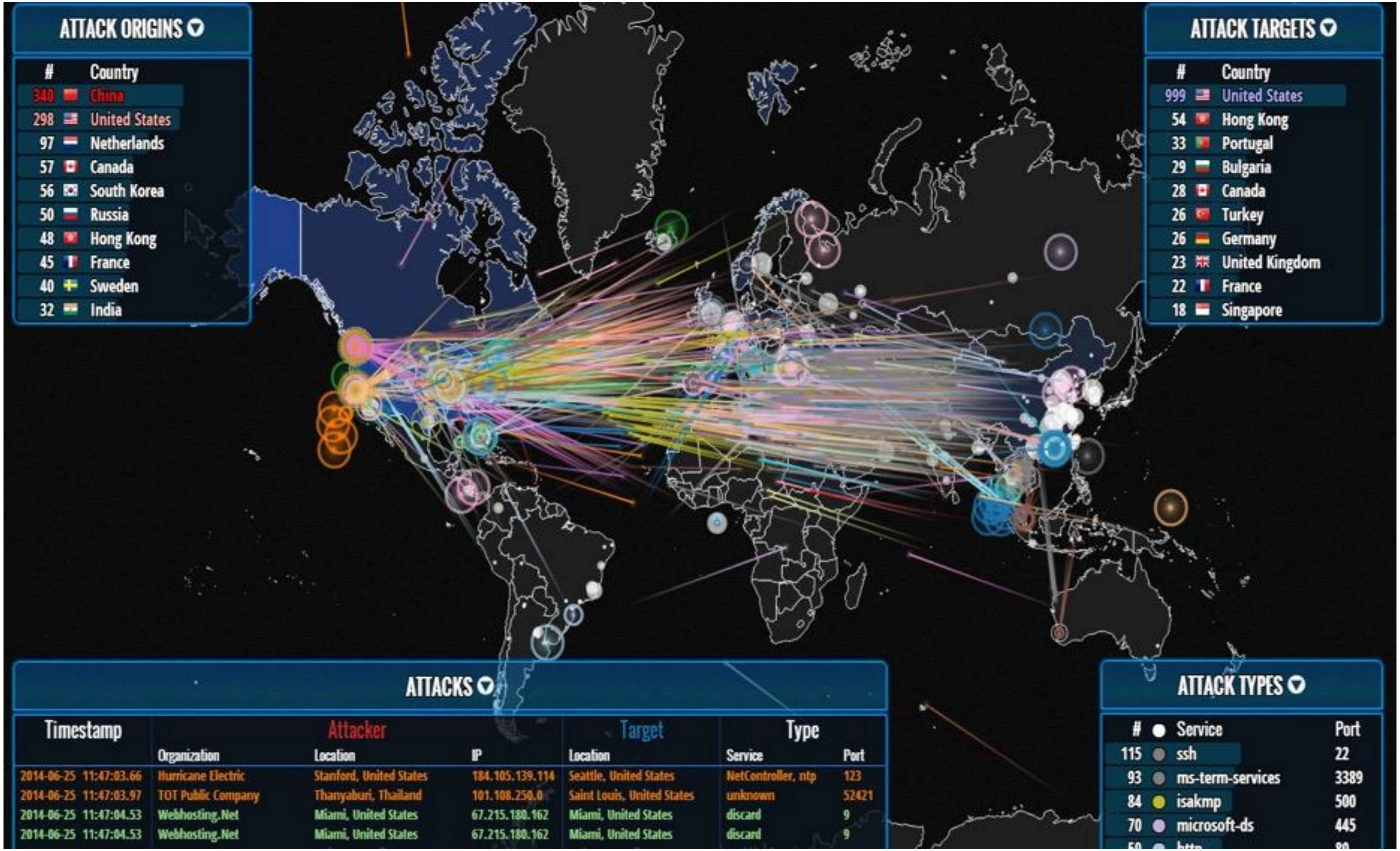
Published on November 25, 2016

Can Botnets Take Out the Internet?

Botnet Architecture


Bots
Bots
Botnet Command and Control (C&C)
Robust, Secure Communication with Multiple C&C
Botnet Software Drop Locations

Typical Botnet Visualization



ATTACK ORIGINS

#	Country
340	China
298	United States
97	Netherlands
57	Canada
56	South Korea
50	Russia
48	Hong Kong
45	France
40	Sweden
32	India

ATTACK TARGETS

#	Country
999	United States
54	Hong Kong
33	Portugal
29	Bulgaria
28	Canada
26	Turkey
26	Germany
23	United Kingdom
22	France
18	Singapore

ATTACKS

Timestamp	Attacker			Target	Type	
	Organization	Location	IP	Location	Service	Port
2014-06-25 11:47:03.66	Hurricane Electric	Stanford, United States	184.105.139.114	Seattle, United States	NetController, ntp	123
2014-06-25 11:47:03.97	TOT Public Company	Thanyaburi, Thailand	101.108.250.0	Saint Louis, United States	unknown	52421
2014-06-25 11:47:04.53	Webhosting.Net	Miami, United States	67.215.180.162	Miami, United States	discard	9
2014-06-25 11:47:04.53	Webhosting.Net	Miami, United States	67.215.180.162	Miami, United States	discard	9

ATTACK TYPES

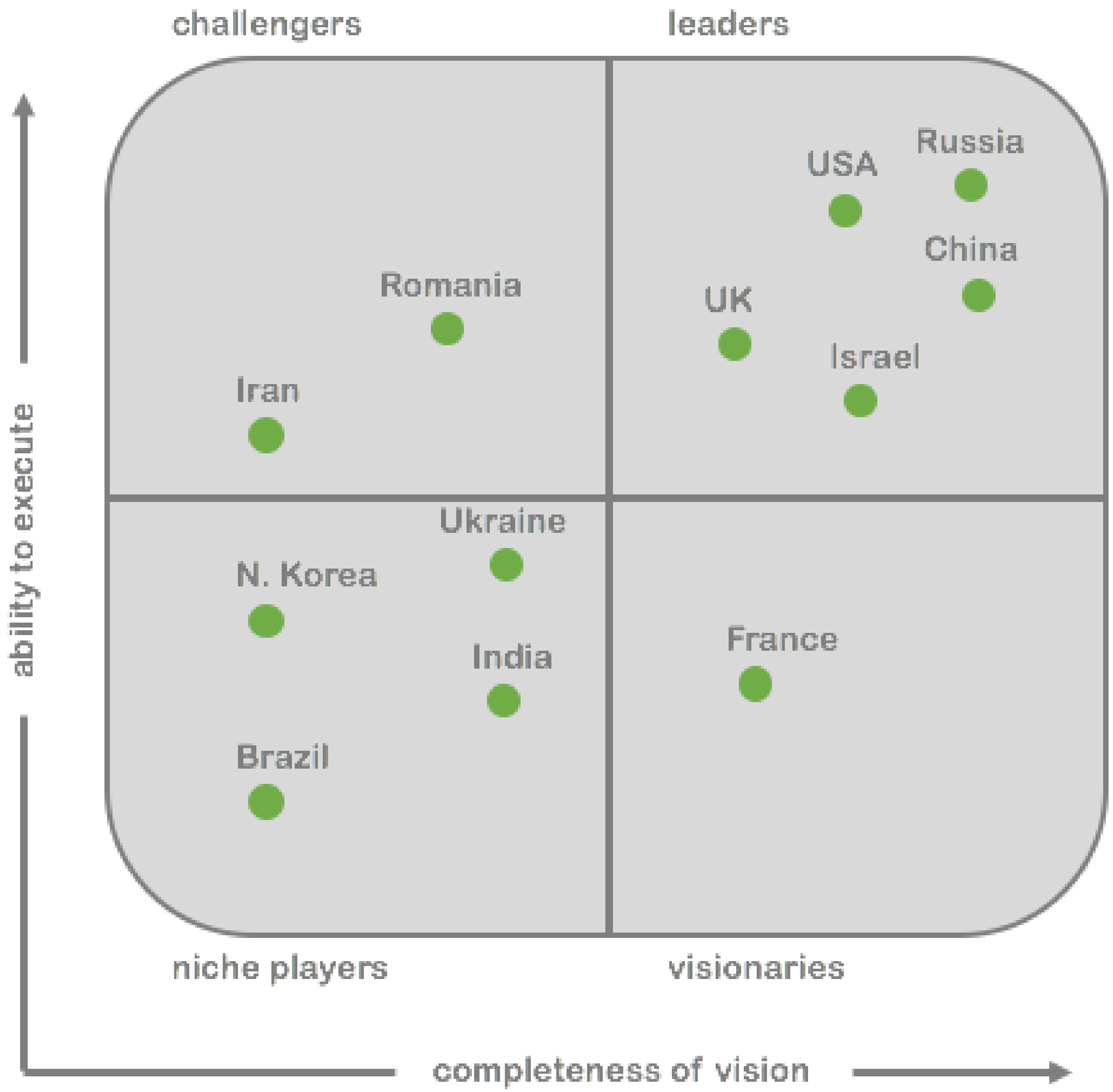
#	●	Service	Port
115	●	ssh	22
93	●	ms-term-services	3389
84	●	isakmp	500
70	●	microsoft-ds	445
50	●	http	80

Botnet Arithmetic

Number of Bots	Outbound Capacity	Size of Attack	Network Size
2	750 Kbps	1.5 Mbps	T1
1,200	1.0 Mbps	1.2 Gbps	OC-24
2,400	1.0 Mbps	2.4 Gbps	OC-48
10,000	1.0 Mbps	10.0 Gbps	OC-192
40,000	1.0 Mbps	40.0 Gbps	OC-768
80,000	1.0 Mbps	80.0 Gbps	*Starts to fill typical ISP backbone*
100,000	1.0 Mbps	100 Gbps	
1,000,000	1.0 Mbps	1000 Gbps	

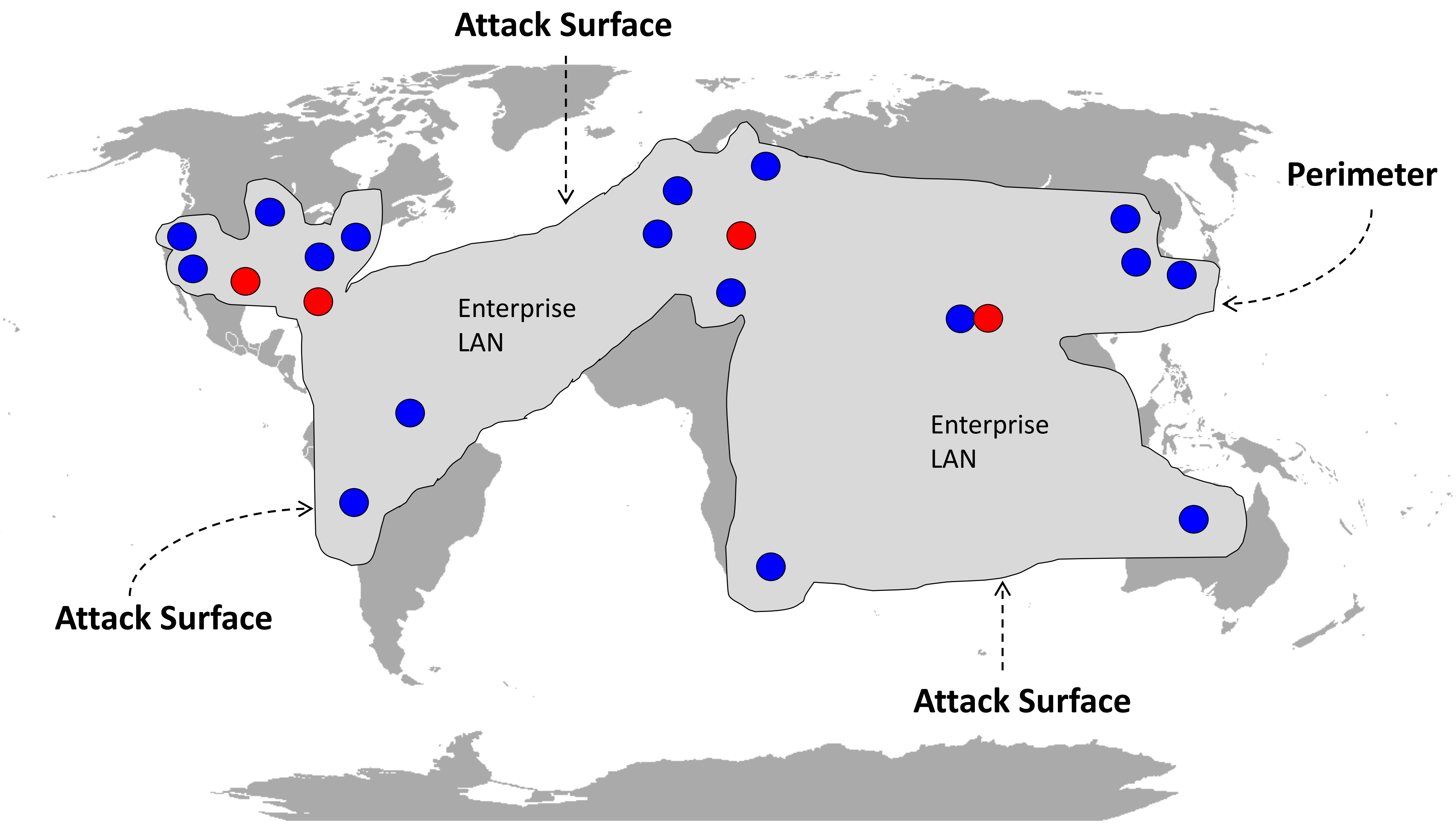
What Countries Have the Best Hackers?

Ranking Countries by Hacking Capability

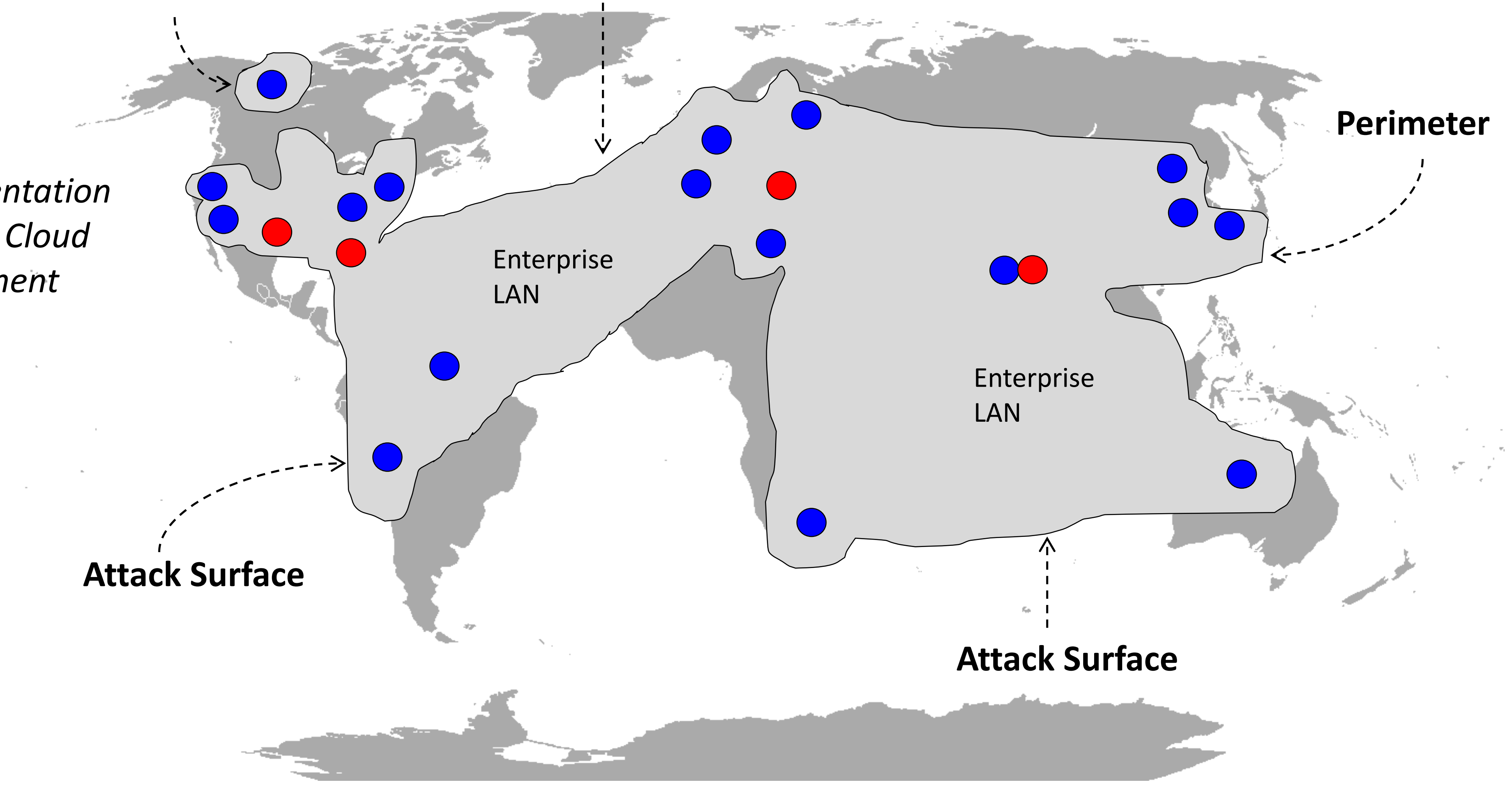


Why Couldn’t the Russians Find the Deleted Clinton Emails?

Warning: Global Perimeters are Not Secure



Isolating a Server from a Perimeter Makes it More Secure



Isolated Server

Attack Surface

Perimeter

Microsegmentation to Secured Cloud Environment

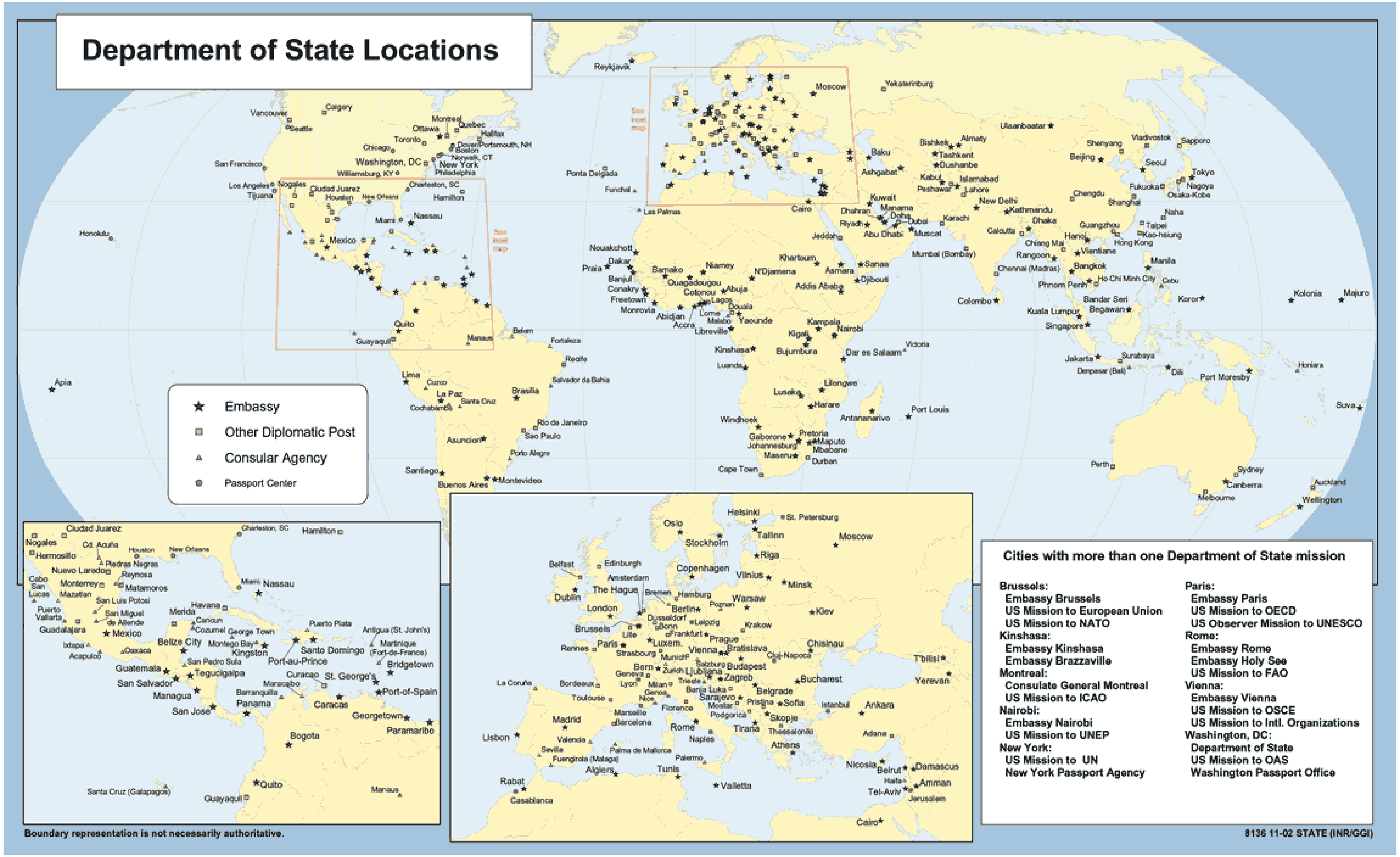
Enterprise LAN

Enterprise LAN

Attack Surface

Attack Surface

Global Department of State Network



Cities with more than one Department of State mission

Brussels:
- Embassy Brussels
- US Mission to European Union
- US Mission to NATO

Kinshasa:
- Embassy Kinshasa
- Embassy Brazzaville

Montreal:
- Consulate General Montreal
- US Mission to ICAO

Nairobi:
- Embassy Nairobi
- US Mission to UNEP

New York:
- US Mission to UN
- New York Passport Agency

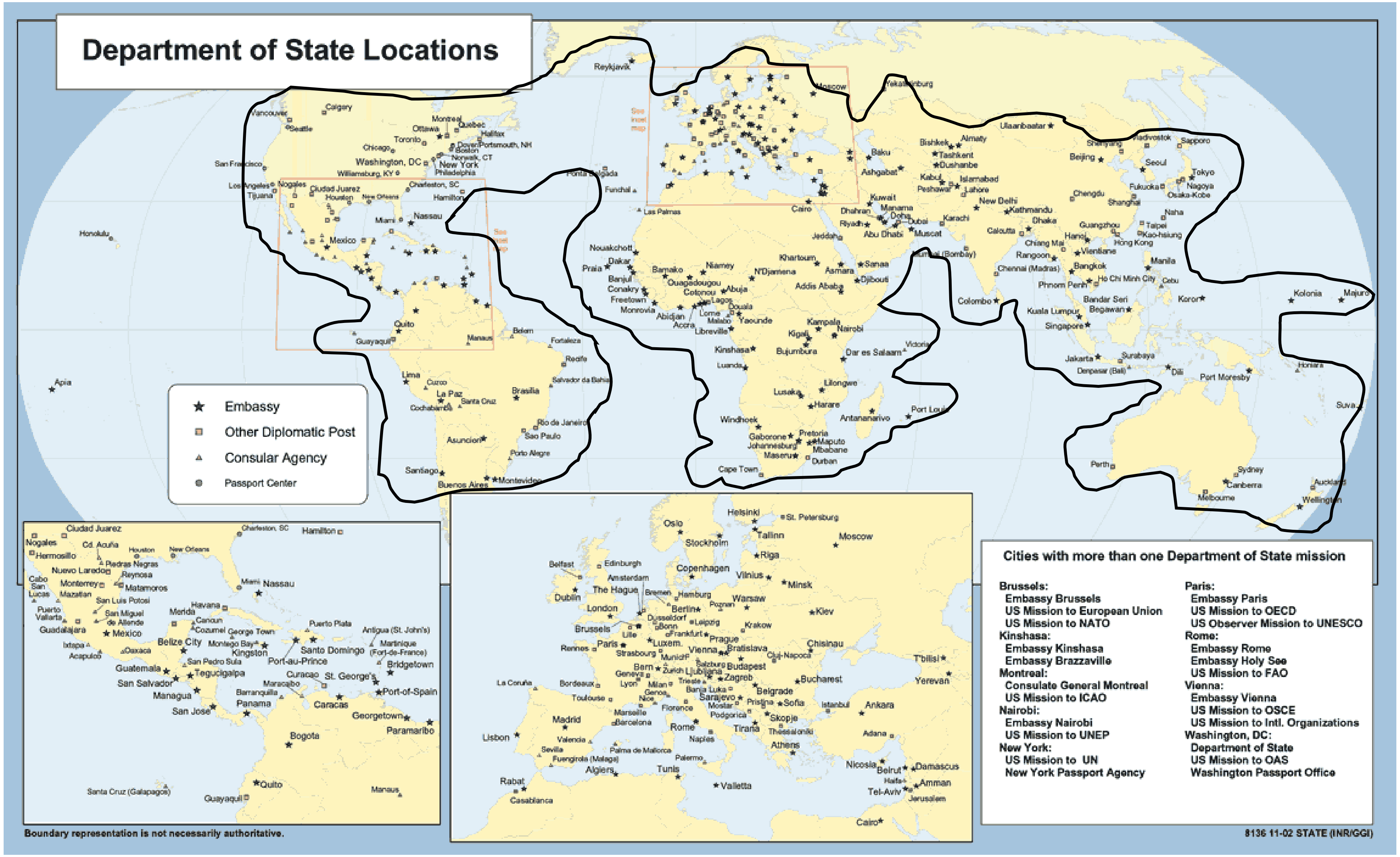
Paris:
- Embassy Paris
- US Mission to OECD
- US Observer Mission to UNESCO

Rome:
- Embassy Rome
- Embassy Holy See
- US Mission to FAO

Vienna:
- Embassy Vienna
- US Mission to OSCE
- US Mission to Intl. Organizations

Washington, DC:
- Department of State
- US Mission to OAS
- Washington Passport Office

Global Department of State Perimeter is Not Secure



★ Embassy

□ Other Diplomatic Post

▲ Consular Agency

● Passport Center

Cities with more than one Department of State mission

Brussels:
Embassy Brussels
US Mission to European Union
US Mission to NATO

Kinshasa:
Embassy Kinshasa
Embassy Brazzaville

Montreal:
Consulate General Montreal
US Mission to ICAO

Nairobi:
Embassy Nairobi
US Mission to UNEP

New York:
US Mission to UN
New York Passport Agency

Paris:
Embassy Paris
US Mission to OECD
US Observer Mission to UNESCO

Rome:
Embassy Rome
Embassy Holy See
US Mission to FAO

Vienna:
Embassy Vienna
US Mission to OSCE
US Mission to Intl. Organizations

Washington, DC:
Department of State
US Mission to OAS
Washington Passport Office

Boundary representation is not necessarily authoritative.

8136 11-02 STATE (INR/GGI)

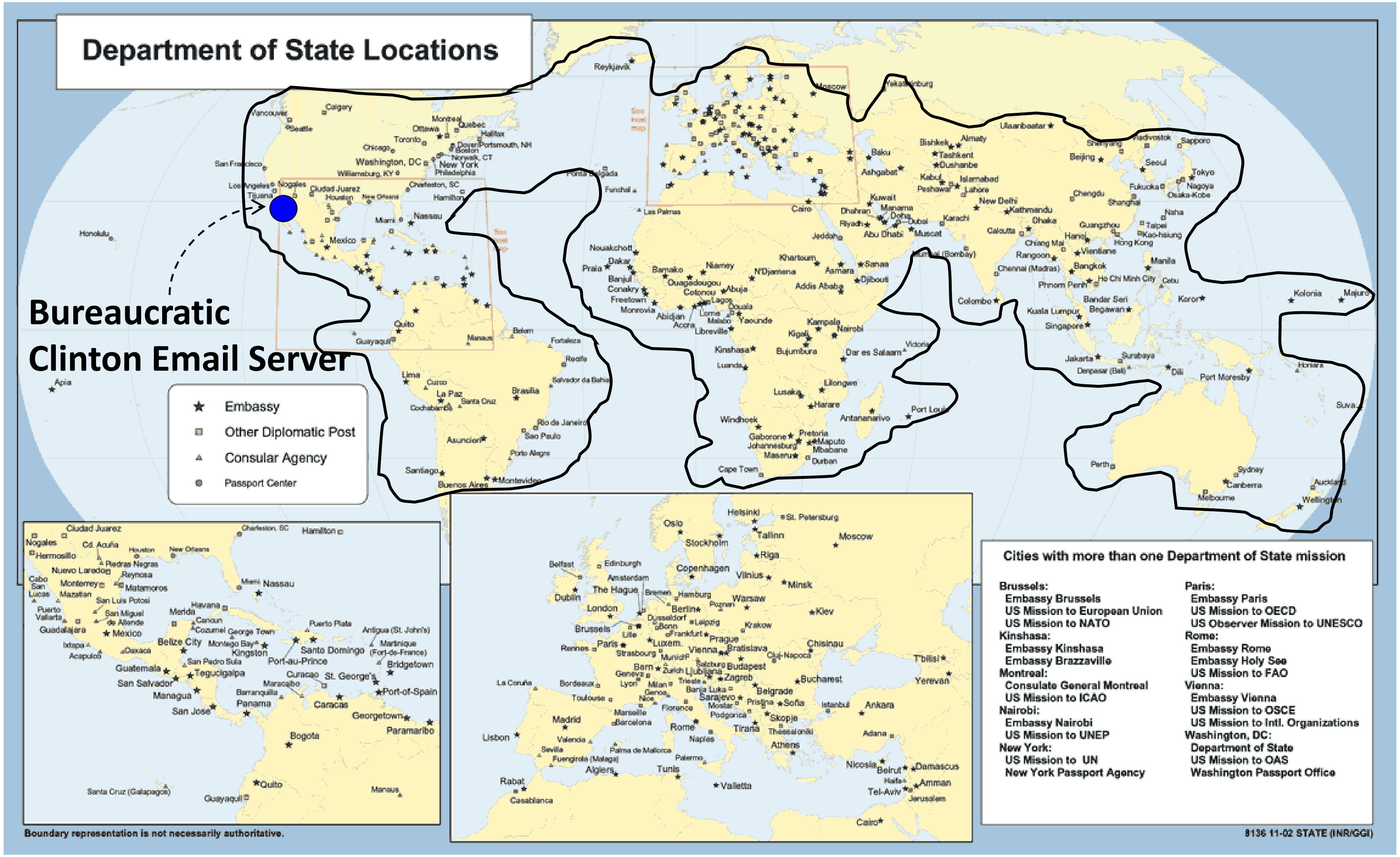
TUE, APR 4, 2017

It Took ‘Hand to Hand’ Cyber Combat for NSA to Remove Russian Hackers From State Department Networks

NATOSource by Ellen Nakashima, Washington Post

Cybersecurity Intelligence Russia Security & Defense United States and Canada

Global Department of State Perimeter is Not Secure



Bureaucratic Clinton Email Server

Cities with more than one Department of State mission

Brussels:
Embassy Brussels
US Mission to European Union
US Mission to NATO

Kinshasa:
Embassy Kinshasa
Embassy Brazzaville

Montreal:
Consulate General Montreal
US Mission to ICAO

Nairobi:
Embassy Nairobi
US Mission to UNEP

New York:
US Mission to UN
New York Passport Agency

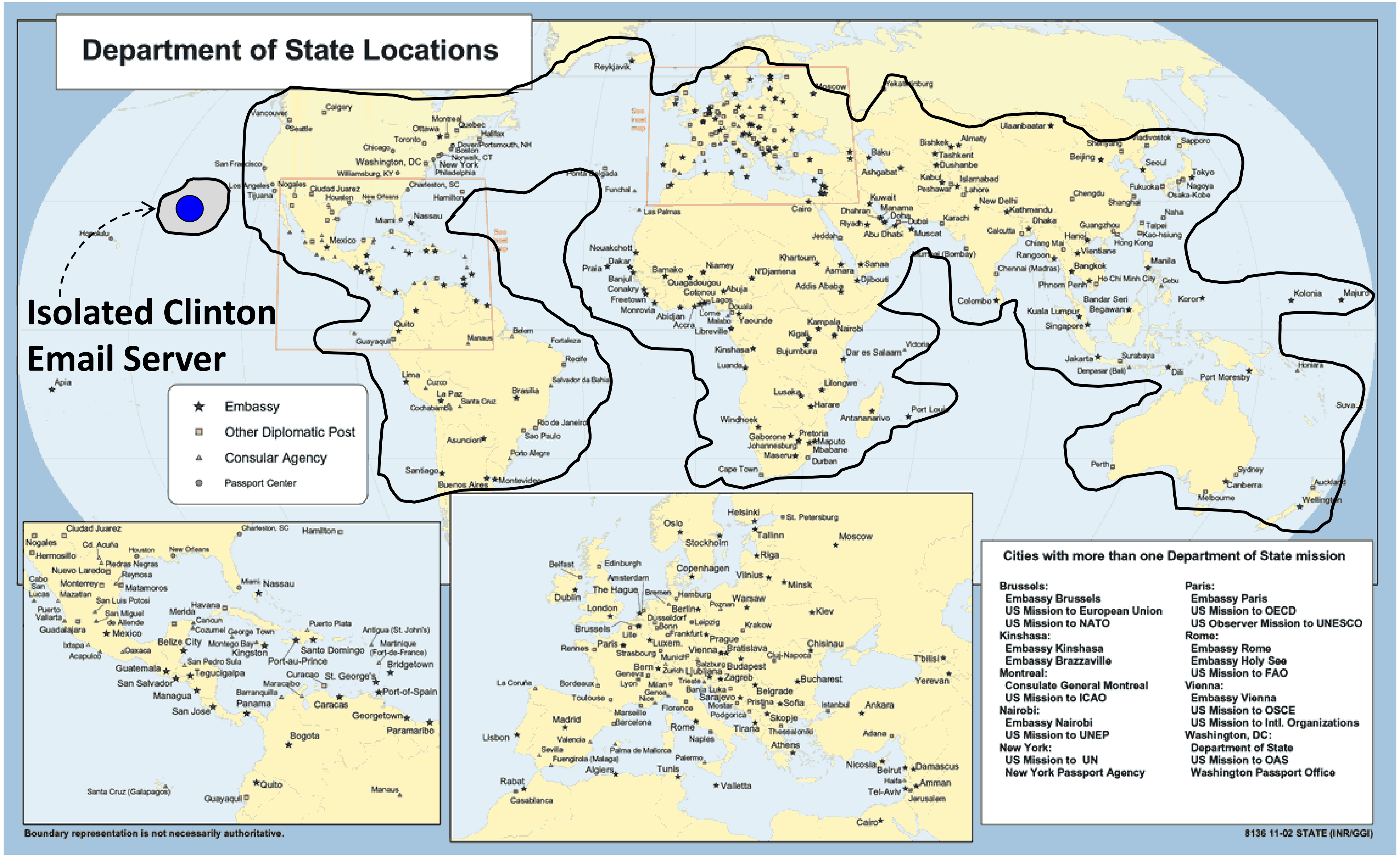
Paris:
Embassy Paris
US Mission to OECD
US Observer Mission to UNESCO

Rome:
Embassy Rome
Embassy Holy See
US Mission to FAO

Vienna:
Embassy Vienna
US Mission to OSCE
US Mission to Intl. Organizations

Washington, DC:
Department of State
US Mission to OAS
Washington Passport Office

Isolating the Clinton Email Server Made it More Secure



Isolated Clinton Email Server

Department of State Locations
★ Embassy
□ Other Diplomatic Post
▲ Consular Agency
● Passport Center
Boundary representation is not necessarily authoritative.
8136 11-02 STATE (INR/GGI)

Cities with more than one Department of State mission

Brussels:
Embassy Brussels
US Mission to European Union
US Mission to NATO

Kinshasa:
Embassy Kinshasa
Embassy Brazzaville

Montreal:
Consulate General Montreal
US Mission to ICAO

Nairobi:
Embassy Nairobi
US Mission to UNEP

New York:
US Mission to UN
New York Passport Agency

Paris:
Embassy Paris
US Mission to OECD
US Observer Mission to UNESCO

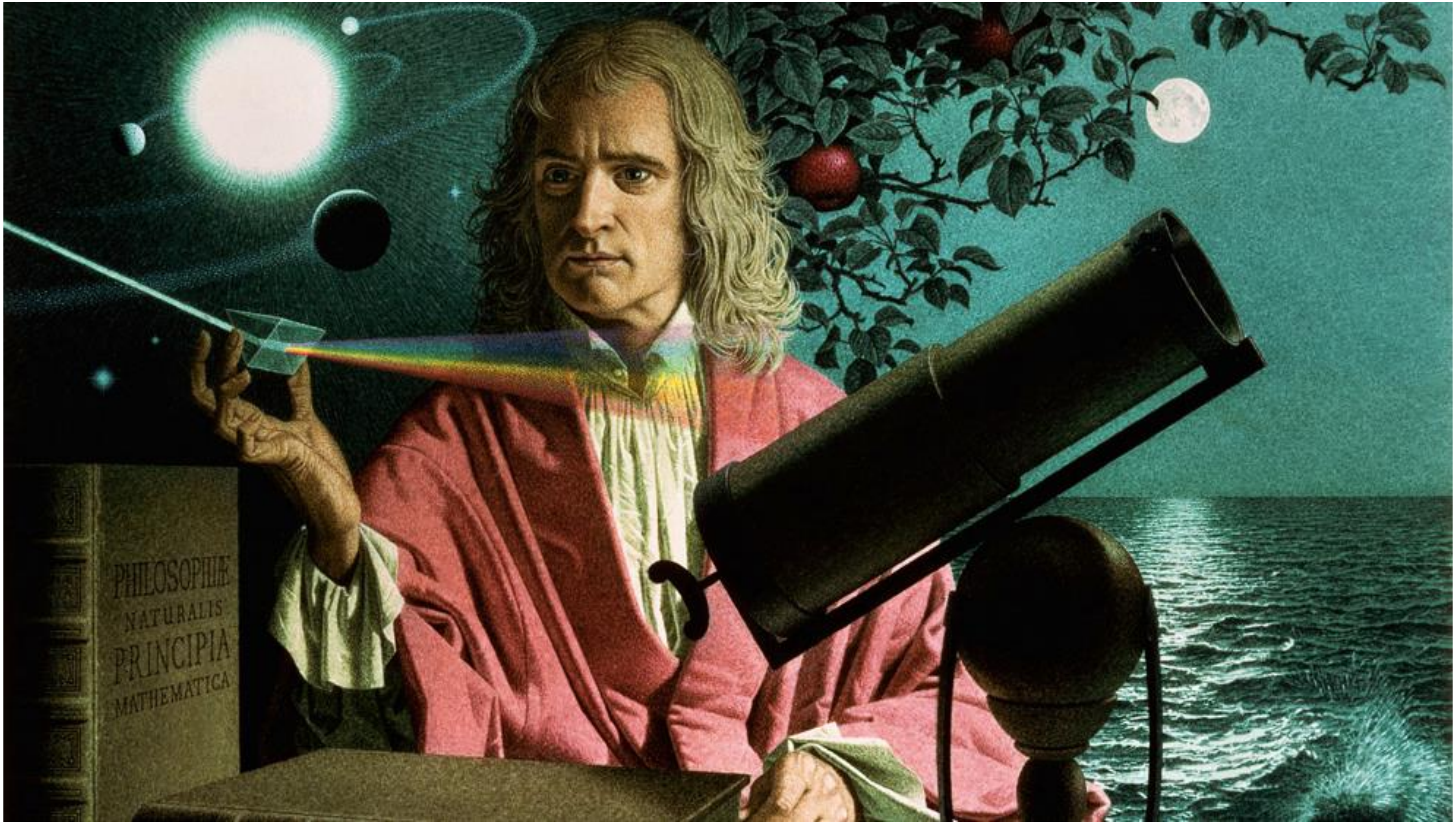
Rome:
Embassy Rome
Embassy Holy See
US Mission to FAO

Vienna:
Embassy Vienna
US Mission to OSCE
US Mission to Intl. Organizations

Washington, DC:
Department of State
US Mission to OAS
Washington Passport Office

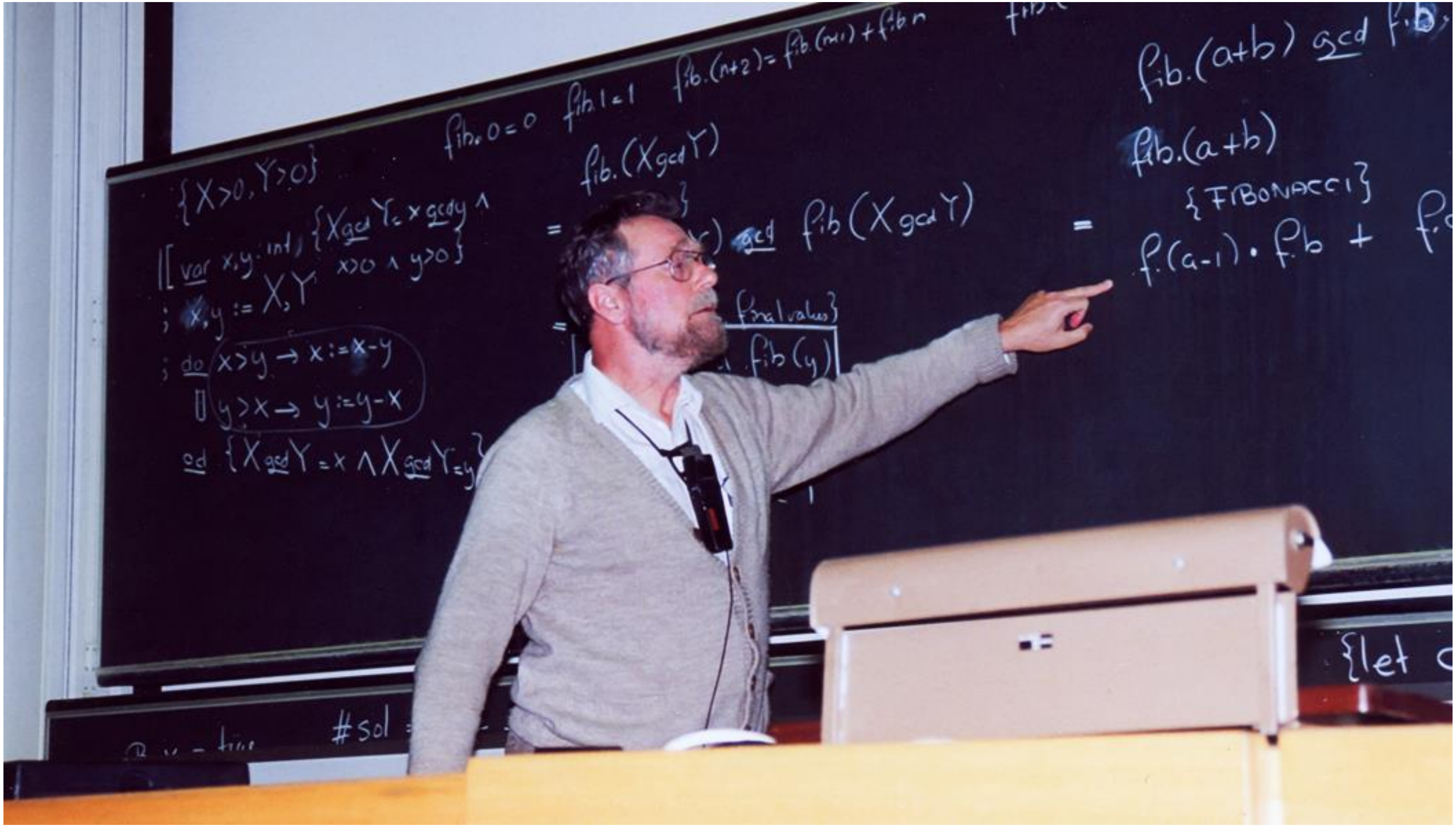
Can Artificial Intelligence Catch Hackers?

“Most Famous Alchemist of All Time . . .”

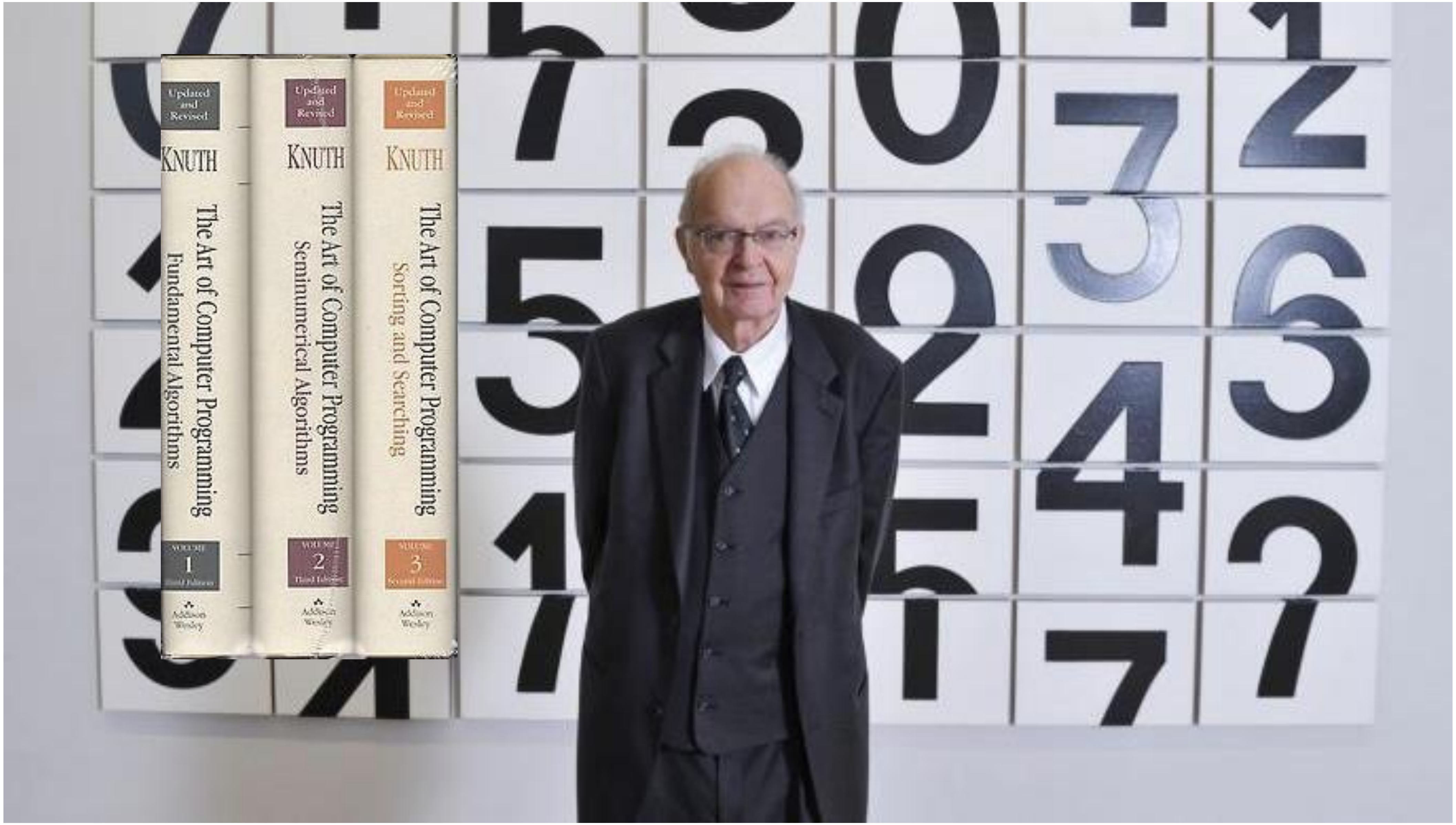


“The Computer and the Brain . . .”

“The Question of Whether Computers Can Think . . .”



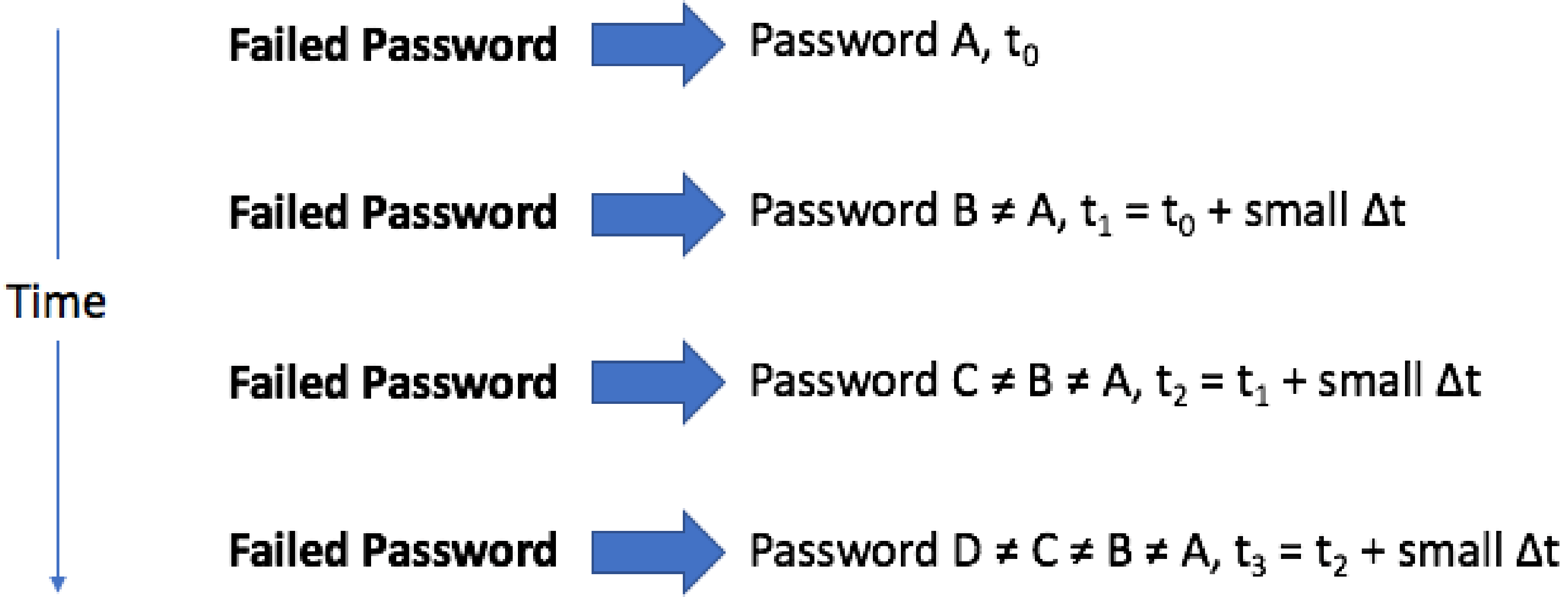
“Sorting, Searching, Matching, . . . ”



Machine Learning Basics: This is a Dog.

Machine Learning Basics: These are all Dogs.

Machine Learning: This is a Password Hack.



Time

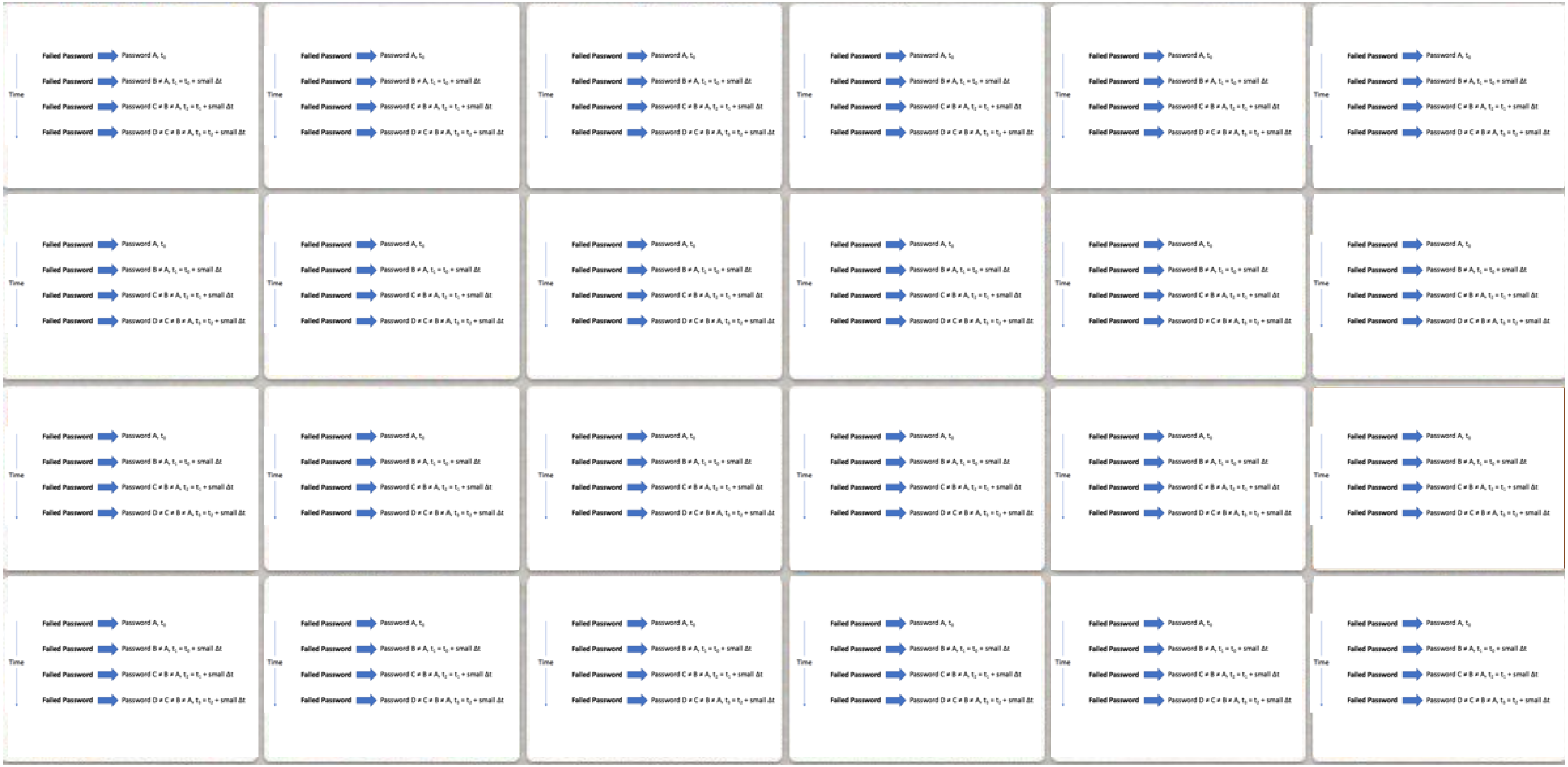
Failed Password → Password A, t_0

Failed Password → Password B ≠ A, $t_1 = t_0 + \text{small } \Delta t$

Failed Password → Password C ≠ B ≠ A, $t_2 = t_1 + \text{small } \Delta t$

Failed Password → Password D ≠ C ≠ B ≠ A, $t_3 = t_2 + \text{small } \Delta t$

Machine Learning: These are all Password Hacks.



Time

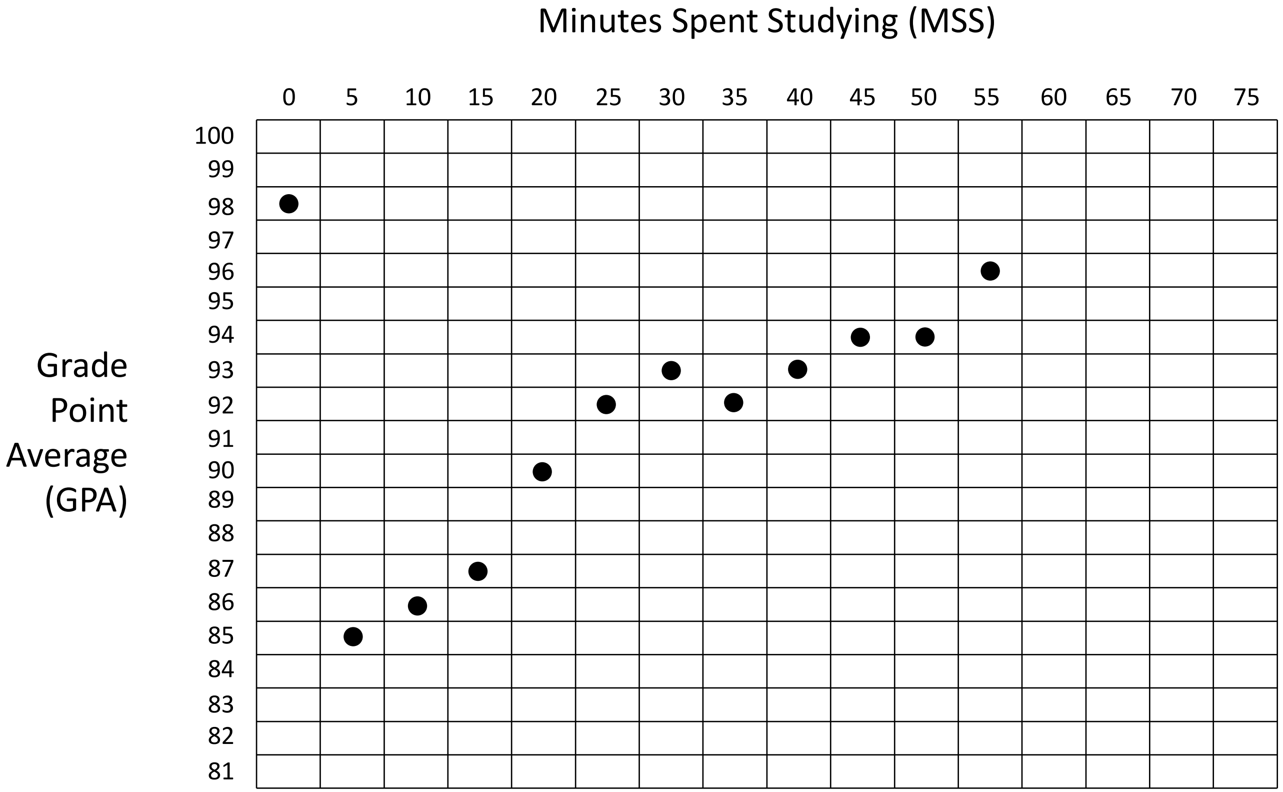
Failed Password → Password A, t_0

Failed Password → Password B ≠ A, $t_1 = t_0 + \text{small } \Delta t$

Failed Password → Password C ≠ B ≠ A, $t_2 = t_1 + \text{small } \Delta t$

Failed Password → Password D ≠ C ≠ B ≠ A, $t_3 = t_2 + \text{small } \Delta t$

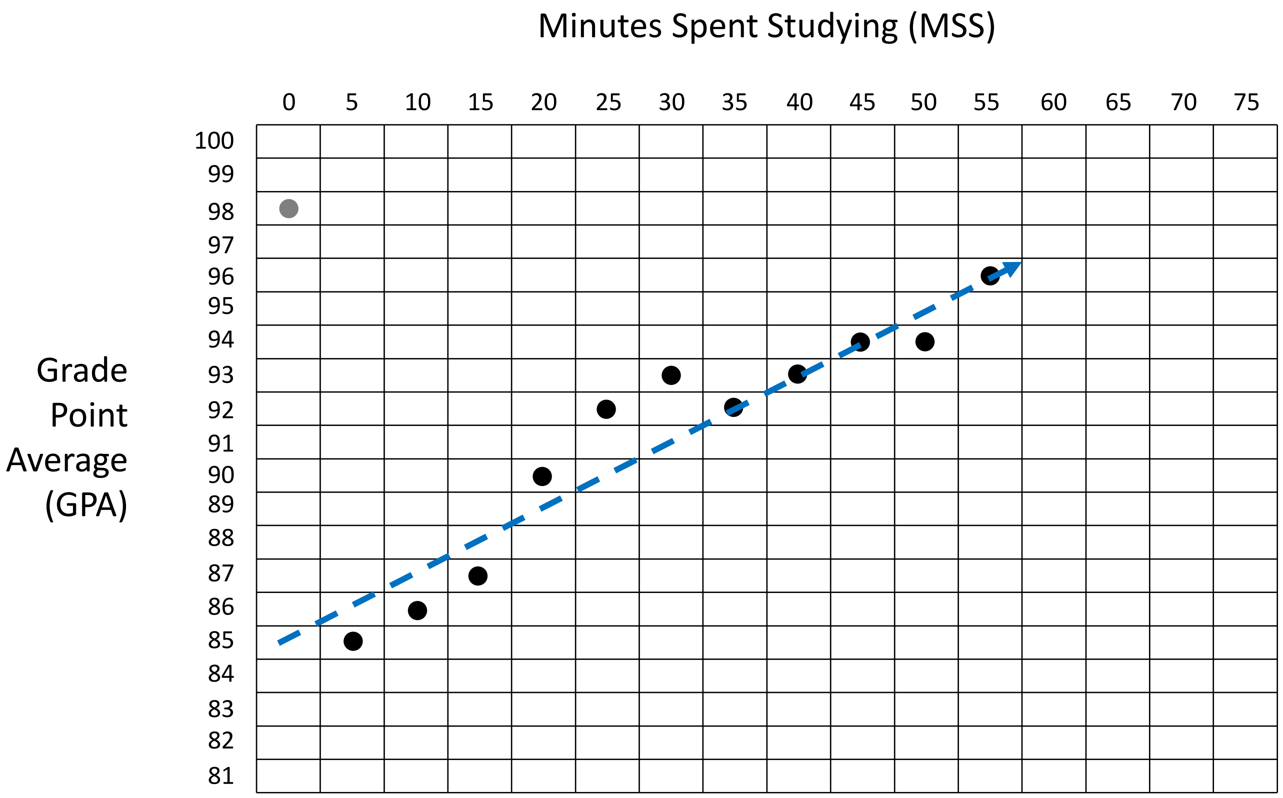
Time
Failed Password → Password A, t_0
Failed Password → Password B ≠ A, $t_1 = t_0 + \text{small } \Delta t$
Failed Password → Password C ≠ B ≠ A, $t_2 = t_1 + \text{small } \Delta t$
Failed Password → Password D ≠ C ≠ B ≠ A, $t_3 = t_2 + \text{small } \Delta t$
Time
Failed Password → Password A, t_0
Failed Password → Password B ≠ A, $t_1 = t_0 + \text{small } \Delta t$
Failed Password → Password C ≠ B ≠ A, $t_2 = t_1 + \text{small } \Delta t$
Failed Password → Password D ≠ C ≠ B ≠ A, $t_3 = t_2 + \text{small } \Delta t$
Time
Failed Password → Password A, t_0
Failed Password → Password B ≠ A, $t_1 = t_0 + \text{small } \Delta t$
Failed Password → Password C ≠ B ≠ A, $t_2 = t_1 + \text{small } \Delta t$
Failed Password → Password D ≠ C ≠ B ≠ A, $t_3 = t_2 + \text{small } \Delta t$
Time
Failed Password → Password A, t_0
Failed Password → Password B ≠ A, $t_1 = t_0 + \text{small } \Delta t$
Failed Password → Password C ≠ B ≠ A, $t_2 = t_1 + \text{small } \Delta t$
Failed Password → Password D ≠ C ≠ B ≠ A, $t_3 = t_2 + \text{small } \Delta t$
Time
Failed Password → Password A, t_0
Failed Password → Password B ≠ A, $t_1 = t_0 + \text{small } \Delta t$
Failed Password → Password C ≠ B ≠ A, $t_2 = t_1 + \text{small } \Delta t$
Failed Password → Password D ≠ C ≠ B ≠ A, $t_3 = t_2 + \text{small } \Delta t$
Time
Failed Password → Password A, t_0
Failed Password → Password B ≠ A, $t_1 = t_0 + \text{small } \Delta t$
Failed Password → Password C ≠ B ≠ A, $t_2 = t_1 + \text{small } \Delta t$
Failed Password → Password D ≠ C ≠ B ≠ A, $t_3 = t_2 + \text{small } \Delta t$
Time
Failed Password → Password A, t_0
Failed Password → Password B ≠ A, $t_1 = t_0 + \text{small } \Delta t$
Failed Password → Password C ≠ B ≠ A, $t_2 = t_1 + \text{small } \Delta t$
Failed Password → Password D ≠ C ≠ B ≠ A, $t_3 = t_2 + \text{small } \Delta t$
Time
Failed Password → Password A, t_0
Failed Password → Password B ≠ A, $t_1 = t_0 + \text{small } \Delta t$
Failed Password → Password C ≠ B ≠ A, $t_2 = t_1 + \text{small } \Delta t$
Failed Password → Password D ≠ C ≠ B ≠ A, $t_3 = t_2 + \text{small } \Delta t$
Time
Failed Password → Password A, t_0
Failed Password → Password B ≠ A, $t_1 = t_0 + \text{small } \Delta t$
Failed Password → Password C ≠ B ≠ A, $t_2 = t_1 + \text{small } \Delta t$
Failed Password → Password D ≠ C ≠ B ≠ A, $t_3 = t_2 + \text{small } \Delta t$
Time
Failed Password → Password A, t_0
Failed Password → Password B ≠ A, $t_1 = t_0 + \text{small } \Delta t$
Failed Password → Password C ≠ B ≠ A, $t_2 = t_1 + \text{small } \Delta t$
Failed Password → Password D ≠ C ≠ B ≠ A, $t_3 = t_2 + \text{small } \Delta t$
Time
Failed Password → Password A, t_0
Failed Password → Password B ≠ A, $t_1 = t_0 + \text{small } \Delta t$
Failed Password → Password C ≠ B ≠ A, $t_2 = t_1 + \text{small } \Delta t$
Failed Password → Password D ≠ C ≠ B ≠ A, $t_3 = t_2 + \text{small } \Delta t$
Time
Failed Password → Password A, t_0
Failed Password → Password B ≠ A, $t_1 = t_0 + \text{small } \Delta t$
Failed Password → Password C ≠ B ≠ A, $t_2 = t_1 + \text{small } \Delta t$
Failed Password → Password D ≠ C ≠ B ≠ A, $t_3 = t_2 + \text{small } \Delta t$
Time
Failed Password → Password A, t_0
Failed Password → Password B ≠ A, $t_1 = t_0 + \text{small } \Delta t$
Failed Password → Password C ≠ B ≠ A, $t_2 = t_1 + \text{small } \Delta t$
Failed Password → Password D ≠ C ≠ B ≠ A, $t_3 = t_2 + \text{small } \Delta t$
Time
Failed Password → Password A, t_0
Failed Password → Password B ≠ A, $t_1 = t_0 + \text{small } \Delta t$
Failed Password → Password C ≠ B ≠ A, $t_2 = t_1 + \text{small } \Delta t$
Failed Password → Password D ≠ C ≠ B ≠ A, $t_3 = t_2 + \text{small } \Delta t$
Time
Failed Password → Password A, t_0
Failed Password → Password B ≠ A, $t_1 = t_0 + \text{small } \Delta t$
Failed Password → Password C ≠ B ≠ A, $t_2 = t_1 + \text{small } \Delta t$
Failed Password → Password D ≠ C ≠ B ≠ A, $t_3 = t_2 + \text{small } \Delta t$
Time
Failed Password → Password A, t_0
Failed Password → Password B ≠ A, $t_1 = t_0 + \text{small } \Delta t$
Failed Password → Password C ≠ B ≠ A, $t_2 = t_1 + \text{small } \Delta t$
Failed Password → Password D ≠ C ≠ B ≠ A, $t_3 = t_2 + \text{small } \Delta t$
Time
Failed Password → Password A, t_0
Failed Password → Password B ≠ A, $t_1 = t_0 + \text{small } \Delta t$
Failed Password → Password C ≠ B ≠ A, $t_2 = t_1 + \text{small } \Delta t$
Failed Password → Password D ≠ C ≠ B ≠ A, $t_3 = t_2 + \text{small } \Delta t$
Time
Failed Password → Password A, t_0
Failed Password → Password B ≠ A, $t_1 = t_0 + \text{small } \Delta t$
Failed Password → Password C ≠ B ≠ A, $t_2 = t_1 + \text{small } \Delta t$
Failed Password → Password D ≠ C ≠ B ≠ A, $t_3 = t_2 + \text{small } \Delta t$
Time
Failed Password → Password A, t_0
Failed Password → Password B ≠ A, $t_1 = t_0 + \text{small } \Delta t$
Failed Password → Password C ≠ B ≠ A, $t_2 = t_1 + \text{small } \Delta t$
Failed Password → Password D ≠ C ≠ B ≠ A, $t_3 = t_2 + \text{small } \Delta t$
Time
Failed Password → Password A, t_0
Failed Password → Password B ≠ A, $t_1 = t_0 + \text{small } \Delta t$
Failed Password → Password C ≠ B ≠ A, $t_2 = t_1 + \text{small } \Delta t$
Failed Password → Password D ≠ C ≠ B ≠ A, $t_3 = t_2 + \text{small } \Delta t$
Time
Failed Password → Password A, t_0
Failed Password → Password B ≠ A, $t_1 = t_0 + \text{small } \Delta t$
Failed Password → Password C ≠ B ≠ A, $t_2 = t_1 + \text{small } \Delta t$
Failed Password → Password D ≠ C ≠ B ≠ A, $t_3 = t_2 + \text{small } \Delta t$
Time
Failed Password → Password A, t_0
Failed Password → Password B ≠ A, $t_1 = t_0 + \text{small } \Delta t$
Failed Password → Password C ≠ B ≠ A, $t_2 = t_1 + \text{small } \Delta t$
Failed Password → Password D ≠ C ≠ B ≠ A, $t_3 = t_2 + \text{small } \Delta t$
Time
Failed Password → Password A, t_0
Failed Password → Password B ≠ A, $t_1 = t_0 + \text{small } \Delta t$
Failed Password → Password C ≠ B ≠ A, $t_2 = t_1 + \text{small } \Delta t$
Failed Password → Password D ≠ C ≠ B ≠ A, $t_3 = t_2 + \text{small } \Delta t$



Minutes Spent Studying	Grade Point Average
0	98
5	85
10	86
15	87
20	90
25	92
30	93
35	92
40	93
45	94
50	94
55	96

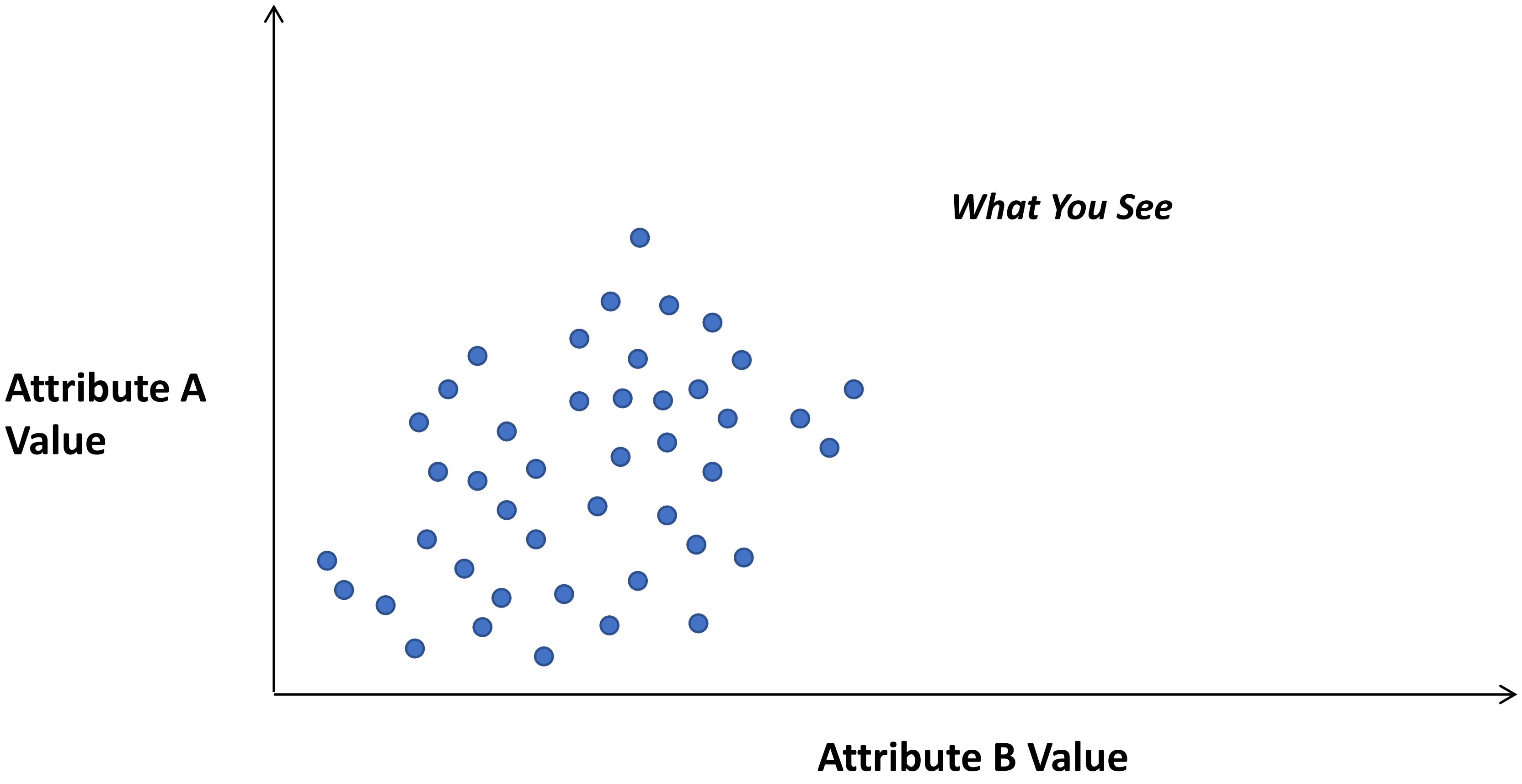
Developing Learning Models from Data (Simple Example)

Developing Learning Models from Data (Simple Example)



Minutes Spent Studying	Grade Point Average
0	98
5	85
10	86
15	87
20	90
25	92
30	93
35	92
40	93
45	94
50	94
55	96

$y = mx + b$ GPA = m (MSS) + b (where (MSS > 0)) **GPA = 0.2 (MSS) + 85**

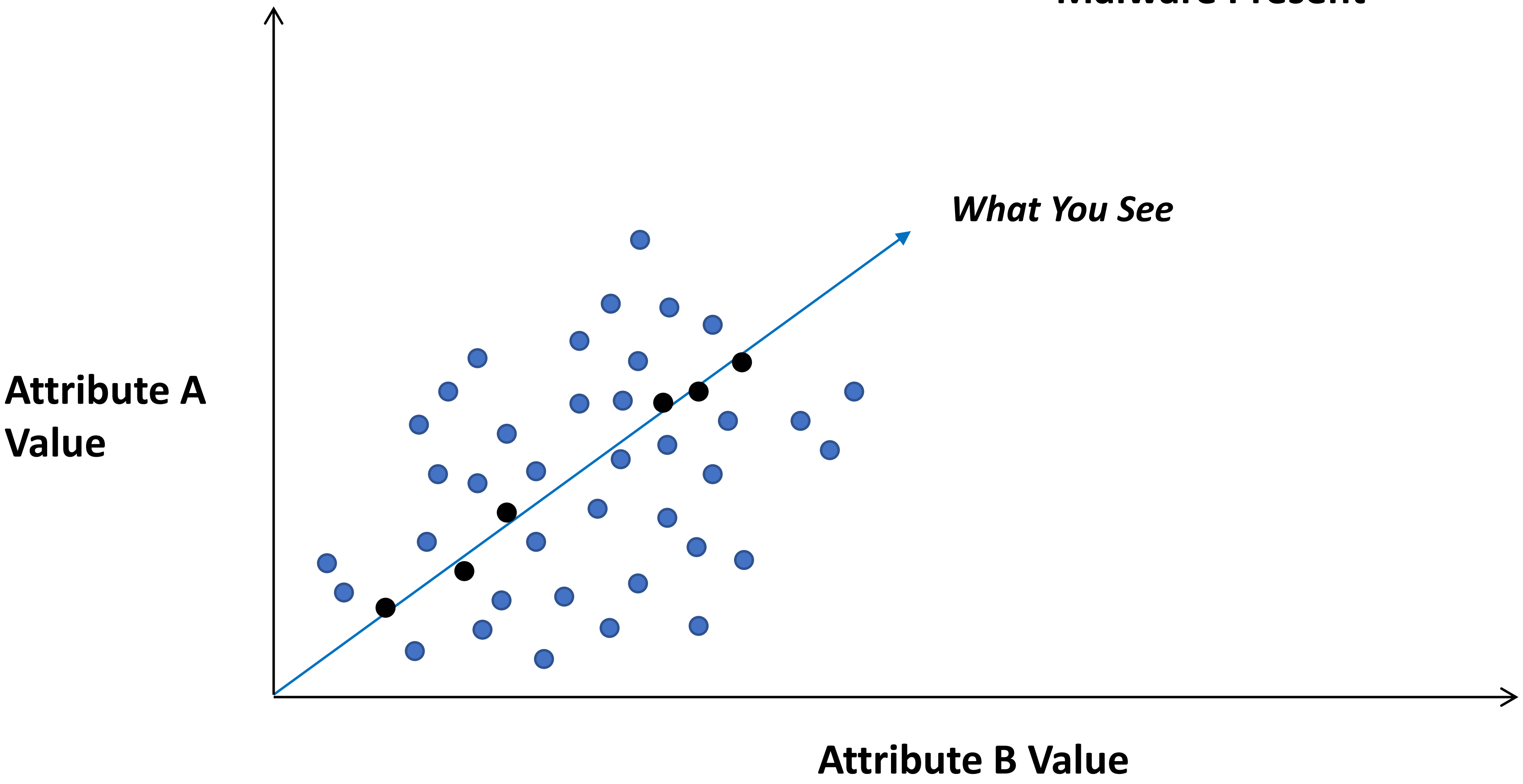


What You See

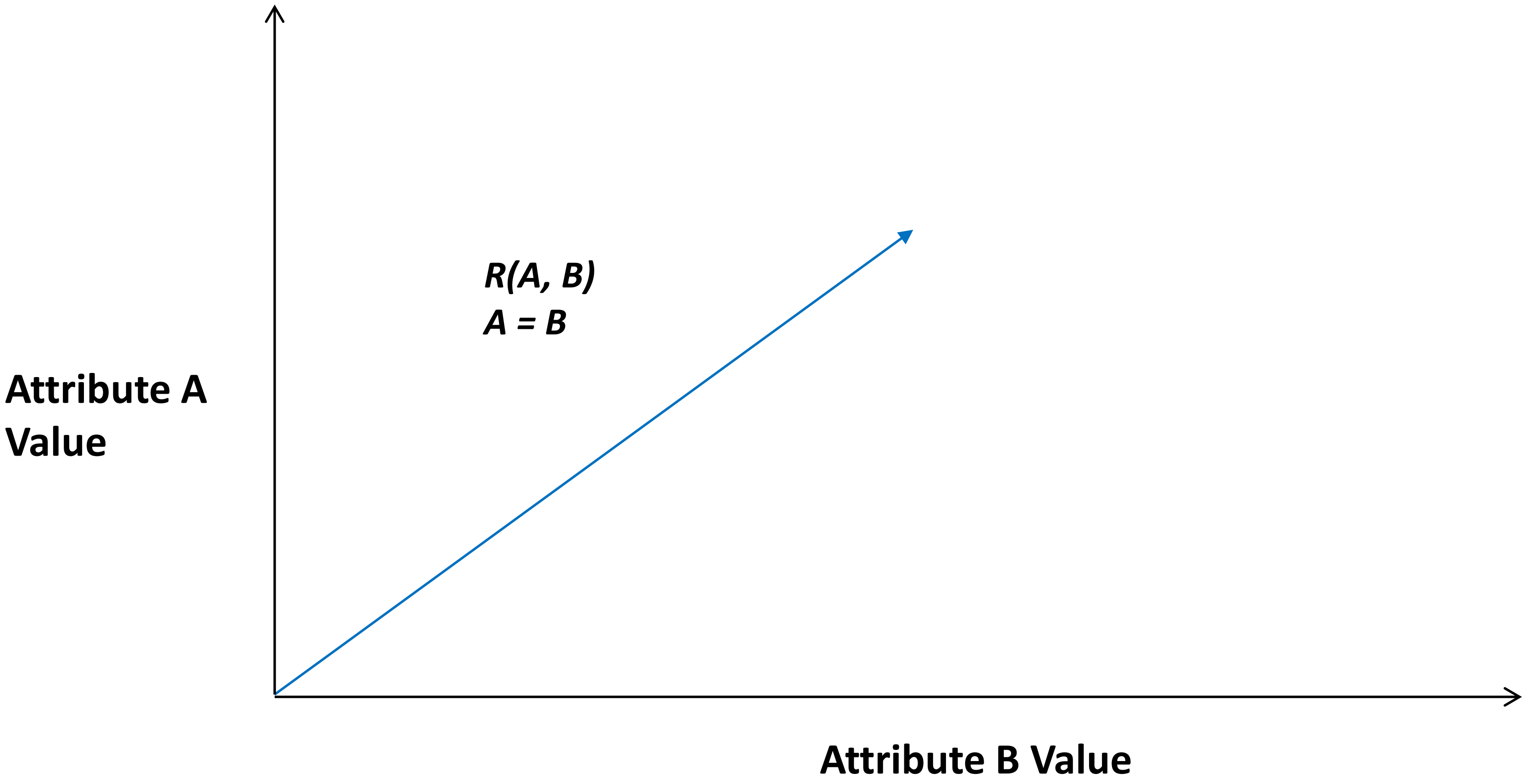
Mapping Data Using Attributes

TYPICAL CYBER SECURITY:

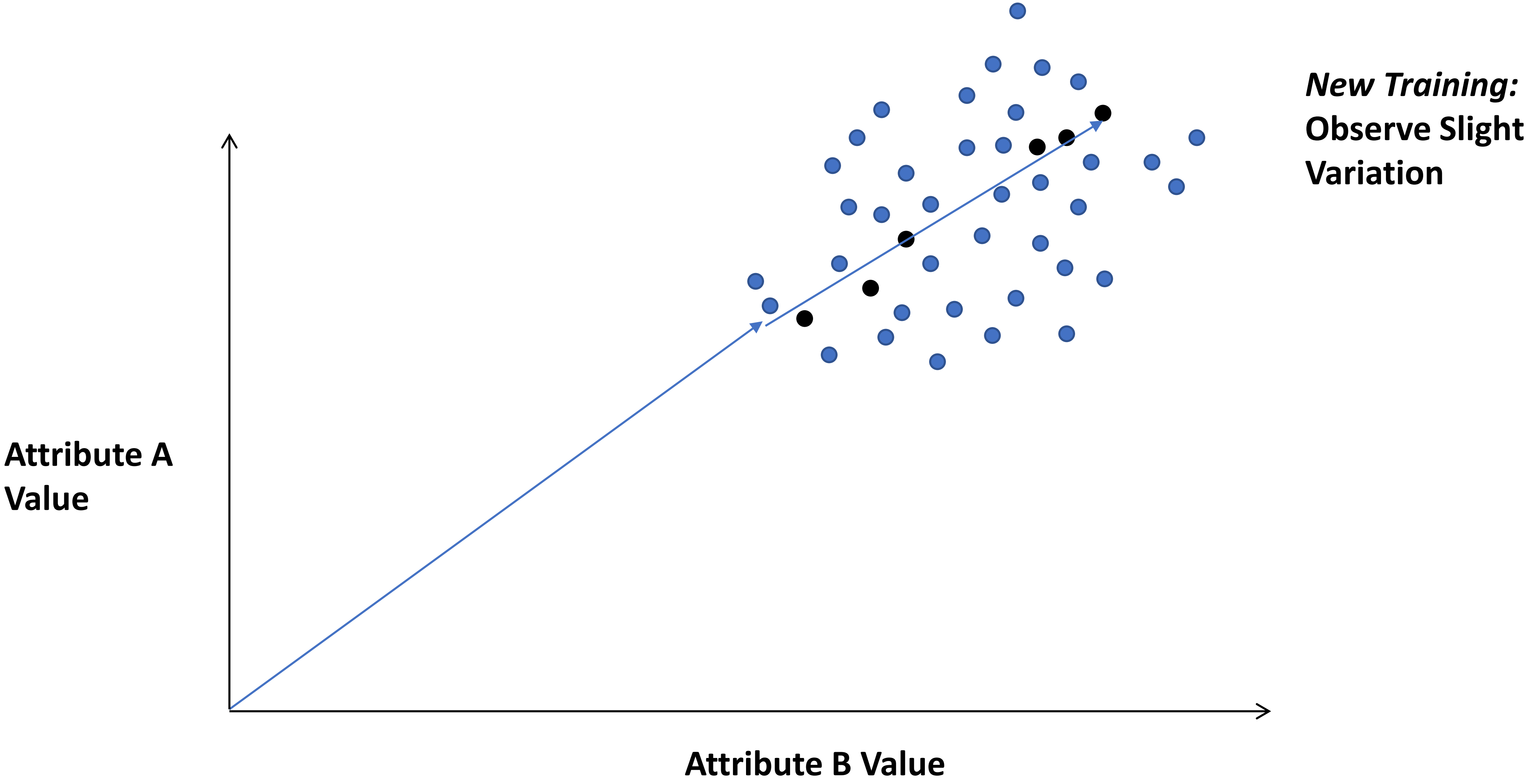
IF Attribute A Value = Attribute B Value THEN Malware Present



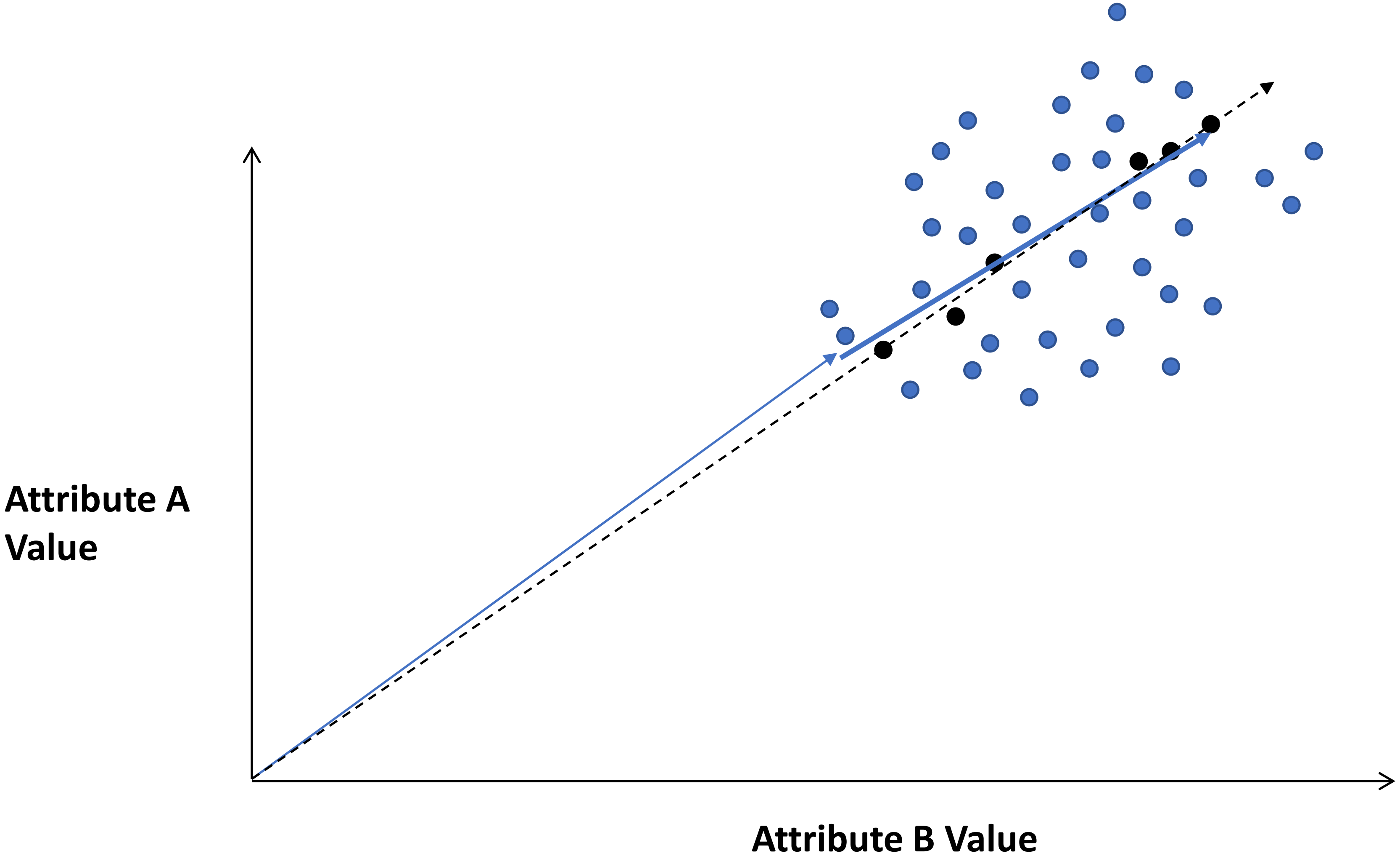
Graphing Attribute Relationships from Observation



Developing an Attribute Model

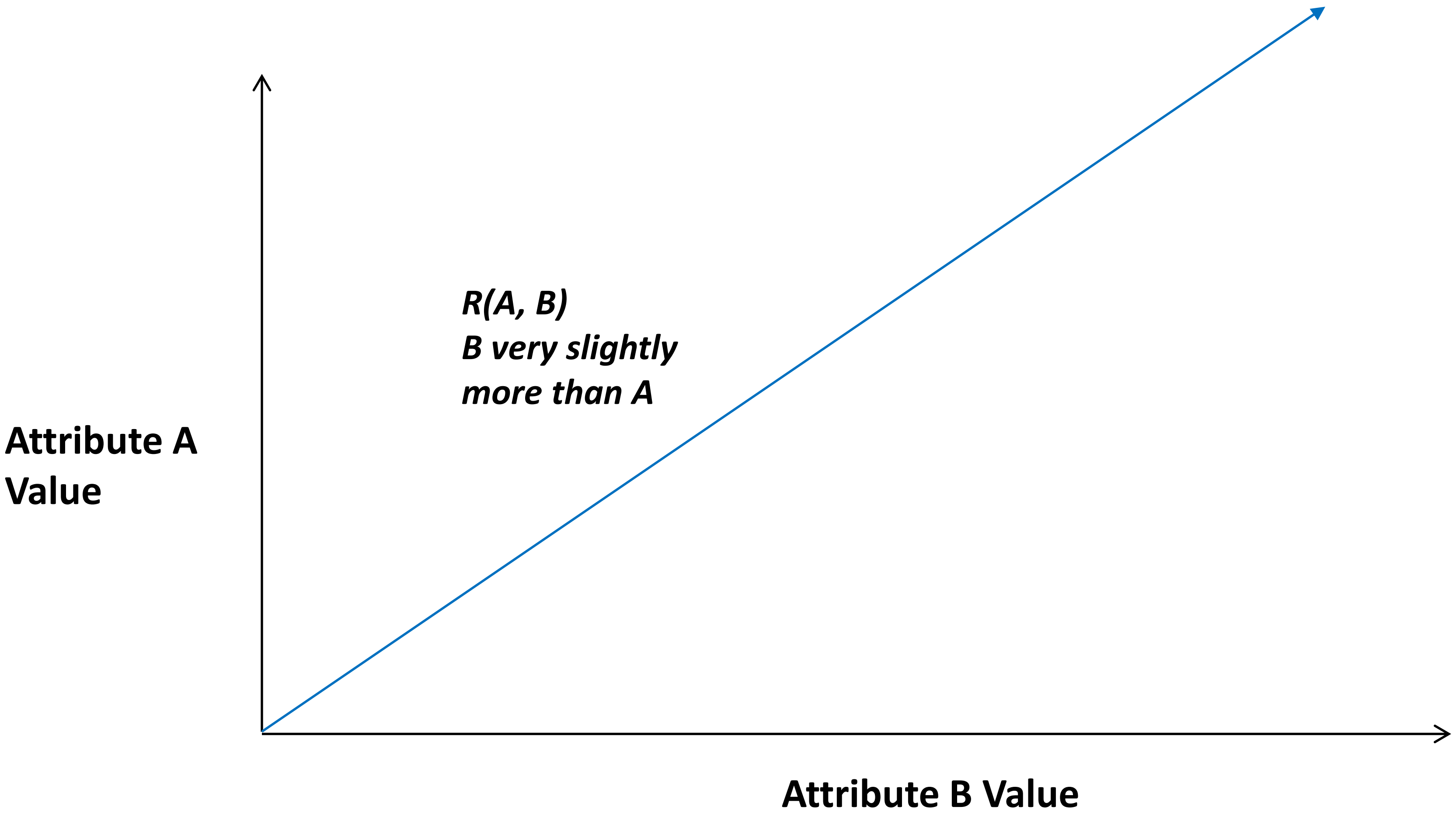


Observing Variation in Practice



New Training:
Observe Slight Variation

Adjusting the Model

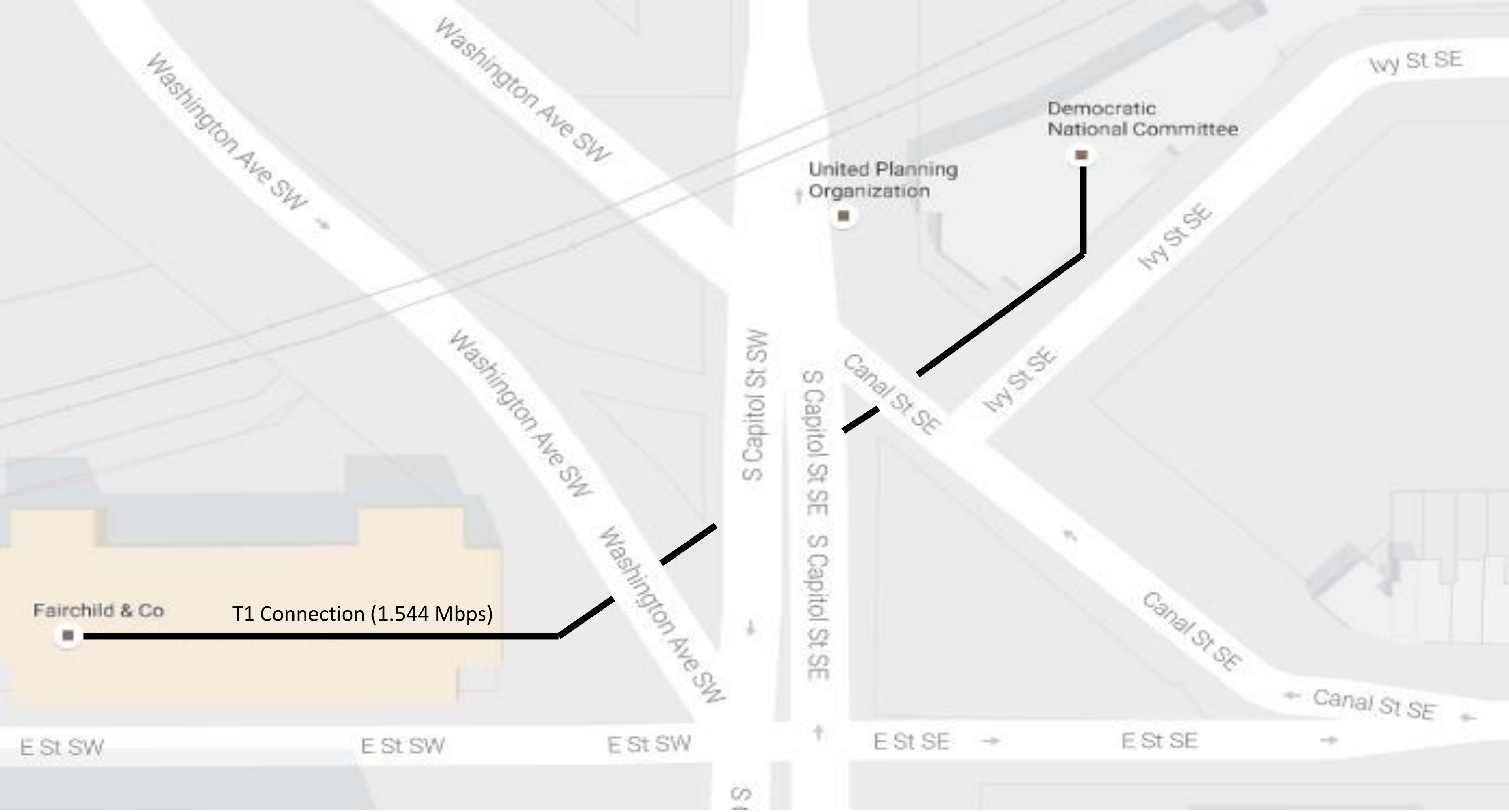


Developing an Updated Attribute Model

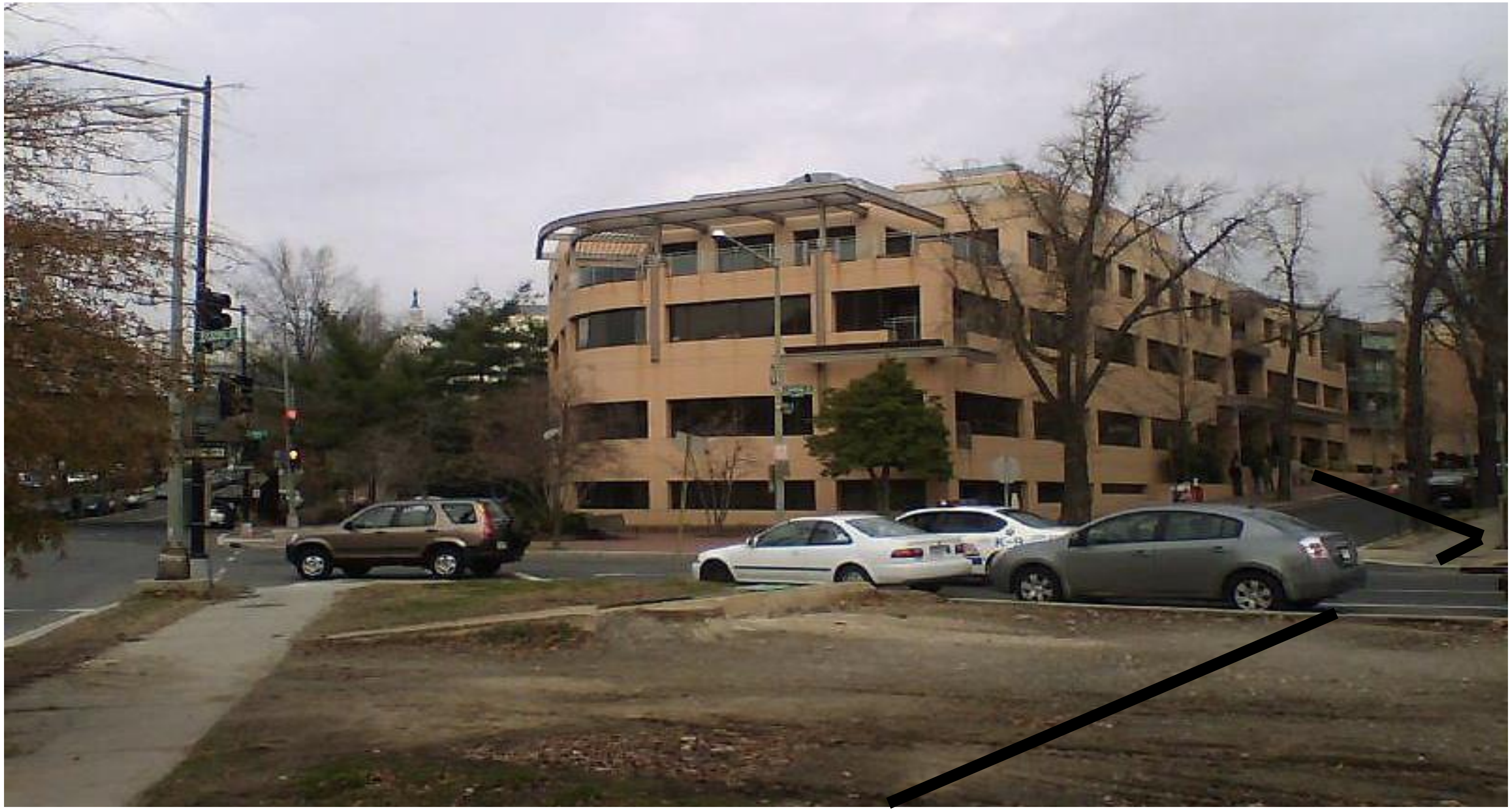
Original Clinton Campaign Fears About Email Security

1996 Presidential Race

DNC Headquarters and Fairchild Building



Dirt Patch Over T1



Hacking a Router

Step 1: Boot the router and interrupt

```
Press Ctrl-B
>
```

Step 2: Change config reg to ignore NVRAM

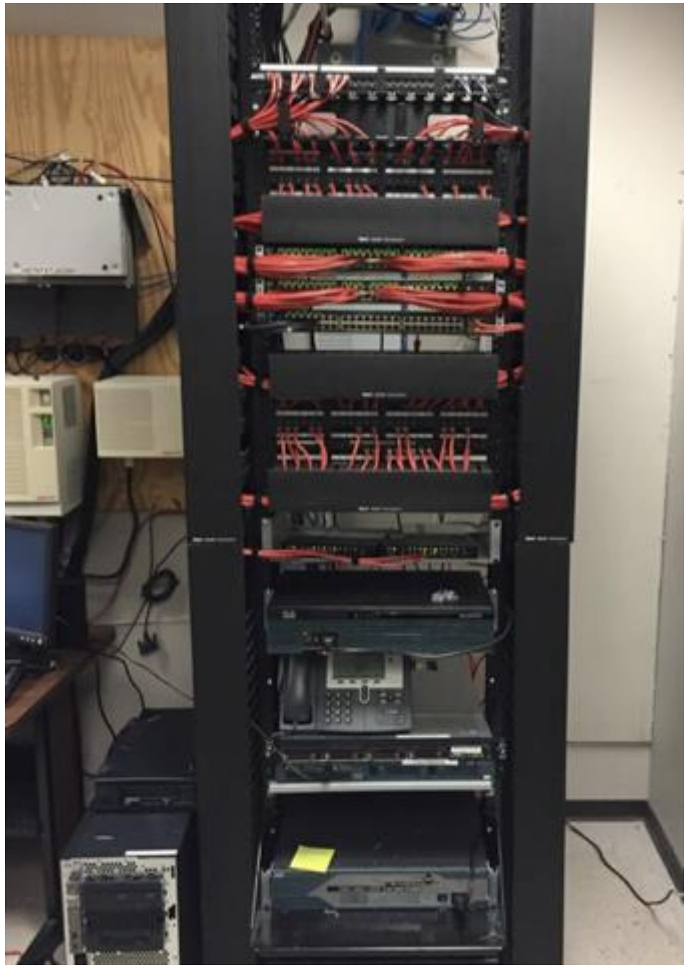
```
>o/r 0x2142
>
```

Step 3: Jump to privileged mode

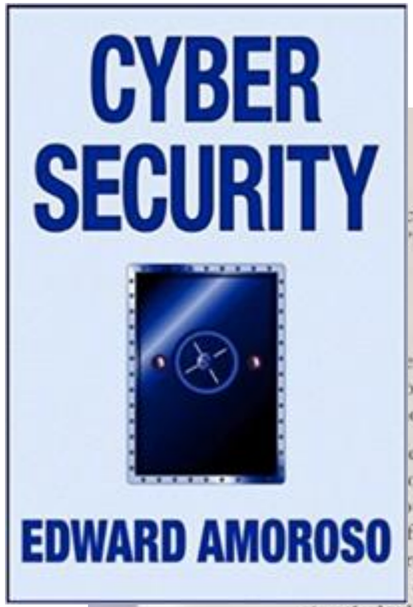
```
Router>enable
Router#
```

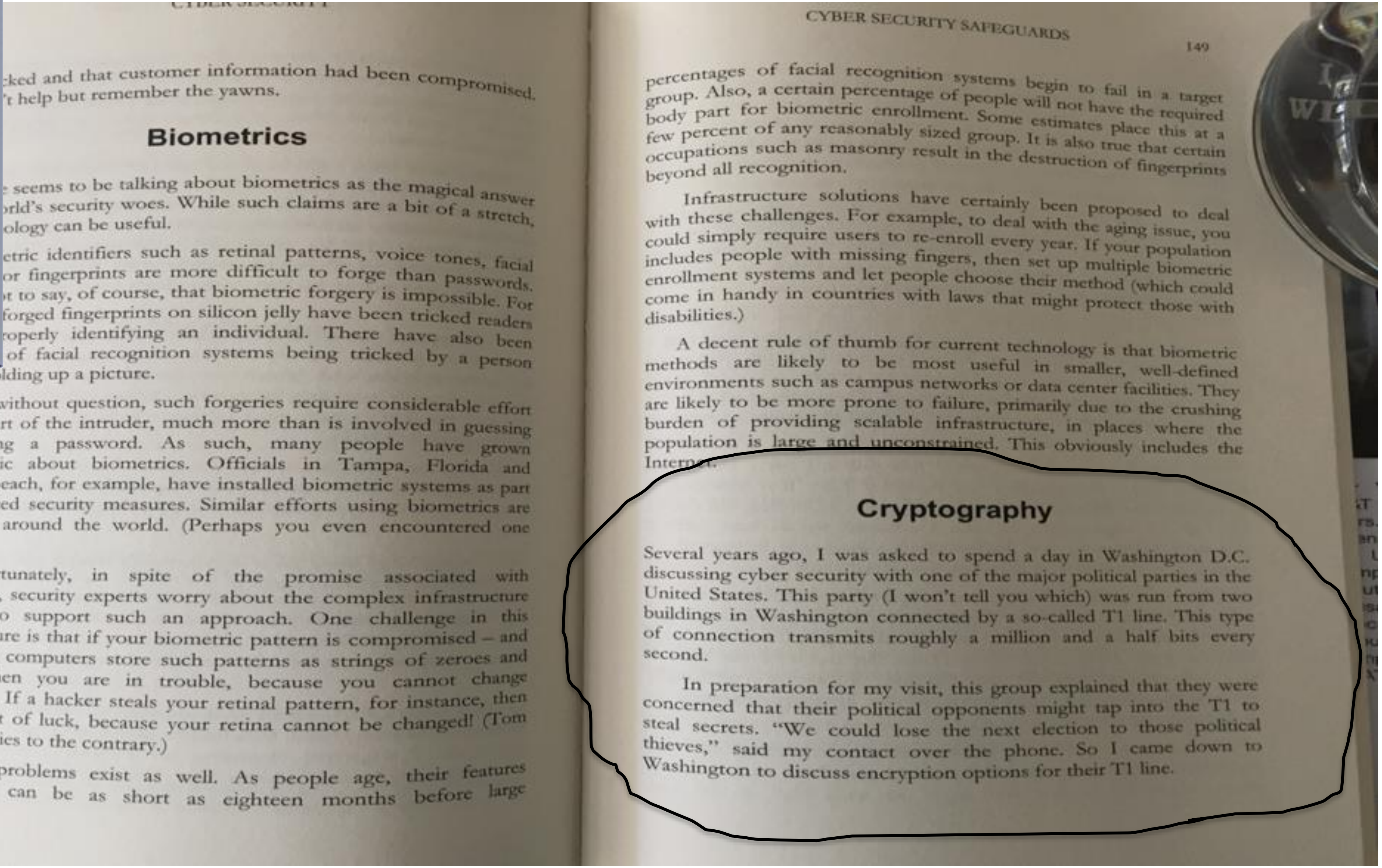
Step 4: Copy startup config to run config

```
. . .<output cut>. . .
#
```



This Really Happened . . .





cked and that customer information had been compromised. 't help but remember the yawns.

Biometrics

seems to be talking about biometrics as the magical answer orld's security woes. While such claims are a bit of a stretch, ology can be useful.

etric identifiers such as retinal patterns, voice tones, facial or fingerprints are more difficult to forge than passwords. t to say, of course, that biometric forgery is impossible. For forged fingerprints on silicon jelly have been tricked readers roperly identifying an individual. There have also been of facial recognition systems being tricked by a person simply holding up a picture.

But without question, such forgeries require considerable effort on the part of the intruder, much more than is involved in guessing or stealing a password. As such, many people have grown enthusiastic about biometrics. Officials in Tampa, Florida and Virginia Beach, for example, have installed biometric systems as part of enhanced security measures. Similar efforts using biometrics are on going around the world. (Perhaps you even encountered one today.)

Unfortunately, in spite of the promise associated with biometrics, security experts worry about the complex infrastructure required to support such an approach. One challenge in this infrastructure is that if your biometric pattern is compromised – and remember, computers store such patterns as strings of zeroes and ones – then you are in trouble, because you cannot change biometrics. If a hacker steals your retinal pattern, for instance, then you are out of luck, because your retina cannot be changed! (Tom Cruise movies to the contrary.)

Other problems exist as well. As people age, their features change. It can be as short as eighteen months before large

percentages of facial recognition systems begin to fail in a target group. Also, a certain percentage of people will not have the required body part for biometric enrollment. Some estimates place this at a few percent of any reasonably sized group. It is also true that certain occupations such as masonry result in the destruction of fingerprints beyond all recognition.

Infrastructure solutions have certainly been proposed to deal with these challenges. For example, to deal with the aging issue, you could simply require users to re-enroll every year. If your population includes people with missing fingers, then set up multiple biometric enrollment systems and let people choose their method (which could come in handy in countries with laws that might protect those with disabilities.)

A decent rule of thumb for current technology is that biometric methods are likely to be most useful in smaller, well-defined environments such as campus networks or data center facilities. They are likely to be more prone to failure, primarily due to the crushing burden of providing scalable infrastructure, in places where the population is large and unconstrained. This obviously includes the Internet.

Cryptography

Several years ago, I was asked to spend a day in Washington D.C. discussing cyber security with one of the major political parties in the United States. This party (I won't tell you which) was run from two buildings in Washington connected by a so-called T1 line. This type of connection transmits roughly a million and a half bits every second.

In preparation for my visit, this group explained that they were concerned that their political opponents might tap into the T1 to steal secrets. "We could lose the next election to those political thieves," said my contact over the phone. So I came down to Washington to discuss encryption options for their T1 line.

Questions?

ega1@nyu.edu
eamoroso@tag-cyber.com