Die digitale Allmacht der „Five Eyes“

Erkenntnisse nach (mehr als) einem Jahr Snowden-Enthüllungen

Thomas Reinhold - reinhold@ifsh.de
cyber-peace.org

Übersicht

- Das IFSH
- Wer sind die Five Eyes
- Die Programme der Five-Eyes
- Juristische Kontrolle der Geheimdienste
- Bündnisse und Kooperationen
- Der Cyberspace und das Militär
- Und nun ?

Grafik: ahoipolloi.blogger.de

Das IFSH

- Institut für Friedensforschung und Sicherheitspolitik an der Universität Hamburg
- Stiftung der Stadt Hamburg 1971
- Wurzeln in nuklearer Abrüstung
- Sicherheitspolitische und naturwissenschaftliche Arbeitsbereiche
- Wissenschaftliche Forschung und Politikberatung

IFSH
Institut für Friedensforschung
und Sicherheitspolitik
an der Universität Hamburg

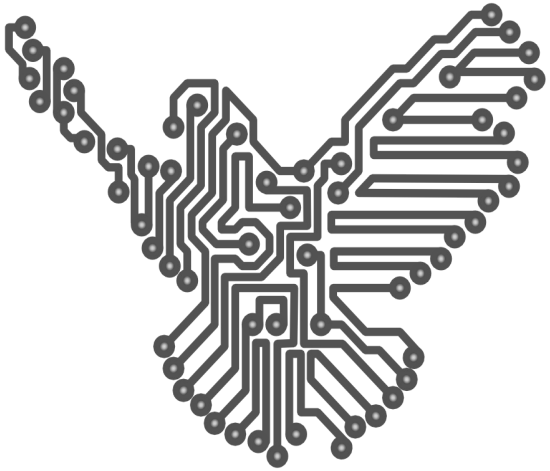
Das IFSH /2

IFSH
Institut für Friedensforschung
und Sicherheitspolitik
an der Universität Hamburg

- Mitarbeiter Arbeitsgruppe IFAR²

  “Interdisziplinäre Forschungsgruppe Abrüstung, Rüstungskontrolle und Risikotechnologien”

- Dipl. Informatiker, Vertiefung Künstliche Intelligenz und Psychologie
- Freiberuflicher Softwareentwickler
- Datenbank/Blog cyber-peace.org



Grafik - FifF e.V. - Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung

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

Die Programme der Five Eyes

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

"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
businessweek.com, 23.5.2013

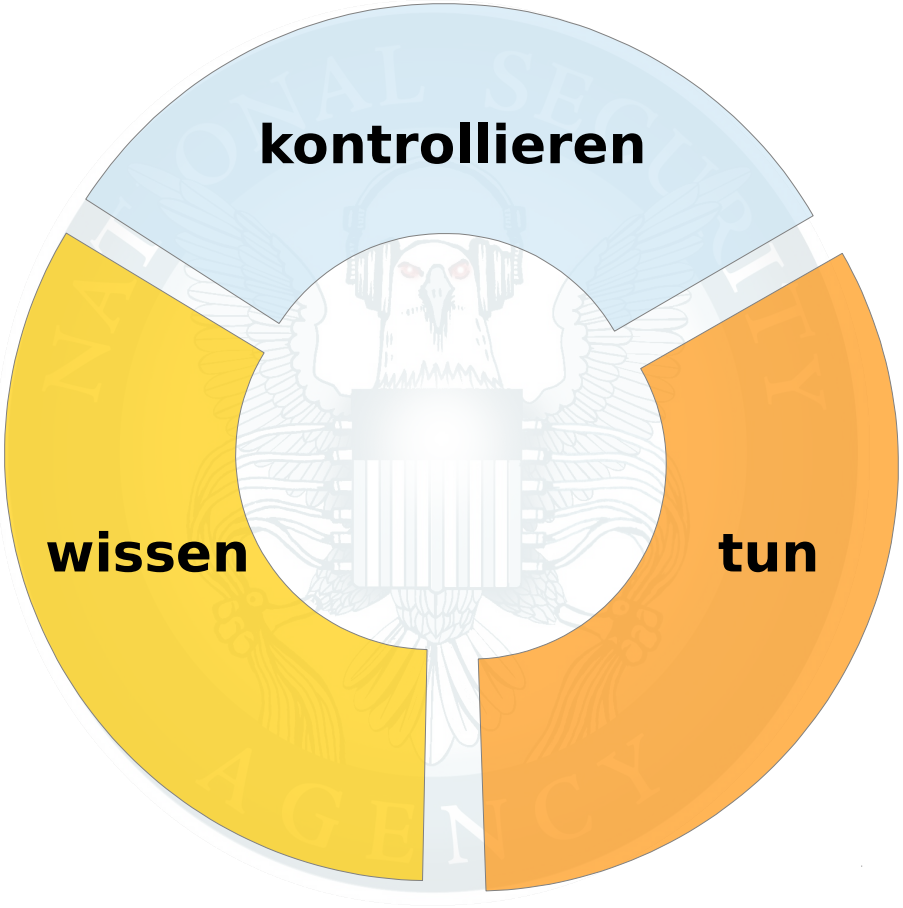
Die Programme der Five Eyes

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

Grafik: eff.org

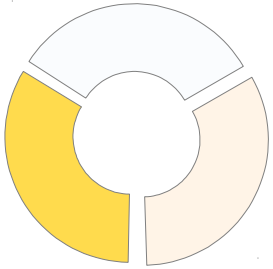
Die Programme der Five Eyes

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



Grafik: eff.org

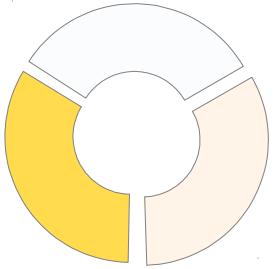
Die Programme /alles wissen



wissen

- PRISM / UPStream / Stormbrew
  - Zugriff auf Daten von Providern und Internet-Dienstleiser
  - Teilweise „full take“ und „Pufferung“ des Internetverkehrs
- 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

Die Programme /alles wissen



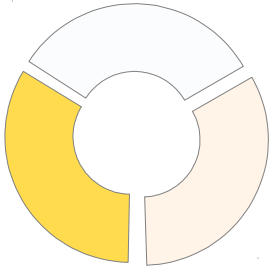
wissen

- PRISM / UPStream / Stormbrew
  - Zugriff auf Daten von Providern und Internet-Dienstleiser
  - Teilweise „full take“ und „Pufferung“ des Internetverkehrs
- 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
- TUNDRA-Freeze: Bilderanalyse und Gesichtserkennungen
  - Soziale Netzwerke, Google, Mails ...
- Finanztransaktionen von VISA und Swift (TRACFIN)

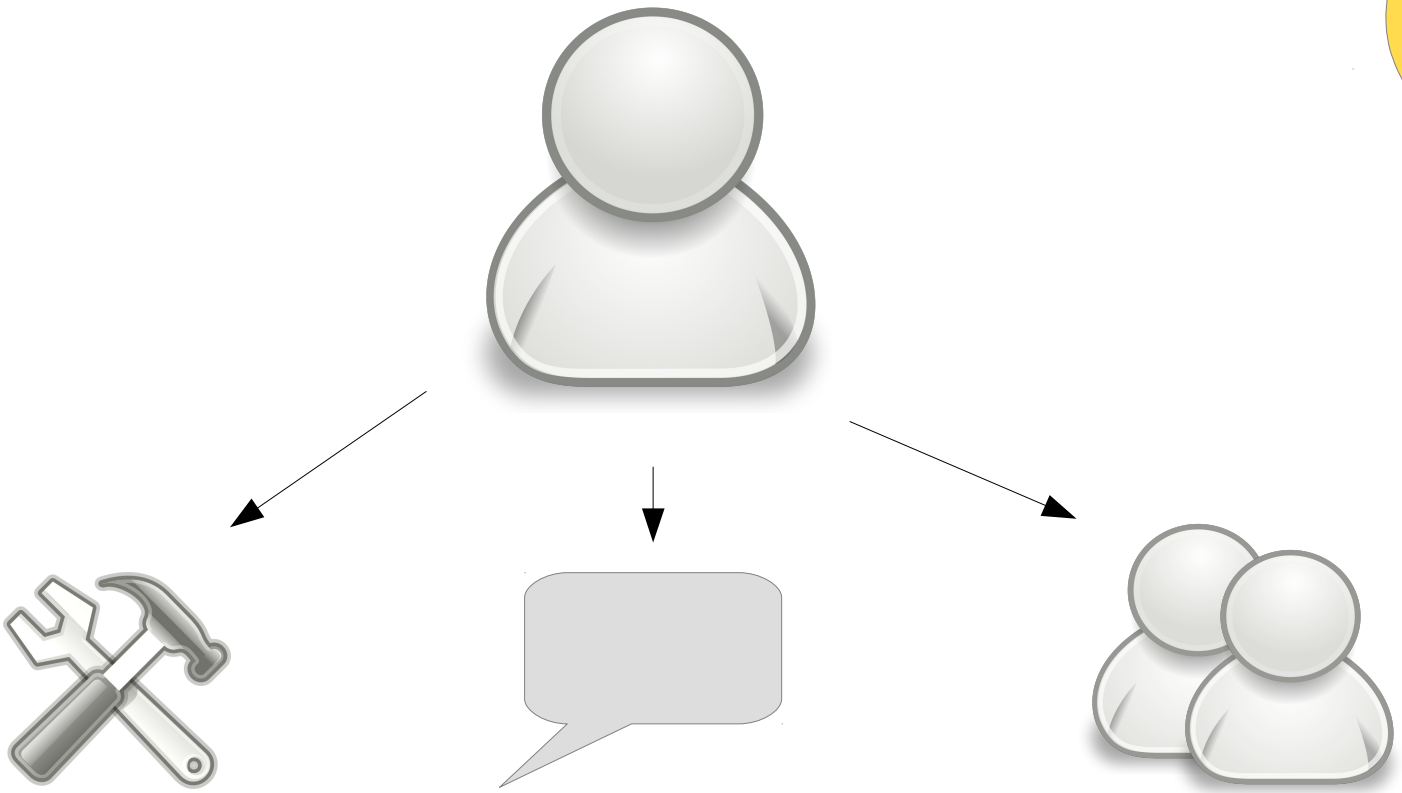
Die Programme /alles wissen

IFSH
Institut für Friedensforschung
und Sicherheitspolitik
an der Universität Hamburg

- „Was macht uns aus ?“



wissen



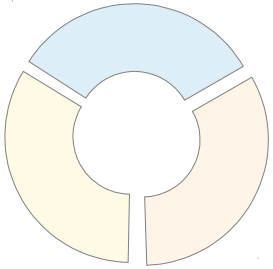
Was wir tun

Was wir kommunizieren

Mit wem wir Umgang haben

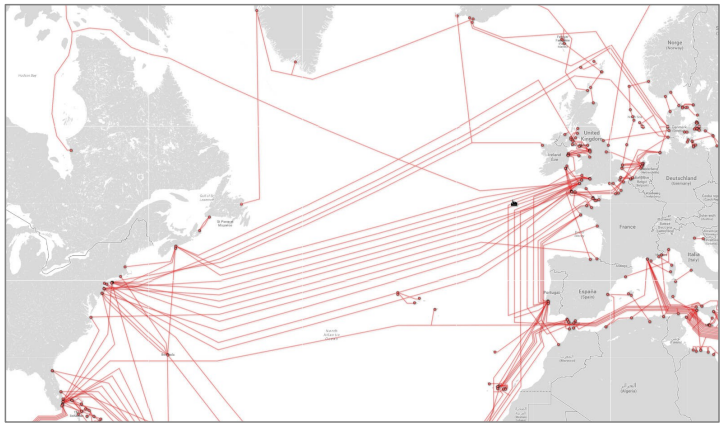
Die Programme /alles kontrollieren

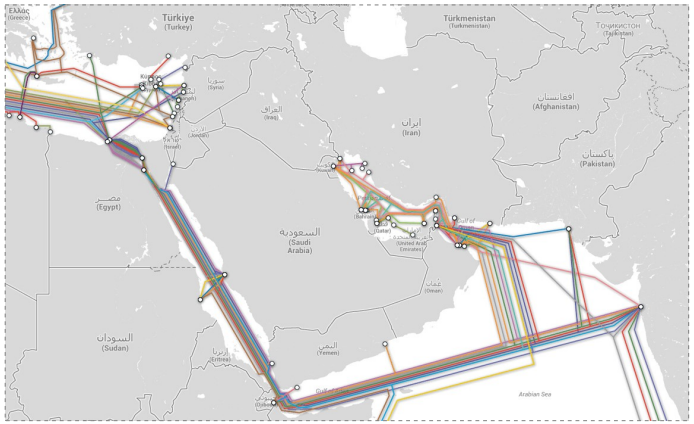
IFSH
Institut für Friedensforschung
und Sicherheitspolitik
an der Universität Hamburg



kontrollieren

- FOXACID / QUANTUM:
  - Eigene Serverinfrastrukturen für Cyber-Attacken
  - Datenmodifikation und Umleitung auf eigene Server
- TEMPORA
  - Zugriff auf zentrale Glasfaserverbindungen
  - 3 Tage Internetpuffer (full take), 30 Tage Metadaten

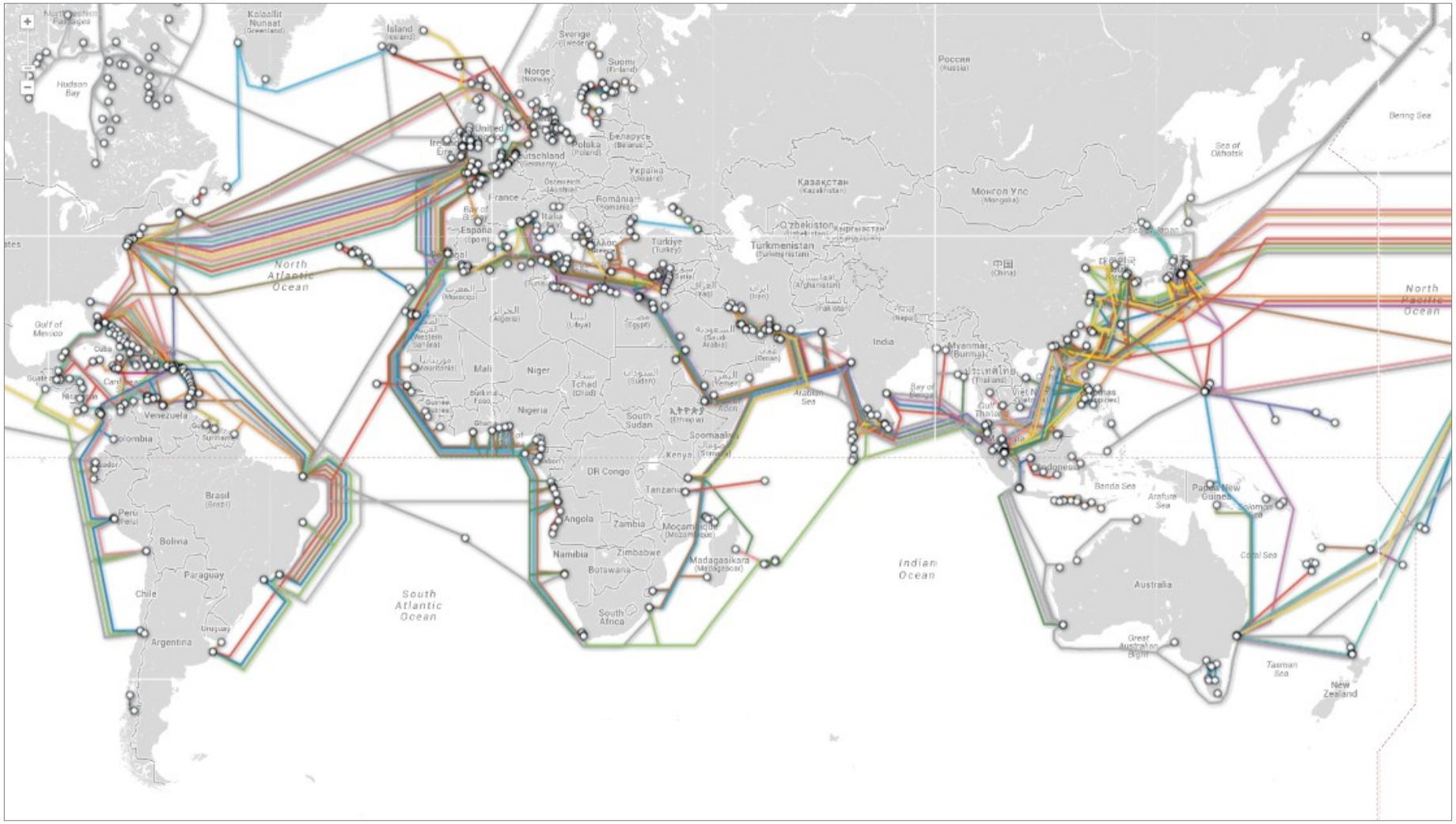




submarinecablemap.com

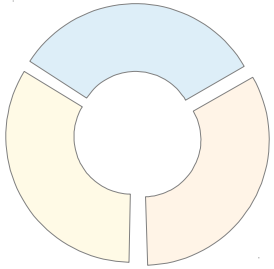
Die Programme /alles kontrollieren

IFSH
Institut für Friedensforschung
und Sicherheitspolitik
an der Universität Hamburg



submarinecablemap.com

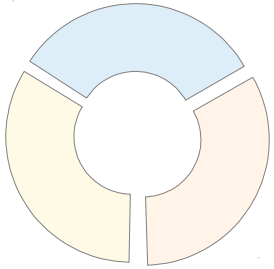
Die Programme /alles kontrollieren



kontrollieren

- HACIENDA
  - Automatische Suche nach Schwachstellen
    und Erstellung einer „Weltkarte der Schwachstellen“
- ANT-Kataloge (Advanced Network Technologies)
  - Hardware-Erweiterungen für führende Hersteller
  - Modifizierte Klein-Elektronik (bspw. USB-Kabel)

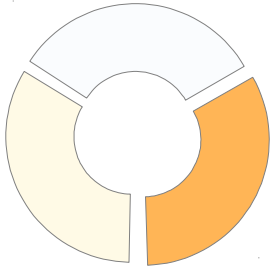
Die Programme /alles kontrollieren



kontrollieren

- HACIENDA
  - Automatische Suche nach Schwachstellen
    und Erstellung einer „Weltkarte der Schwachstellen“
- ANT-Kataloge (Advanced Network Technologies)
  - Hardware-Erweiterungen für führende Hersteller
  - Modifizierte Klein-Elektronik (bspw. USB-Kabel)
- Bullrun
  - Gezielte Schwächung von Kryptographie-Standards
- 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

Die Programme /alles tun

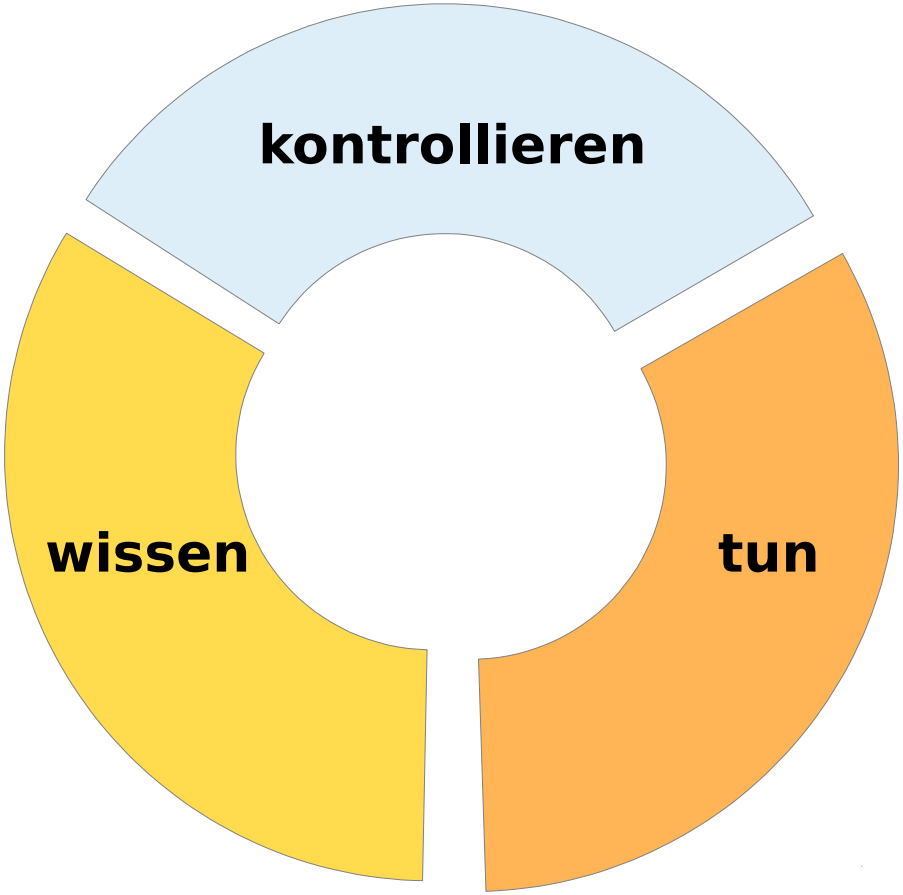


tun

- 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
- Monstermind
  - Automatisches Sensornetzwerk für die Detektion von IT-Angriffen
  - Möglichkeit für automatische Cyber-Gegenschläge
- U-Boot USS „Jimmy Carter“

Die Programme

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



Juristische Kontrolle

- 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)

Juristische Kontrolle /2

- 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

    „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)
  - Ausschuss für Nachrichten- und Sicherheitsdienste (Intelligence and Security Committee – ISC) als parlamentarisches Kontrollgremium ohne Exekutiv-Gewalt, informiert seit 2013 über Operationen der Nachrichtendienste
- 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) 9 vorwiegend europäische Länder (Dänemark, Norwegen, Schweden, Frankreich)
  - Tier 3 (Limited Cooperation): 14 Länder, u.a. Israel, Indien & Deutschland
  - Tier 4 (Exceptional Cooperation) Länder feindlichen Interessen

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) 9 vorwiegend europäische Länder (Dänemark, Norwegen, Schweden, Frankreich)
  - Tier 3 (Limited Cooperation): 14 Länder, u.a. Israel, Indien & Deutschland
  - Tier 4 (Exceptional Cooperation) Länder feindlichen Interessen
- Deutschland

  "*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)

  - Aktive BND-NSA-Kooperationen (Datenaustausch, Bad Aibling, Xkeyscore...)

Der Cyberspace und das Militär

- 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

Ein historischer Rückblick

IFSH
Institut für Friedensforschung
und Sicherheitspolitik
an der Universität Hamburg

- Stuxnet 2010
- Politisches Nachspiel
  - Was kommt als nächstes
  - Gibt es Cyberwaffen
  - Eigene Verwundbarkeit
  - Konsequenzen für die internationale Sicherheit
- Urheber: Israel und USA*
- Belastung zwischen-staatlicher Beziehungen
  - Abschreckung
  - Rüstungswettläufe

Ein historischer Rückblick /2

- „To Kill a Centrifuge“ - A Technical Analysis of What Stuxnet’s Creators Tried to Achieve, R. Langner, Nov. 2013
- Zwei Sabotage-Versionen von Stuxnet

„Whatever the hard-fact results of Stuxnet were at Ground Zero, apparently they were not viewed as disappointing failure by its creators. (..) 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“

Was seit Stuxnet geschah

- UN-Bericht zur Militarisierung des Cyberspace (UNIDIR* / CSIS*) 40 Staaten mit offensiven militärischen Cyberprogrammen
- Tallin Manual zur Anwendung des Völkerrechts im Cyberspace
- MADIANT Bericht zur chinesischen Militär-Hackereinheit PLA 61398

Was seit Stuxnet geschah

- UN-Bericht zur Militarisierung des Cyberspace (UNIDIR* / CSIS*) 40 Staaten mit offensiven militärischen Cyberprogrammen
- Tallin Manual zur Anwendung des Völkerrechts im Cyberspace
- MADIANT Bericht zur chinesischen Militär-Hackereinheit PLA 61398

- Veröffentlichungen von E. Snowden zu den FIVE-Eyes und ihren Ressourcen
- Obamas Presidential Policy Directive PPD 20/2012

Einige Erkenntnisse gewonnen, viele neue Probleme aufgeworfen

Einige Erkenntnisse gewonnen, viele neue Probleme aufgeworfen

?

Was kommt als nächstes

Gibt es Cyberwaffen

Die eigene Verwundbarkeit

Konsequenzen für die internationale Sicherheit

Einige Erkenntnisse gewonnen, viele neue Probleme aufgeworfen

?

Was kommt als nächstes

Gibt es Cyberwaffen

Die eigene Verwundbarkeit

Konsequenzen für die internationale Sicherheit

IFSH
Institut für Friedensforschung
und Sicherheitspolitik
an der Universität Hamburg

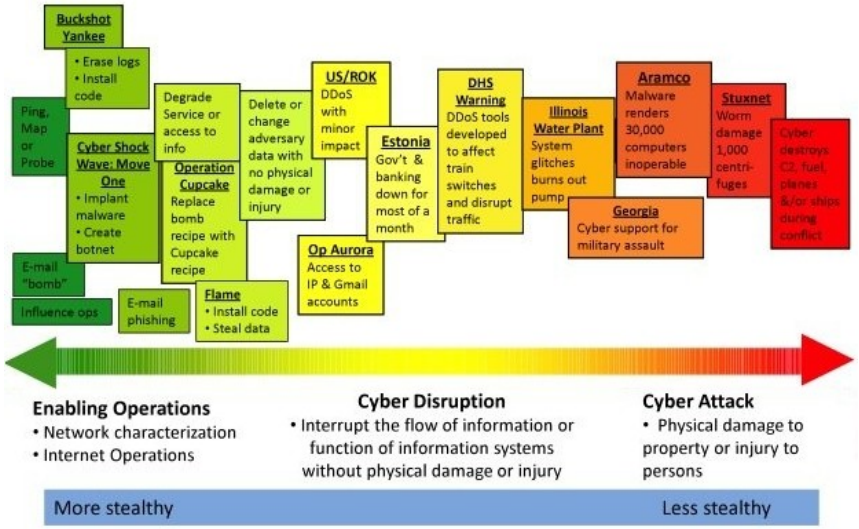
? Anwendbarkeit etablierter Normen des Völkerrechts

- Das Recht zum Krieg (ius ad bellum)
  - UN Charta Art. 2 (4) → Gewaltverzicht (“use of force”)
  - UN Charta Art. 51 → Recht zur Selbstverteidigung
- Das Recht im Krieg (ius in bello)
  - Genfer Konventionen
  - Prinzip der Proportionalität
- Das Attributions-Problem

IFSH
Institut für Friedensforschung und Sicherheitspolitik an der Universität Hamburg

? Anwendbarkeit etablierter Normen des Völkerrechts

- Talin Manual (CCDCOE)
  - Analogien zu “kinetischen Wirkmitteln”
- Definition von Cyberwaffen
  - OECD Studie “Reducing Systemic Cybersecurity Risk” (2010)
  - Kontinuums-Klassifikation nach Brown & Tullos



Rüstungskontrolle & Non-Proliferation

- Ausbreitung militärischer Rüstungsgüter
  - regulieren
  - kontrollieren
  - unterbinden
- Dual-Use-Problematik
- Verifikationsmöglichkeiten oder “wie zählt man Malware”

… und weitere Fragen

- Cyberattacken zwischenstaatlicher Akteure
- Internet Governance
  - Netzpolitik
  - Selbstregulation vs. Steuerung durch internationale Gremien (ITU)
- Freiheit vs. Kontrolle
- Spionage und wirtschaftliche Schäden
- Einschätzung und Eingrenzung der eigenen Verwundbarkeit

Einige Erkenntnisse gewonnen, viele neue Probleme aufgeworfen

!

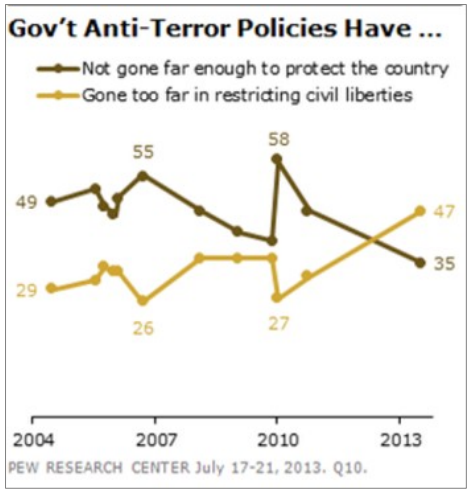
Wir können die Technik nicht aus unserem Leben verbannen, die Verkehrsmittel nicht und inzwischen auch die Computer nicht. Umso wichtiger aber ist es, dass wir darüber nachdenken, wie wir mit den Errungenschaften der Technik in Zukunft umgehen sollen und wollen.

Joseph Weizenbaum, 1978*

* aus „Die Macht der Computer und die Ohnmacht der Vernunft“, 1978

Grafik: xkcd.com

Anhang: (Inter)nationale 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*". (The Guardian)
  - US-Kongress „*Momentum Builds Against N.S.A. Surveillance*" (NY Times)

Anhang: (Inter)nationale Reaktionen /2

- 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