IFSH
Institut für Friedensforschung
und Sicherheitspolitik
an der Universität Hamburg

PRISM, Tempora und die „offensive cyber effect operations“

Militärische Fähigkeiten im Cyberwar im Lichte der NSA-Enthüllungen

Thomas Reinhold - reinhold@ifsh.de

Übersicht

IFSH
Institut für Friedensforschung
und Sicherheitspolitik
an der Universität Hamburg

- Die NSA-Programme im Überblick
- Technische Möglichkeiten der NSA aus Sicht des „cyberwar“
- „Offensive cyber effect operations“ und die „Cyberwar-Liste“
- Einschätzung

NSA-Programme im Überblick

IFSH
Institut für Friedensforschung
und Sicherheitspolitik
an der Universität Hamburg

- Daten erfassen
  - PRISM & Upstream
  - Tailored Access Operations
  - Bullrun
  - Tempora
- Daten auswerten und Metadaten generieren
  - Xkeyscore
  - Boundless Informant
- Speichern

“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

NSA-Programme - Erfassen

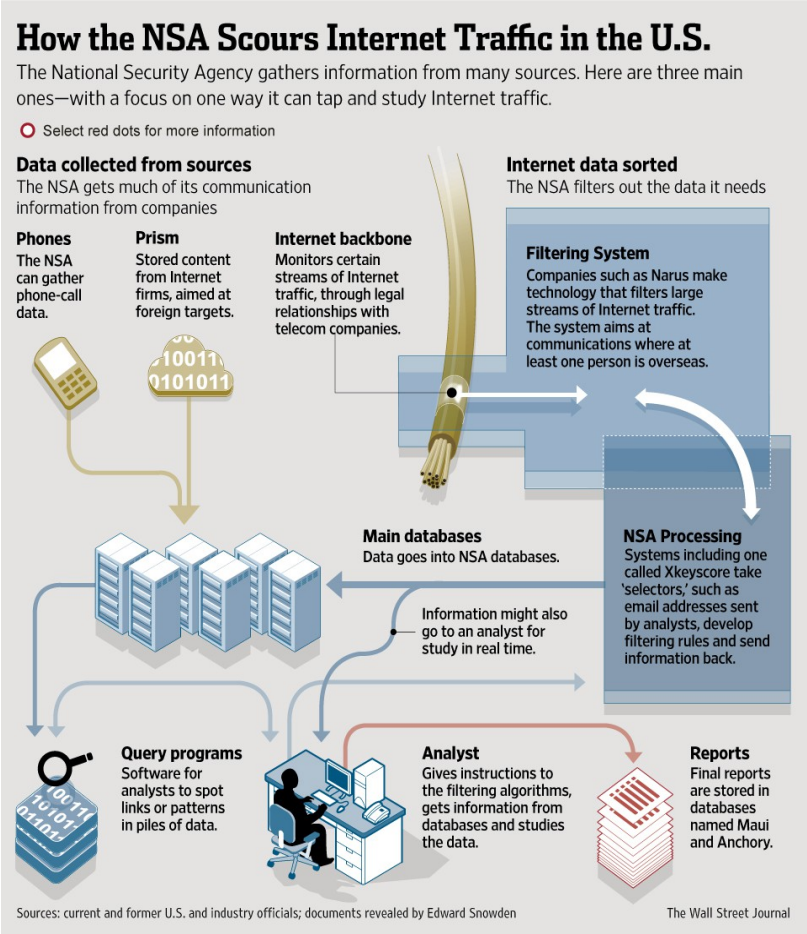
IFSH
Institut für Friedensforschung
und Sicherheitspolitik
an der Universität Hamburg

- 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)
- Tailored Access Operations
  - 600 Personen-Hacker-Einheit inkl. „Field-Unit“ für Vor-Ort-Zugriff
  - 60k++ Zugriffe weltweit (viele chinesische Systeme, DE-CIX)
- Bullrun
  - Schwächung und Knacken von Kryptographie-Systemen
- Tempora (UK Government Communications HQ)
  - Abhören und Mitschneiden von Datenübertragungen (Atlantik, naher Osten)

NSA-Programme - Auswerten

IFSH
Institut für Friedensforschung
und Sicherheitspolitik
an der Universität Hamburg

- Xkeyscore
  - Analyse-Tool für Zugriff auf Datenbestände
  - Zusammenführung von Daten
  - Zugriff auf *„fast alles, was ein typischer Nutzer im Internet macht“*
  - z.T. auch vom BND genutzt
- Boundless Informant
  - Frontend für Überblick über Datenbestände und Überwachungsmaßnahmen



NSA-Programme - Speichern

IFSH
Institut für Friedensforschung
und Sicherheitspolitik
an der Universität Hamburg

- NSA-eigene Rechenzentren
  - Utah, Vollbetrieb Ende 2013
  - Fort Meade, Washington, Vollbetrieb 2015
- Datenaufkommen
  - Weltweit 1.826 Petabyte pro Tag (1.826.000 TB)
  - 29 Petabyte täglich durch NSA „touched“
  - 0.007 PB (7TB) täglich ausgewertet == 270 Mio. Seiten Fließtext
- Speicherung von Inhalten, Verbindungs- und Meta-Daten
  - Einige Tage bis teilweise mehrere Jahre
  - EvilOlive und ShellTrumpet, Stellar Wind
- Zusätzliche weitere, primär militärische Datenquellen

Technische Möglichkeiten der NSA (I)

IFSH
Institut für Friedensforschung
und Sicherheitspolitik
an der Universität Hamburg

- Q: „How will cyber weapons look like“
  A: „Have a look at the Snowden papers“
- Hacking-Einheiten
  - 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, 652 Mio $ Budget (Ende 2013: auf 85.000 strategisch ausgewählten Computern zu platzieren)

Technische Möglichkeiten der NSA (II)

IFSH
Institut für Friedensforschung
und Sicherheitspolitik
an der Universität Hamburg

- Abhören und Anzapfen von Glasfaser-Backbones
  - Knoten in USA, UK, naher Osten angezapft
  - USS Jimmy Carter, Spezial-U-Boot für das unterseeische Anzapfen (2004)
  - „Field Unit“ der Einheit für „Tailored Access Operations“
- Industriekooperationen
  - Zugriff auf Nutzerdaten und Datentraffic
  - Meldung von unbekannten Sicherheitslücken an die NSA
  - "Sigint Enabling Projects" mit jährlich 250 Mio $ Budget
  - Gezielter Einbau von Hintertüren in Software / Hardware (Cisco/IBM)
  - NSA haben direkten Zugriff auf Router & Firewalls namhafter Hersteller
  - Insiderwissen für targeted attacks (Stuxnet & Siemens)
  - Einflussnahme auf Standarisierungsprozeße und Protokolle

Technische Möglichkeiten der NSA (III)

IFSH
Institut für Friedensforschung
und Sicherheitspolitik
an der Universität Hamburg

- Kryptographie angreifen
  - Verschlüsselung von Daten (TLS/SSL, https, E-Mail, VPN, Skype)
  - Brute Force Knacken: 2^n Versuche => nur „schwache“ Krypto ist knackbar
  - Schwächen entweder „by design“ oder in der konkreten Code-Umsetzung
  - Gezielte Einflussnahme bei Standarisierungsprozeßen, Richtlinienverfahren und technischen Spezifikationen (4G-Telefonie, Zufallszahlen-Generatoren)
  - „Consolidated Cryptologic Program“ mit 35.000 Mitarbeitern und einem jährlichen Budget von 11 Mrd. Dollar
  - Möglicherweise mathematisch geknackte Kryptoverfahren
  - Betrieb eigener Rechenzentren für brute force Angriffe
  - „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”)
  - Lieferung von Master-Schlüssel durch Industriepartner

Obamas „Cyberwar Liste“

IFSH
Institut für Friedensforschung
und Sicherheitspolitik
an der Universität Hamburg

- Presidential Policy Directive PPD-20, Oktober 2012
  - Entwickeln von "Offensive Cyber Effects Operations“ (OCEO) und Identifikation potentieller Ziele im Cyberspace „to advance US national objectives“
  - 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“
  - Operationserlaubnis auch ohne Zustimmung der Gegenseite

    "*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*"
  - Offensive, eigenverantwortliche Operationsbefugnis ohne explizite Begrenzung auf reine Vergeltungsschläge
  - Auswirkungen „ranging from subtle to severely damaging“

Einschätzung (I)

IFSH
Institut für Friedensforschung
und Sicherheitspolitik
an der Universität Hamburg

- Internationale Zusammenarbeit der Geheimdienste
  - USA, Großbritanniens, Kanada, Neuseelands & Australien (Five Eyes)
  - Schweden, Deutschland ...
- 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)

IFSH
Institut für Friedensforschung
und Sicherheitspolitik
an der Universität Hamburg

- 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

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 - PRISM

- PRISM ein Teil des militärischen GCCS-J (Command, Control, Communications, Computer, and Intelligence
- Datenfreigabe genehmigungspflichtig
  - Foreign Intelligence Surveillance Court (FISC), tagt geheim
  - Kooperierende Unternehmen müssen die Informationen über Daten-Weitergabe geheim halten
  - FISA (Foreign Intelligence Surveillance Act) erlaubt Weitergabe ohne Richtervorbehalt bzgl. Nicht-US-Bürger oder bzgl. US-Bürger im Ausland (aber 2011 auch für „zufällige Funde“ erlaubt)
  - Der Foreign Intelligence Surveillance Court (FISC) habe nicht die Kapazitäten, Regelverstöße der US-Sicherheitsbehörden zu untersuchen, erklärte dessen Vorsitzender Reggie Walton gegenüber der Washington Post (http://heise.de/-1937397)
  - Rückwirkende FISC-Genehmigung auch im Inland bei „Gefahr im Verzug“ sowie bei Verdacht auf Spionage ausländischer Mächte, Hackerattacken oder Massenvernichtungswaffen

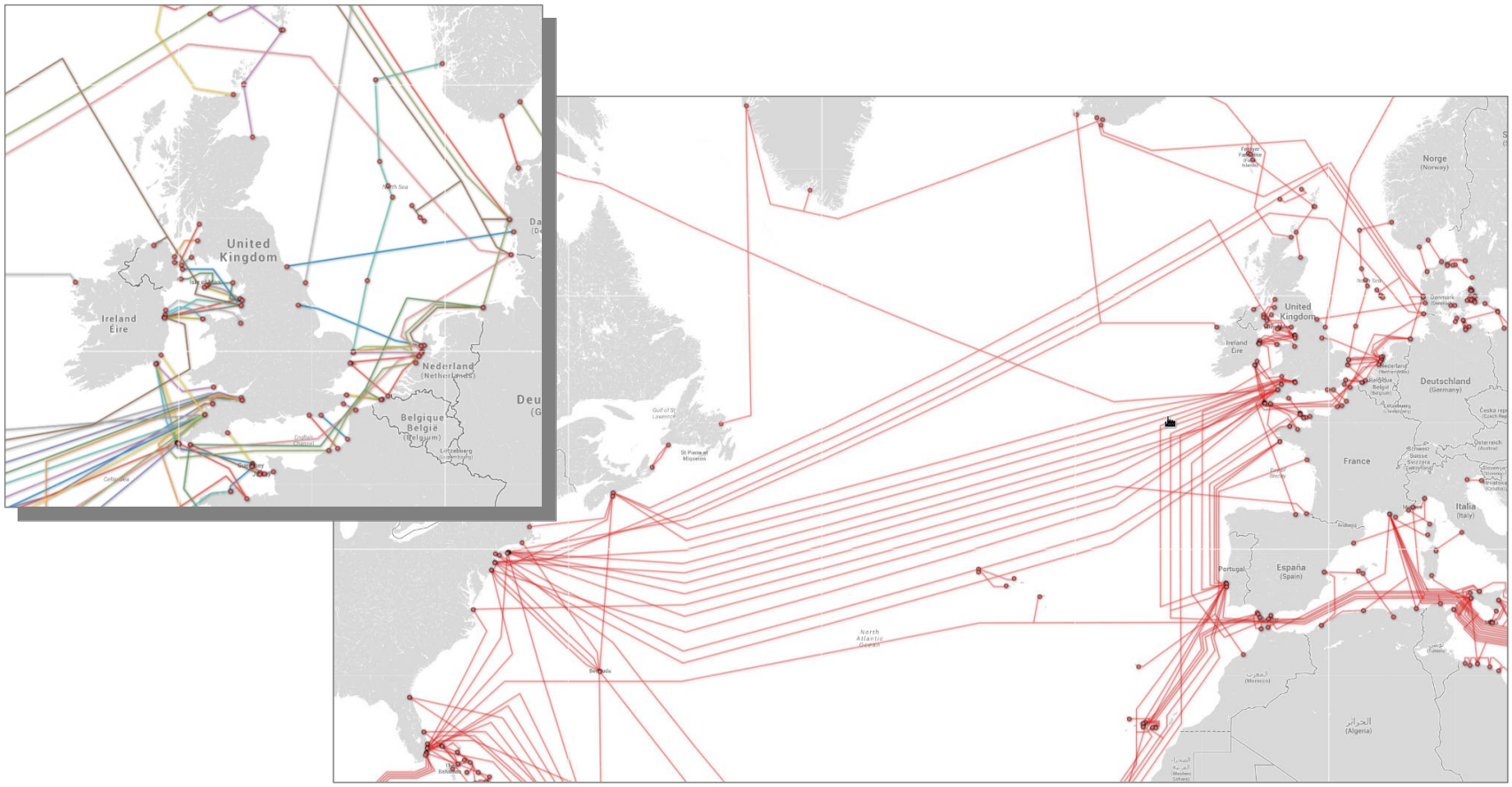
Anhang – Tempora

- 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