NSA, GCHQ und die „offensive cyber effect operations“

Nachrichtendienstliche Fähigkeiten im Cyberspace

Thomas Reinhold – info@cyber-peace.org

Institut für Friedensforschung und
Sicherheitspolitik an der Universität Hamburg

Übersicht

- Die Five-Eyes-Programme im Überblick
- Technische Möglichkeiten aus Sicht des „Cyberwar“
- „Offensive cyber effect operations“ und die „Cyberwar-Liste“
- Juristische Kontrolle der Geheimdienste
- Bündnisse und Kooperationen
- Außen- und Innenpolitische Reaktionen
- Einschätzung

Die „Five Eyes“

- Offiziell „UKUSA“
- Vertrag von 1947 zwischen Großbritannien & den USA
- Zusammenarbeit der Geheimdienste
  - USA: NSA – National Security Agency
  - UK: GCQH - Government Communications Headquarters
- Später zusätzlich beigetreten
  - Australien: DSD - Defence Signals Directorate
  - Kanada: Communications Security Establishment Canada
  - Neuseeland: GCSB - Government Communications Security Bureau

5 Eyes-Programme im Überblick

- Daten erfassen und kontrollieren
  - Nutzerdaten von Internetdiensten
  - Kommunikationsdaten
  - Wirtschaftsrelevante Informationen
  - Daten über/von fremden Regierungen
- Daten auswerten und Metadaten generieren
  - Wer-Wann-Wo-Mit-Wem-Wie lange
  - „Metadaten aussagekräftiger als Einzelinformationen“
- Speichern und (Ver)Teilen

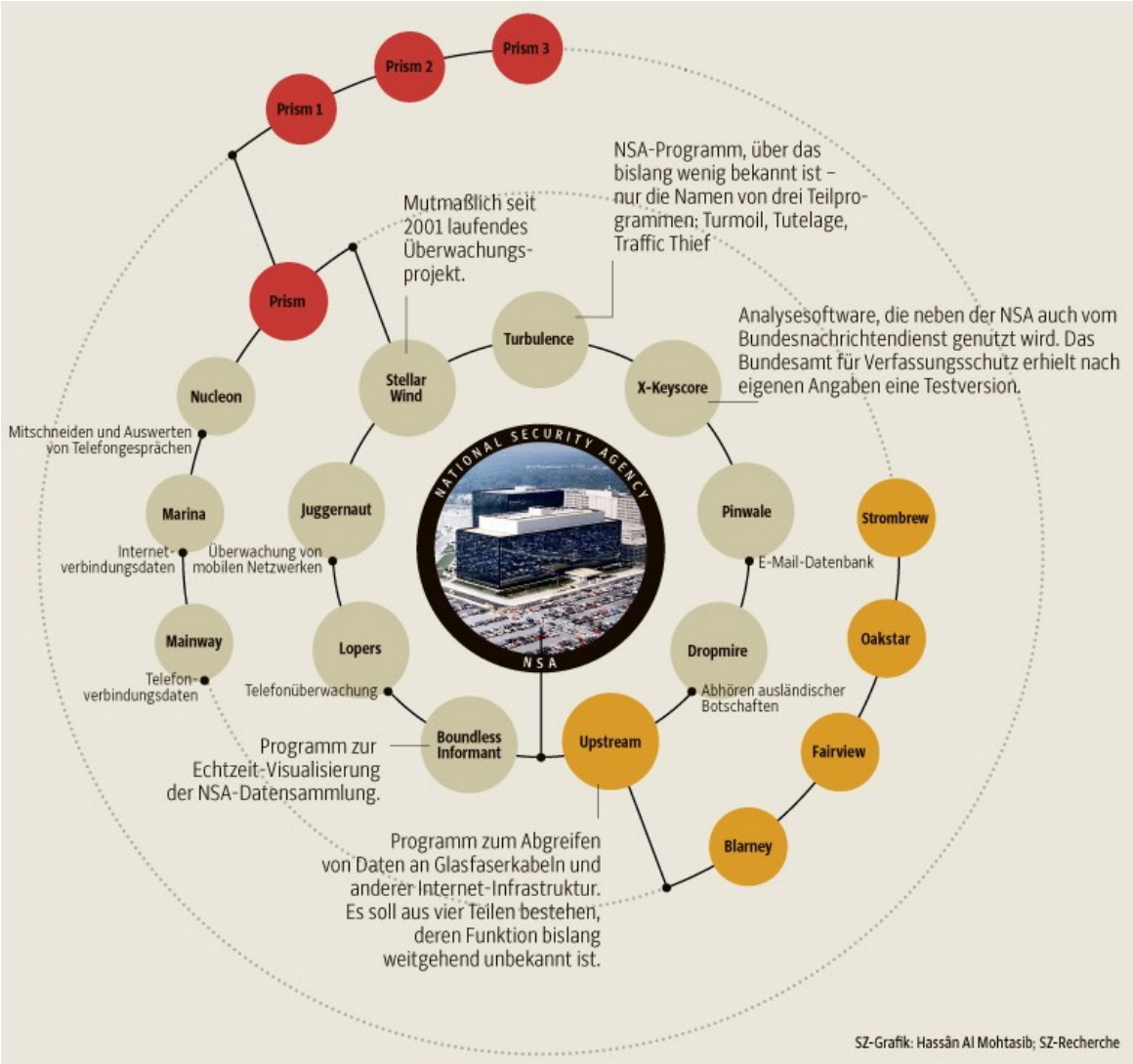
“You’re not waiting for someone to decide to turn information into electrons and photons and send it (..) You’re commuting to where the information is stored and extracting the information from the adversaries’ network. We are the best at doing it. Period.”

Michael Hayden, ehemaliger Leiter der NSA/CIA unter G.W. Bush

5 Eyes-Programme im Überblick II

IFSH
Institut für Friedensforschung
und Sicherheitspolitik
an der Universität Hamburg

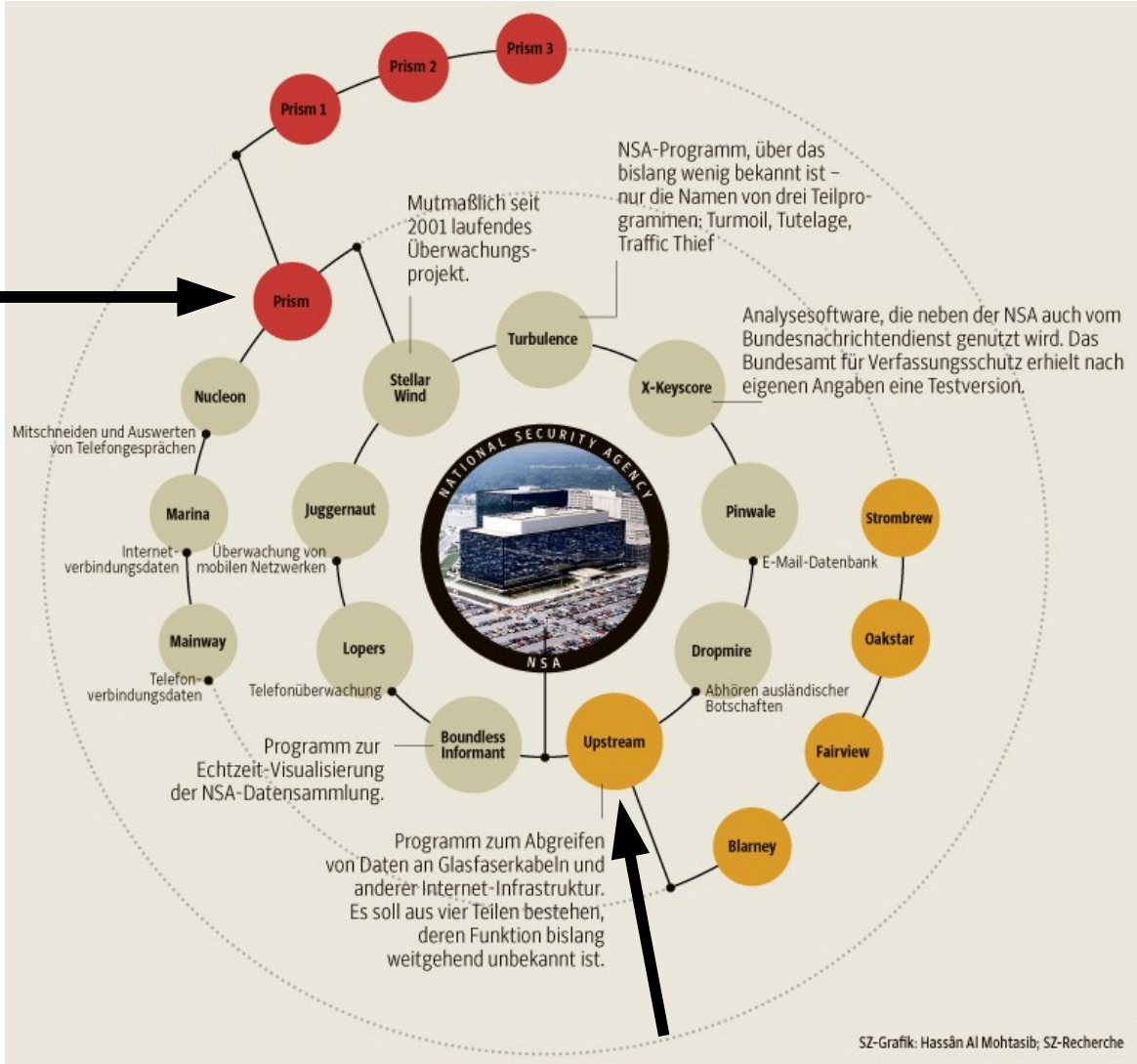
- Daten erfassen und kontrollieren
- Daten auswerten
- Speichern



5 Eyes-Programme – Erfassen

IFSH
Institut für Friedensforschung
und Sicherheitspolitik
an der Universität Hamburg

- Daten erfassen und kontrollieren
- Daten auswerten
- Speichern



5 Eyes-Programme – Erfassen II

- PRISM & Upstream
  - Bezahlte Dienstleistung für den Direktzugriff auf Daten von Google, Microsoft, Apple, Yahoo, Youtube, Facebook, AOL, Skype und Paltalk
  - Kooperationen mit großen Traffic-Carriern (Level 3, Verizon, AT&T), Zusammenarbeit mit FBI-Einheit DITU (Data Intercept Technology Unit)
- U-Boot USS „Jimmy Carter“
- Tailored Access Operations
  - 600 Personen-Hacker-Einheit inkl. „Field-Unit“ für Vor-Ort-Zugriff
  - 60k++ Zugriffe weltweit (viele chinesische Systeme, DE-CIX)
- Tracfin
  - Informationen zu weltweiten Finanztransaktionen
  - bis 2011 dort 180 Millionen Datensätze gesammelt haben. (84 % von Visa stammen, weitere von der europäischen Swift)

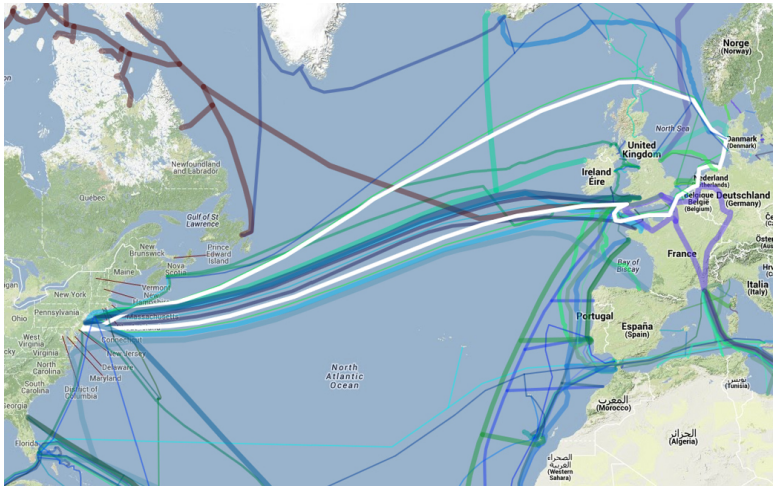
5 Eyes-Programme – Erfassen III

- ACIDFOX
  - Server-Infrastruktur zur gezielten Infektion von verschlüsselten Datenverbindungen (TOR etc)
  - Packet Injection und Man-in-the-middle-Attacken
- Bullrun
  - Schwächung und Knacken (?) von Kryptographie-Systemen
- GENIE
  - 652 Millionen US-Dollar Budget (lt. „Black Budget 2011“)
  - Einbruch und Kontrolle ausländischer Netzwerke
  - Bis Ende 2013 85.000 strategisch ausgewählte Computern zu infizieren
  - System "Turbine" für automatischen Betrieb der Spionage-Tools
- Zugriff weitere Quellen...

5 Eyes-Programme – Erfassen IV

IFSH
Institut für Friedensforschung
und Sicherheitspolitik
an der Universität Hamburg

- Tempora (UK GCHQ)
  - Abhören und Mitschneiden von Datenübertragungen insbesondere von Glasfaser-Backbones (Atlantik, Zypern, naher Osten)



- Quantum Insert (UK GCHQ)
  - Man-in-the-Middle-Attacken auf auf strategisch wichtige Unternehmen
  - OPEC, belgische Belgacom (EU-Parlament,...), Mobilfunk-Provider

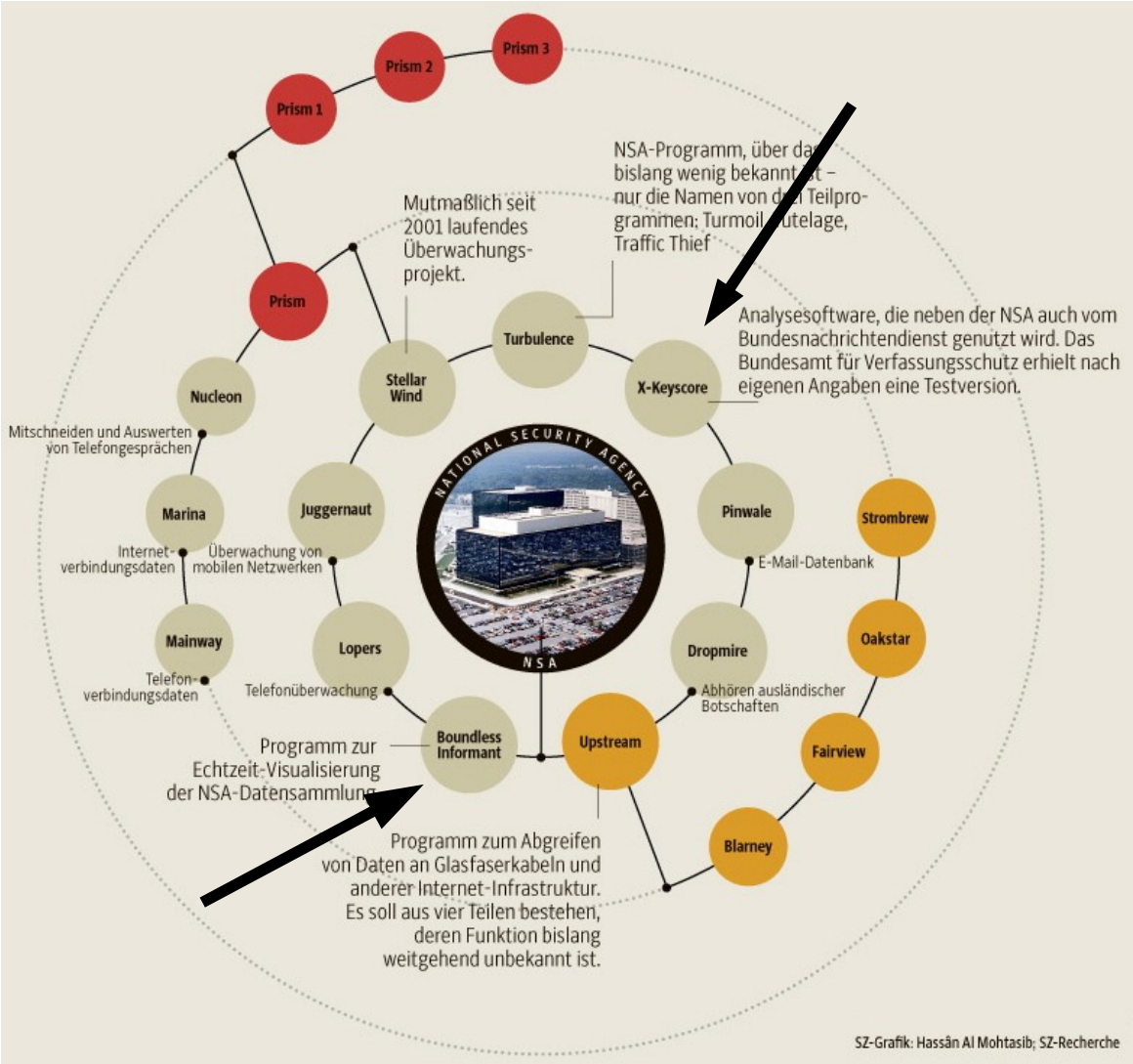
5 Eyes-Programme – Erfassen V

- Zusammenfassung
  - Daten der Nutzer von Internetdiensten
  - Kommunikationsdaten und Kommunikationsinhalte
  - Daten zu weltweiten Finanztransaktionen
  - Umfassender Direktzugriff auf weltweite IT-Infrastruktur und das Glasfaser-Backbone-Netz
  - „Full take“ des Datentransfers
  - Zugriff und Kontrolle strategisch entscheidender Computersysteme
  - Hackereinheit für gezielten Zugriff
  - Angriff auf Kryptographie

5 Eyes-Programme – Auswerten

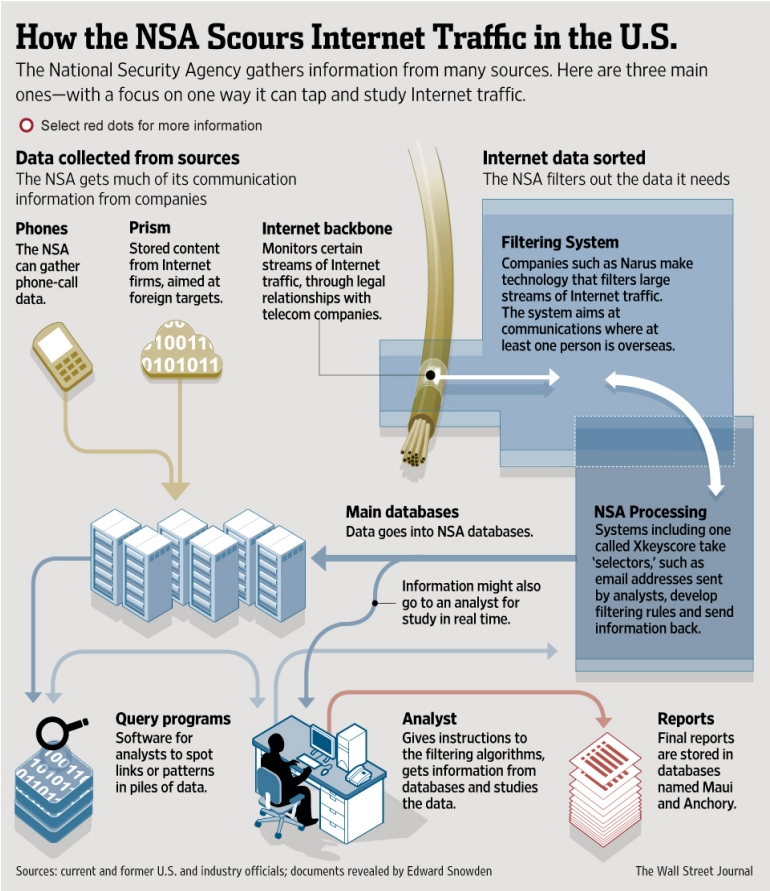
IFSH
Institut für Friedensforschung
und Sicherheitspolitik
an der Universität Hamburg

- Daten erfassen und kontrollieren
- Daten auswerten
- Speichern



5 Eyes-Programme – Auswerten II

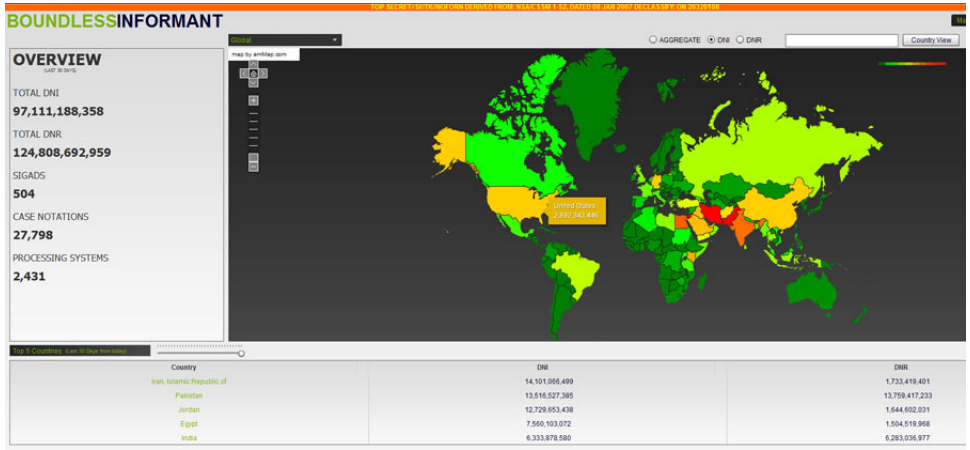
- Xkeyscore
  - Analyse-Tool für Datenbestände
  - Automatisierte Analyse und Filter
  - Zusammenführung von Daten unterschiedlichster Quellen (Marina, Mainway, Nucleon und Pinwale)
  - Zugriff auf *„fast alles, was ein typischer Nutzer im Internet macht“*
  - Bei BND seit 2007 in Bad Aibling und an „zwei weiteren Stellen seit 02.2013“ im Einsatz
  - BfV testet auf Einsatzfähigkeit



5 Eyes-Programme – Auswerten III

IFSH
Institut für Friedensforschung
und Sicherheitspolitik
an der Universität Hamburg

- Boundless Informant
  - Frontend für Überblick über Datenbestände und Überwachungsmaßnahmen

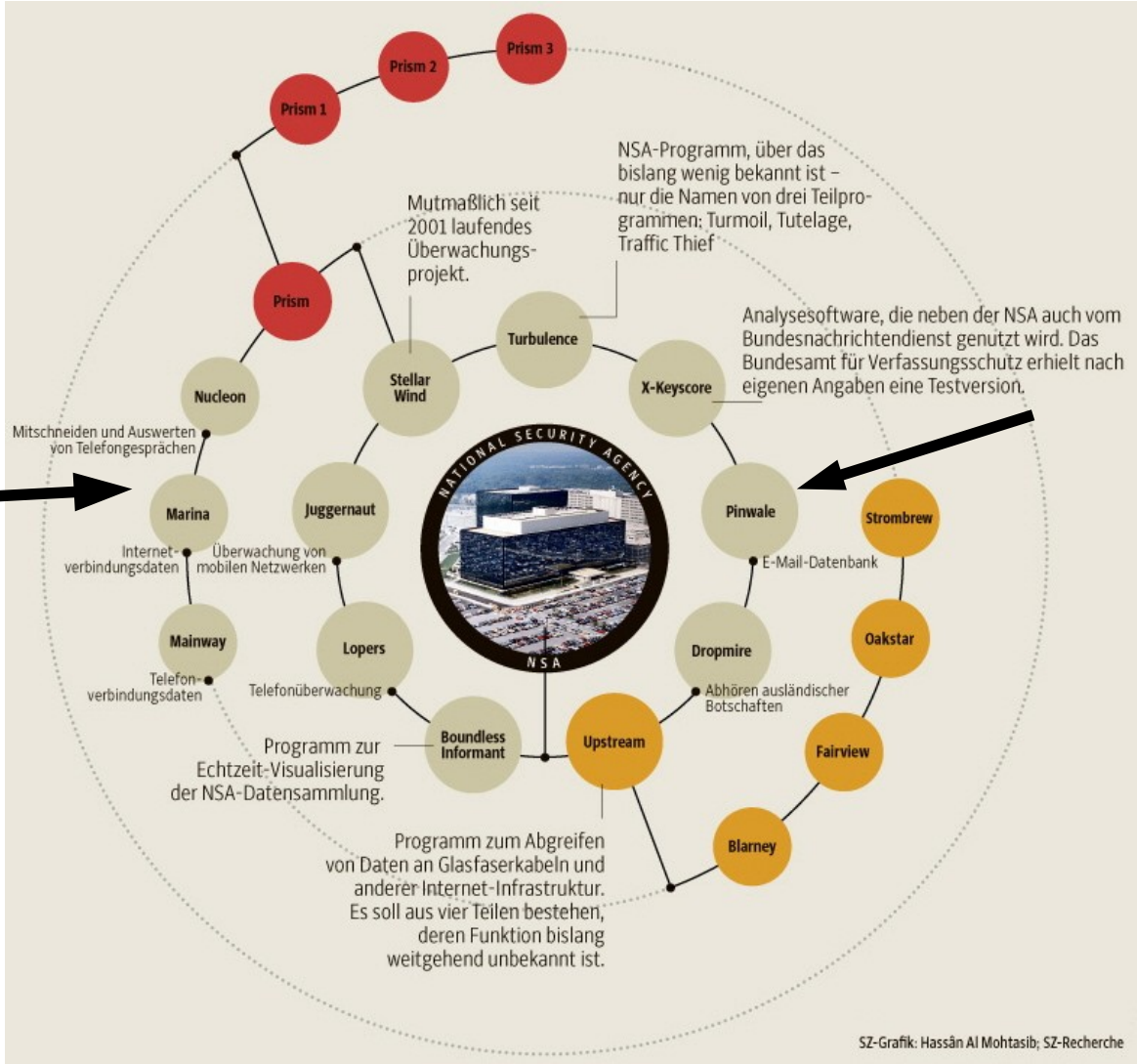


- Tempora
  - Schlagwortliste und Zielkontaktliste für die automatisierte Auswahl von Daten und spätere Detail-Analyse
  - Mehrere 10.000 Schlagworte

5 Eyes-Programme – Auswerten

IFSH
Institut für Friedensforschung
und Sicherheitspolitik
an der Universität Hamburg

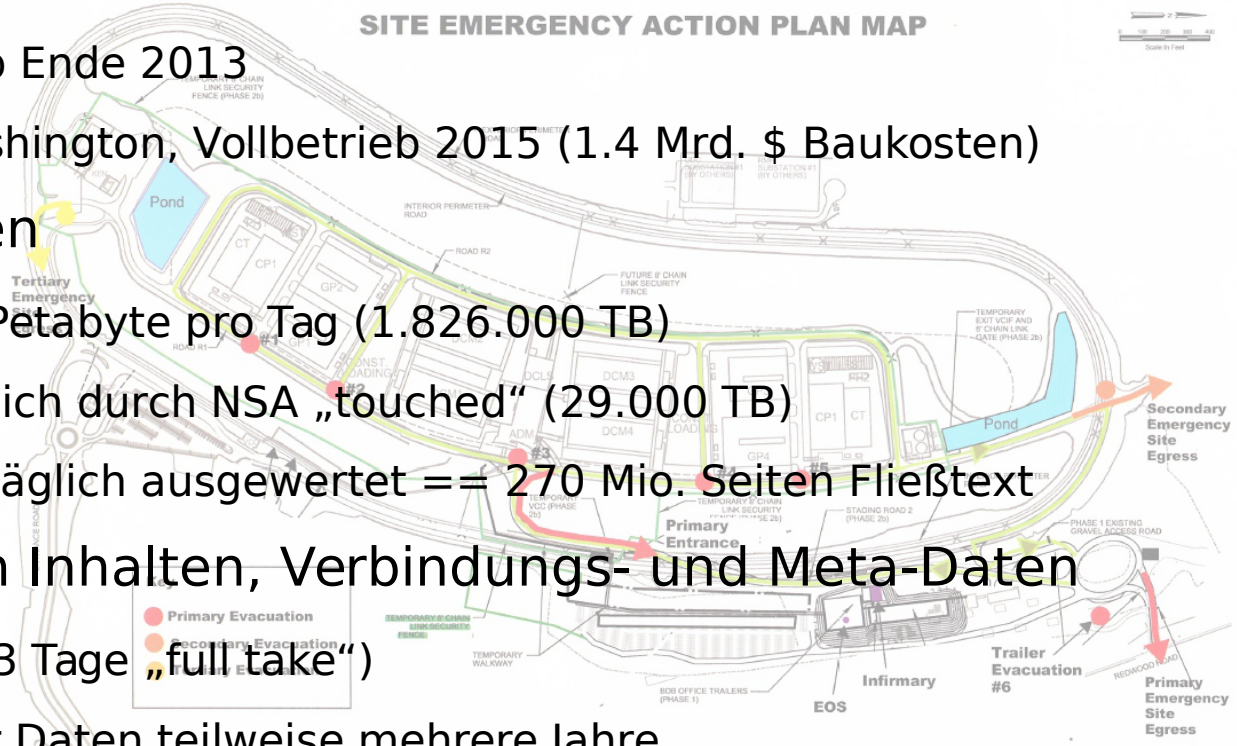
- Daten erfassen und kontrollieren
- Daten auswerten
- Speichern



5 Eyes-Programme - Speichern

IFSH
Institut für Friedensforschung
und Sicherheitspolitik
an der Universität Hamburg

- NSA-eigene Rechenzentren
  - Utah, Vollbetrieb Ende 2013
  - Fort Meade, Washington, Vollbetrieb 2015 (1.4 Mrd. $ Baukosten)
- Datenaufkommen
  - Weltweit 1.826 Petabyte pro Tag (1.826.000 TB)
  - 29 Petabyte täglich durch NSA „touched“ (29.000 TB)
  - 0.007 PB (7TB) täglich ausgewertet == 270 Mio. Seiten Fließtext
- Speicherung von Inhalten, Verbindungs- und Meta-Daten
  - Internet-Puffer (3 Tage „full take“)
  - Speicherung der Daten teilweise mehrere Jahre
  - EvilOlive und ShellTrumpet, Stellar Wind, Pinwale



Die Technik des Cyberwar

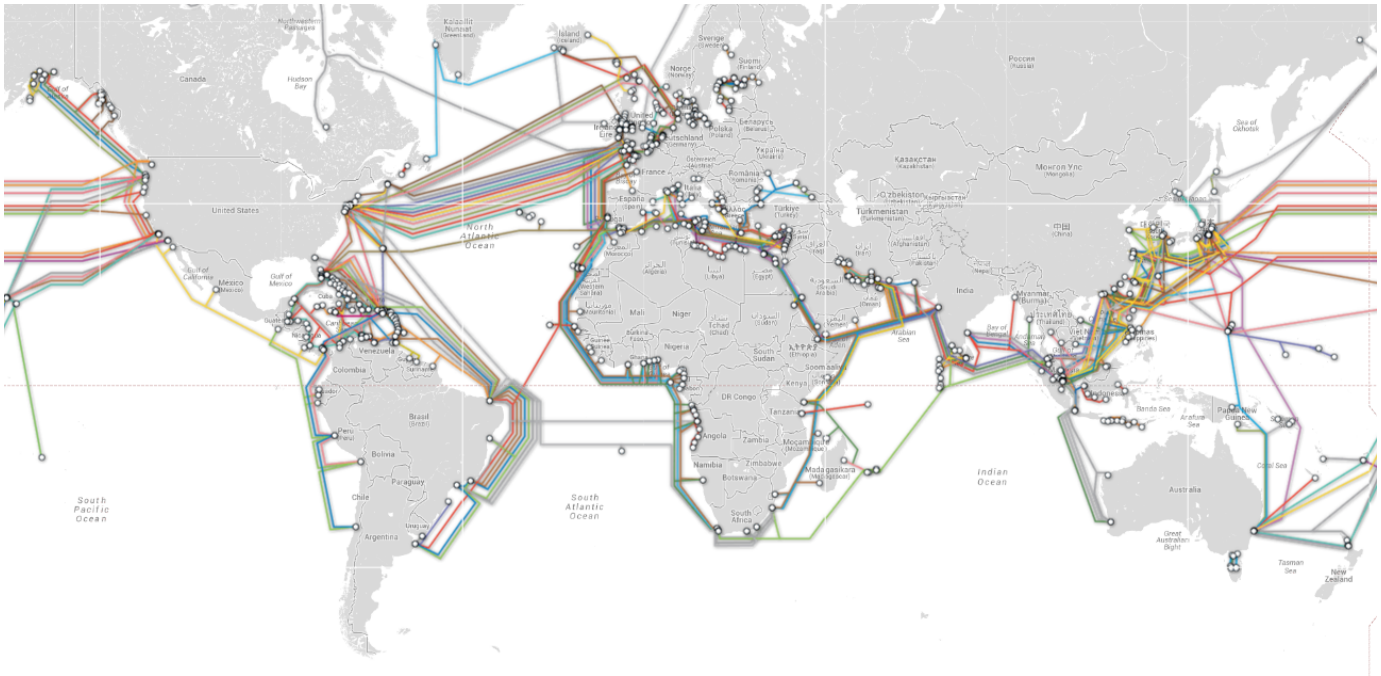
Q: *How will „cyber weapons“ look like*
A: *Have a look at the Snowden papers*

Die Technik des Cyberwar II

- Hacking-Einheiten
  - NSA: Tailored Access Operations: „*we hack backbones*“
  - 25 Mio. $/2013 für Aufkauf von Sicherheitslücken und 0-Day-Exploits
  - Entwicklung eigener Malware, insbesondere für spätere, erweiterte Zugriffe
  - Botnetz mit „Millionen infizierter Computer“ („digitale Schläfer“, DDoS)
  - Zugriff auf alle mobilen Betriebssysteme (iOS/Android/Blackberry)
  - 2011: 231 gezielte Cyberangriffe (~3/4 gegen Ziele mit höchster Priorität)
  - 2011: Mehr Rechner geknackt als mit ~1800 Mitarbeitern ausbeutbar
  - Programm "Genie" für Kontrolle ausländischer Netzwerke
  - UK: MyNOC - My Network Operations Centre

Die Technik des Cyberwar III

- Kontrolle großer Teile des Glasfaser-Backbones
  - Knoten in USA, UK, naher Osten, Zypern angezapft
  - USS Jimmy Carter für das unterseeische Anzapfen
  - „Field Unit“ der Einheit für „Tailored Access Operations“
  - Eigene Server im Backbone für Man-in-the-Middle-Attacken (ACIDFOX)



Die Technik des Cyberwar IV

- Industrie- und Wirtschaftskooperationen
  - Gespeicherte Nutzerdaten von Dienste und Traffic
  - Meldung von unbekannten Sicherheitslücken an die NSA
  - Gezielter Einbau von Hintertüren in Software / Hardware (Cisco/IBM)
  - Direkter Zugriff auf Router & Firewalls namhafter Hersteller
  - Insiderwissen für targeted attacks (Stuxnet & Siemens)
  - Einflussnahme auf Standarisierungsprozeße und Protokolle

Die Technik des Cyberwar V

- Kryptographie angreifen
  - Verschlüsselung von Daten (TLS/SSL, https, E-Mail, VPN, Skype)
  - Gute Krypto theoretisch nicht knackbar => „schwache“ Krypto ist knackbar
  - Schwächen entweder „by design“ oder in der konkreten Code-Umsetzung
  - Gezielte Einflussnahme bei Standarisierungsprozeßen, Richtlinienverfahren und technischen Spezifikationen
  - „Consolidated Cryptologic Program“ mit 35.000 Mitarbeitern und einem jährlichen Budget von 11 Mrd. Dollar
  - Möglicherweise mathematisch geknackte Kryptoverfahren
  - „Human Intelligence division“ für Direktkontakte zur ICT-Industrie
  - Datenbank mit Schlüsseln für bestimmte kommerzielle Produkte („Key Provisioning Service”) und den Zugriff auf diese („Key Recovery Service”)

Die Technik des Cyberwar VI

- Zusammenfassung
  - Hacking-Einheiten, Entwicklung und Einsatz von Schadsoftware
  - Zugriff und großflächige Kontrolle des Internet-Backbones
  - Industrie- und Wirtschaftskooperationen
  - Angriff und Schwächen von Kryptographie

Obamas „Cyberwar Liste“

- Presidential Policy Directive PPD-20, Oktober 2012
  - "Offensive Cyber Effects Operations“ (OCEO) für Ziele im Cyberspace
  - Cyber Operations Policy Working Group aus Verteidigungsministerium und Geheimdiensten:

    „shall prepare (..) a plan that identifies potential systems, processes and infrastructure against which the United States should establish and maintain OCEO capabilities“
  - Auswirkungen „ranging from subtle to severely damaging“
  - Offensive, eigenverantwortliche Operationsbefugnis ohne explizite Begrenzung auf reine Vergeltungsschläge

    "*whenever US national interests and equities require such nonconsensual attacks. It expressly reserves the right to use cyber tactics as part of what it calls "anticipatory action taken against imminent threats*"
  - Auftrag zur Identifikation potentieller Ziele im Cyberspace „to advance US national objectives“
- NSA Strategiepaper (02.2012) „SIGINT battle space“

Juristische Kontrolle d. Geheimdienste

- NSA: FISC
  - Foreign Intelligence Surveillance Court, Bundesgericht seit 1978, soll Überwachungsaktionen der nationalen Auslandsgeheimdienste regeln
  - Tagt im Geheimen, Beschlüsse nicht öffentlich, durch Patriot Act umgehbar
  - FISA (Foreign Intelligence Surveillance Act) 2008: Exekutive kann ohne konkrete Gefahrenbenennung Beschlüsse zur Überwachung erwirken, teilweise ohne Richtervorbehalt

    „Der FISC habe nicht die Kapazitäten, Regelverstöße der US-Sicherheitsbehörden zu untersuchen, erklärte dessen Vorsitzender Reggie Walton gegenüber der Washington Post“
    (http://heise.de/-1937397)

    "*They've had tens of thousands of requests and turned down maybe six at most*"
    (ehemal. NSA-Analyst Russell Tice, Guardian-Interview)
  - Rückwirkende Genehmigung bei „Gefahr im Verzug“ sowie bei Verdacht auf Spionage ausländischer Mächte, Hackerattacken oder WMD

Juristische Kontrolle d. Geheimdienste II

- GCHQ:
  - Intelligence Services Act (1994)
  - Regulation of Investigatory Powers Act (2000)
  - Verpflichtung für Operationen die Genehmigung eines Ministers einzuholen, in der Regel die des Außenministers oder des Innenministers
  - Ausschuss für Nachrichten- und Sicherheitsdienste (Intelligence and Security Committee – ISC) als parlamentarisches Kontrollgremium ohne Exekutiv-Gewalt, informiert seit 2013 über Operationen der Nachrichtendienste

    „Die zunehmenden und immer diffuseren Bedrohungen durch Terrorismus, Kriminalität oder Spionage haben unsere nachrichtendienstliche Zusammenarbeit mit den USA nur noch wichtiger gemacht“ (britischer Außenminister William Hague, Juni 2013)
- Umweg der Datensammlung durch Partner

Bündnisse und Kooperationen

- Vier Level an Kooperationen
  - Tier 1 (Comprehensive Cooperation) bestehend aus den Five-Eyes (USA, UK, Kanada, Australien, Neuseeland)
  - Tier 2 (Focused Cooperation) bestehend aus 9, vorwiegend europäischen, Ländern (Dänemark, Norwegen, Schweden, Frankreich)
  - Tier 3 (Limited Cooperation) besteht 14 Ländern, u.a. Israel, Indien und Pakistan, Deutschland
  - Tier 4 (Exceptional Cooperation) umfasst Länder mit denen die USA nur in Ausnahmefällen kooperieren würden, da diese feindliche Interessen haben

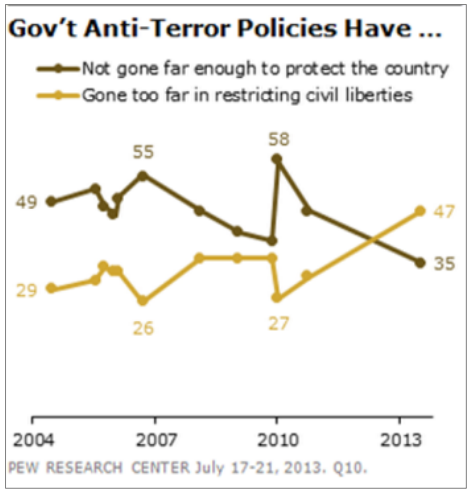
Bündnisse und Kooperationen II

- Deutschland
  - Aktive BND-NSA-Kooperationen (Datenaustausch, Xkeyscore et. al.)

    "*Germans were a little grumpy at not being invited to join the 9-Eyes group*"
    (NSA-Dokument von 2009)
  - Hintergrund der aktuellen Proteste der dt. Regierung

    „Significantly, amid the German protestations of outrage over US eavesdropping on Merkel and other Germans, Berlin is using the controversy as leverage for an upgrade to 5-Eyes" (Guardian)

Außen- & Innenpolitische Reaktionen



- Innenpolitische Reaktionen
  - Wirtschaftlicher Schaden 35-180 Mrd. $
  - Öffentliche Ablehnung der NSA-Programme von PRISM-Partner (Google, Yahoo)
  - Bemühungen um stärkere Transparenz durch Disclosure von NSA-Dokumenten
  - B. Obama, General K. Alexander (NSA) James R. Clapper Jr., (National Intelligence) verteidigen Programme
  - Abhören von US-Amerikanern als innenpolitische Grenze
  - *"47% say their greater concern about government anti-terrorism policies is that they have gone too far in restricting the average person's civil liberties, while 35% say they are more concerned that policies have not gone far enough to protect the country". This is the first time in Pew Research polling that more have expressed concern over civil liberties than protection from terrorism since the question was first asked in 2004".* (Guardian)
  - US-Kongress „*Momentum Builds Against N.S.A. Surveillance*" (NY Times)

Außen- & Innenpolitische Reaktionen

- Außenpolitische Reaktionen
  - Abhören von EU-Gremien: Diskussion um Aussetzen SWIFT & Safe Harbor
  - Verhandlungen zu EU-USA-Freihandelsabkommen in Frage gestellt
  - Abhören von 35 Spitzen-Politikern (Frankreich, Brasilien, Deutschland, Italien, Spanien …): Vertrauensreise in Europa geplant, bilaterale Gespräche angesetzt
  - Brasilien: Resolutionsentwurf gegen das Ausspähen von elektronischer Kommunikation bei Ausschuss für humanitäre Fragen der UN-Vollversammlung eingereicht
  - Russland & China auffallend öffentlich still, aber erhalten Aufschwung für ihre Initiativen der stärkeren UN-Kontrolle über das Internet (ITU-Debatten) und nationalstaatliche Souveränität

Einschätzung

- Internationale Zusammenarbeit der Geheimdienste
  - USA, Großbritanniens, Kanada, Neuseelands & Australien (Five Eyes et. al.)
  - Weitere Kooperationen auf unterschiedlichen Leveln
- Aktive „Cyberdefence“-Orientierung der Programme
  - Tailored Access Operations: Informationen zur Bereitschaft ausländischer Streitkräfte
  - Tempora: „data had been used in the field of cyberdefence“
- US-Direktive zu Offensive Cyber Effects Operations
  - erste „potentially aggressive cyber warfare doctrine“ mit expliziter Schadwirkung

Einschätzung II

- Technischer Stand der Programme
  - Potentieller Zugriff auf beliebige Daten unabhängig von deren Schutz
  - Zugriff auf die zentralen ICT Infrastrukturen (KRITIS)
  - Industriekooperationen (Backdoors, Zero Day Exploits, Standards)
- Fähigkeiten „offensiver Cybertools“
  - Schaden durch Cybertools nicht mehr eine Frage des „ist es machbar“ als vielmehr des „wollen wir das machen“
  - Verbleibende technische Schwellen für Cyberoperationen bleiben Grad der Geheimhaltung und die verfügbare Vorbereitungszeit

Einschätzung III

- Zukünftige Debatten – wie Weiter?
  - Datenschutz und das Recht auf Privatsphäre weltweit?
  - Zwischenstaatliches Vertrauen und internationale Regelungen zu Spionage
  - „Power“ im Internet, Multi-Stakeholder-Modell vs. UN
  - Definitionen, Einsatzregeln und Grenzen von Cyberwaffen

Links

- Golem.de Glossar zu PRISM & Co.: http://goo.gl/oislVL
- Blog Bruce Schneier: www.schneier.com/blog/
- Guardian: „The NSA-Files“: http://www.theguardian.com/world/the-nsa-files
- Datenbank der „Cyberwar“-Vorfälle: http://cyber-peace.org

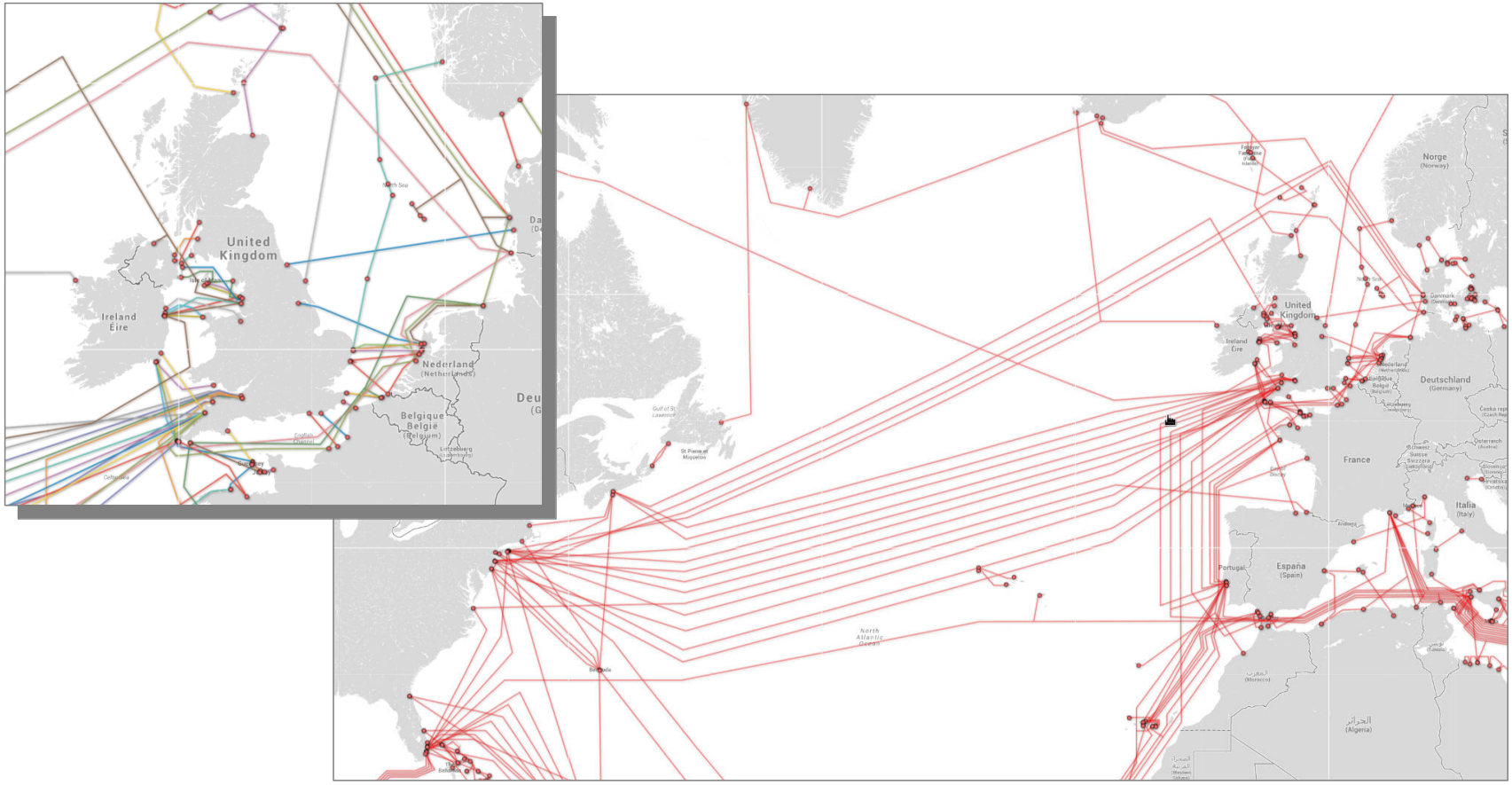
Anhang – Tempora

- Tempora (UK)
  - GCHQ (Government Communications Headquarters)
  - Zugriff auf 200 Transatlantik-Glasfaserkabel und im nahen Osten
  - Überwachung des kompletten Datenverkehrs über UK
  - 21.000 Terra-Bytes per Tag verarbeitet
  - Internet-Buffer für 3 Tage Komplettspeicherung, bis zu 30 Tage Speicherung von Verbindungsdaten
  - Automatische Analyse, Suche nach Stichworten und Vorselektion, Generierung von Metadaten
  - 300 GCHQ & 250 Mitarbeiter für Detail-Analyse
  - weltweit 850.000 Personen mit Zugriff auf Datenbanken

Anhang – Transatlantik-Traffic

IFSH
Institut für Friedensforschung
und Sicherheitspolitik
an der Universität Hamburg

- Transatlantische Glasfaserverbindungen



Quelle: submarinecablemap.com