Die digitale Allmacht der NSA

Erkenntnisse nach (mehr als) einem Jahr Snowden-Enthüllungen

Thomas Reinhold - reinhold@ifsh.de

Übersicht

IFSH
Institut für Friedensforschung
und Sicherheitspolitik
an der Universität Hamburg

- Die NSA-Programme im Überblick
- Verbindungen zw. NSA und US-Militär
- Stuxnet – ein finaler Rückblick

Die NSA-Programme im Überblick

> ***We hack everyone everywhere. We like to make a distinction between us and the others. But we are in almost every country in the world***
> US Cybercommand official, The Guardian, 7.Juni 2013

Die NSA-Programme im Überblick

> ***We hack everyone everywhere. We like to make a distinction between us and the others. But we are in almost every country in the world***
> US Cybercommand official, The Guardian, 7.Juni 2013

- Die „digitale Allmacht die NSA“
  - alles wissen
  - alles kontrollieren
  - alles tun

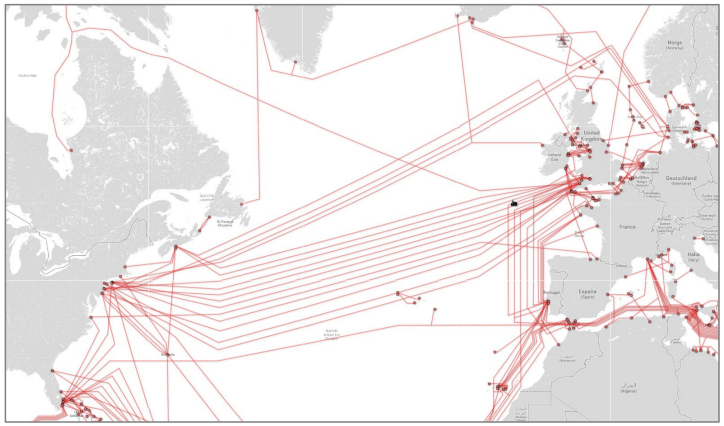
Die NSA-Programme: alles wissen

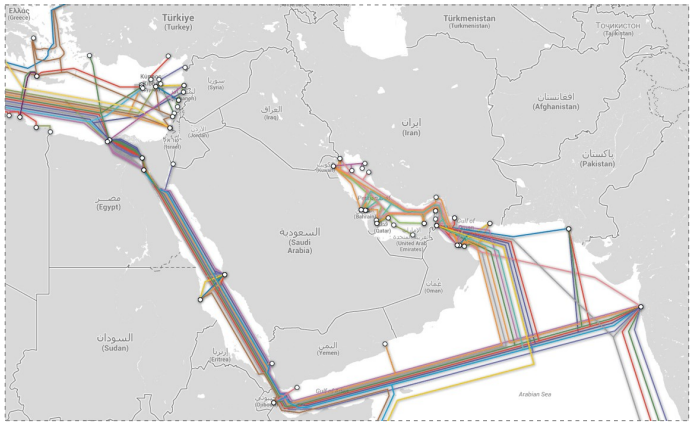
- PRISM / UPStream / Stormbrew
  - Zugriff auf Daten von Providern und ISP mit Standorten in den USA /Five Eyes
- Datenbanken und Datenzentren
  - Utah (2013), Fort Meade (2015), 29.000 TB/touched per day
  - 6 Mrd. Metadaten/Tag (Stand 2010)
- Telefonverkehr (CO-Traveller)
  - Handystandorte, Roaming-Verbindungen, Anruflisten, Metadaten
- TUNDA-Freeze: Bilderanalyse und Gesichtserkennungen
  - Soziale Netzwerke, Google, Mails ...
- Finanztransaktionen von VISA und Swift (TRACFIN)

Die NSA-Programme: alles kontrollieren

IFSH
Institut für Friedensforschung
und Sicherheitspolitik
an der Universität Hamburg

- FOXACID / QUANTUM:
  - Eigene Serverinfrastrukturen im Backbone für MITM-Attacken
  - Paket Injection und Umleitung auf eigene Server für Angriffe
- TEMPORA
  - Zugriff auf zentrale Glasfaserverbindungen (Atlantik, Naher Osten)
  - 3 Tage Internetpuffer (full take), 30 Tage Metadaten

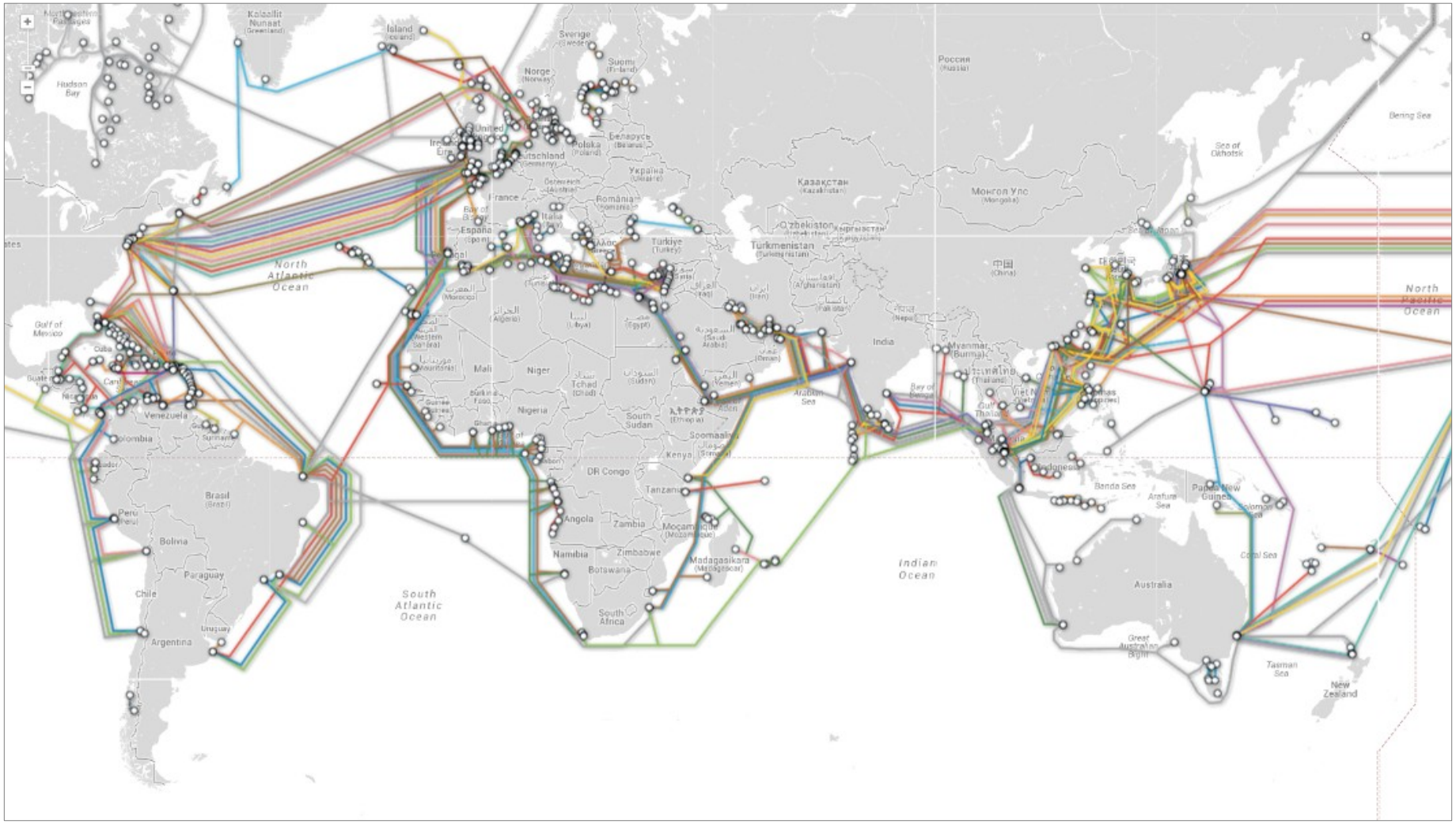




submarinecablemap.com

Die NSA-Programme: alles kontrollieren

IFSH
Institut für Friedensforschung
und Sicherheitspolitik
an der Universität Hamburg



submarinecablemap.com

Die NSA-Programme: alles kontrollieren

- HACIENDA
  - Automatische Suche nach Schwachstellen von ganzen Netzwerken und Ländern (2009: 27 Länder)
  - „Weltkarte der Schwachstellen“
- ANT-Kataloge (Advanced Network Technologies)
  - Hardware-Erweiterungen für namhafte Netzwerk- und Serverhersteller
  - Modifizierte Kleinelektronik (bspw. USB-Kabel)
- Bullrun
  - Gezielte Schwächung von Kryptographie-Standards
  - „Consolidated Cryptologic Program“ (35.000 Mitarbeiter / 11 Mrd. $/Jahr)

Die NSA-Programme: alles tun

- Mindestens 5 Länder vollständig abgehört
  - TK von Bahamas & Irak für 30 Tage gespeichert
- Xkeyscore / ICREACH
  - Datenbanken und Suchmaschinen für Analyse und Aggregation der Daten
  - Partnerorganisationen mit teilweisen oder vollständigen Zugriff
- Hacienda / Landmark
  - Aufbau von Zwischenknoten um Urpsrung bei Zugriffen zu verschleiern
- Monstermind
  - Automatisches Sensornetzwerk für die Detektion von IT-Angriffen
  - Möglichkeit für automatische Cyber-Gegenschläge

Verbindungen NSA - Militär

- Presidential Policy Directive PPD-20, Oktober 2012
  - Working Group aus Verteidigungsministerium und Geheimdiensten
  - "Offensive Cyber Effects Operations“ (OCEO) und Identifikation potentieller Ziele im Cyberspace „to advance US national objectives“
- Michael Rogers (NSA-Direktor, Nachfolger von Keith Alexander)
  - Direktor US Cyber Command mit explizit offensiver Ausrichtung
  - Direktor Central Security Service (CSS)
    „assistance to military crythologic community“
  - Direktor des Joint Functional Component Command – Network Warfare (JFCC-NW) → Koordination weltweiter „computer network operations“
- „Combat Mission Forces“ des US Cyber Command
  - Cyber als integraler Bestandteil aller zukünftigen Militäroperationen

Stuxnet – ein finaler Rückblick

- „To Kill a Centrifuge“ - A Technical Analysis of What Stuxnet’s Creators Tried to Achieve, R. Langner, Nov. 2013
- Zwei Sabotage-Versionen von Stuxnet
  - *„Both attacks aim at damaging centrifuge rotors, but use different tactics. The first (and more complex) attack attempts to over-pressurize centrifuges, the second attack tries to over-speed centrifuge rotors and to take them through their critical (resonance) speeds*
  - Spätere (aufgedeckte) Version „much simpler and much less stealthy“
  - Erste Version eher Produkt einer *„limited (..) in-group of top notch industrial control system security experts“*, zweite Version eher Planungsbestandteil einer höherrangigen Abteilung *„where the original crew is taken out of command by a casual 'we’ll take it from here' by people with higher pay grades“*

Stuxnet – ein finaler Rückblick

„Whatever the hard-fact results of Stuxnet were at Ground Zero, apparently they were not viewed as disappointing failure by its creators. Otherwise it would be difficult to explain the fact that New York Times reporter David Sanger was able to find maybe five to ten high-ranking government officials who were eager to boast about the top secret operation and highlight its cleverness“

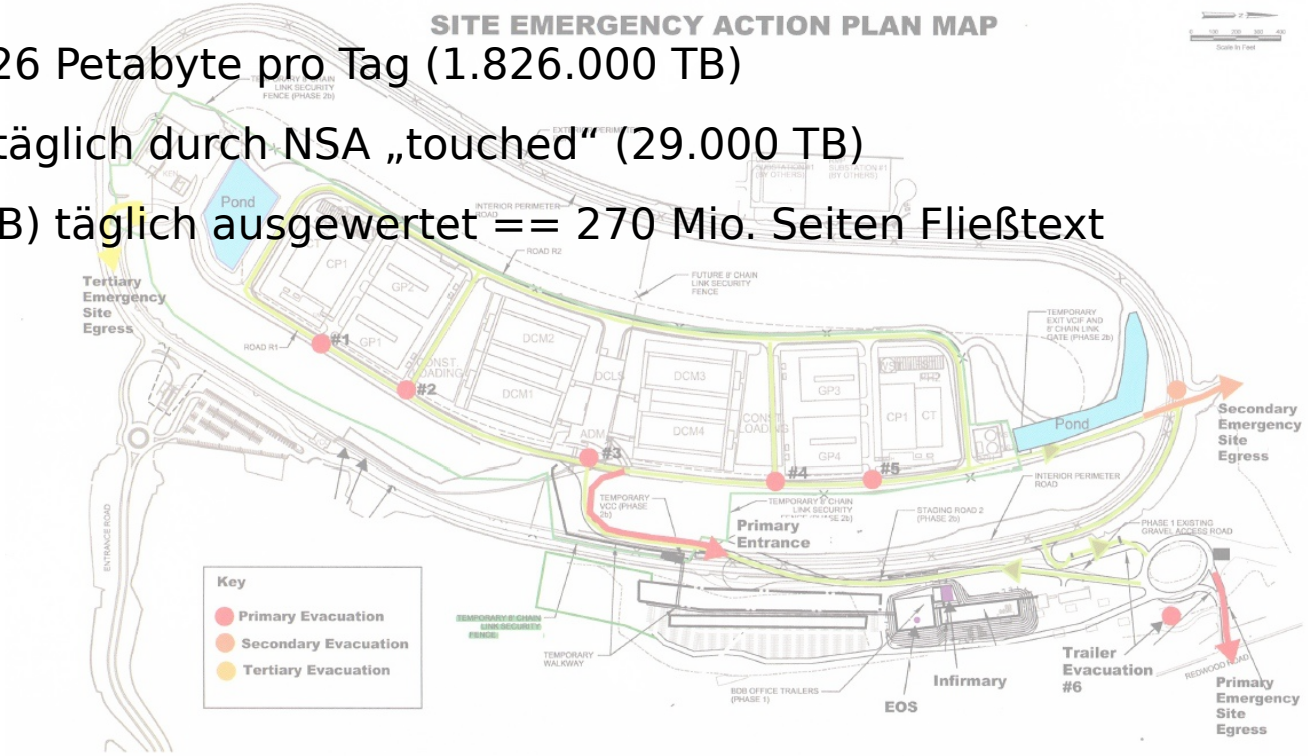
„Stuxnet will not be remembered as a significant blow against the Iranian nuclear program. It will be remembered as the opening act of cyber warfare“

Ralph Langner

Anhang: Staatliche Kooperationen

- Großbritannien
  - Tempora / Zugriffe auf Glasfaserbackbone
- Kanada
  - Hacienda und Landmark
- Neuseeland
  - Zugriffe asiatischen Internet-Backbone
  - Überwachungsprogramme als Daten-Bestandteil von Xkeyscore
- Deutschland
  - Zugriff auf das DE-CIX direkt / Umweg BND
  - Zugriff auf Netze der Telekom im Rahmen von TREASUREMAP
  - IT Zentrum in Wiesbaden → European Technical Center (ETC)

Anhang: alles wissen

IFSH
Institut für Friedensforschung
und Sicherheitspolitik
an der Universität Hamburg

- 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