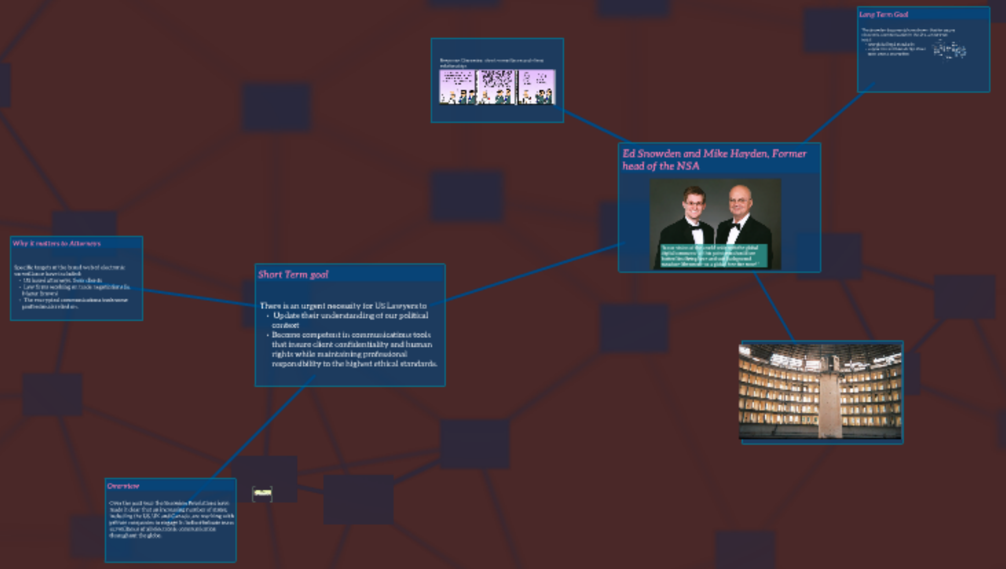


Ed Snowden and Mike Hayden, Former head of the NSA

Short Term goal

There is an urgent necessity for US Lawyers to
- Update their understanding of our political context
- Become competent in communications tools that insure client confidentiality and human rights while maintaining professional responsibility to the highest ethical standards.

Cybersecurity CLE

Constitutional Communications - Concomms.org

What is Mass Surveillance:

The UN defines “mass surveillance” as a situation in which “states with high levels of Internet penetration can...gain access to the telephone and e-mail content of an effectively unlimited number of users and maintain an overview of Internet activity associated with particular websites.”

The UN reports that in a system of “mass surveillance, all of this is possible without any prior suspicion related to a specific individual or organization.”

Why it matters to Attorneys

Specific targets of the broad web of electronic surveillance have included:

- US based attorneys, their clients
- Law firms working on trade negotiations (ie. Mayer Brown)
- The encrypted communications tools some professionals relied on.

Current NSA impacts:

- The NSA Targets Muslim-American leaders for intensive FISA Surveillance, including:
  - Attorney Faisal Gill, a longtime Republican Party operative who served in the DHS under Bush
  - Nihad Awad, the executive director of the Council on American-Islamic Relations (CAIR)

How the NSA intercepts are currently being used in domestic drug prosecutions:

- **One current federal prosecutor told Reuters that in a Florida drug case he was handling, a DEA agent lied and told him the investigation of a U.S. citizen began with a tip from an informant.**
- **But the investigation actually began with NSA intercepts.**

- The NSA works with a $125 million unit of DEA that is called the Special Operations Division, or SOD.

- Two dozen partner agencies and several hundred employees comprise the unit, including FBI, CIA, NSA, Internal Revenue Service and the Department of Homeland Security.

- SOD uses "parallel construction" to re- engineer US criminal cases to remove evidence of electronic monitoring.

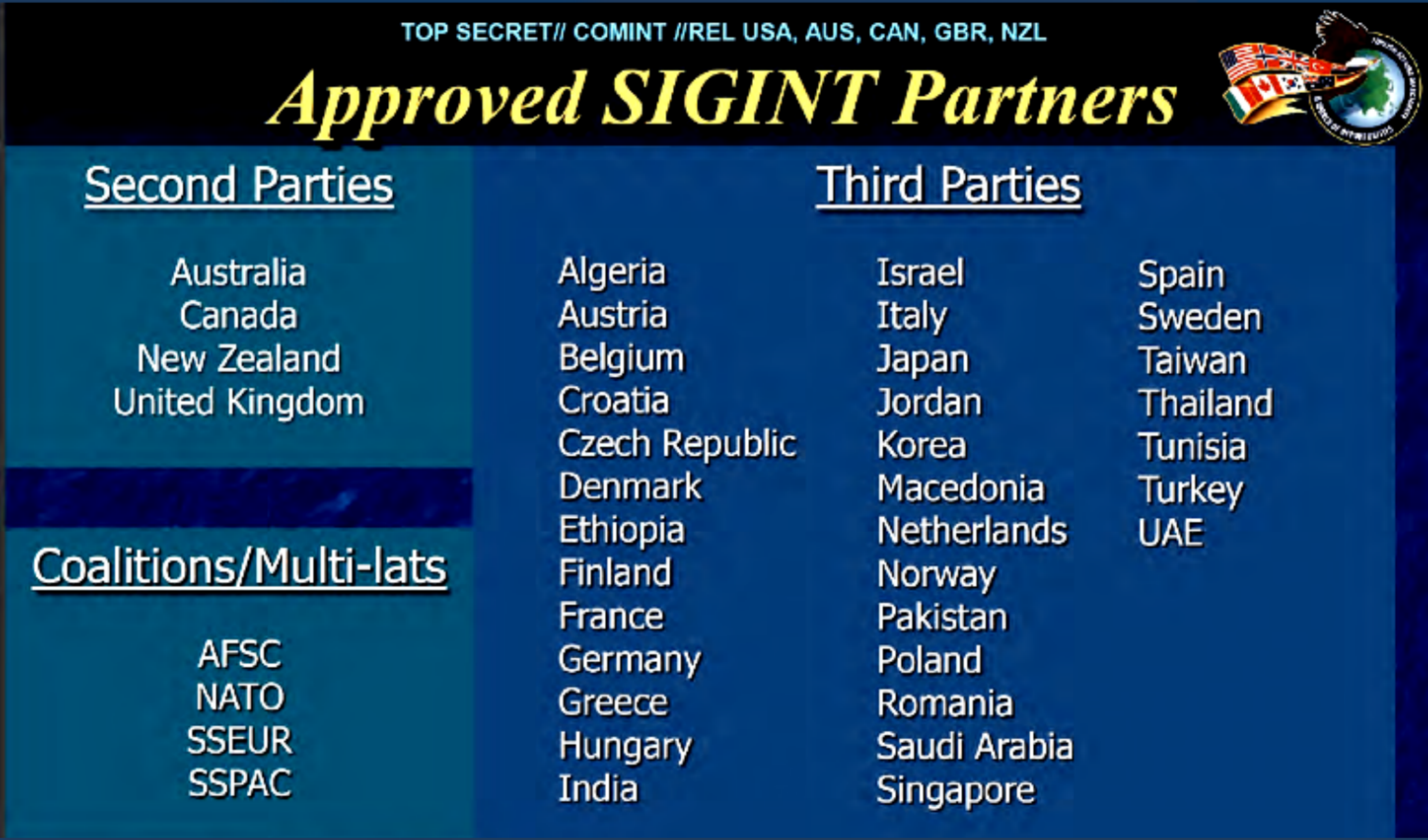
The Who: What do these 5 countries have in common?

The US, UK, Canada, New Zealand, and Australia

Answer!

They are all:

- Britain or former British colonies,
- White english-speaking majorities and power structures.
- All of the intelligence agencies were in tight coordination in WWII and
- They are all part of the FIVE EYES!!



TOP SECRET// COMINT //REL USA, AUS, CAN, GBR, NZL

Approved SIGINT Partners

Second Parties

Australia
Canada
New Zealand
United Kingdom

Coalitions/Multi-lats

AFSC
NATO
SSEUR
SSPAC

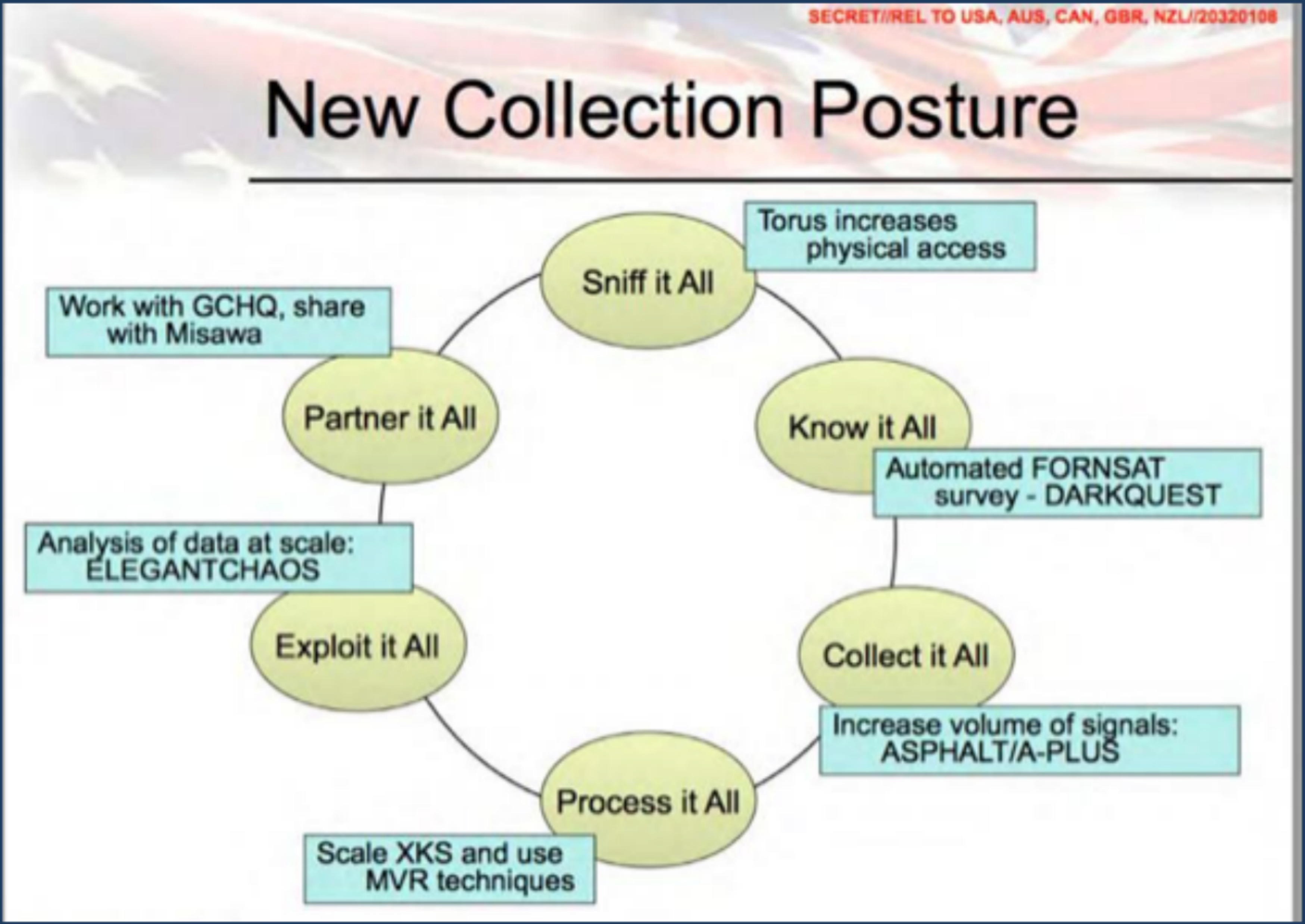
Third Parties

Algeria
Austria
Belgium
Croatia
Czech Republic
Denmark
Ethiopia
Finland
France
Germany
Greece
Hungary
India

Israel
Italy
Japan
Jordan
Korea
Macedonia
Netherlands
Norway
Pakistan
Poland
Romania
Saudi Arabia
Singapore

Spain
Sweden
Taiwan
Thailand
Tunisia
Turkey
UAE

From 2011 Five Eye Conference:



SECRET//REL TO USA, AUS, CAN, GBR, NZL//20320108

New Collection Posture

Sniff it All

Torus increases physical access

Know it All

Automated FORNSAT survey - DARKQUEST

Collect it All

Increase volume of signals: ASPHALT/A-PLUS

Process it All

Scale XKS and use MVR techniques

Exploit it All

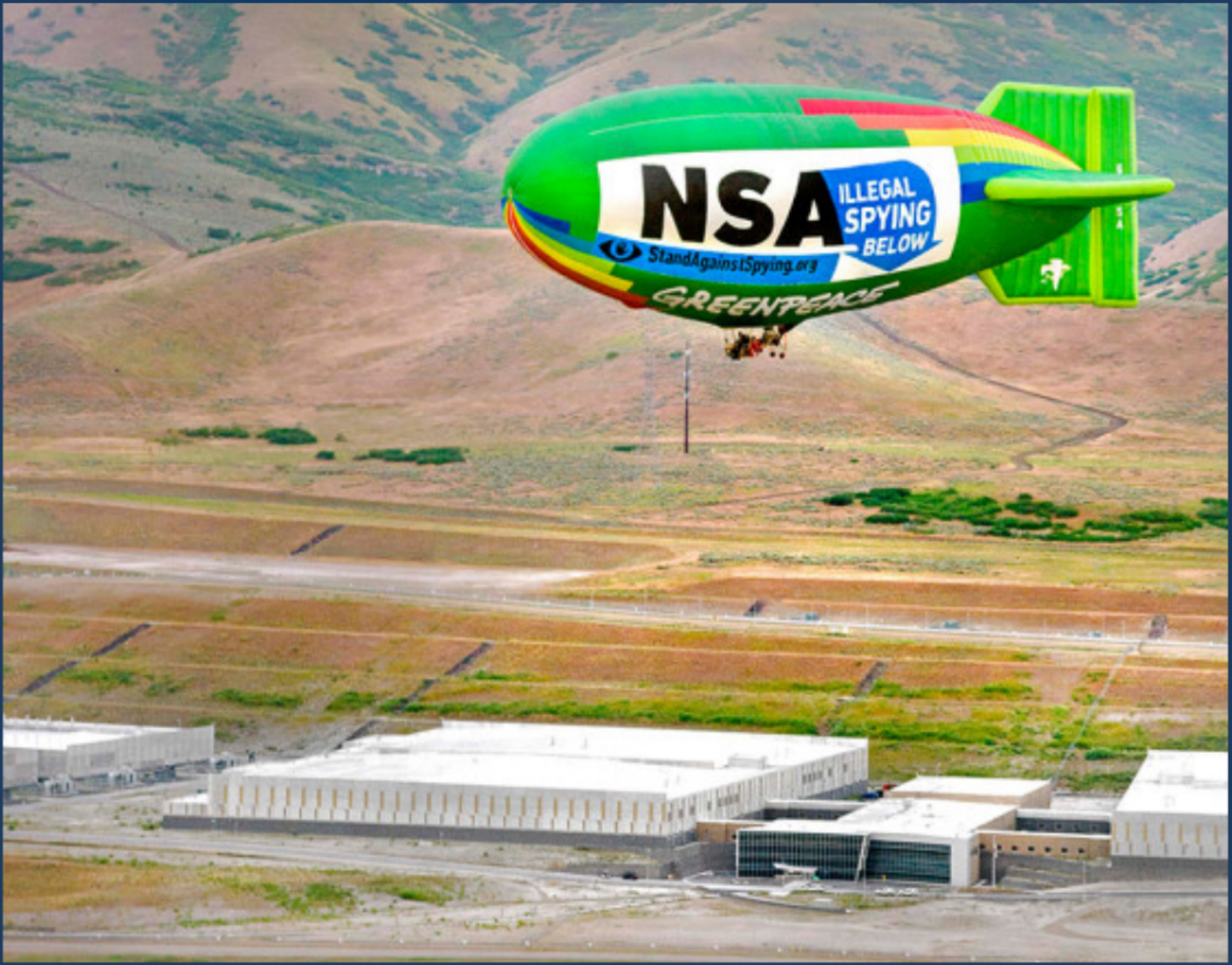
Analysis of data at scale: ELEGANTCHAOS

Partner it All

Work with GCHQ, share with Misawa

But how can they technically collect and sort all that information?

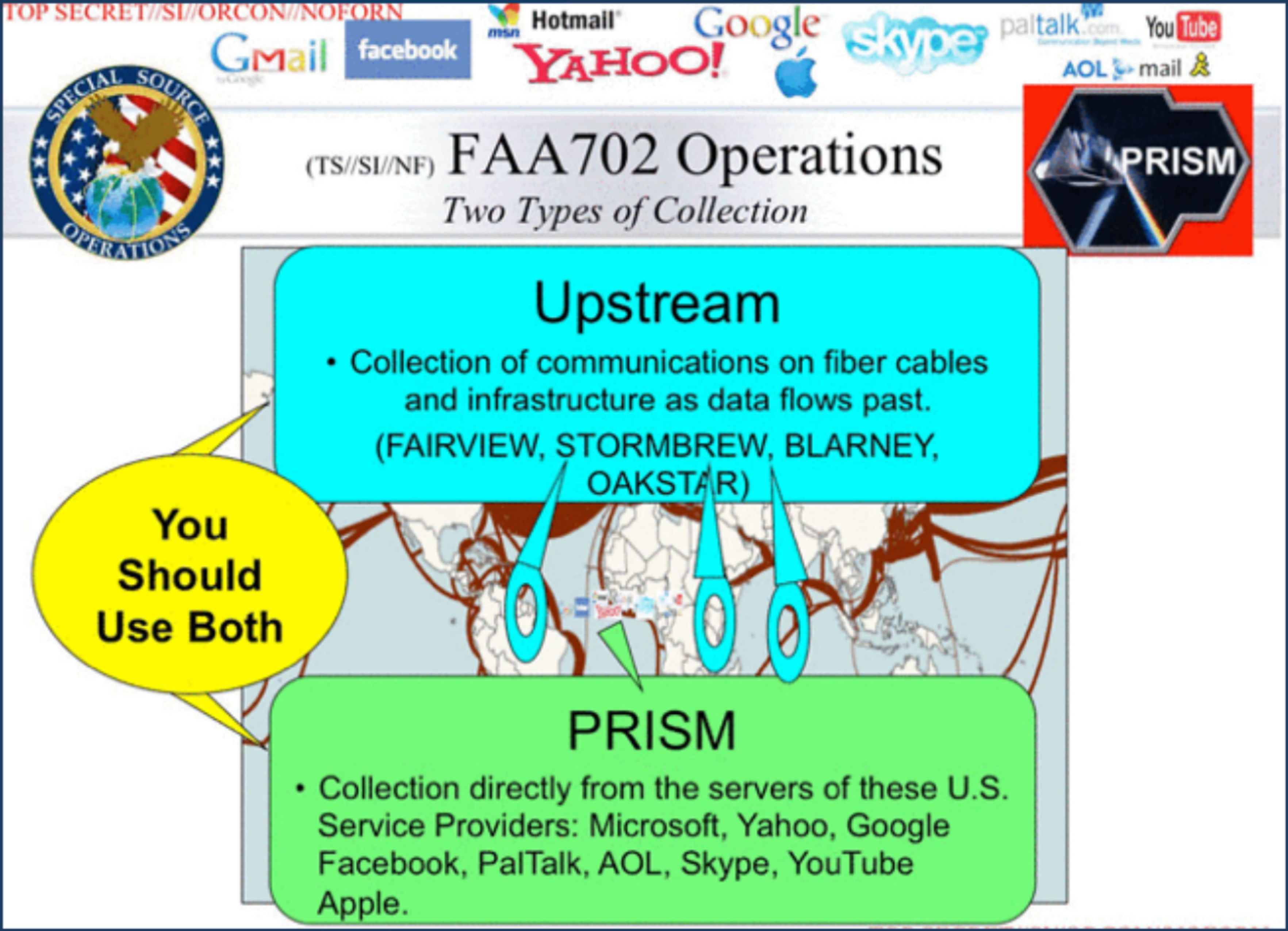
Bluffsdale, Utah NSA Data-center (2013) Designed to hold a Yottabyte of data



That is a lot of data collection!

- A Yottabyte is the biggest data metric that has been defined.
- It is 1000X more data then the whole Internet will be in 2015

Where are they getting the all that data from?



TOP SECRET//SI//ORCON//NOFORN

(TS//SI//NF) FAA702 Operations

Two Types of Collection

Upstream

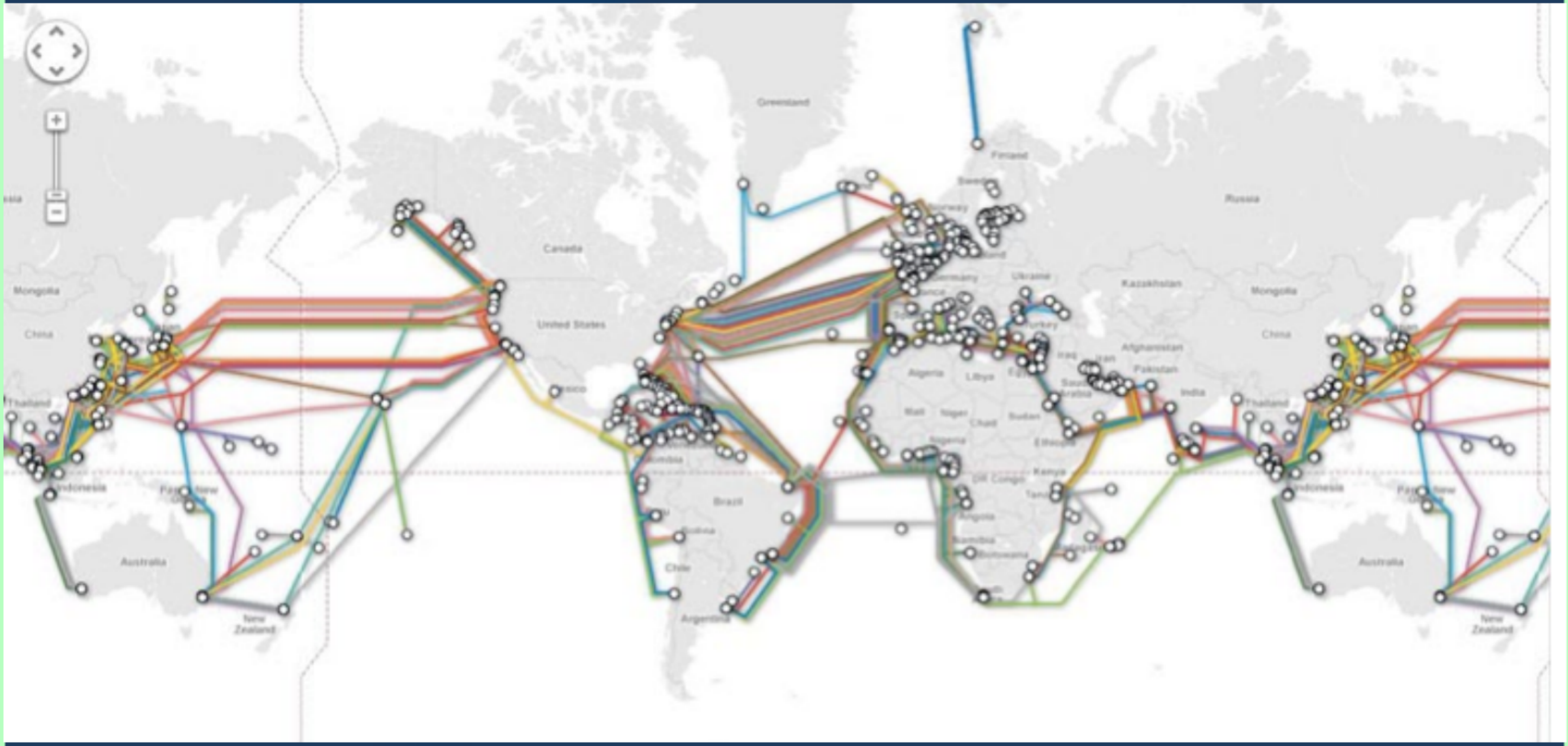
- Collection of communications on fiber cables and infrastructure as data flows past. (FAIRVIEW, STORMBREW, BLARNEY, OAKSTAR)

You Should Use Both

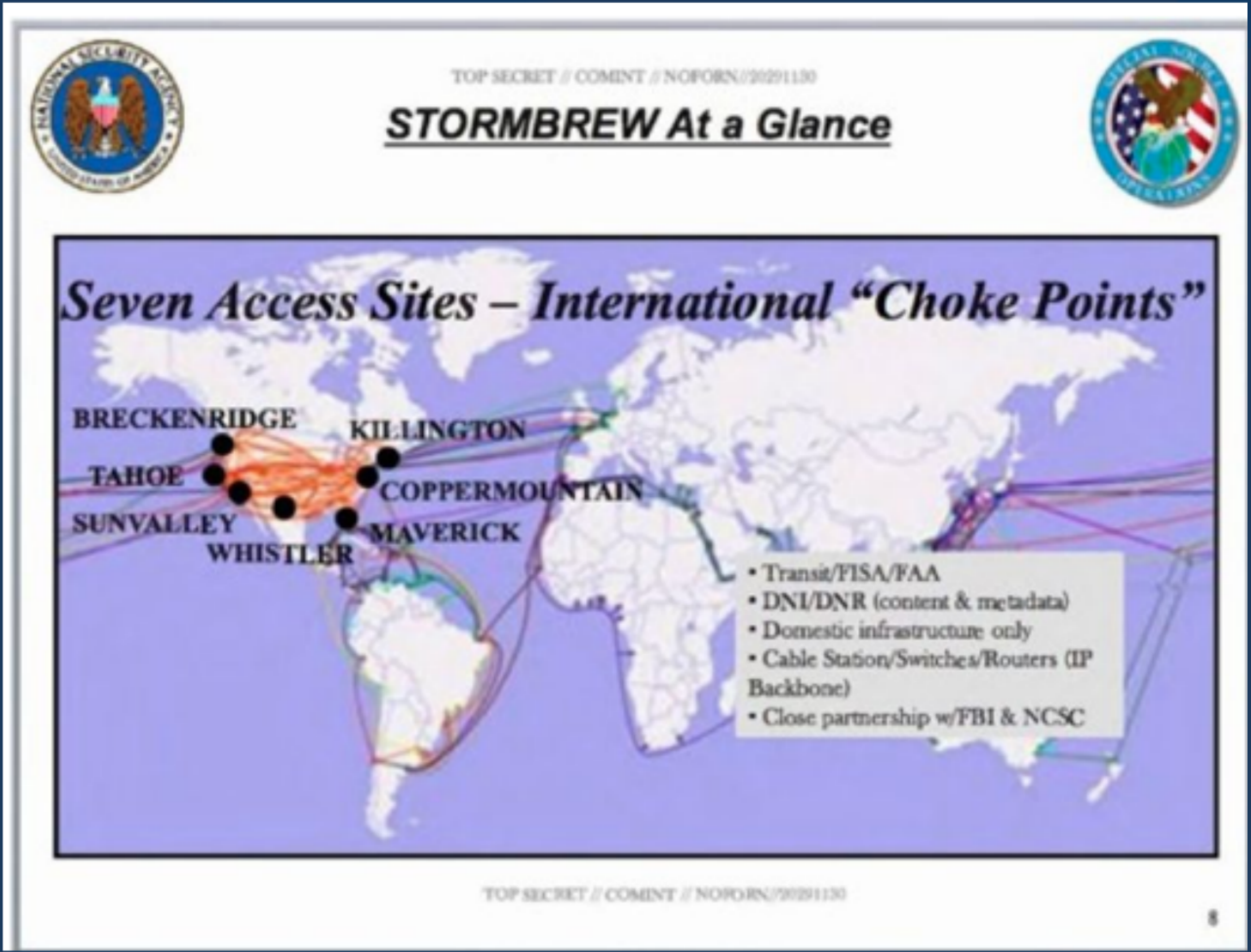
PRISM

- Collection directly from the servers of these U.S. Service Providers: Microsoft, Yahoo, Google Facebook, PalTalk, AOL, Skype, YouTube Apple.

Undersea cables pass through the "five eyes" and can collect most internet traffic



How they tap the whole Internet:



TOP SECRET // COMINT // NOFORN//20291130

STORMBREW At a Glance

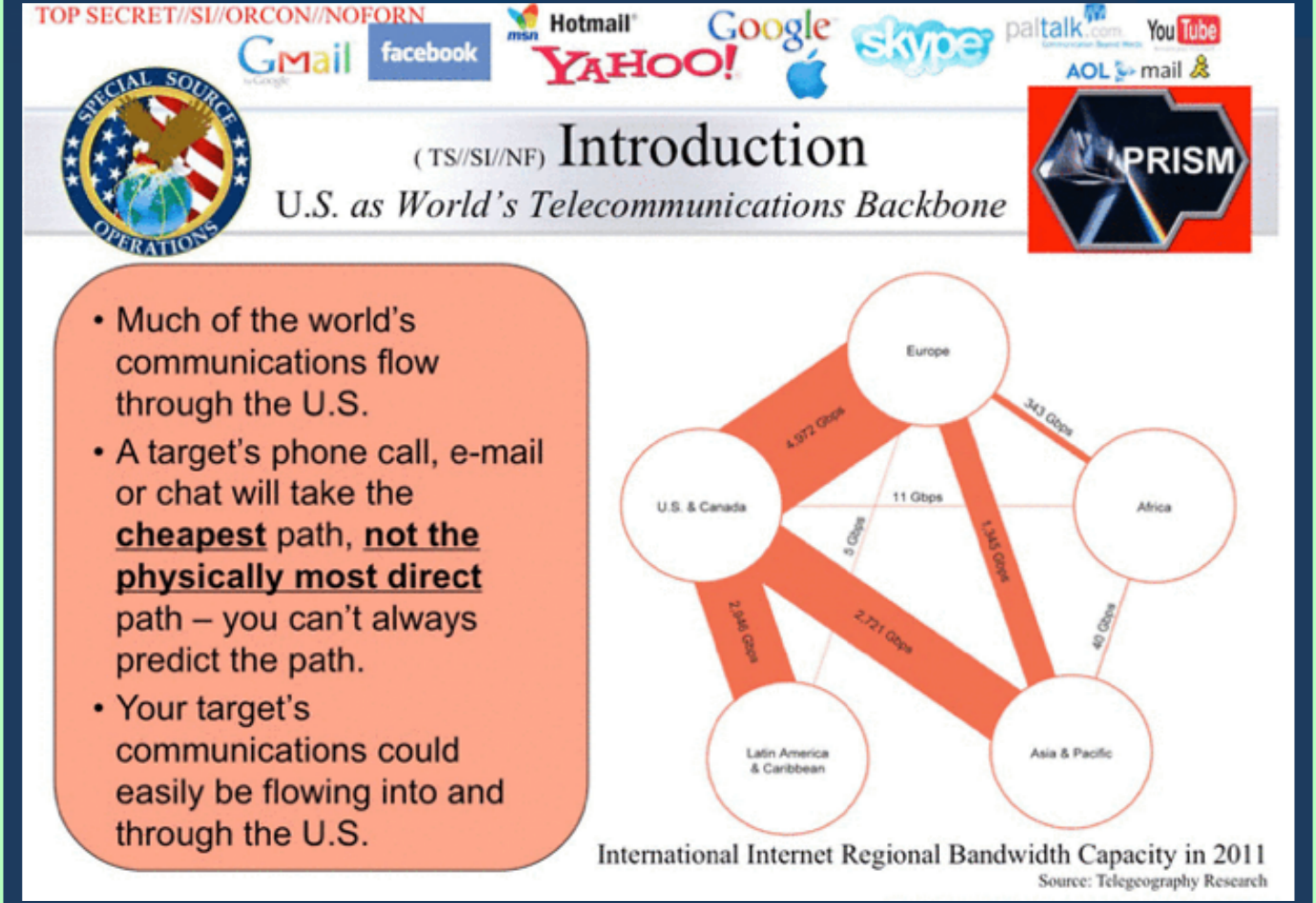
Seven Access Sites – International "Choke Points"

- Transit/FISA/FAA
- DNI/DNR (content & metadata)
- Domestic infrastructure only
- Cable Station/Switches/Routers (IP Backbone)
- Close partnership w/FBI & NCSC

TOP SECRET // COMINT // NOFORN//20291130

8

US: The worlds Telecomm backbone



TOP SECRET//SI//ORCON//NOFORN

(TS//SI//NF) Introduction

U.S. as World's Telecommunications Backbone

- Much of the world's communications flow through the U.S.
- A target's phone call, e-mail or chat will take the **cheapest** path, **not the physically most direct** path – you can't always predict the path.
- Your target's communications could easily be flowing into and through the U.S.

International Internet Regional Bandwidth Capacity in 2011

Source: Telegeography Research

Three technical areas of concern.
How IT technology works:

a) Content of communications: The "WHAT"
Written emails, posts and texts.

b) Metadata: The "WHO" And the "WHEN"

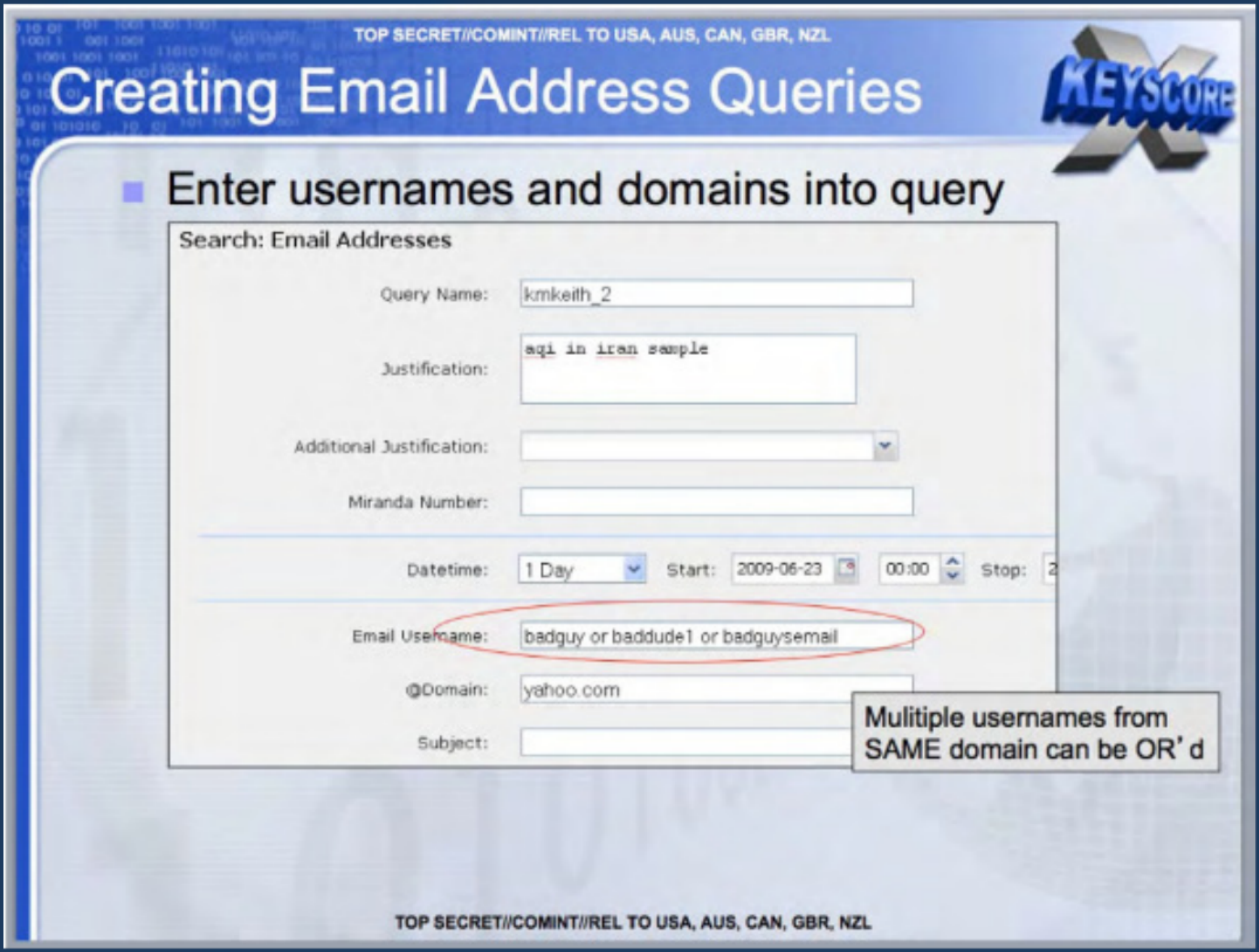
Its the fingerprint of every electronic interaction and allows for the simple creation of a social network of relationships.

c) Geolocation data: The "WHERE"

To get a signal for calls, cell phone networks constantly track the movement of the phone.

Each Computer has an address which is the individual machine and location or network of use.

Its like a Google search for all content:



TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

Creating Email Address Queries

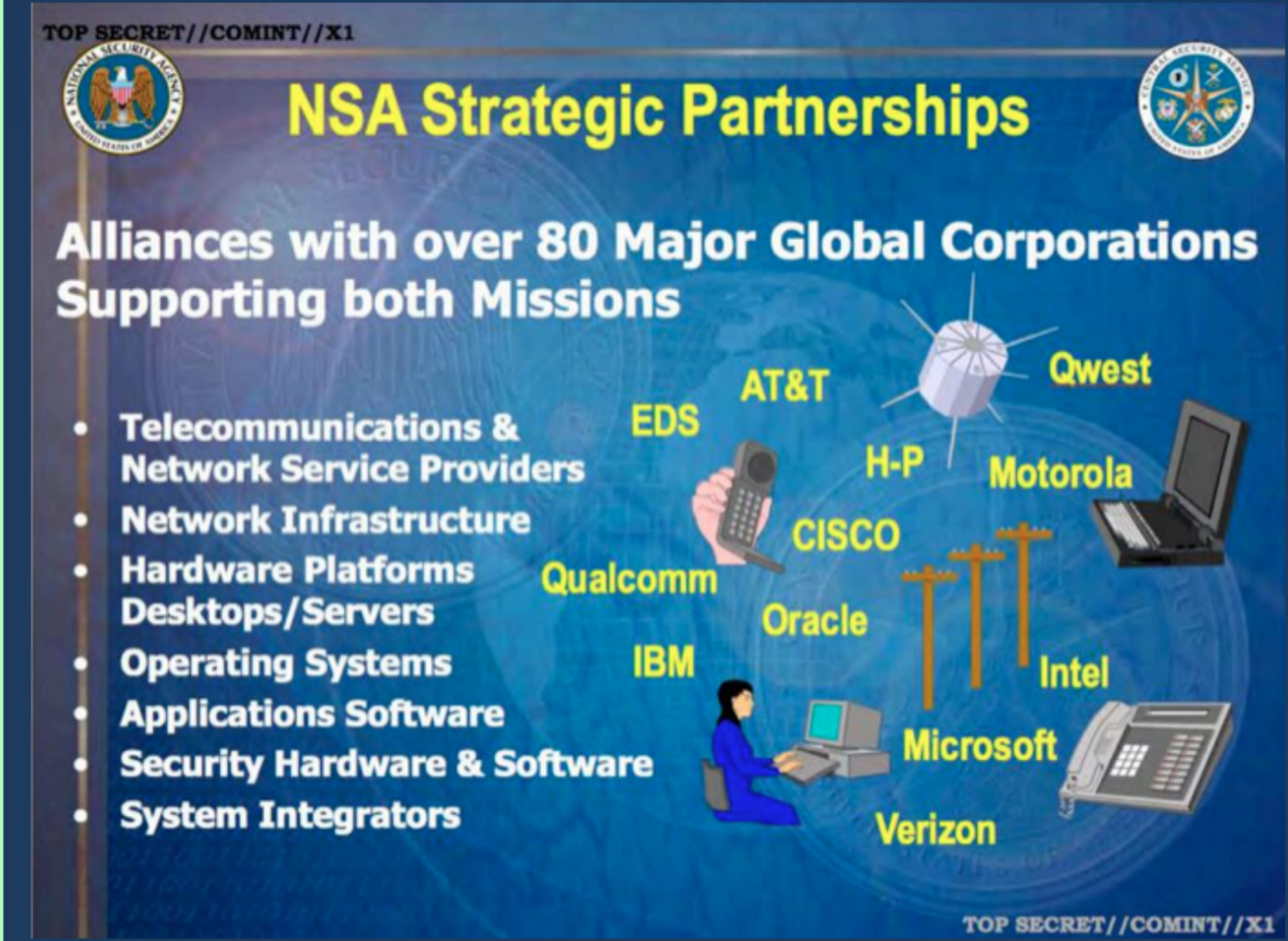
- Enter usernames and domains into query

Search: Email Addresses

Query Name:	kmkeith_2
Justification:	aqi in iran sample
Additional Justification:	
Miranda Number:	
Datetime:	1 Day Start: 2009-06-23 00:00 Stop: 2
Email Username:	badguy or baddude1 or badguysemail
@Domain:	yahoo.com
Subject:	

Mulitiple usernames from SAME domain can be OR'd

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL



TOP SECRET//COMINT//X1

NSA Strategic Partnerships

Alliances with over 80 Major Global Corporations Supporting both Missions

- Telecommunications & Network Service Providers
- Network Infrastructure
- Hardware Platforms Desktops/Servers
- Operating Systems
- Applications Software
- Security Hardware & Software
- System Integrators

AT&T

Qwest

EDS

H-P

Motorola

CISCO

Qualcomm

Oracle

IBM

Intel

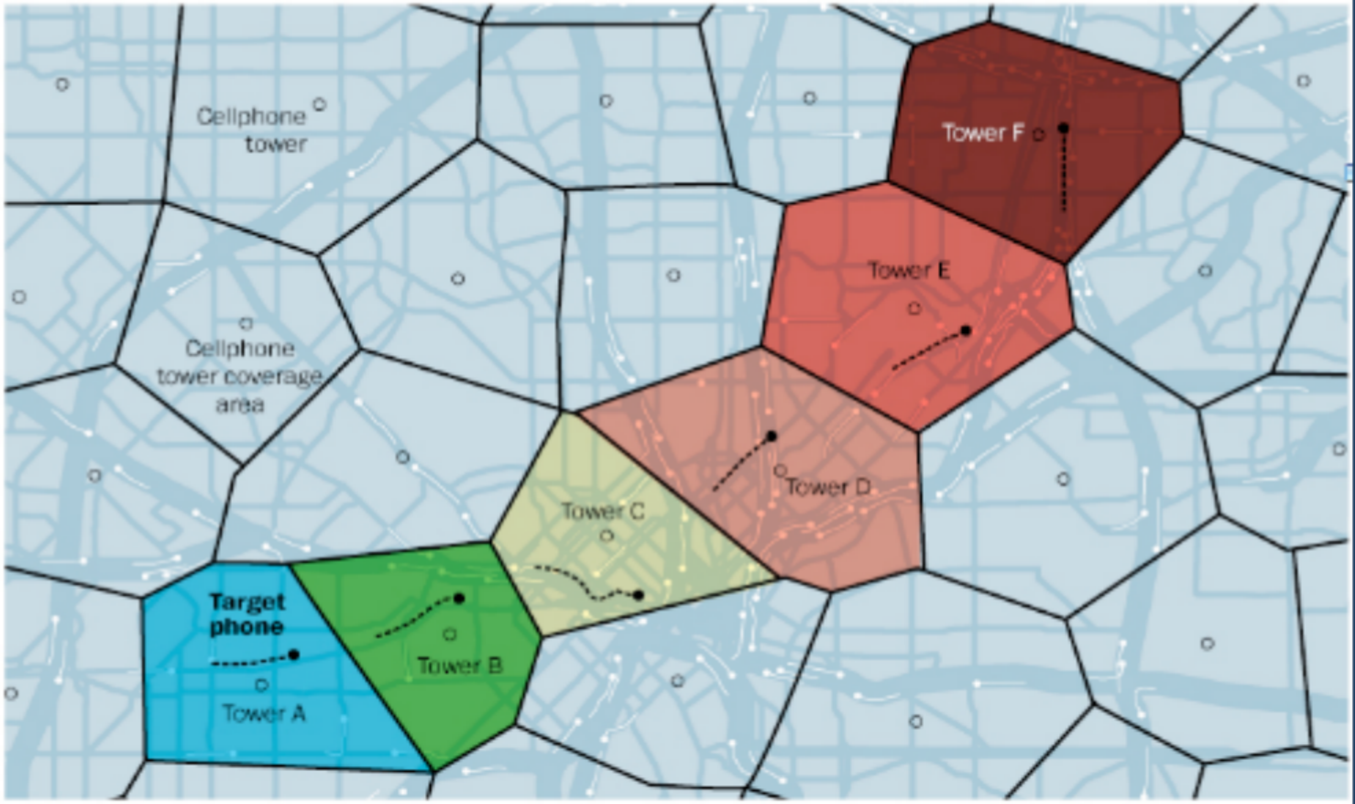
Microsoft

Verizon

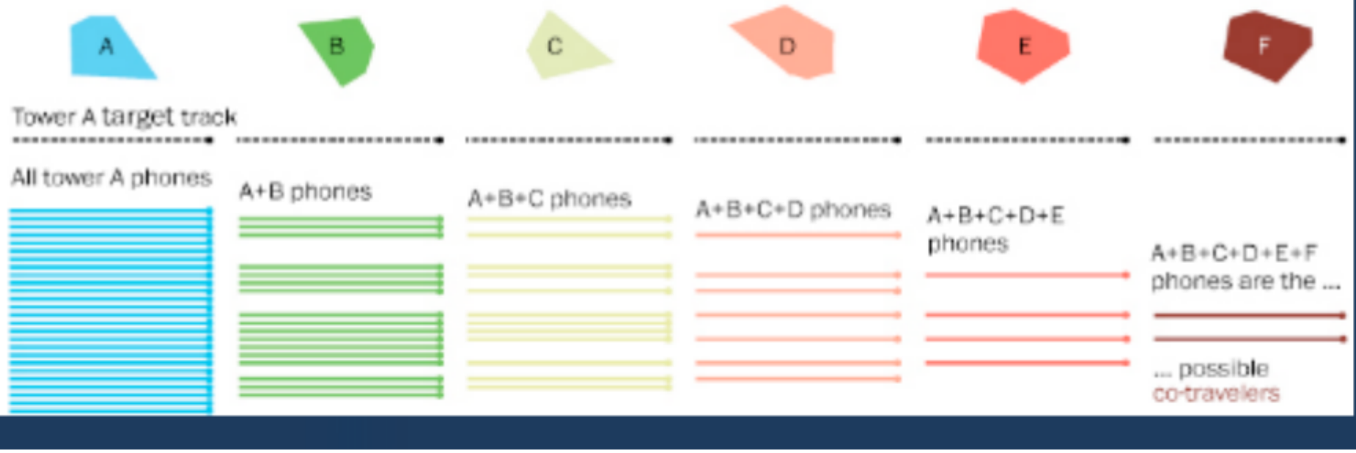
TOP SECRET//COMINT//X1

- NSA is tracking most cell phone movement globally. The info it is being used to show connections between people.

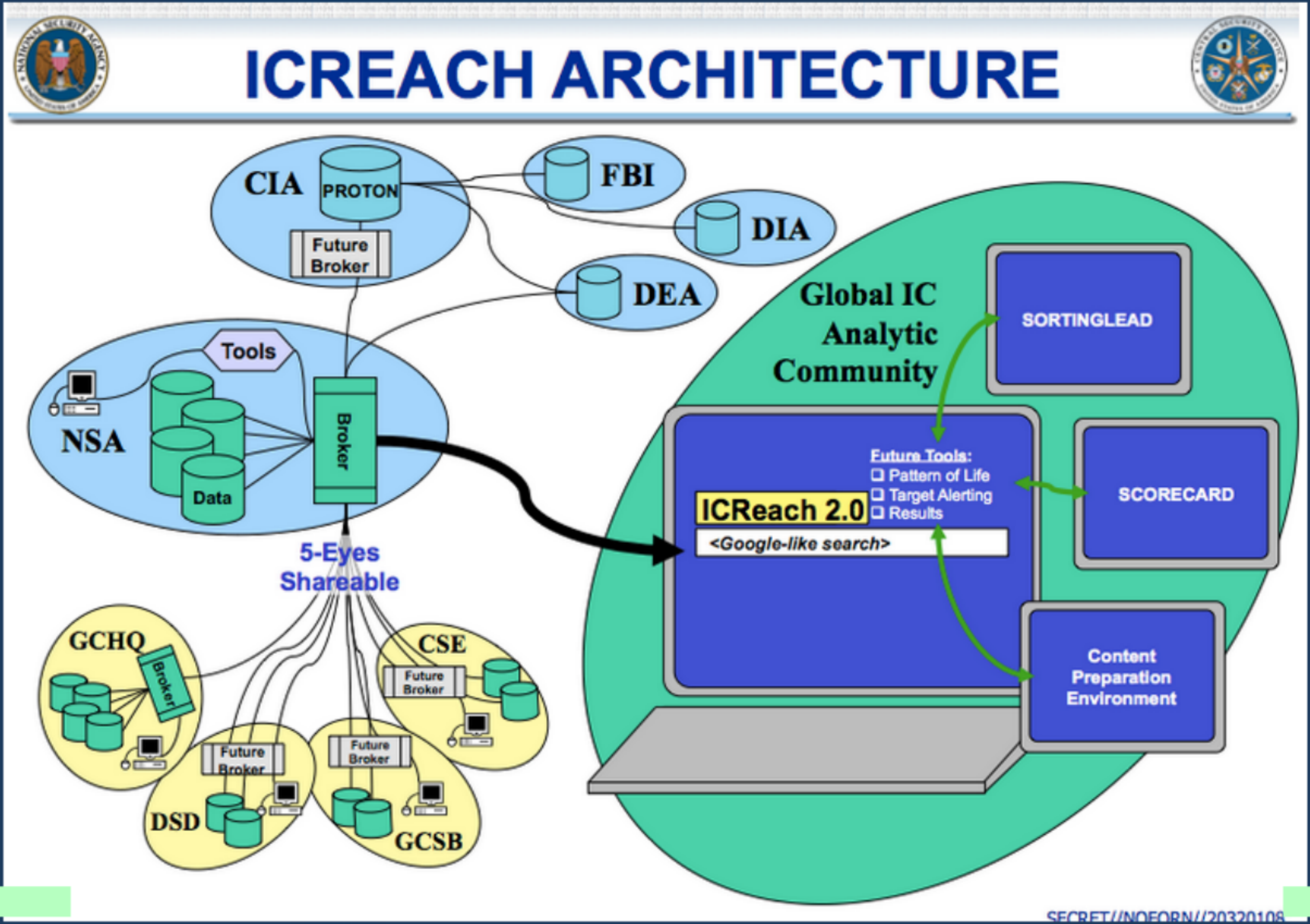
By tracking all phones within a cell tower area along with the target phone, co-travelers can be isolated.



As the target phone moves from tower to tower, fewer and fewer potential co-travelers remain.



Domestic uses of “google like” SOD metadata search through Five Eyes data bases:

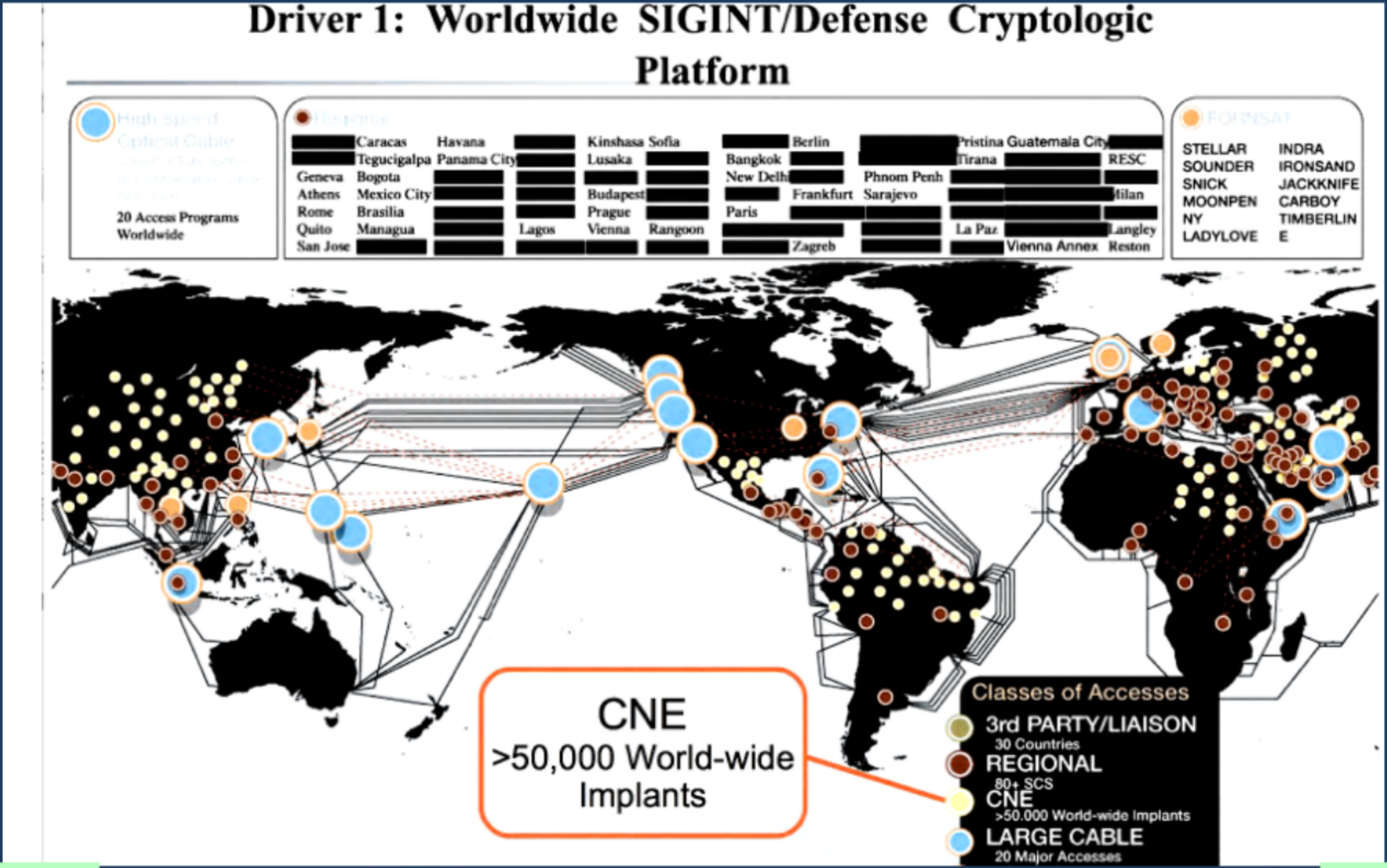


ICREACH ARCHITECTURE

SECRET//NOFORN//20320108

NSA installs surveillance programs onto between 50,000 and 100,000 computers globally.

Red dots are CNE keylogging malware



Driver 1: Worldwide SIGINT/Defense Cryptologic Platform

● High Speed Optical Cable
[illegible]
20 Access Programs Worldwide

● Regional

[redacted] Caracas Havana [redacted] Kinshasa Sofia [redacted] Berlin [redacted] Pristina Guatemala City [redacted]
[redacted] Tegucigalpa Panama City [redacted] Lusaka [redacted] Bangkok [redacted] [redacted] Tirana [redacted] RESC
Geneva Bogota [redacted] [redacted] [redacted] [redacted] New Delhi [redacted] Phnom Penh [redacted] [redacted] [redacted]
Athens Mexico City [redacted] [redacted] Budapest [redacted] [redacted] Frankfurt Sarajevo [redacted] [redacted] Milan
Rome Brasilia [redacted] [redacted] Prague [redacted] Paris [redacted] [redacted] [redacted] [redacted] [redacted]
Quito Managua [redacted] Lagos Vienna Rangoon [redacted] [redacted] La Paz [redacted] Langley
San Jose [redacted] [redacted] [redacted] [redacted] [redacted] [redacted] Zagreb [redacted] [redacted] Vienna Annex Reston

● FORNSAT

STELLAR
SOUNDER
SNICK
MOONPEN
NY
LADYLOVE

INDRA
IRONSAND
JACKKNIFE
CARBOY
TIMBERLIN
E

CNE
>50,000 World-wide Implants

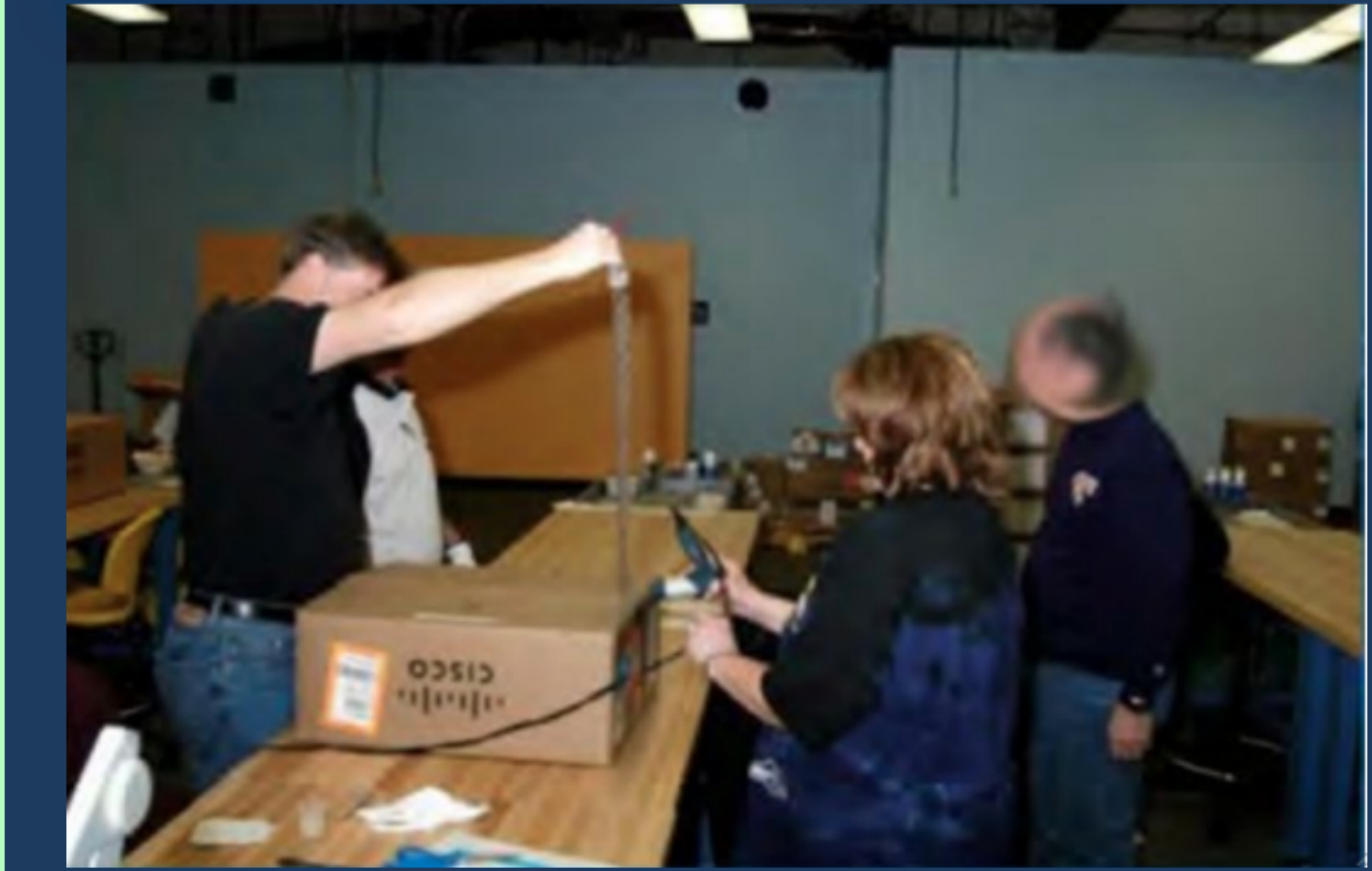
Classes of Accesses

- ● 3rd PARTY/LIAISON
  30 Countries
- ● REGIONAL
  80+ SCS
- ● CNE
  >50,000 World-wide Implants
- ● LARGE CABLE
  20 Major Accesses

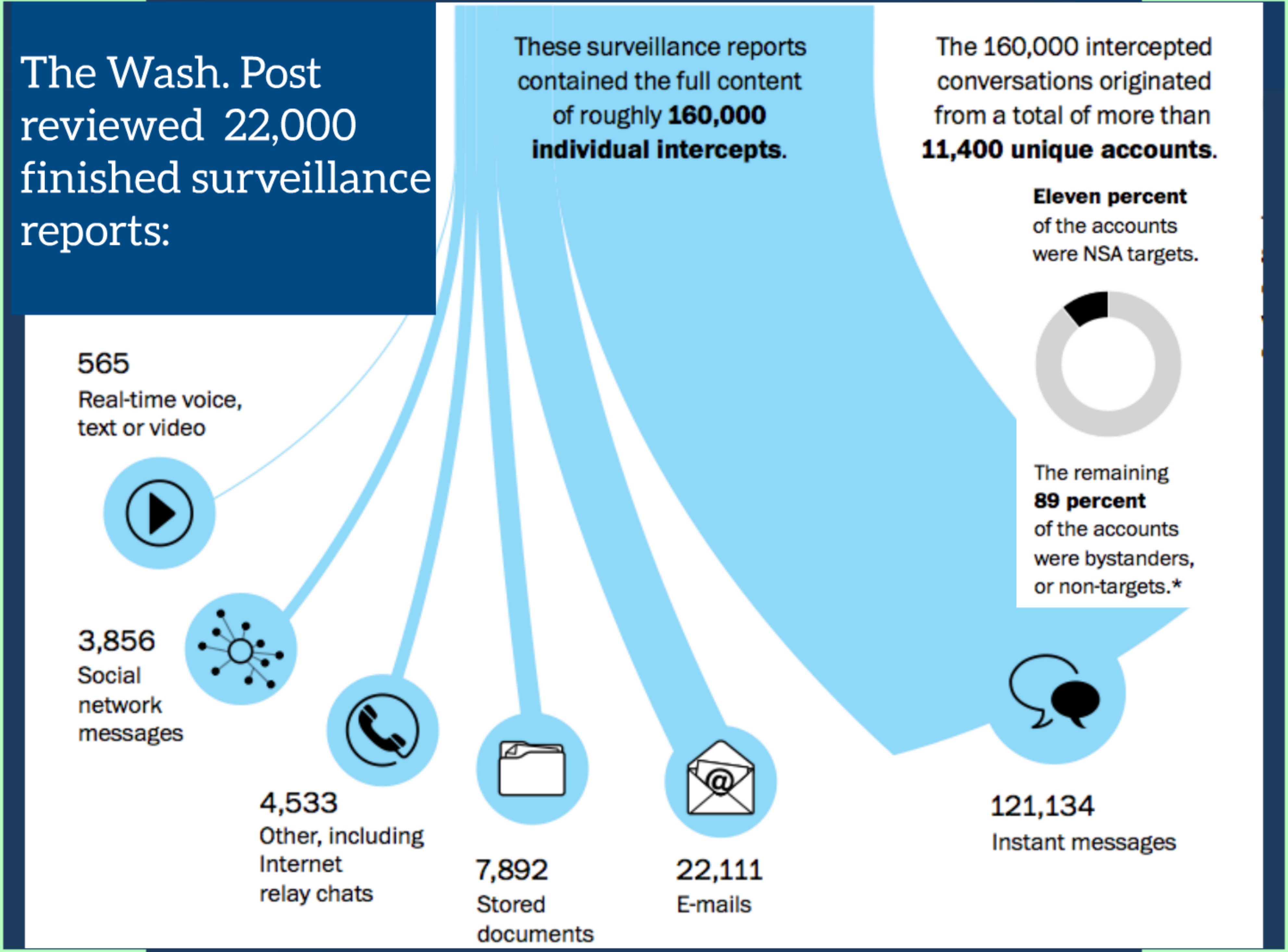
NSA and proprietary software vendors

Microsoft shares its software bugs with the NSA before releasing them to the public or anti-virus vendors

For some targets they use "package interception" to insert surveillance technology:



The Wash. Post reviewed 22,000 finished surveillance reports:



These surveillance reports contained the full content of roughly **160,000 individual intercepts.**

The 160,000 intercepted conversations originated from a total of more than **11,400 unique accounts.**

Eleven percent of the accounts were NSA targets.

The remaining **89 percent** of the accounts were bystanders, or non-targets.*

565
Real-time voice, text or video

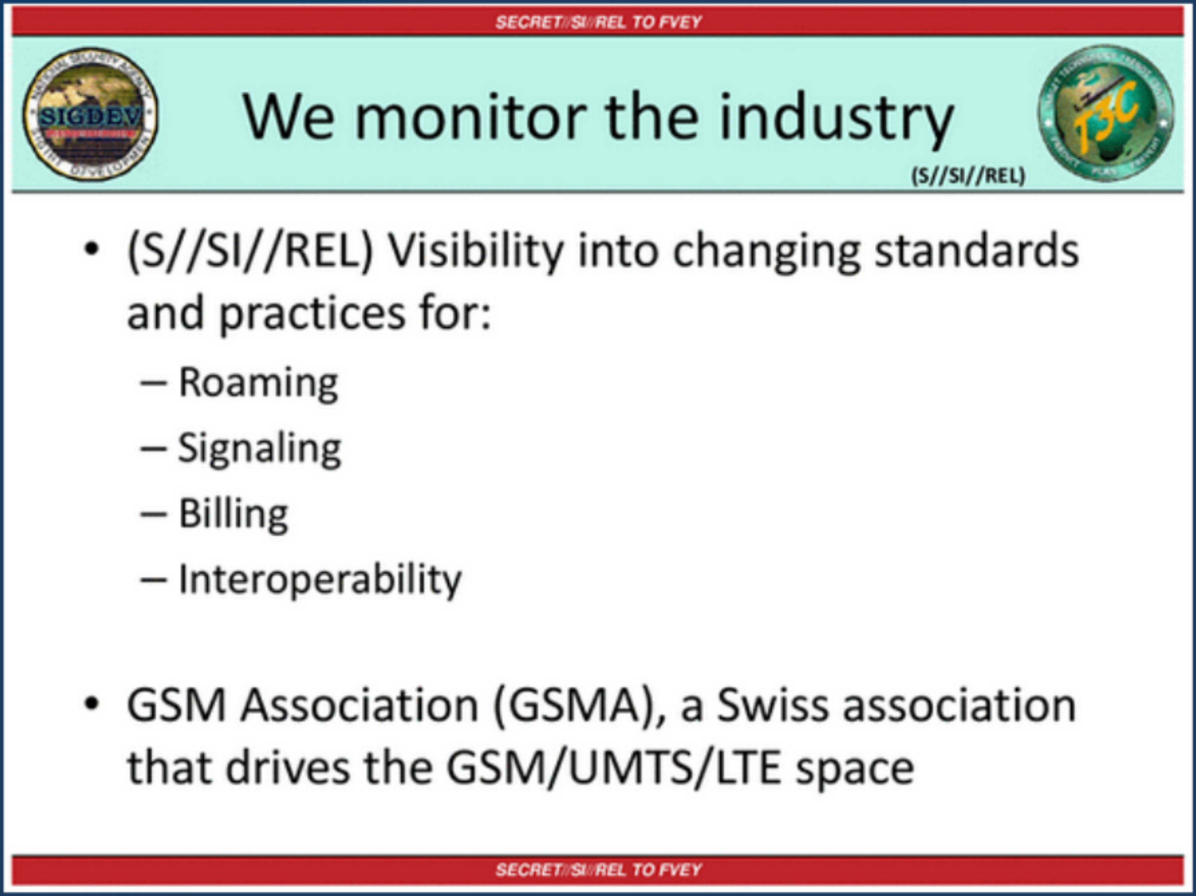
3,856
Social network messages

4,533
Other, including Internet relay chats

7,892
Stored documents

22,111
E-mails

121,134
Instant messages



SECRET//SI//REL TO FVEY

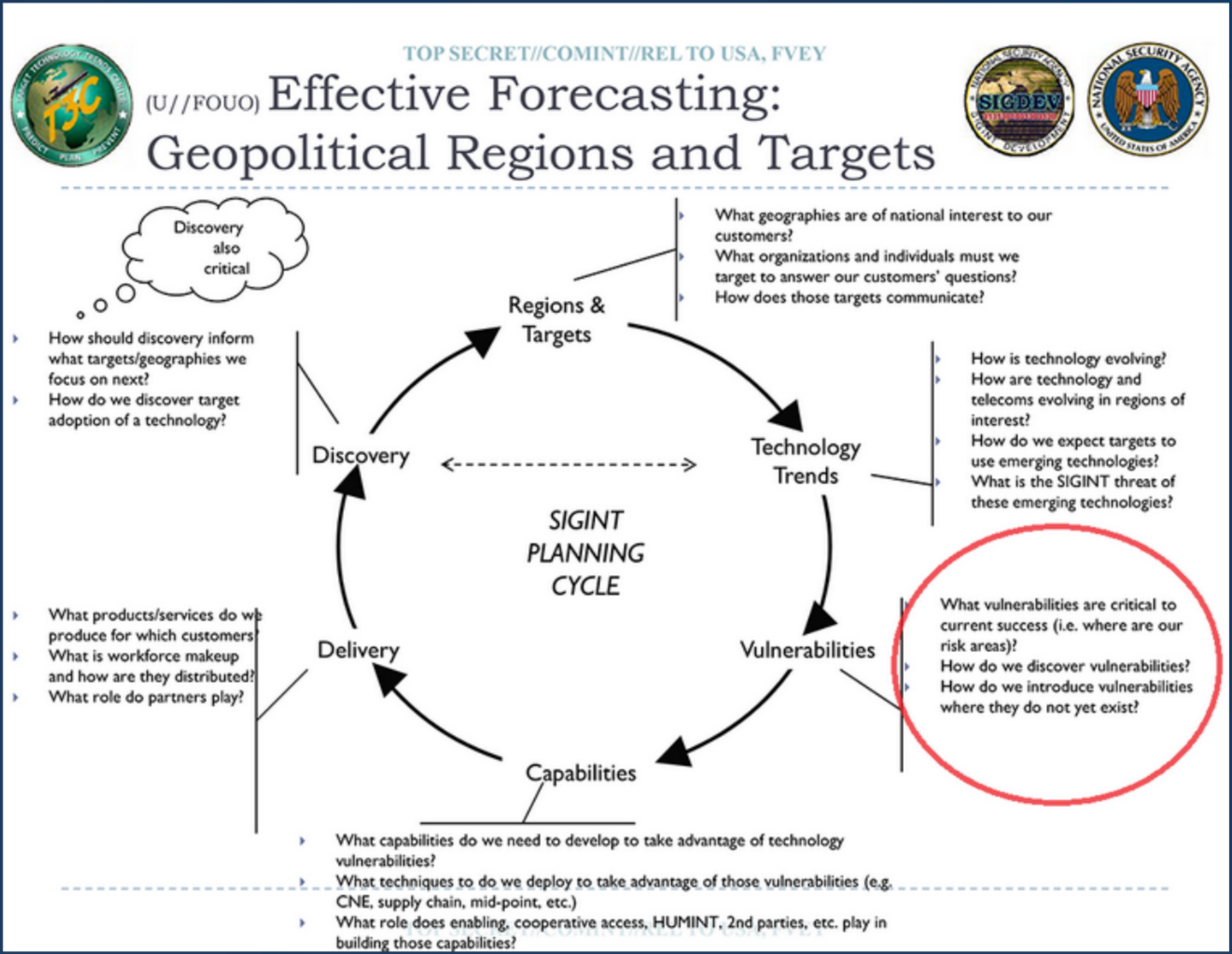
We monitor the industry

(S//SI//REL)

- (S//SI//REL) Visibility into changing standards and practices for:
  - Roaming
  - Signaling
  - Billing
  - Interoperability

- GSM Association (GSMA), a Swiss association that drives the GSM/UMTS/LTE space

SECRET//SI//REL TO FVEY



TOP SECRET//COMINT//REL TO USA, FVEY

(U//FOUO) Effective Forecasting: Geopolitical Regions and Targets

Discovery also critical

- How should discovery inform what targets/geographies we focus on next?
- How do we discover target adoption of a technology?

Regions & Targets

- What geographies are of national interest to our customers?
- What organizations and individuals must we target to answer our customers' questions?
- How does those targets communicate?

Technology Trends

- How is technology evolving?
- How are technology and telecoms evolving in regions of interest?
- How do we expect targets to use emerging technologies?
- What is the SIGINT threat of these emerging technologies?

Discovery

SIGINT PLANNING CYCLE

Vulnerabilities

- What vulnerabilities are critical to current success (i.e. where are our risk areas)?
- How do we discover vulnerabilities?
- How do we introduce vulnerabilities where they do not yet exist?

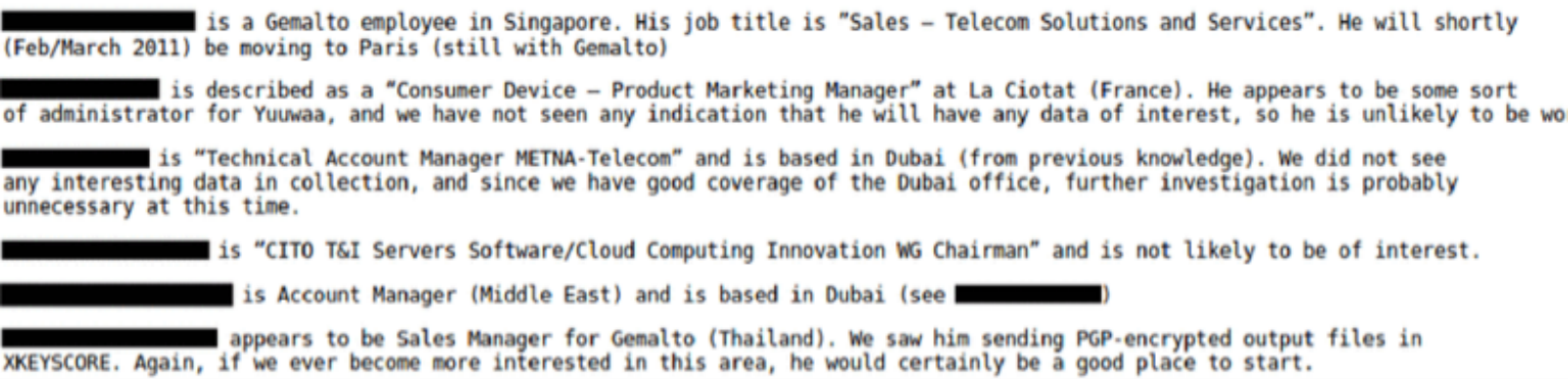
Delivery

- What products/services do we produce for which customers?
- What is workforce makeup and how are they distributed?
- What role do partners play?

Capabilities

- What capabilities do we need to develop to take advantage of technology vulnerabilities?
- What techniques to do we deploy to take advantage of those vulnerabilities (e.g. CNE, supply chain, mid-point, etc.)
- What role does enabling, cooperative access, HUMINT, 2nd parties, etc. play in building those capabilities?

TOP SECRET//COMINT//REL TO USA, FVEY



[redacted] is a Gemalto employee in Singapore. His job title is "Sales – Telecom Solutions and Services". He will shortly (Feb/March 2011) be moving to Paris (still with Gemalto)

[redacted] is described as a "Consumer Device – Product Marketing Manager" at La Ciotat (France). He appears to be some sort of administrator for Yuuwaa, and we have not seen any indication that he will have any data of interest, so he is unlikely to be wo

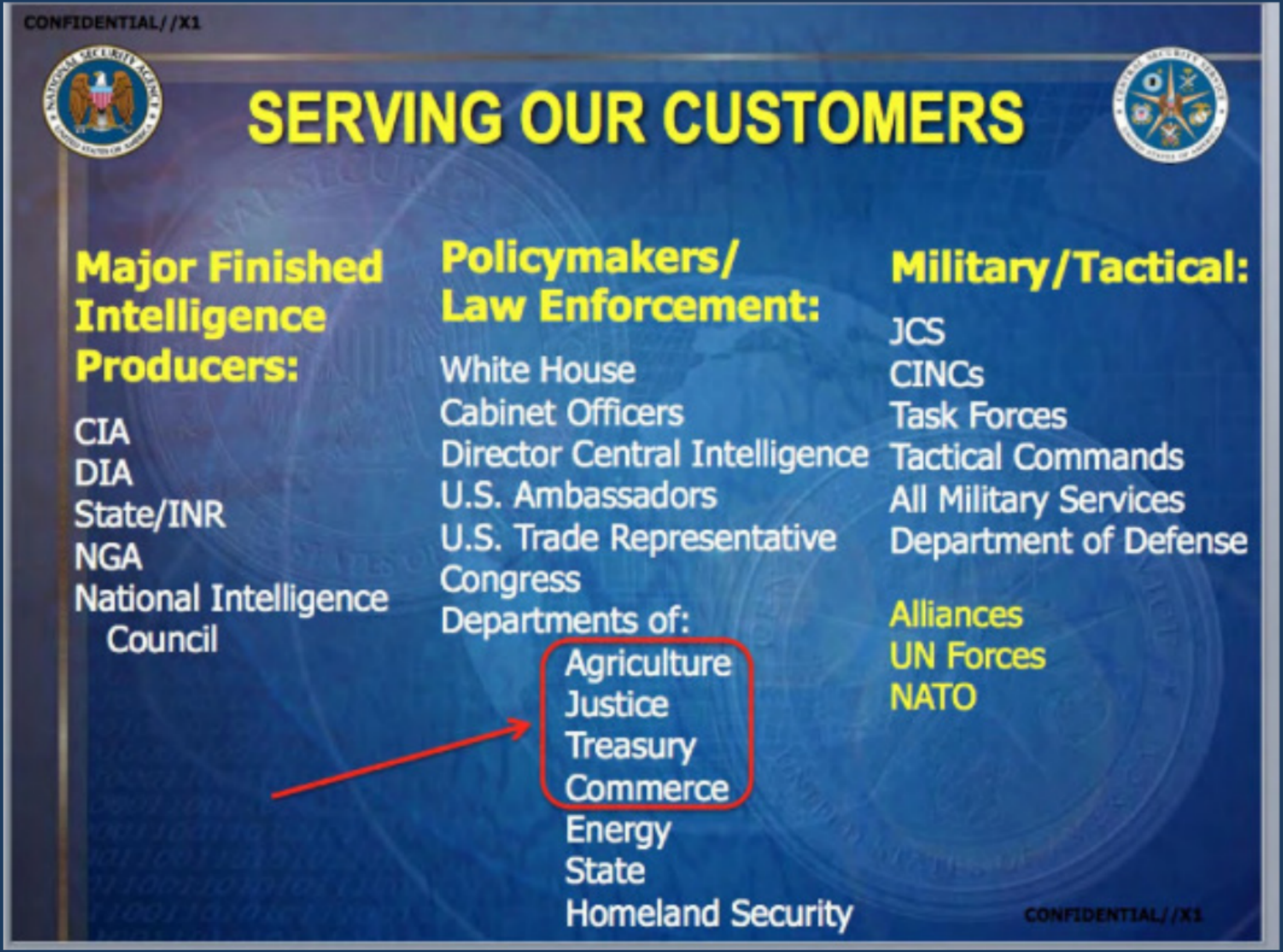
[redacted] is "Technical Account Manager METNA-Telecom" and is based in Dubai (from previous knowledge). We did not see any interesting data in collection, and since we have good coverage of the Dubai office, further investigation is probably unnecessary at this time.

[redacted] is "CITO T&I Servers Software/Cloud Computing Innovation WG Chairman" and is not likely to be of interest.

[redacted] is Account Manager (Middle East) and is based in Dubai (see [redacted])

[redacted] appears to be Sales Manager for Gemalto (Thailand). We saw him sending PGP-encrypted output files in XKEYSCORE. Again, if we ever become more interested in this area, he would certainly be a good place to start.

The Why: Not just for security but economic theft and control:



CONFIDENTIAL//X1

SERVING OUR CUSTOMERS

Major Finished Intelligence Producers:

CIA
DIA
State/INR
NGA
National Intelligence Council

Policymakers/ Law Enforcement:

White House
Cabinet Officers
Director Central Intelligence
U.S. Ambassadors
U.S. Trade Representative
Congress
Departments of:

- Agriculture
- Justice
- Treasury
- Commerce
- Energy
- State
- Homeland Security

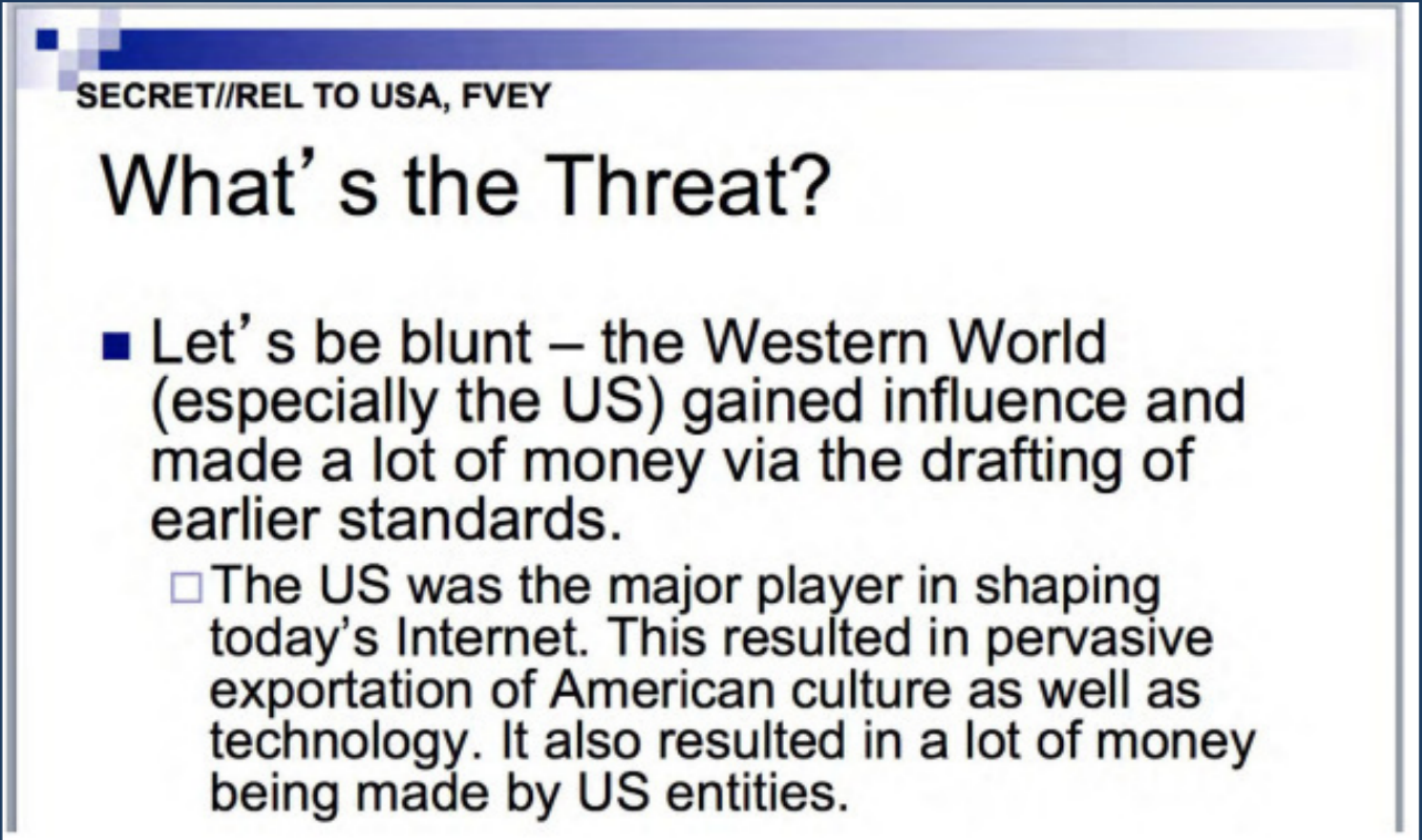
Military/Tactical:

JCS
CINCs
Task Forces
Tactical Commands
All Military Services
Department of Defense

Alliances
UN Forces
NATO

CONFIDENTIAL//X1

NSA programs are more about control and influence then security:

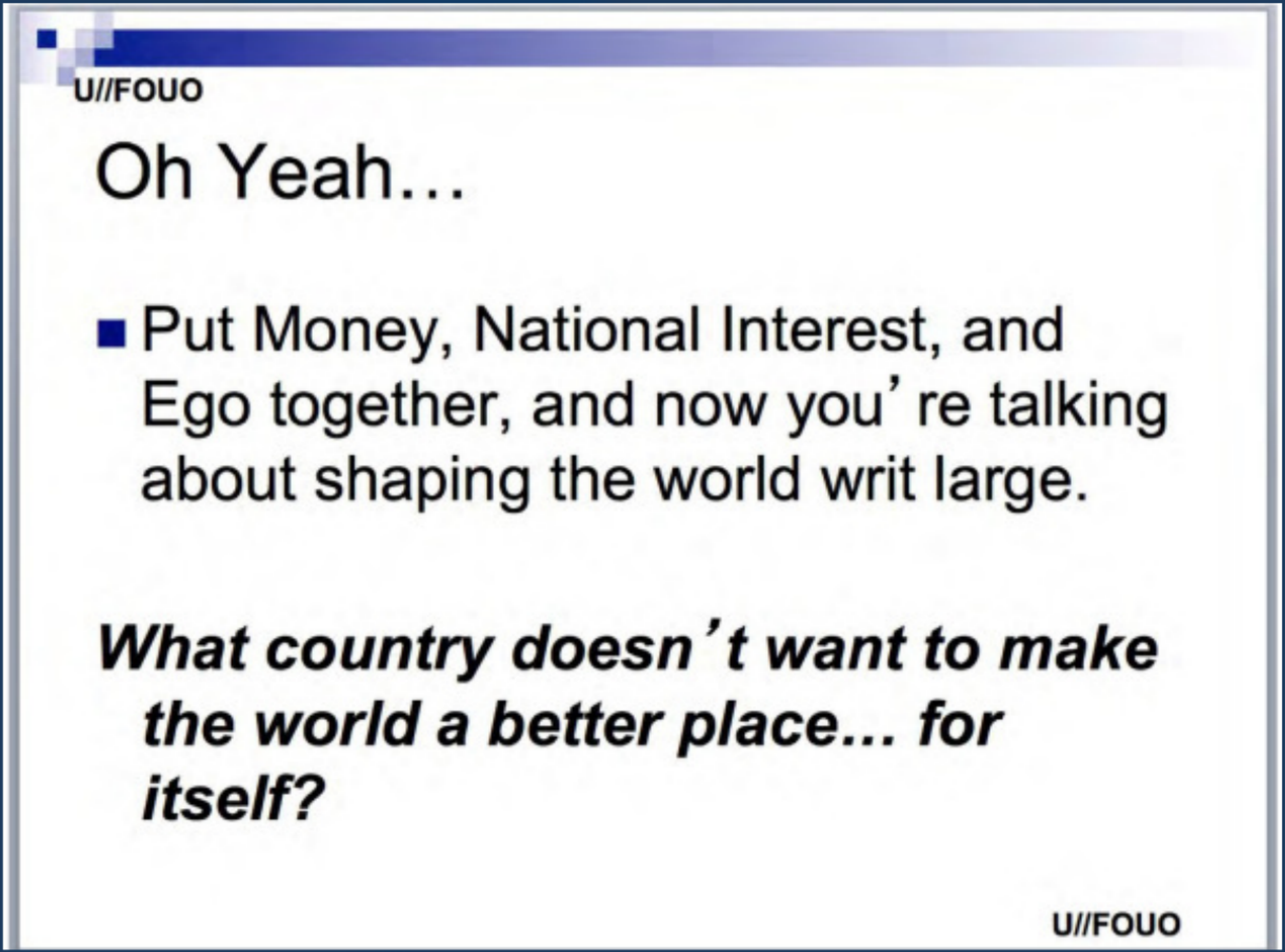


SECRET//REL TO USA, FVEY

What’ s the Threat?

- Let’ s be blunt – the Western World (especially the US) gained influence and made a lot of money via the drafting of earlier standards.
  - □ The US was the major player in shaping today’s Internet. This resulted in pervasive exportation of American culture as well as technology. It also resulted in a lot of money being made by US entities.

From a NSA officers presentation "The Role of National Interest, Money and Ego."



U//FOUO

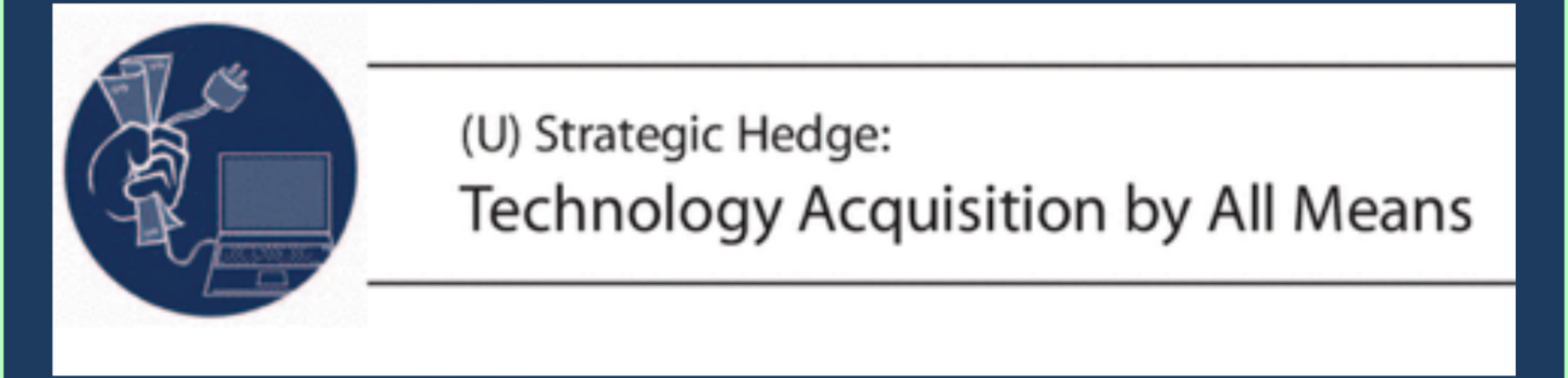
Oh Yeah…

- Put Money, National Interest, and Ego together, and now you' re talking about shaping the world writ large.

What country doesn' t want to make the world a better place… for itself?

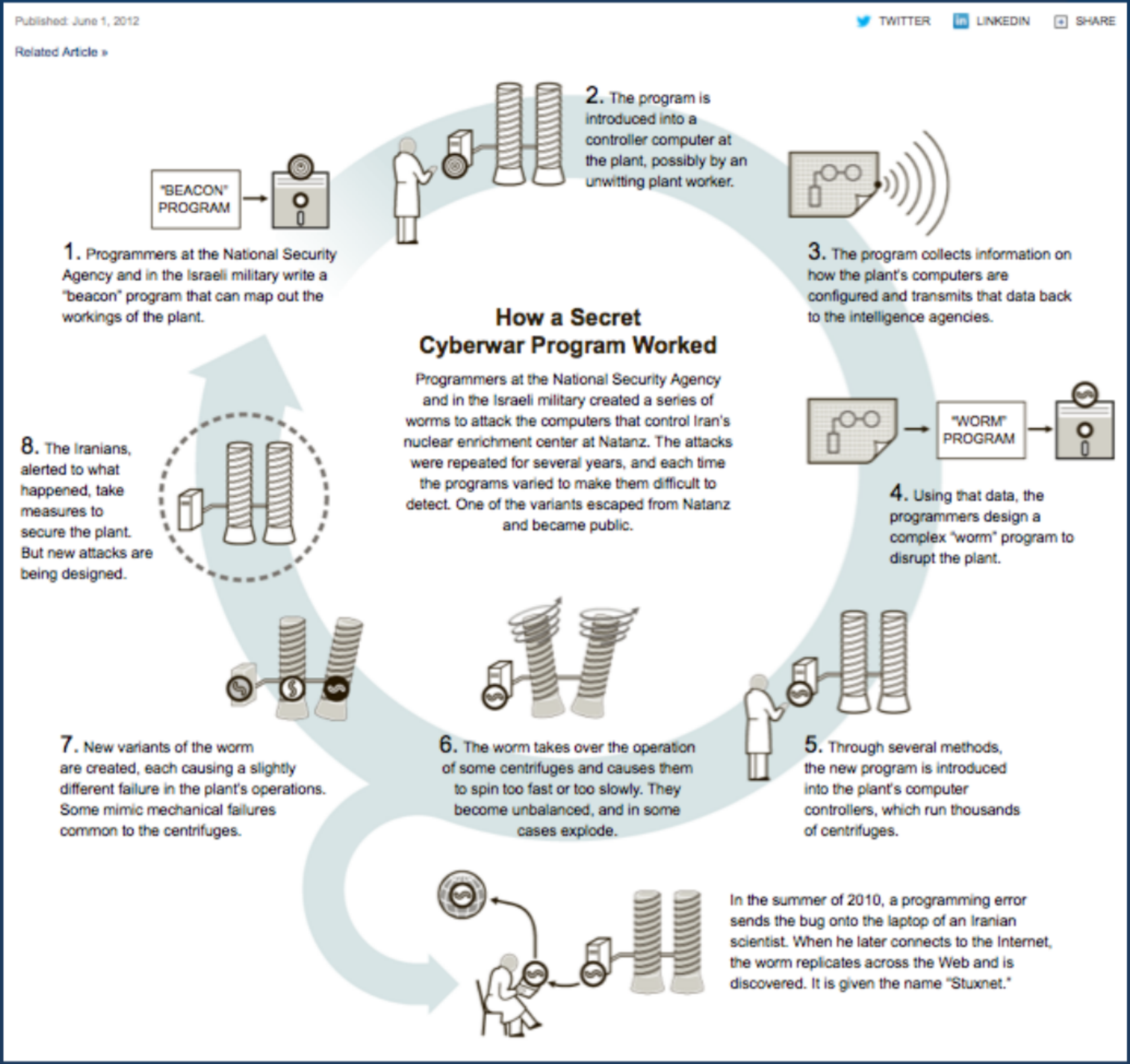
U//FOUO

2009 Quadrennial Intelligence Community Review (NSA Planing from 2009-2025)



(U) Strategic Hedge:

Technology Acquisition by All Means



Published: June 1, 2012

Related Article »

How a Secret Cyberwar Program Worked

Programmers at the National Security Agency and in the Israeli military created a series of worms to attack the computers that control Iran's nuclear enrichment center at Natanz. The attacks were repeated for several years, and each time the programs varied to make them difficult to detect. One of the variants escaped from Natanz and became public.

1. Programmers at the National Security Agency and in the Israeli military write a "beacon" program that can map out the workings of the plant.

2. The program is introduced into a controller computer at the plant, possibly by an unwitting plant worker.

3. The program collects information on how the plant's computers are configured and transmits that data back to the intelligence agencies.

4. Using that data, the programmers design a complex "worm" program to disrupt the plant.

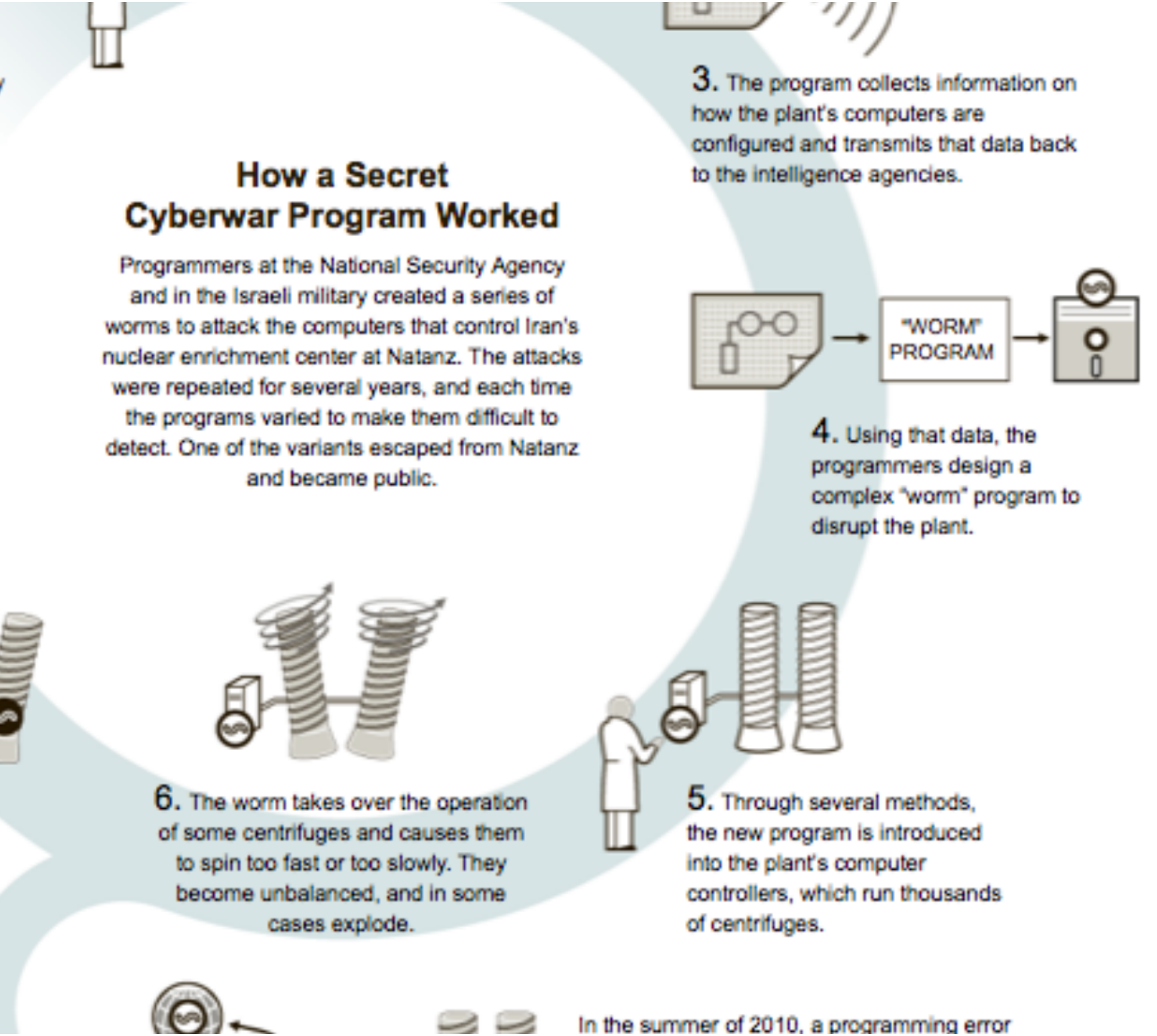
5. Through several methods, the new program is introduced into the plant's computer controllers, which run thousands of centrifuges.

6. The worm takes over the operation of some centrifuges and causes them to spin too fast or too slowly. They become unbalanced, and in some cases explode.

7. New variants of the worm are created, each causing a slightly different failure in the plant's operations. Some mimic mechanical failures common to the centrifuges.

8. The Iranians, alerted to what happened, take measures to secure the plant. But new attacks are being designed.

In the summer of 2010, a programming error sends the bug onto the laptop of an Iranian scientist. When he later connects to the Internet, the worm replicates across the Web and is discovered. It is given the name "Stuxnet."



How a Secret Cyberwar Program Worked

Programmers at the National Security Agency and in the Israeli military created a series of worms to attack the computers that control Iran's nuclear enrichment center at Natanz. The attacks were repeated for several years, and each time the programs varied to make them difficult to detect. One of the variants escaped from Natanz and became public.

3. The program collects information on how the plant's computers are configured and transmits that data back to the intelligence agencies.

4. Using that data, the programmers design a complex "worm" program to disrupt the plant.

5. Through several methods, the new program is introduced into the plant's computer controllers, which run thousands of centrifuges.

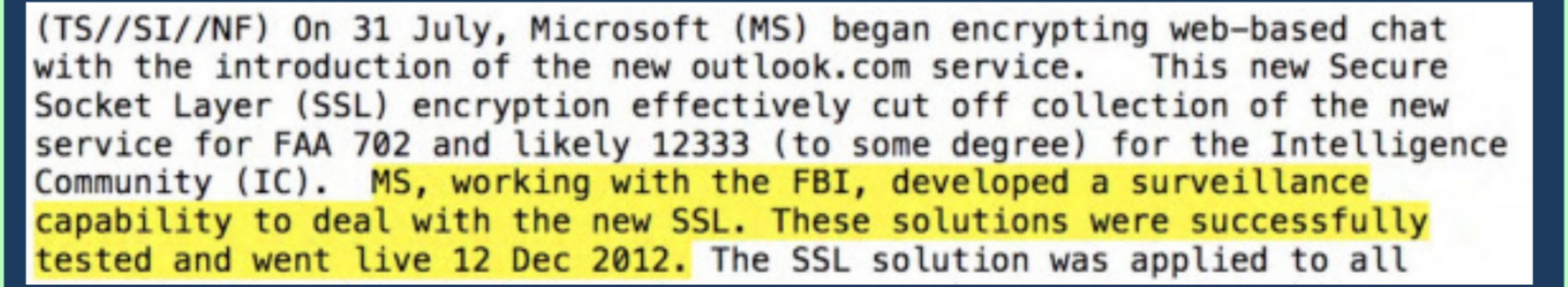
6. The worm takes over the operation of some centrifuges and causes them to spin too fast or too slowly. They become unbalanced, and in some cases explode.

In the summer of 2010, a programming error

NSA (Cont)

- The NSA created an industry front group and paid off major encryption companies to put “backdoors” into some proprietary encryption so that the NSA could open them

- NSA/FBI worked with Microsoft to break encryption advertised by Microsoft/Skype:



(TS//SI//NF) On 31 July, Microsoft (MS) began encrypting web-based chat with the introduction of the new outlook.com service. This new Secure Socket Layer (SSL) encryption effectively cut off collection of the new service for FAA 702 and likely 12333 (to some degree) for the Intelligence Community (IC). MS, working with the FBI, developed a surveillance capability to deal with the new SSL. These solutions were successfully tested and went live 12 Dec 2012. The SSL solution was applied to all

Problem with proprietary encryption: Case study RSA and the NSA

- The NSA put “back doors” (a term for a flaw in the software construction that allows surveillance programs to access supposedly secured information) in Dual_EC_DRBG proprietary encryption.

- The NSA did this by paying $10 million to an encryption manufacturer, named RSA, to weaken the math that secured its encryption algorithm.

- The companies that have implemented the Dual_EC_DRBG into their products include Blackberry, Microsoft, Certicom, RSA, Cisco, Juniper Networks, McAfee, Symantec, Samsung, Lancope, SafeLogic, GE Healthcare, Thales eSecurity, Panzura, Catbird Networks, ARX, Kony, CoCo Communications, Riverbed Technology, The OpenSSL Foundation, Certicom, and Mocana.

- In 2014 NIST removed Dual_EC_DRBG as a cryptographic algorithm from its draft guidance on random number generators, recommending "that current users of Dual_EC_DRBG transition" to a different algorithm.

Problems with proprietary encryption: Continued

- Skype claimed it was encrypting user calls, while it was working with the government to provide a backdoor to its service.

- Snapchat claimed it was using properly implemented encryption, but its data bases were hacked and the hackers were able to access allegedly encrypted content.

What is the legal framework for this:

Strategy has been to keep most of it secret from legislature and judges and "drive a truck thru legal loopholes"

Internet backbone is collected in the US under the law of: FAA/FISA

The law for collecting:
E.O. 12333--- FISA--- Patriot Act 215 --- FAA 702

Questions persist around: Use international routing of domestic communications to allow for five eye collection

What is open source?

Where engineers and users can see the "source codes" that make the software program and interact with the computer hardware.

Open Source Encryption Works Better:

- Open source computer programs legally and technically allow the person working with the machine to have access to all the "code" that builds the software and interacts with the computer hardware.
- Open source programs are often "free" because the code is unencumbered by proprietary constraints .
- NSA's own documents show they can't break the basis for OTR, PGP, and Truecrypt, all open source encryption standards
- User-side encryption, like PGP, is important to ensuring implementation is under organizational control.

Why Open Source algorithms are necessary for secure encryption:

- Kerchoff's Principle

  The security of the system has to be based on the assumption that the attacker has full knowledge of the design and implementation details of the cryptographic system. The only missing information for the attacker is a short, easily exchangeable random number sequence, the secret key

- All of the security in these algorithms is based in the key (or keys); none is based in the details of the algorithm.

- This means that the algorithm should be published and analyzed.

- The best algorithms we have are the ones that have been made public, have been attacked by the world's best cryptographers for years, and are still unbreakable. (PGP, OTR, ZRTP)

What is End-to-end encryption?

- Encryption system built to be readable only by the intended recipient, and the receiving party decrypting it
- No involvement in encryption by third parties.
- The intention of end-to-end encryption is to prevent intermediaries, such as Internet providers or application service providers, from being able to discover or tamper with the content of communications.
- End-to-end encryption generally includes protections of both confidentiality and integrity.
- Sometime called “Client-side” or “User-side”

Lawyers play a key role!

- Currently lawyers are extremely weak on digital security.
- Even if hack confirmed no reason to publicize.
- Threatens trust and effectiveness of global profession as a whole

Ethics and encryption:

- MA requires encryption for personal data held by private companies, including out of state entities dealing with MA residents data.

- NV also requires encryption for resident data.

- In July 2014 MA Att. Gen. reached $150,000 settlement with RI business that lost unencrypted data of MA residents

Massachusetts information security law, M.G.L. c. 93H

- Massachusetts information security law, M.G.L. c. 93H, applies to “persons who own, license, store or maintain personal information about a resident of the Commonwealth of Massachusetts”.

- The law applies to all private businesses including lawyers and law firms and requires a written organization wide security plan that includes "to the extent technically feasible, encryption of all transmitted records and files containing personal information that will travel across public networks, and encryption of all data containing personal information to be transmitted wirelessly."

Legal ethics and encryption (cont)

Rule 1.6 of the Model Rules of Professional Responsibility:

> "A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client."

Legal ethics and encryption (cont)

- In 2012 the ABA increased its interpretation of the Ethical standards in rule 1.6 in the MRPR to create an explicit obligation on lawyers to take affirmative steps to protect confidentiality.

- This protection is based on a "reasonable effort" standard.
- NY Bar defines reasonable effort based on the client's needs.
- PA Bar encourages attorneys to regularly use encryption to protect their clients when using cloud services

Proposed change to 1.6 ethics

A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure or use of, or unauthorized access to, information protected by Rules 1.6, 1.9(c), or 1.18(b).

Redefine “reasonable effort” to require:

- “provision of end-to-end open source encryption for private information and at client request.”