weizenbaum
institut

Six years after Snowden

A summary of lessons learned and lessons lost for the networked society

5th of June 2019, Weizenbaum Institute, Berlin

Rainer Rehak
rainer.rehak@wzb.eu
0496 A3A6 DC10 9851 A09F
04A3 FF25 0994 CE9E FB45
🐦 @Rainer_Rehak

WZB
Berlin Social Science Center

Presentation Overview

1) Introduction (Speaker, Situation, Spies, Source, Scandal)
2) The Snowden-Revelations
3) Global Reactions
4) Three scenarios
5) Lessons learned, lessons lost

The Speaker

The Speaker

- Researcher at the Weizenbaum Institute for the Networked Society
  - The German Internet Insitute
  - Research interests: IT security, privacy, data protection, critical compute science
- CS & Philosophy (Humboldt-University Berlin, Freie University Berlin)
  - Chair Prof. Wolfgang Coy (Computer science and society)
  - Diploma thesis about government hacking and its societal implications

weizenbaum
institut

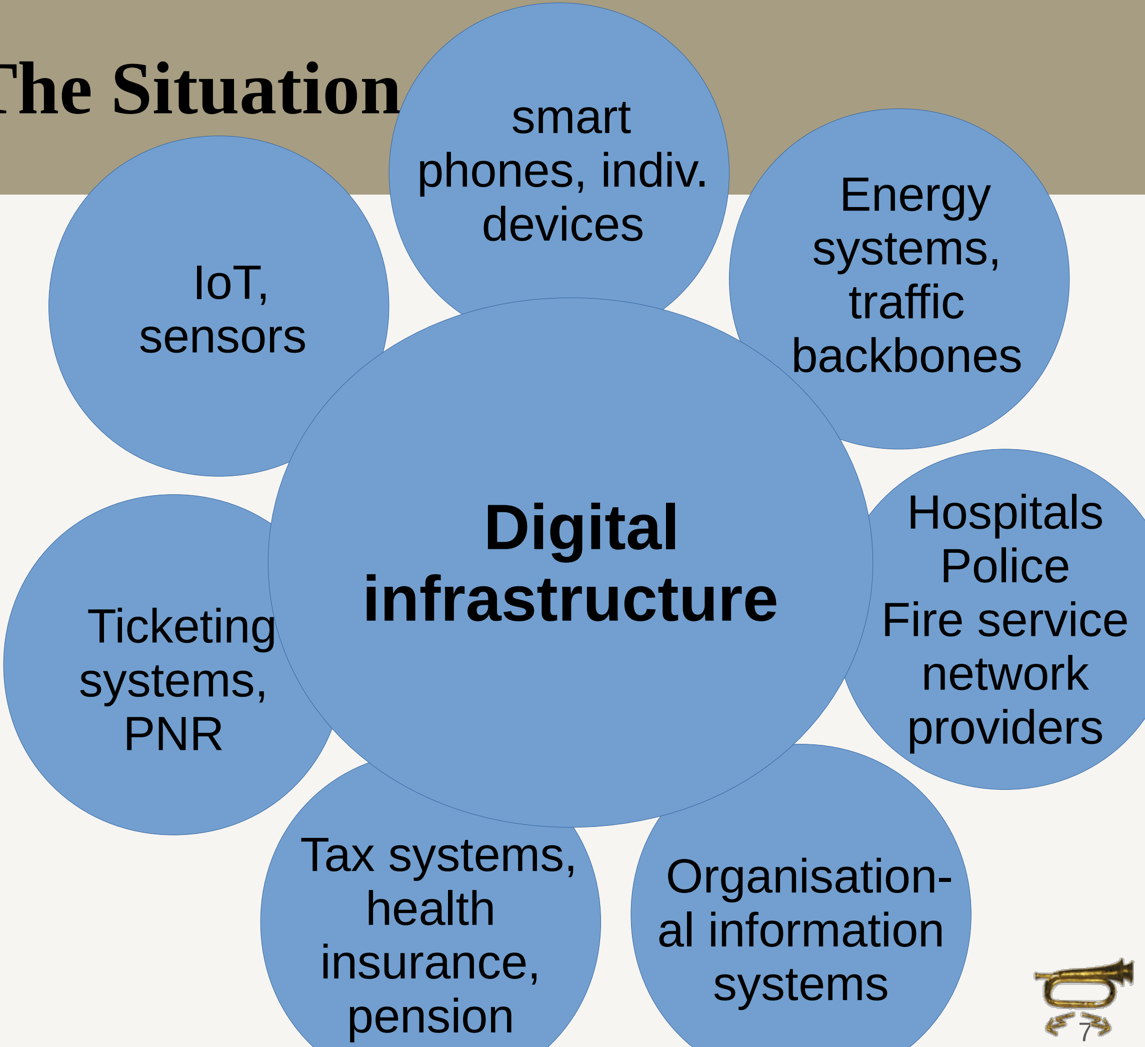
The Speaker

- Computer Professionals for Peace and Social Responsibility (FIfF, co-founded by J. Weizenbaum in 1984)
  - Board member
- German Informatics Society (GI)
  - Focus group “CS & ethics”
- Amnesty International Germany
  - Expert group “Human rights in the digital age”
- Transatlantic Cyber Forum (snv)
  - Expert groups “Government hacking” and “Vulnerability managemnt”

The Situation

The Situation

- Society under the digital condition
- Digital (network) infrastructure everywhere
- From playground to infrastructure



Digital infrastructure

smart phones, indiv. devices

Energy systems, traffic backbones

Hospitals
Police
Fire service
network providers

Organisational information systems

Tax systems, health insurance, pension

Ticketing systems, PNR

IoT, sensors

Basics of IT security

- Core issue: Insecure systems
  - IT security (Confidentiality, Integrity, Availability)
- Vulnerabilities (=possibility to violate ITSec)
- Exploit (piece of software using vulns)
  - 0day, Zeroday, Zeroday-Exploit
  - So far undisclosed exploit (no necessarily unknown!)
  - Grey market, up to millions of €
- Threat to Availability: DDoS (distributed denial-of-service)
  - System overload

Documentary by
Alex Gibney

Fair use

The Spies

The Spies

- 1943: “Five eyes” IC cooperation: US, UK, NZ, AU and CAN
- 1952: Truman establishes the NSA (No Such Agency)
- SIGINT, originated from military deciphering unit
- Black budget >$10 Mrd. p. a.
- Est. 30.000 – 40.000 employees
- Owns ships and airplanes (z. B. USS Liberty)

Public domain

- Became largely known in the EU b/c of the „ECHELON“ programm in 2001
  - Right before 9/11, so no publicity was generated

The Source

Edward Joseph Snowden

- Born 1983
- United States Army Reserve / Special Forces
- Worked for CIA, NSA, DELL
  Booz Allen Hamilton (Administrator /
  Data Analyst / Trainer)
- Published nothing, passed-on thousands of documents to journalists e.g. Glenn Greenwald (the Guardian), contents never contested
- According to US law not a Whistleblower
- Charged with Espionage Act (1917) → secret court / "arcane World War I law" (Radack)
- Passport revoked by the USA while in Moscow

CC-BY Laura Poitras

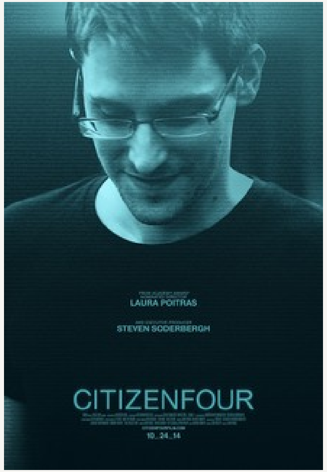
The Scandal

2013

Summer of Snowden

2013

Summer of Snowden

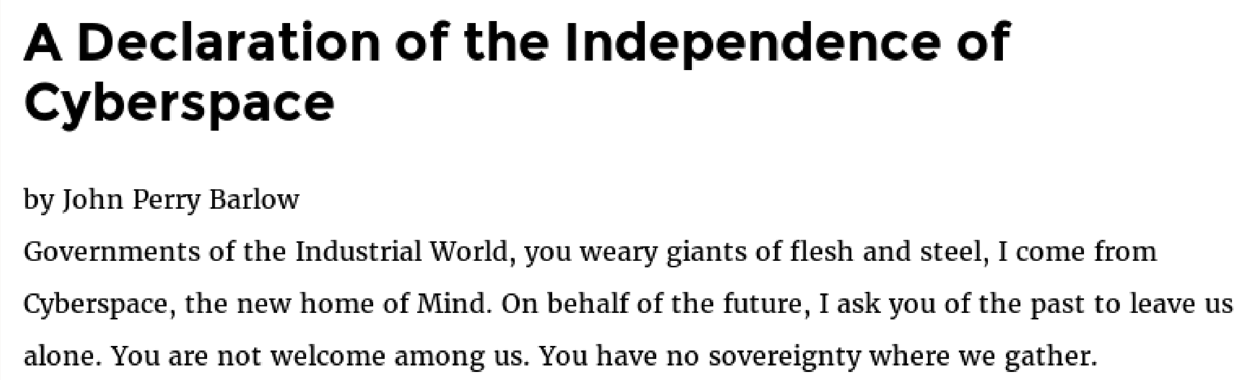


Fair use

Documentary by
Laura Poitras

Why „Summer of Snowden“?

- 1996: New digital world!



A Declaration of the Independence of Cyberspace

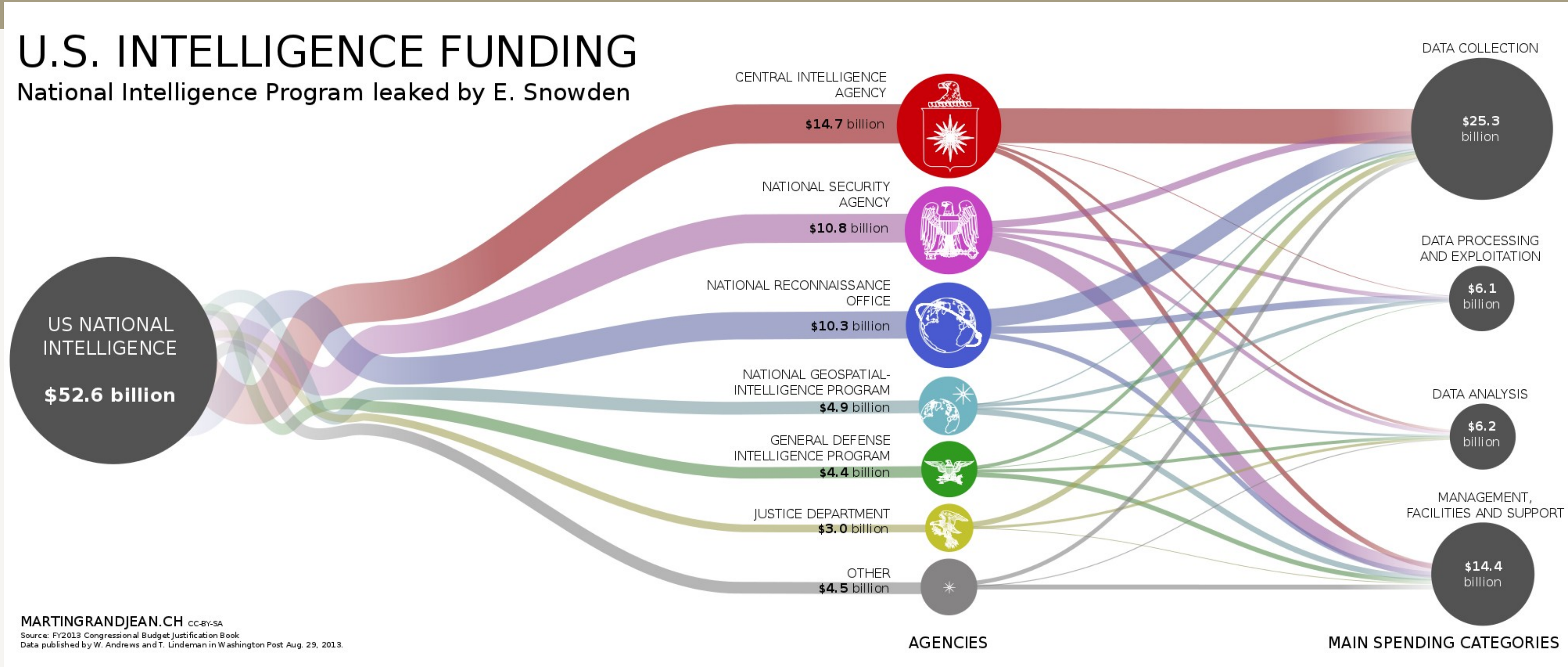
by John Perry Barlow

Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather.

8. Feb 1996, https://www.eff.org/cyberspace-independence

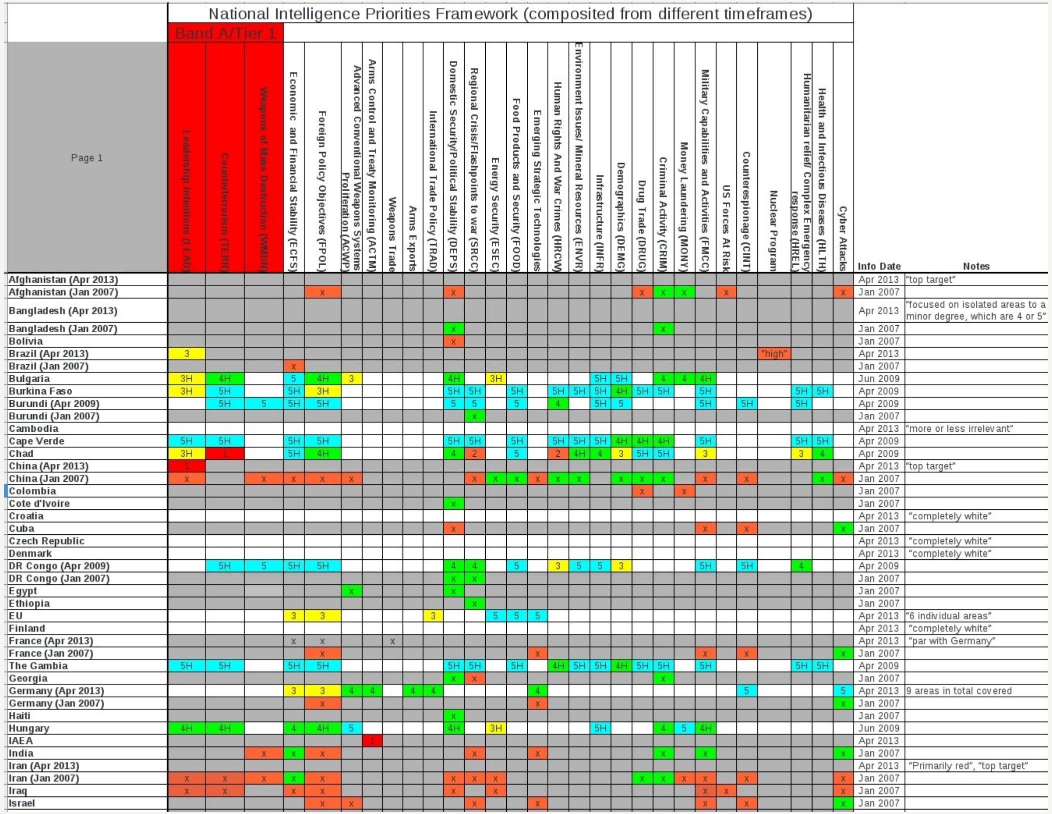
- 2013: Summer of Snowden
  “Manhattan Project” of CS

Black budget

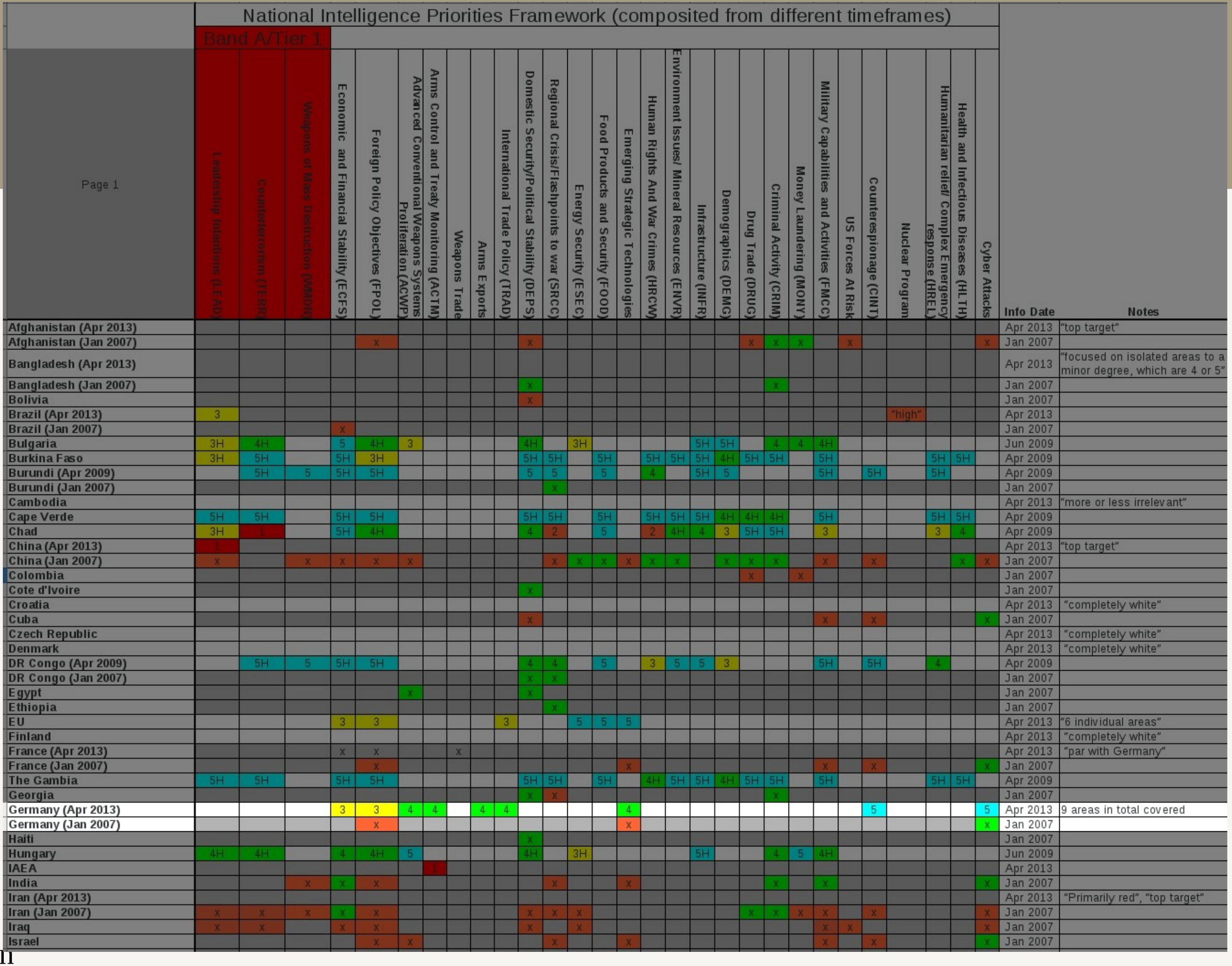


MARTINGRANDJEAN.CH CC-BY-SA
Source: FY2013 Congressional Budget Justification Book
Data published by W. Andrews and T. Lindeman in Washington Post Aug. 29, 2013.

National Intelligence Priorities

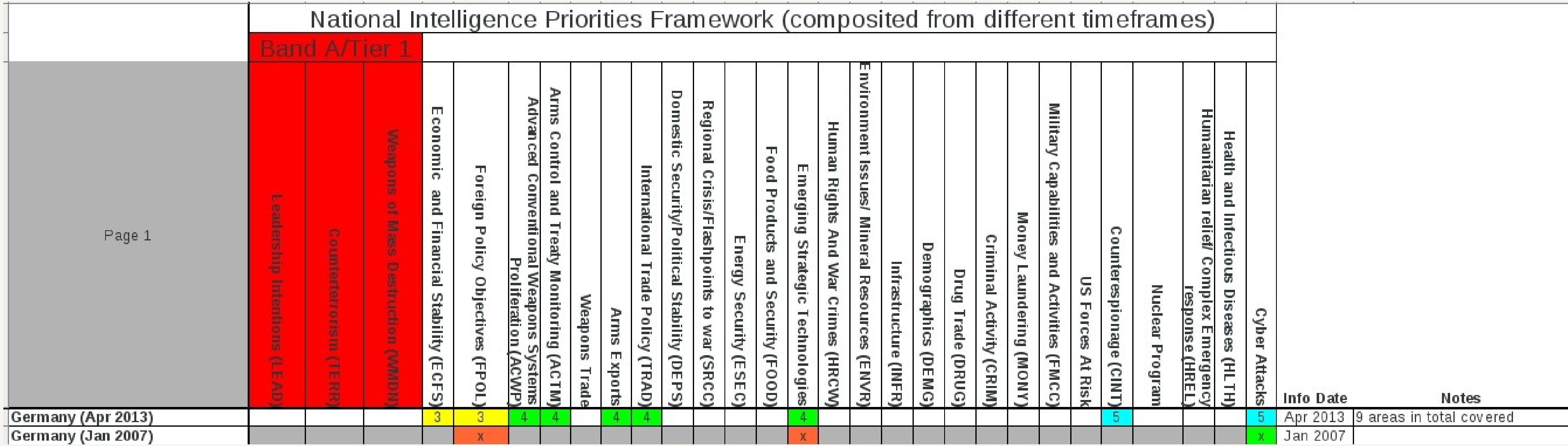


	National Intelligence Priorities Framework (composited from different timeframes)																														
	Band A/Tier 1																														
Page 1	Leadership Intentions (LEAD)	Counterterrorism (TERR)	Weapons of Mass Destruction (WMDN)	Economic and Financial Stability (ECFS)	Foreign Policy Objectives (FPOL)	Advanced Conventional Weapons Systems Proliferation (ACWP)	Arms Control and Treaty Monitoring (ACTM)	Weapons Trade	Arms Exports	International Trade Policy (TRAD)	Domestic Security/Political Stability (DEPS)	Regional Crisis/Flashpoints to war (SRCC)	Energy Security (ESEC)	Food Products and Security (FOOD)	Emerging Strategic Technologies	Human Rights And War Crimes (HRCW)	Environment Issues/ Mineral Resources (ENVR)	Infrastructure (INFR)	Demographics (DEMG)	Drug Trade (DRUG)	Criminal Activity (CRIM)	Money Laundering (MONY)	Military Capabilities and Activities (FMCC)	US Forces At Risk	Counterespionage (CINT)	Nuclear Program	Humanitarian relief/ Complex Emergency response (HREL)	Health and Infectious Diseases (HLTH)	Cyber Attacks	Info Date	Notes
Afghanistan (Apr 2013)																														Apr 2013	“top target”
Afghanistan (Jan 2007)					x						x									x	x	x		x					x	Jan 2007	
Bangladesh (Apr 2013)																														Apr 2013	“focused on isolated areas to a minor degree, which are 4 or 5”
Bangladesh (Jan 2007)											x										x									Jan 2007	
Bolivia											x																			Jan 2007	
Brazil (Apr 2013)	3																									“high”				Apr 2013	
Brazil (Jan 2007)				x																										Jan 2007	
Bulgaria	3H	4H		5	4H	3					4H		3H					5H	5H		4	4	4H							Jun 2009	
Burkina Faso	3H	5H		5H	3H						5H	5H		5H		5H	5H	5H	4H	5H	5H		5H				5H	5H		Apr 2009	
Burundi (Apr 2009)		5H	5	5H	5H						5	5		5		4		5H	5				5H		5H		5H			Apr 2009	
Burundi (Jan 2007)												x																		Jan 2007	
Cambodia																														Apr 2013	“more or less irrelevant”
Cape Verde	5H	5H		5H	5H						5H	5H		5H		5H	5H	5H	4H	4H	4H		5H				5H	5H		Apr 2009	
Chad	3H	1		5H	4H						4	2		5		2	4H	4	3	5H	5H		3				3	4		Apr 2009	
China (Apr 2013)	1																													Apr 2013	“top target”
China (Jan 2007)	x		x	x	x	x						x	x	x	x	x	x		x	x	x		x		x			x	x	Jan 2007	
Colombia																				x		x								Jan 2007	
Cote d'Ivoire											x																			Jan 2007	
Croatia																														Apr 2013	“completely white”
Cuba											x												x		x				x	Jan 2007	
Czech Republic																														Apr 2013	“completely white”
Denmark																														Apr 2013	“completely white”
DR Congo (Apr 2009)		5H	5	5H	5H						4	4		5		3	5	5	3				5H		5H		4			Apr 2009	
DR Congo (Jan 2007)											x	x																		Jan 2007	
Egypt						x					x																			Jan 2007	
Ethiopia												x																		Jan 2007	
EU				3	3					3			5	5	5															Apr 2013	“6 individual areas”
Finland																														Apr 2013	“completely white”
France (Apr 2013)				x	x			x																						Apr 2013	“par with Germany”
France (Jan 2007)					x										x								x		x				x	Jan 2007	
The Gambia	5H	5H		5H	5H						5H	5H		5H		4H	5H	5H	4H	5H	5H		5H				5H	5H		Apr 2009	
Georgia											x	x									x									Jan 2007	
Germany (Apr 2013)				3	3	4	4		4	4					4										5				5	Apr 2013	9 areas in total covered
Germany (Jan 2007)					x										x														x	Jan 2007	
Haiti											x																			Jan 2007	
Hungary	4H	4H		4	4H	5					4H		3H					5H			4	5	4H							Jun 2009	
IAEA							1																							Apr 2013	
India			x	x	x							x			x						x		x						x	Jan 2007	
Iran (Apr 2013)																														Apr 2013	“Primarily red”, “top target”
Iran (Jan 2007)	x	x	x	x	x						x	x	x							x	x	x	x		x				x	Jan 2007	
Iraq	x	x		x	x						x		x										x	x					x	Jan 2007	
Israel					x	x						x			x								x		x				x	Jan 2007	



	National Intelligence Priorities Framework (composited from different timeframes)																														
	Band A/Tier 1																														
Page 1	Leadership Intentions (LEAD)	Counterterrorism (TERR)	Weapons of Mass Destruction (WMDN)	Economic and Financial Stability (ECFS)	Foreign Policy Objectives (FPOL)	Advanced Conventional Weapons Systems Proliferation (ACWP)	Arms Control and Treaty Monitoring (ACTM)	Weapons Trade	Arms Exports	International Trade Policy (TRAD)	Domestic Security/Political Stability (DEPS)	Regional Crisis/Flashpoints to war (SRCC)	Energy Security (ESEC)	Food Products and Security (FOOD)	Emerging Strategic Technologies	Human Rights And War Crimes (HRCW)	Environment Issues/ Mineral Resources (ENVR)	Infrastructure (INFR)	Demographics (DEMG)	Drug Trade (DRUG)	Criminal Activity (CRIM)	Money Laundering (MONY)	Military Capabilities and Activities (FMCC)	US Forces At Risk	Counterespionage (CINT)	Nuclear Program	Humanitarian relief/ Complex Emergency response (HREL)	Health and Infectious Diseases (HLTH)	Cyber Attacks	Info Date	Notes
Afghanistan (Apr 2013)																														Apr 2013	"top target"
Afghanistan (Jan 2007)					x						x									x	x	x		x					x	Jan 2007	
Bangladesh (Apr 2013)																														Apr 2013	"focused on isolated areas to a minor degree, which are 4 or 5"
Bangladesh (Jan 2007)											x										x									Jan 2007	
Bolivia											x																			Jan 2007	
Brazil (Apr 2013)	3																									"high"				Apr 2013	
Brazil (Jan 2007)				x																										Jan 2007	
Bulgaria	3H	4H		5	4H	3					4H		3H					5H	5H		4	4	4H							Jun 2009	
Burkina Faso	3H	5H		5H	3H						5H	5H		5H		5H	5H	5H	4H	5H	5H		5H				5H	5H		Apr 2009	
Burundi (Apr 2009)		5H	5	5H	5H						5	5		5		4		5H	5				5H		5H		5H			Apr 2009	
Burundi (Jan 2007)												x																		Jan 2007	
Cambodia																														Apr 2013	"more or less irrelevant"
Cape Verde	5H	5H		5H	5H						5H	5H		5H		5H	5H	5H	4H	4H	4H		5H				5H	5H		Apr 2009	
Chad	3H	1		5H	4H						4	2		5		2	4H	4	3	5H	5H		3				3	4		Apr 2009	
China (Apr 2013)	1																													Apr 2013	"top target"
China (Jan 2007)	x		x	x	x	x						x	x	x	x	x	x		x	x	x		x		x			x	x	Jan 2007	
Colombia																				x		x								Jan 2007	
Cote d'Ivoire											x																			Jan 2007	
Croatia																														Apr 2013	"completely white"
Cuba											x												x		x				x	Jan 2007	
Czech Republic																														Apr 2013	"completely white"
Denmark																														Apr 2013	"completely white"
DR Congo (Apr 2009)		5H	5	5H	5H						4	4		5		3	5	5	3				5H		5H		4			Apr 2009	
DR Congo (Jan 2007)											x	x																		Jan 2007	
Egypt						x					x																			Jan 2007	
Ethiopia												x																		Jan 2007	
EU				3	3					3			5	5	5															Apr 2013	"6 individual areas"
Finland																														Apr 2013	"completely white"
France (Apr 2013)				x	x			x																						Apr 2013	"par with Germany"
France (Jan 2007)					x										x								x		x				x	Jan 2007	
The Gambia	5H	5H		5H	5H						5H	5H		5H		4H	5H	5H	4H	5H	5H		5H				5H	5H		Apr 2009	
Georgia											x	x									x									Jan 2007	
Germany (Apr 2013)				3	3	4	4		4	4					4										5				5	Apr 2013	9 areas in total covered
Germany (Jan 2007)					x										x														x	Jan 2007	
Haiti											x																			Jan 2007	
Hungary	4H	4H		4	4H	5					4H		3H					5H			4	5	4H							Jun 2009	
IAEA							1																							Apr 2013	
India			x	x	x							x			x						x		x						x	Jan 2007	
Iran (Apr 2013)																														Apr 2013	"Primarily red", "top target"
Iran (Jan 2007)	x	x	x	x	x						x	x	x							x	x	x	x		x				x	Jan 2007	
Iraq	x	x		x	x						x		x										x	x					x	Jan 2007	
Israel					x	x						x			x								x		x				x	Jan 2007	

National Intelligence Priorities



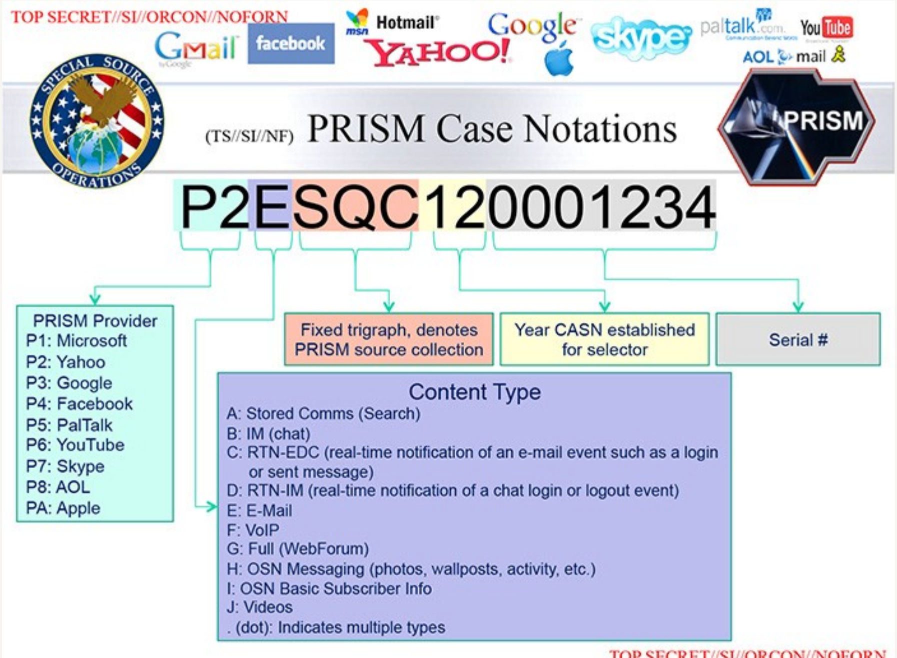
	National Intelligence Priorities Framework (composited from different timeframes)																														
	Band A/Tier 1																														
Page 1	Leadership Intentions (LEAD)	Counterterrorism (TERR)	Weapons of Mass Destruction (WMDN)	Economic and Financial Stability (ECFS)	Foreign Policy Objectives (FPOL)	Advanced Conventional Weapons Systems Proliferation (ACWP)	Arms Control and Treaty Monitoring (ACTM)	Weapons Trade	Arms Exports	International Trade Policy (TRAD)	Domestic Security/Political Stability (DEPS)	Regional Crisis/Flashpoints to war (SRCC)	Energy Security (ESEC)	Food Products and Security (FOOD)	Emerging Strategic Technologies	Human Rights And War Crimes (HRCW)	Environment Issues/ Mineral Resources (ENVR)	Infrastructure (INFR)	Demographics (DEMG)	Drug Trade (DRUG)	Criminal Activity (CRIM)	Money Laundering (MONY)	Military Capabilities and Activities (FMCC)	US Forces At Risk	Counterespionage (CINT)	Nuclear Program	Humanitarian relief/ Complex Emergency response (HREL)	Health and Infectious Diseases (HLTH)	Cyber Attacks	Info Date	Notes
Germany (Apr 2013)				3	3	4	4		4	4					4										5				5	Apr 2013	9 areas in total covered
Germany (Jan 2007)					x										x														x	Jan 2007	

NSA-Programs

Revelations

- PRISM: Direct access (Apple (iCloud), Google (gmail, calendar, youtube, gdocs), Facebook, Skype and Microsoft (Office 365)

(c) Adam Hart-Davis
WaPo, Free to use



GMail
facebook
msn Hotmail
YAHOO!
Google
skype
paltalk.com
YouTube
AOL mail
SPECIAL SOURCE OPERATIONS
PRISM

TOP SECRET//SI//ORCON//NOFORN

(TS//SI//NF) PRISM Case Notations

P2ESQC120001234

PRISM Provider
P1: Microsoft
P2: Yahoo
P3: Google
P4: Facebook
P5: PalTalk
P6: YouTube
P7: Skype
P8: AOL
PA: Apple

Fixed trigraph, denotes PRISM source collection

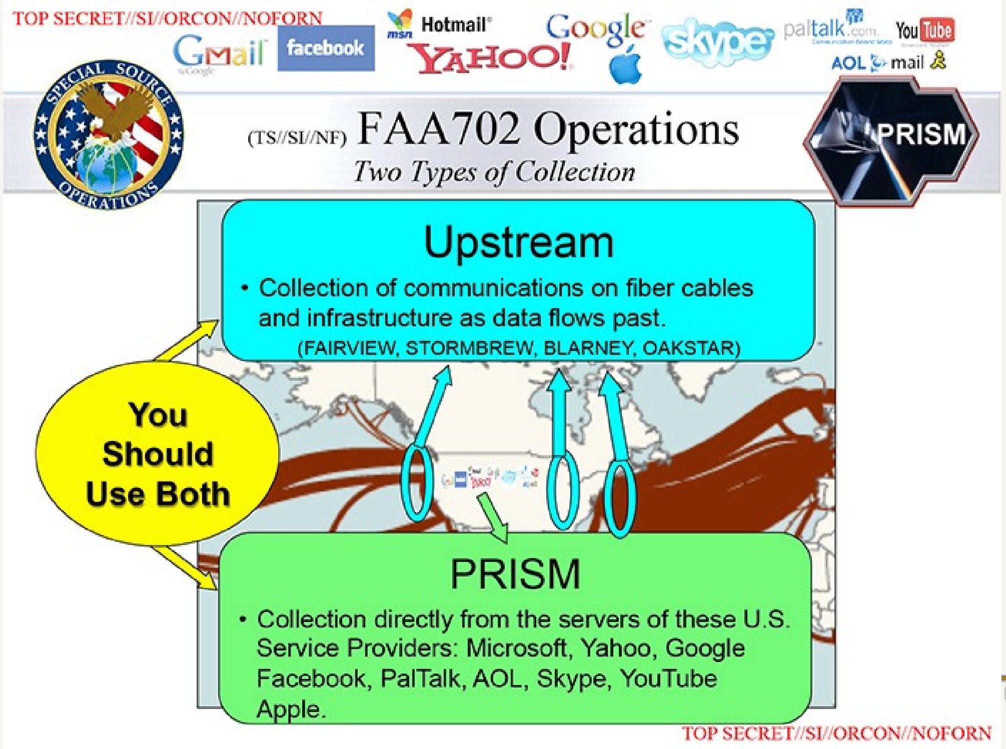
Year CASN established for selector

Serial #

Content Type
A: Stored Comms (Search)
B: IM (chat)
C: RTN-EDC (real-time notification of an e-mail event such as a login or sent message)
D: RTN-IM (real-time notification of a chat login or logout event)
E: E-Mail
F: VoIP
G: Full (WebForum)
H: OSN Messaging (photos, wallposts, activity, etc.)
I: OSN Basic Subscriber Info
J: Videos
. (dot): Indicates multiple types

TOP SECRET//SI//ORCON//NOFORN

- Data access via sea cables (Upstream) GCHQ: Tempora



Gmail
facebook
msn Hotmail
YAHOO!
Google
skype
paltalk.com
YouTube
AOL mail
SPECIAL SOURCE OPERATIONS
PRISM

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)

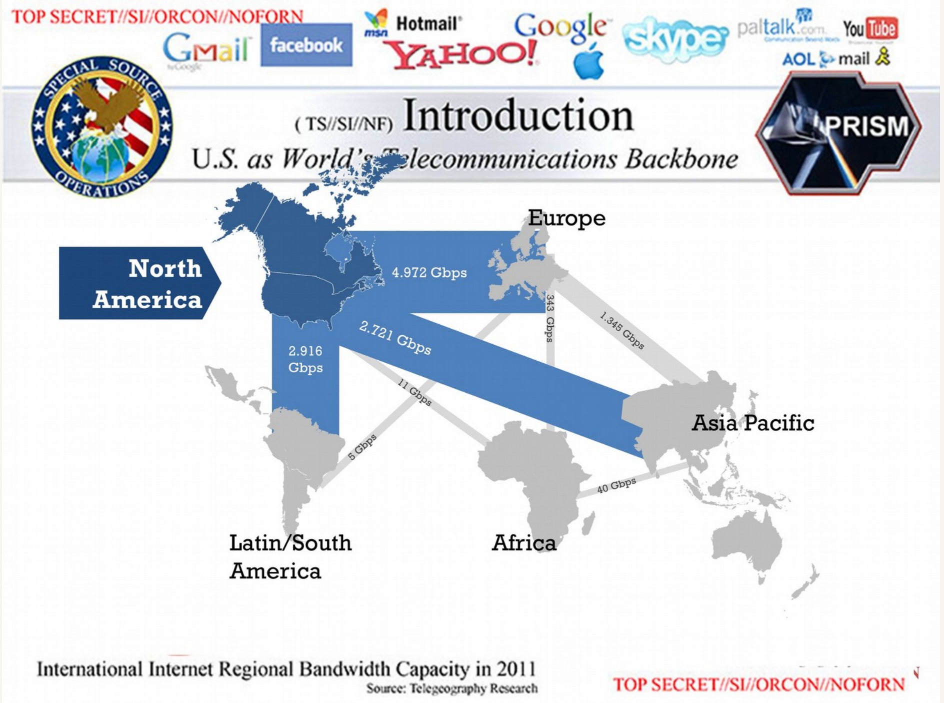
You Should Use Both

PRISM

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

TOP SECRET//SI//ORCON//NOFORN

- Ingest internal corporate traffic at core traffic nodes



TOP SECRET//SI//ORCON//NOFORN

(TS//SI//NF) Introduction

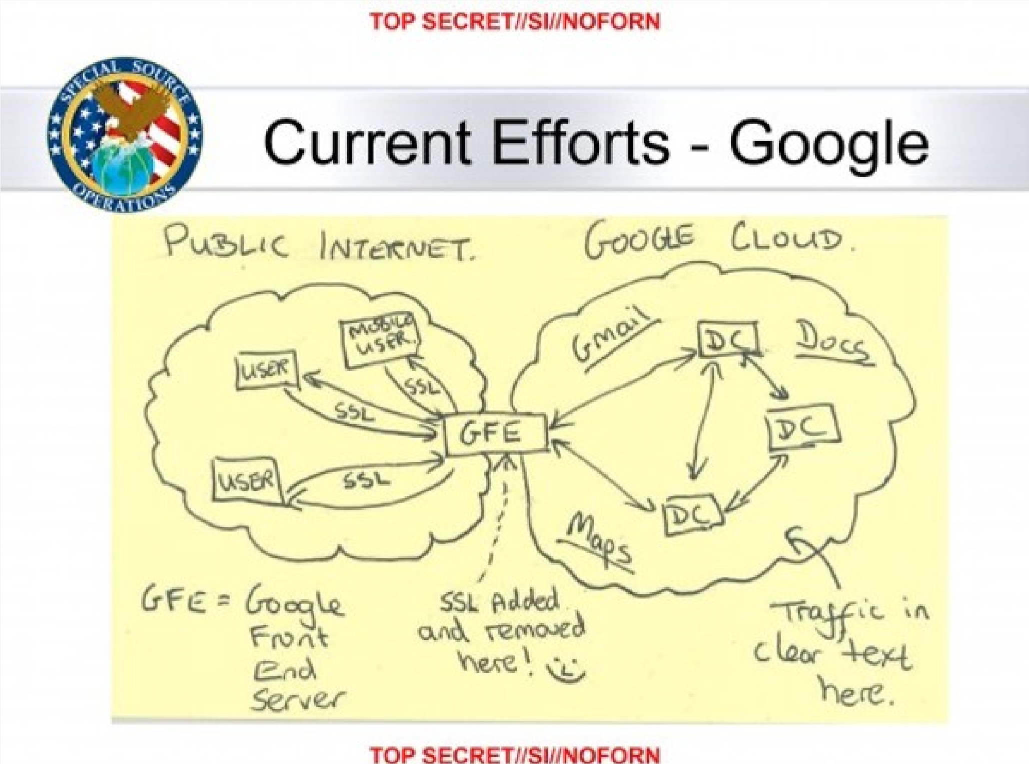
U.S. as World's Telecommunications Backbone

International Internet Regional Bandwidth Capacity in 2011

Source: Telegeography Research

TOP SECRET//SI//ORCON//NOFORN

- Ingest internal corporate traffic at core traffic nodes



TOP SECRET//SI//NOFORN

Current Efforts - Google

GFE = Google Front End Server

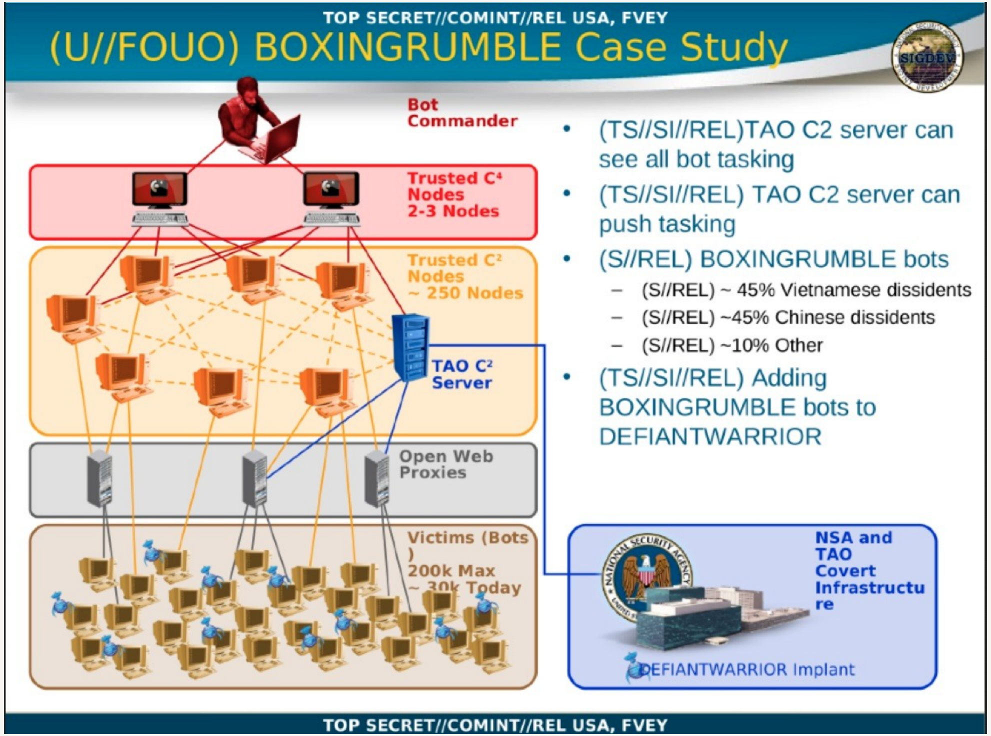
SSL Added and removed here! ☺

Traffic in clear text here.

TOP SECRET//SI//NOFORN

- **Metadata** of communication (calls, sms, internet) via providers (Verizon, Orange), down to HTTP headers
- Stockpiling of **exploits** for Blackberry, Android, iPhone, Microsoft
  - Cooperation with companies (Microsoft Active Protection Program, MAPP)
  - Surveillance of security forums

- Automated creation of NSA-Botnets



TOP SECRET//COMINT//REL USA, FVEY

(U//FOUO) BOXINGRUMBLE Case Study

- (TS//SI//REL)TAO C2 server can see all bot tasking
- (TS//SI//REL) TAO C2 server can push tasking
- (S//REL) BOXINGRUMBLE bots
  - (S//REL) ~ 45% Vietnamese dissidents
  - (S//REL) ~45% Chinese dissidents
  - (S//REL) ~10% Other
- (TS//SI//REL) Adding BOXINGRUMBLE bots to DEFIANTWARRIOR

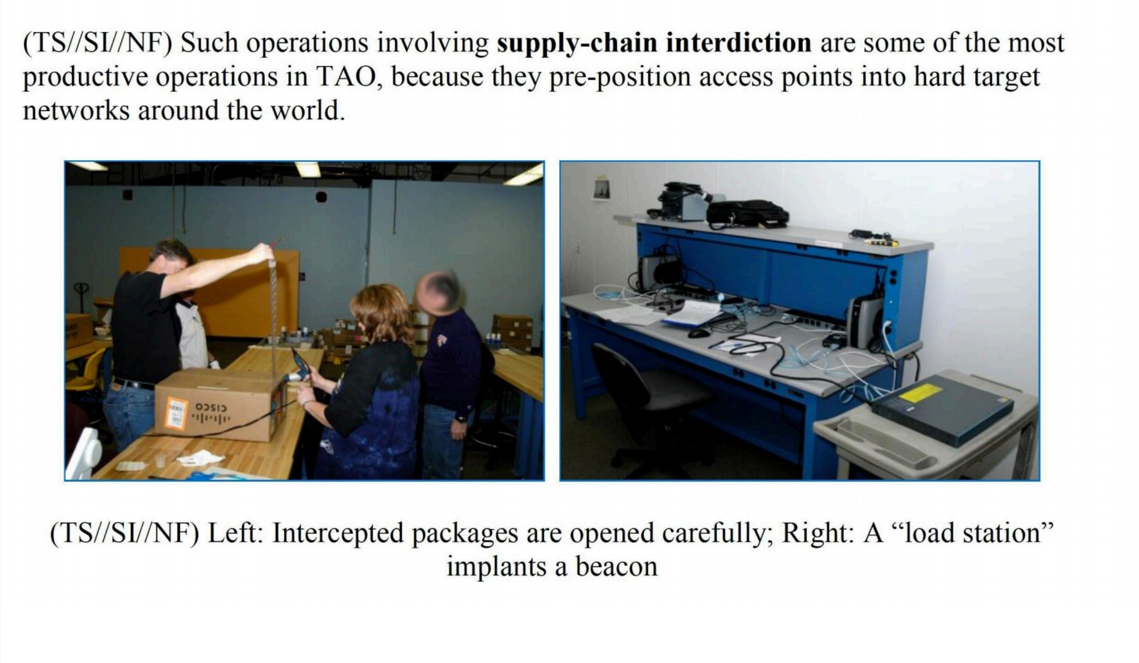
SIGDEV
Bot Commander
Trusted C⁴ Nodes 2-3 Nodes
Trusted C² Nodes ~ 250 Nodes
TAO C² Server
Open Web Proxies
Victims (Bots) 200k Max ~ 30k Today
NSA and TAO Covert Infrastructu re
DEFIANTWARRIOR Implant

TOP SECRET//COMINT//REL USA, FVEY

- Hacking of infrastructure
  - Belgian provider Belgacom: serves **EU** offices
  - Blackberrys at **G20** in London 2009
  - **UN** VC system in New York
  - **SWIFT** system
  - **CIX** in HK/China
  - 2012: Internet down in **Syria**, configuration error

- **Imitation** of Websites such as **Facebook** (Quantum Insert) or **Linked-In**
- **G20** (2009): fake internetcafés near the venue
- **Cookies and Ad-networks** of private actors
  - Google-Play-Connections, Windows crash reports
  - “Fingerprinting across devices”

- Interception of mailings, addition of so-called Implants, transmit data via radio, supposedly also parcels to Germany

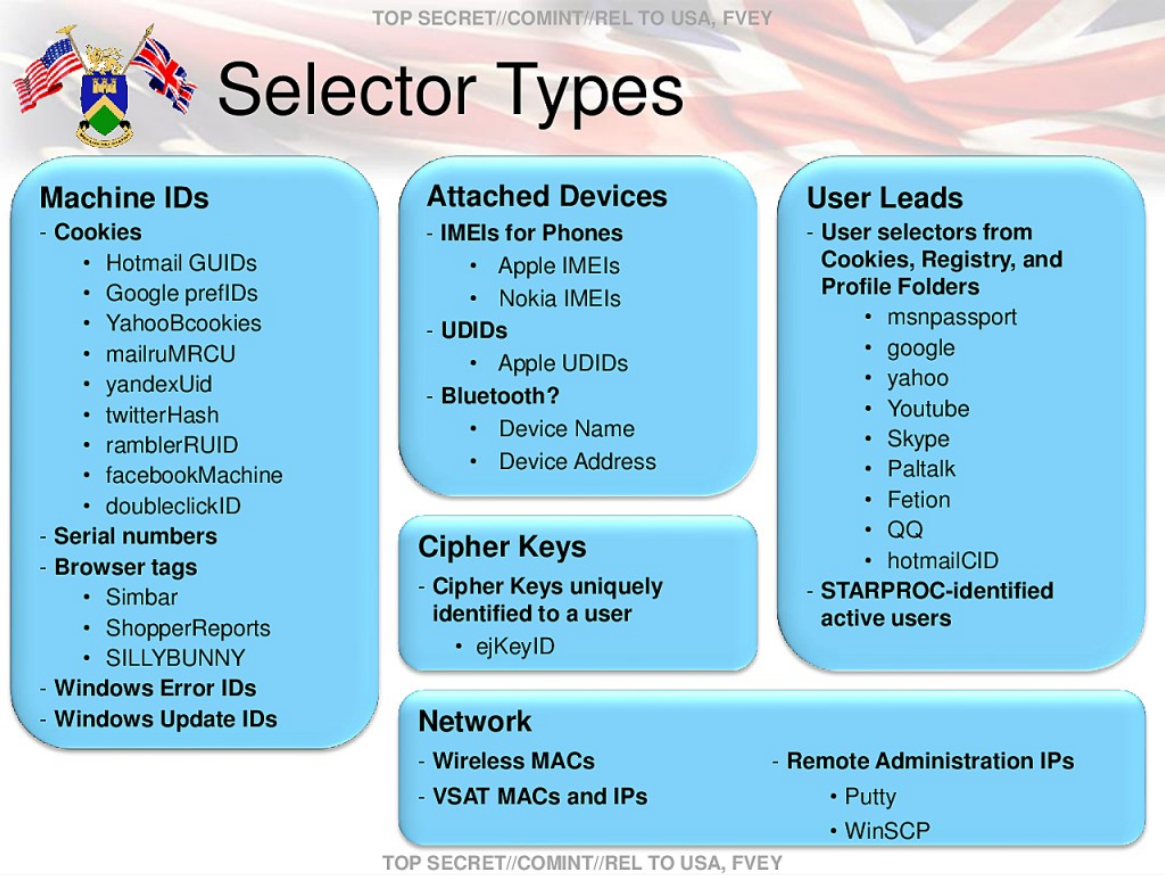


(TS//SI//NF) Such operations involving **supply-chain interdiction** are some of the most productive operations in TAO, because they pre-position access points into hard target networks around the world.

(TS//SI//NF) Left: Intercepted packages are opened carefully; Right: A "load station" implants a beacon

- Weakening of encryption standards (Edgehill/Bullrun)
  - Interference with NIST for standard encryption key **sizes**
  - Cooperation with tech companies, adding **backdoors** (RSA securities)
  - Secret agents in tech companies to retrieve TLS root keys (**HTTPS**)
- Utilising **Anti-Virus-Software**
  - Use Vulnerability reports to find vulnerabilies
  - Hack AVS (jackpot)
- **Gemalto-**Hack (globally largest SIM card producer)
  - Probably copied private Keys of SIM cards

Selectors



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

Selector Types

Machine IDs

- Cookies
  - Hotmail GUIDs
  - Google prefIDs
  - YahooBcookies
  - mailruMRCU
  - yandexUid
  - twitterHash
  - ramblerRUID
  - facebookMachine
  - doubleclickID
- Serial numbers
- Browser tags
  - Simbar
  - ShopperReports
  - SILLYBUNNY
- Windows Error IDs
- Windows Update IDs

Attached Devices

- IMEIs for Phones
  - Apple IMEIs
  - Nokia IMEIs
- UDIDs
  - Apple UDIDs
- Bluetooth?
  - Device Name
  - Device Address

Cipher Keys

- Cipher Keys uniquely identified to a user
  - ejKeyID

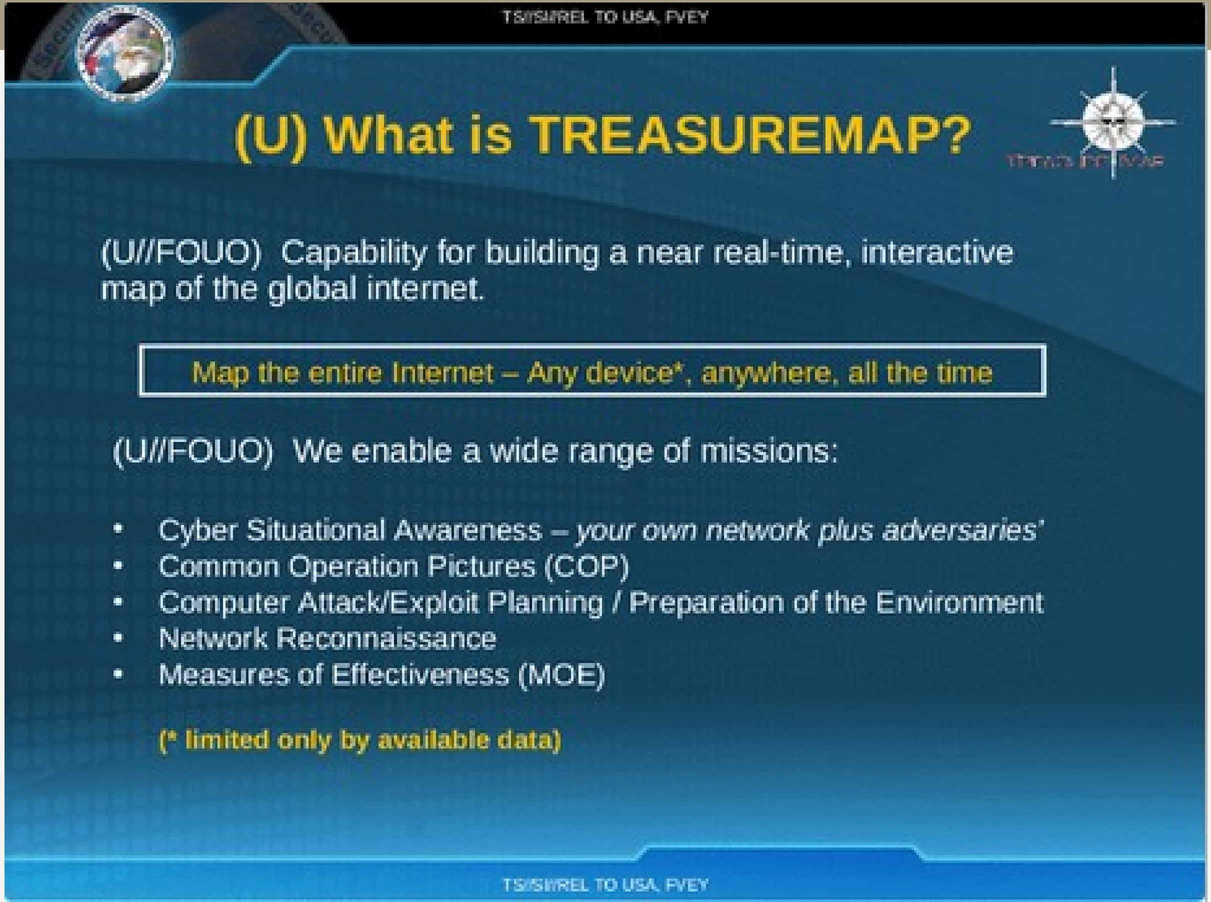
User Leads

- User selectors from Cookies, Registry, and Profile Folders
  - msnpassport
  - google
  - yahoo
  - Youtube
  - Skype
  - Paltalk
  - Fetion
  - QQ
  - hotmailCID
- STARPROC-identified active users

Network

- Wireless MACs
- VSAT MACs and IPs
- Remote Administration IPs
  - Putty
  - WinSCP

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



TS//SI//REL TO USA, FVEY

(U) What is TREASUREMAP?

(U//FOUO) Capability for building a near real-time, interactive map of the global internet.

Map the entire Internet – Any device*, anywhere, all the time

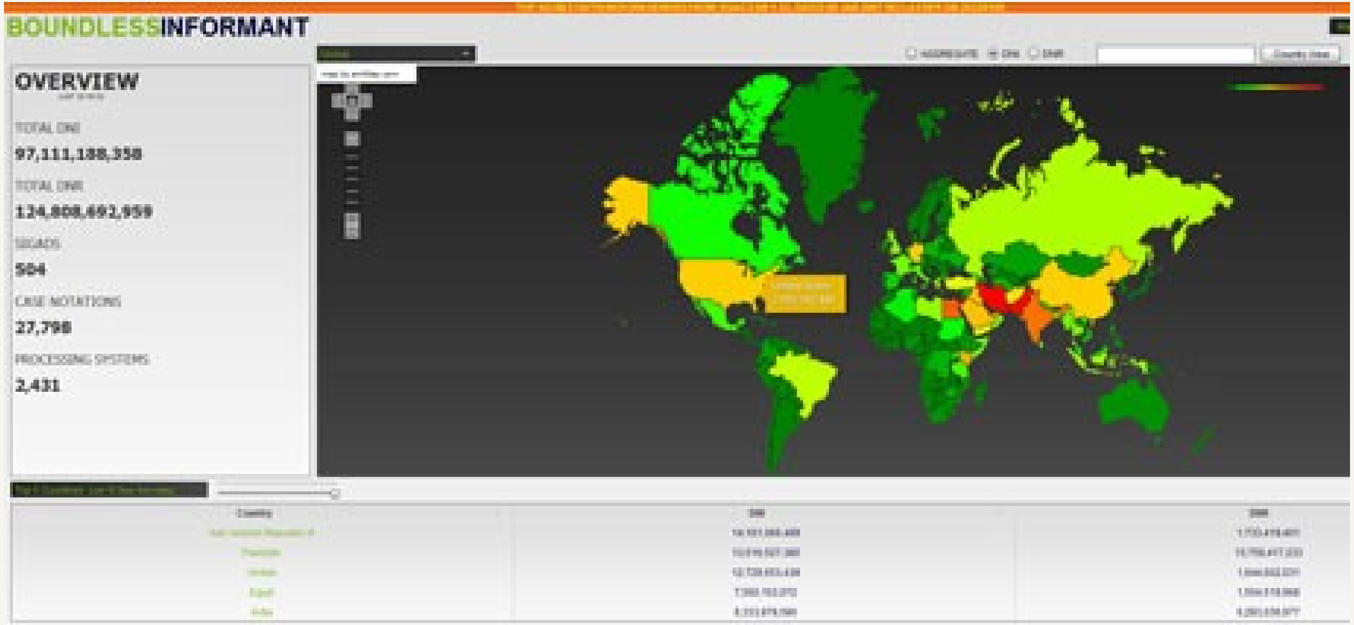
(U//FOUO) We enable a wide range of missions:

- Cyber Situational Awareness – *your own network plus adversaries'*
- Common Operation Pictures (COP)
- Computer Attack/Exploit Planning / Preparation of the Environment
- Network Reconnaissance
- Measures of Effectiveness (MOE)

(* limited only by available data)

TS//SI//REL TO USA, FVEY

- Global overview: Boundless Informant



BOUNDLESSINFORMANT

OVERVIEW

TOTAL DNI

97,111,188,358

TOTAL DNR

124,808,692,959

SIGADS

504

CASE NOTATIONS

27,798

PROCESSING SYSTEMS

2,431

Country	DNI	DNR
Iran, Islamic Republic of	[illegible]	[illegible]
Pakistan	[illegible]	[illegible]
Jordan	[illegible]	[illegible]
Egypt	[illegible]	[illegible]
India	[illegible]	[illegible]

- XKEYSCORE: Search engine
- **150** locations with **700** servers
- Query and configuration tool
  - In data centers and CIX
- Retention
  - Full take 3 to 5 days
  - Metadata 30 to 45 days
- AppIDs, fingerprints and microplugins
  - Protocol, contents and GENESIS

Micah Lee, The Intercept

FOSS detour

„XKEYSCORE is a piece of **Linux** software that is typically deployed on **Red Hat** servers. It uses the **Apache** web server and stores collected data in **MySQL** databases. File systems in a cluster are handled by the **NFS** distributed file system and the **autofs** service, and scheduled tasks are handled by the **cron** scheduling service. Systems administrators who maintain XKEYSCORE servers use **SSH** to connect to them, and they use tools such as **rsync** and **vim**, as well as a comprehensive command-line tool, to manage the software. [...]

Analysts connect to XKEYSCORE over HTTPS using standard web browsers such as **Firefox**. Internet Explorer is **not** supported.“

https://firstlook.org/theintercept/2015/07/02/look-under-hood-xkeyscore/

FOSS detour

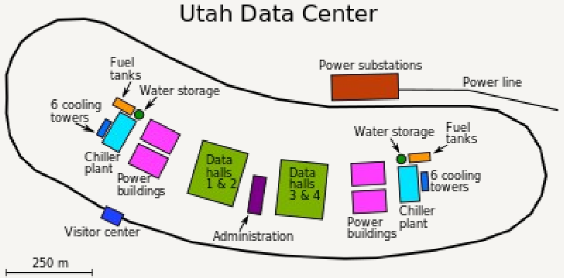
- **Free** Software Movement (1983, MIT AI Lab)
- How about software with a NOINTL/NOMIL clause?
  - R. Stallmann says “No, then it’s not free software anymore!”
- Understanding of “freedom”?

Stallmann GPL

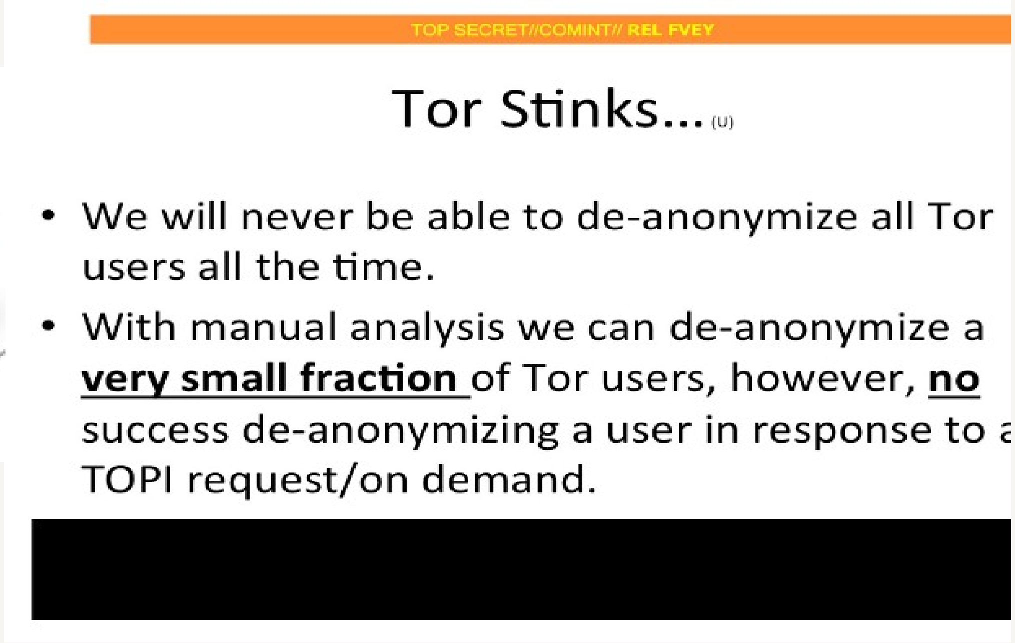
NSA data centers

- **Goal**: Keep all data of the internet for 100 years
  - Retrospective access
  - Breaking of crypto ciphers
- Detail: United States Cyber Command
  - Unification of military and NSA capabilities

By Cory Doctorow, CC-BY-SA



- A note on Tor


TOP SECRET//COMINT// REL FVEY

Tor Stinks... (U)

- We will never be able to de-anonymize all Tor users all the time.
- With manual analysis we can de-anonymize a **<u>very small fraction</u>** of Tor users, however, **<u>no</u>** success de-anonymizing a user in response to a TOPI request/on demand.

[redacted]

What for?

Targets so far

- Surveillance of the EU, the UN (including Ban Ki-Moon), the IAEA, the French Ministry of Foreign Affairs, G8-summit, G20-summit, COP15 (UN Climate Change Conference in Copenhagen), German Chancellor Angela Merkel, her Cabinett, the Turkish and Brasillian government, southamerican oil companies, Visa, Mastercard, the Society for Worldwide Interbank Financial Telecommunication (SWIFT), Huawei, Chinese Government, US-Lawyers, Canadian candidates for „WTO director general“, Media organisations (Spiegel) etc.

- Collecting compromising data on certain subjects
  - Wikileaks, pirate bay, porn sites, … (LOVEINT)
- The US knew the positions of members
  - of the climate negotiations in 2009
  - Sanction talks regarding Iran
  - Energy and oil talks in South America
- Snowden: “If the NSA need Siemens tech knowledge, they know where to look.”

Evaluation

- Bulk-collection evaluated by **Privacy and Civil Liberties Oversight Board** (PCLOB, with access to all classified documents)
  - "lacks a viable legal foundation"
  - "little evidence that […] NSA's bulk collection of telephone records actually have yielded material counterterrorism results that could not have been achieved without the NSA's Section 215 program."
    - Rather use terror prevention and local informats & tips from local communities
  - report recommended to **end** US-bulk data collection
- Similar results from Max Planck Institute for Foreign and International Criminal Law, etc.

Reactions and Consequences

Reactions and Consequences

- US government:

“We need those powers.”

- Public vulnerabilities equities process (VEP)
- IT sec and data protection came into focus in politics and business

Reactions and Consequences

- Thought experiment:

  What would you do as sovereign nation?

Reactions and Consequences

- What would you do as sovereign nation?
  - Have national digital services?
  - Make your own hardware?
  - Make your own software?
  - Have a firewall around your country?

Reactions and Consequences

- What would you do as sovereign nation?
  - Have national digital services!
  - Make your own hardware!
  - Make your own software!
  - Have a firewall around your country!
- Not good, but maybe understandable

- What would you do as sovereign nation partnering with the US?
  - Catch up, also get such capabilities
    - **BND**: SIT (Strategische Initiative Technik)
    - **Military** upgrading (Bundeswehr CIR, offensive IT-Sec, Hackback)
    - **ZITiS**: Hacking assistance for German agencies
      - Headed by an ex-BND director, located at Bundeswehr campus in Munich

Players

- Military/IC (NSA, GCHQ, BND, BfV, ZITiS, Bundeswehr)
  - „Offensive is better than defensive."
- Police (FBI, LKA, BKA, Polizeien)
  - „We want to solve cases, give us hacking tools.
- HR-Organisations
  - „Western countries finance and export hacking tools."
- CS (Universities)
  - „IT-Security cannot provide government exceptions."

Cyber- und Informationsraum
Wir. Dienen. Deutschland.

Players

- Businesses (Siemens, Huawei, Facebook, Google
  - „We need good IT security, we stick to local laws.”
- IT security businesses (Norton, Symantec)
  - „Fear is our business”
- Civil IT security agencies (BSI)
  - „We need IT security without exceptions for the networked society.”
- Civil society (ACLU, EFF, CCC, FIfF)
  - „We need good (IT) security in a peaceful society. We have division of labour.”

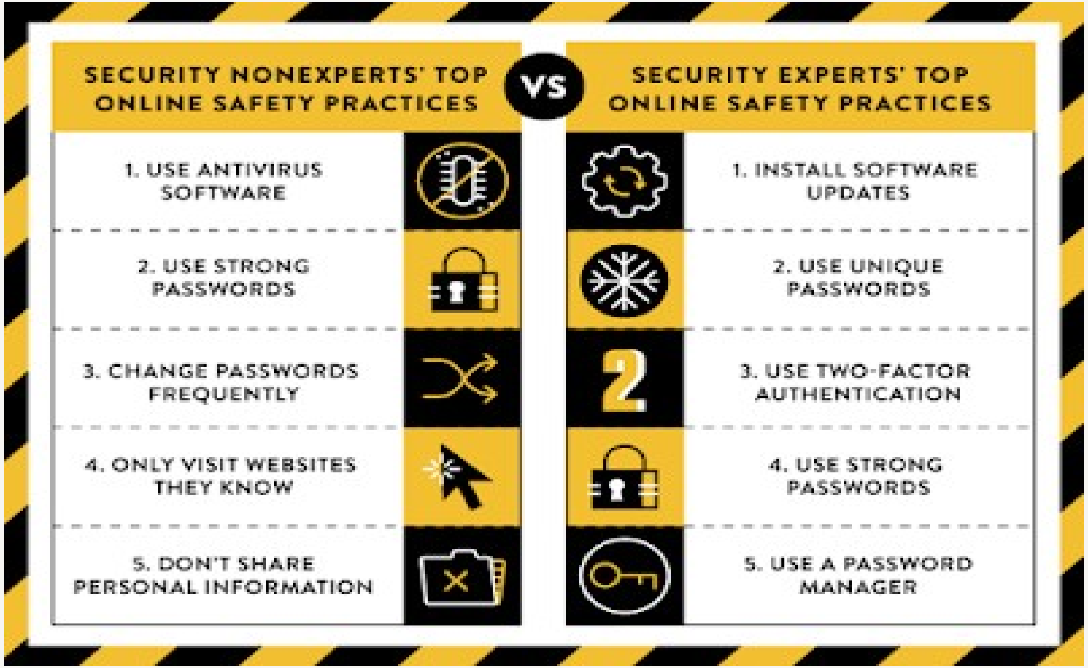
Individual actions?

- Encrypt email?
  - Yes, but…
- Use Signal?
  - Yes, but…
- Delete Facebook?
  - Yes, but…

Individual actions?

- Update regularly?
  - Yes, but...
- Use anti-virus software?
  - Yes, well nooo!!

Self-defense?



SECURITY NONEXPERTS' TOP ONLINE SAFETY PRACTICES	VS	SECURITY EXPERTS' TOP ONLINE SAFETY PRACTICES
1. USE ANTIVIRUS SOFTWARE		1. INSTALL SOFTWARE UPDATES
2. USE STRONG PASSWORDS		2. USE UNIQUE PASSWORDS
3. CHANGE PASSWORDS FREQUENTLY		3. USE TWO-FACTOR AUTHENTICATION
4. ONLY VISIT WEBSITES THEY KNOW		4. USE STRONG PASSWORDS
5. DON'T SHARE PERSONAL INFORMATION		5. USE A PASSWORD MANAGER

https://security.googleblog.com/2015/07/new-research-comparing-how-security.html

Three Scenarios

Preparation by examples

Example 1

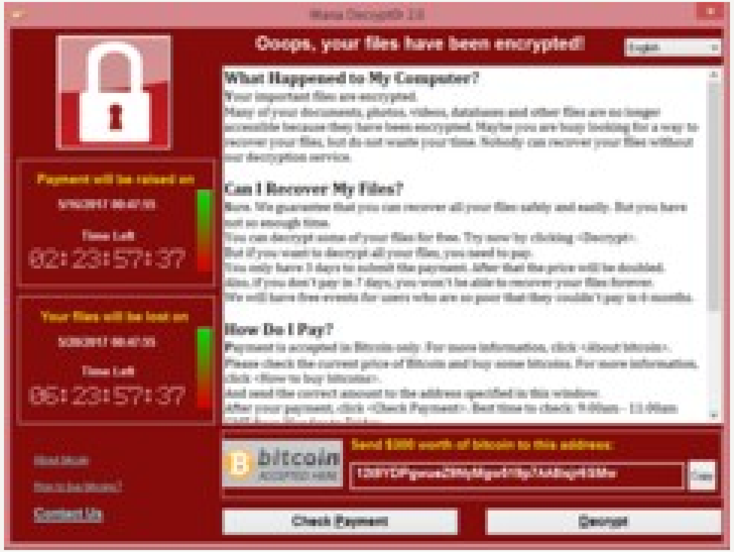
- Target: Blog of IT security journalist Brian Krebs
- DDoS traffic: 665 Gigabit per second

- Source: Botnet, IoT devices, IP cameras, digital video recorders (DVRs), smart fridges
  - Probably continued working

Preparation by examples

Example 2: **WannaCry** 2017

- May 2017, four days active, ca. 300.000 systems infected
  - Crypto trojan, Ransomware
- Affected: individuals, companies, hospitals, train systems, mobile providers
- Financial damage: hundred millions to billions USD
- Technical details:
  - Windows exploits: EternalBlue (SMB) and DoublePulsar (kernel)
  - Source: Shadow Brokers (TSB), prob. developed by the NSA “Equation group”, kept in spite of VEP



Ooops, your files have been encrypted!

Payment will be raised on
[illegible]
Time Left
02:23:57:37

Your files will be lost on
[illegible]
Time Left
06:23:57:37

What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

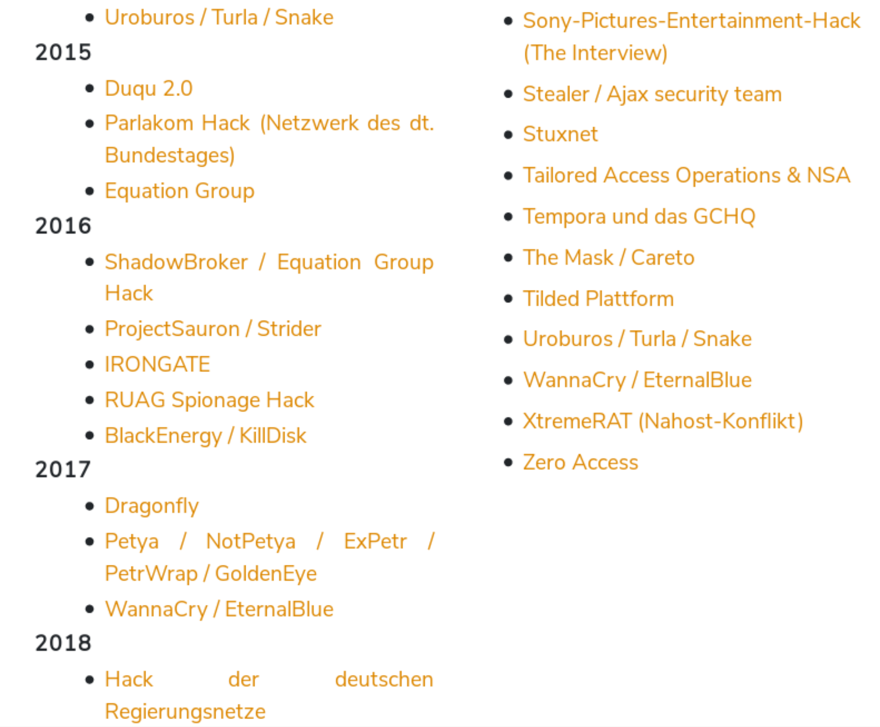
How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Send $300 worth of bitcoin to this address:
[illegible]

Wannacry cont.

- Vuln **EternalBlue** still in use
  - Internal DoD criticism
  - NotPetya in Ukraine
  - Last year attacks on public city systems in **Dallas**, **Los Angeles**, **New York**
    - Damage: millions of USD and counting

A note on incidents



- Uroburos / Turla / Snake

2015

- Duqu 2.0
- Parlakom Hack (Netzwerk des dt. Bundestages)
- Equation Group

2016

- ShadowBroker / Equation Group Hack
- ProjectSauron / Strider
- IRONGATE
- RUAG Spionage Hack
- BlackEnergy / KillDisk

2017

- Dragonfly
- Petya / NotPetya / ExPetr / PetrWrap / GoldenEye
- WannaCry / EternalBlue

2018

- Hack der deutschen Regierungsnetze

- Sony-Pictures-Entertainment-Hack (The Interview)
- Stealer / Ajax security team
- Stuxnet
- Tailored Access Operations & NSA
- Tempora und das GCHQ
- The Mask / Careto
- Tilded Plattform
- Uroburos / Turla / Snake
- WannaCry / EternalBlue
- XtremeRAT (Nahost-Konflikt)
- Zero Access

cyber-peace.org

trust building in cyberspace

Scenarios

- **Scenario 1**: Insecure infrastructure
  - Software crisis, “Bananaware”
  - Systems largely insecure, no regulation
  - Selective exploitation
- **Scenario 2**: Silent Infiltration
  - Systems are largely hacked/infiltrated
  - Leverage in diplomatic negotiations
  - Industrial espionage, digital domination
- **Scenario 3**: Open confrontation
  - Direct action, concrete attacks
  - Burning buildings, lights out, deaths and mayhem

Scenarios

- **Scenario 1**: Insecure infrastructure
  - Software crisis, “Bananaware”
  - Systems largely insecure, no regulation
  - Selective exploitation
- **Scenario 2**: Silent Infiltration
  - Systems are largely hacked/infiltrated
  - Leverage in diplomatic negotiations
  - Industrial espionage, digital domination
- **Scenario 3**: Open confrontation
  - Direct action, concrete attacks
  - Burning buildings, lights out, deaths and mayhem

Scenarios

- **Scenario 1**: Insecure infrastructure
  - Software crisis, “Bananaware”
  - Systems largely insecure, no regulation
  - Selective exploitation
- **Scenario 2**: Silent Infiltration
  - Systems are largely hacked/infiltrated
  - Leverage in diplomatic negotiations
  - Industrial espionage, digital domination
- **Scenario 3**: Open confrontation
  - Direct action, concrete attacks
  - Burning buildings, lights out, deaths and mayhem

Lessons learned

Lessons learned

Everyone **sees** a problem:

- We want to use crypto everywhere, we want data protection everywhere, **clashes** with some business models and LI practices
- Initiative from IGF 2018: Paris Call for Trust and Security in Cyberspace (Macron)
  - coordinated vulnerability disclosure and prevention of the proliferation of malicious ICT tools in peacetime
    - France, UK, Germany; **not** USA, China, Israel, Russia
    - Microsoft, Google, Facebook; **not** Apple, Amazon
- Several calls for “Digital Geneva Convention” by Companies

Lessons lost

A note on data protection in the networked society

- DP does not protect data, it protects **people/society**
- Protection targets (also in GDPR)
  - Transparency (of data and processes for DS)
  - Intervenability (of data and processes for DS)
  - Non-linkability (of data from diff. sources)
  - Confidentiality (of data rel. to DS)
  - Integrity (of data rel. to DS)
  - Availability (of data and services for DS)

Lessons lost

- **Safe Harbour Privacy Principles** dropped in 2015 by ECJ because of the US-activities that Snowden revealed
  - Thanks to Max(imilian) Schrems (see noyb.eu)
- Since 2016: **EU-US Privacy Shield**
  - What has changed?
  - Technically probably not much
    - strategic litigation needed?

A note on IT security in the networked society

- If other systems are hacked, everyone is vulnerable
  - There are no “uncritical systems” (anymore)
  - **“Networked society”**
- No one **fully controls** their system, all have vulns in
  - Hardware
  - OS
  - Devices of employees
  - Used libraries/frameworks
- Political problems
  - Missing **knowledge** concerning global effects
  - Low **priority** for those issues

Lessons lost

- We can **invalidate** exploits (compare ABC-Weapons)
  - Export /service control for ICT anyone?
- **NOBUS** (NSAish for Nobody But Us) doesn’t work anymore
  - Huge grey market for exploits and services, **legitimized** by state actors
- **Militarisation** of the Internet hurts everyone (Weizenbaum would strongly oppose anyway)
  - No public safety/security without IT security
- In need of **stricter** rules, e.g. time-to-market should not be primary goal
  - Market does not work with hygiene rules, environmeltal rules, road traffic rules

So far, our Digitalisation is built on sand

So far, our Digitalisation is built on sand…
but we know how to change that:
stricter laws, software liability, decentralized systems, political education, data protection, demilitarisation, slow digitalisation, strategic litigation...

Thank you

CC BY Rainer Rehak

Literature, Links and Leisure

- Clement, Andrew et al.: Snowden Digital Surveillance Archive
  - https://snowdenarchive.cjfe.org
- Anderson, Ross: Security Engineering:
  A Guide to Building Dependable Distributed Systems, 2008
- Schneier, Bruce: Secrets & Lies
  Digital Security in a Networked World, 2015
  https://www.schneier.com/books/secrets_and_lies/
- Explanatory Cyberwar-Clip: https://vimeo.com/216584485
- Documentary “Zero Days”: https://www.imdb.com/title/tt5446858/
- Now You Know. Vier Jahre Snowden: https://www.nowyouknow.eu/

fiff.de