IT-Sicherheit im Kontext der NSA-Affäre

Dr. Michael Beck

Edward Snowden
oder - das Ende der Privatsphäre

Techn. Mitarbeiter des CIA, NSA und DIA

Snowden übermittelte geheime Informationen an den Guardian-Journalisten Glenn Greenwald, der diese im Juni 2013 ohne Angabe einer Quelle in Teilen veröffentlichte.

9. Juni 2013	Snowden gab in Hongkong seine Identität gegenüber der Öffentlichkeit preis.
14. Juni 2013	Haftbefehl des FBI u. a. wegen Spionage
23. Juni 2013	Flucht nach Moskau, Transitbereich Flughafen Scheremetjewo
1. August 2013	Snowden erhält von Russland Asyl

Chronologie der Veröffentlichungen

6. Juni 2013

PRISM
Zugriff und Auswertung der Daten von
Microsoft, Google, Apple, Yahoo,
Facebook, Youtube, Skype, etc.

8. Juni 2013

„Boundless Informant“
Data Mining Tool
Auskunft über einzelne Personen

21. Juni 2013

Tempora Programm GHQC
Anzapfen und Auswerten von internationalen Datenleitungen

8. Juli 13

XKeyScore
Software stellt in Echtzeit verschiedene Daten zu einer Person dar

5. September 2013

„Bullrun“ „Sigint“
Gezielter Angriff auf Verschlüsselung
Schwächung von Krypto-Standards

7. September 2013

Ausspähen von Smartphones
Blackberry, Android, iOS

10. September 2013

„Dual_EC_DRBG“
Zufallszahlengenerator mit
NSA-Hintertür

30. Dezember 2013

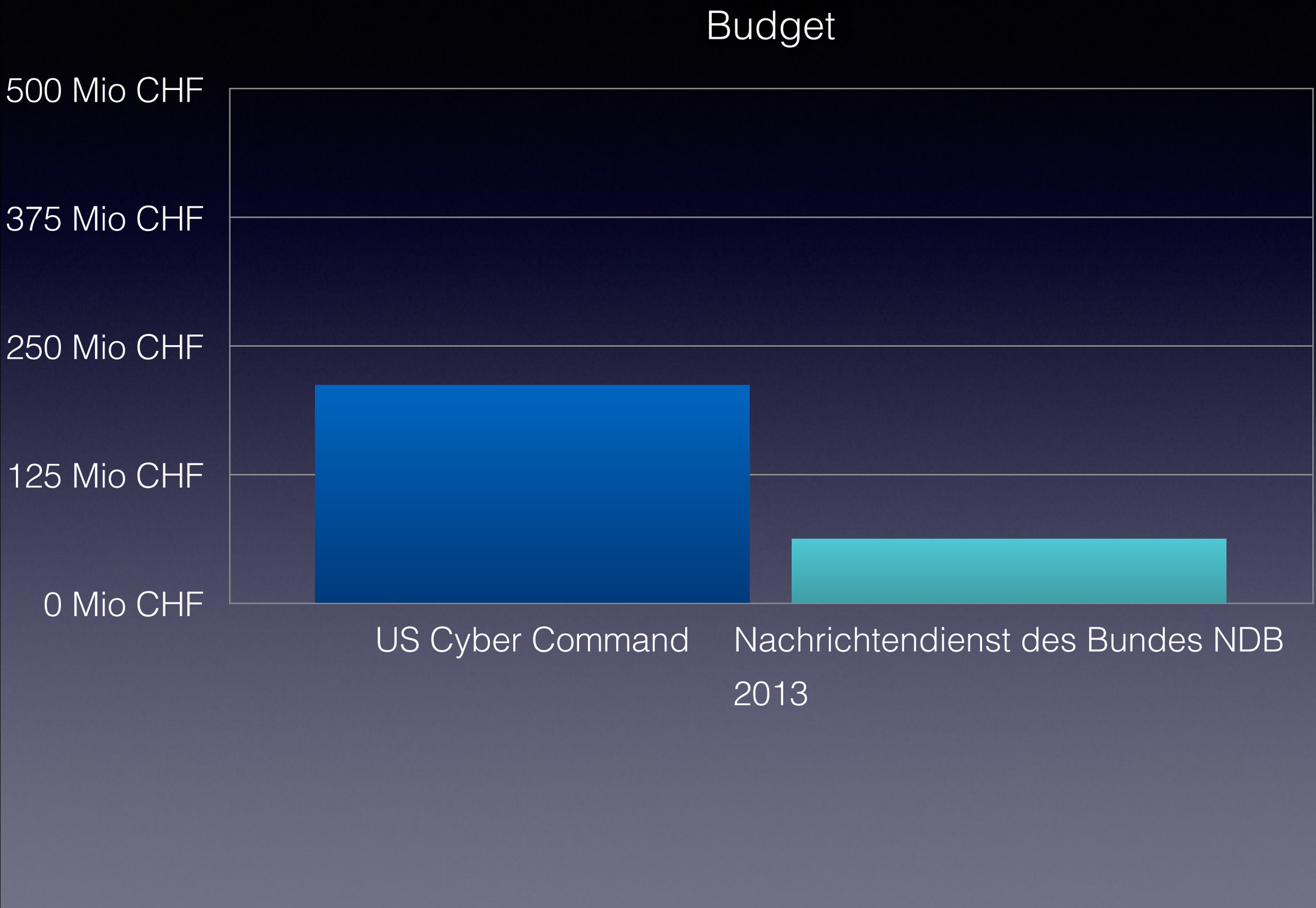
Werkzeugkasten
für gezielte Angriffe
NSA-Abteilung ANT

2. Januar 2014

„Penetrating Hard Targets Project“
Bau eines Quantencomputers
für Kryptosysteme mit grossen Schlüssellängen

National Security Agency
NSA

- Direktor: Keith B. Alexander
  - Gleichzeitig auch Kommandant des United States Cyber Command und der Chef des Central Security Service.
- Auftrag: Weltweite Überwachung, Entschlüsselung und Auswertung elektronischer Kommunikation
- Budget 2013: 10.8 Mrd $
- ca. 40’000 Mitarbeiter


Budget
500 Mio CHF
375 Mio CHF
250 Mio CHF
125 Mio CHF
0 Mio CHF
US Cyber Command
Nachrichtendienst des Bundes NDB
2013

Cyber-Risiken

- 27. Juni 2012: Der Bundesrat hat die «**Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken**» gutgeheissen.

- Mit der Strategie will der Bundesrat in **Zusammenarbeit mit Behörden, Wirtschaft und den Betreibern kritischer Infrastrukturen** die **Cyber-Risiken minimieren**, welchen sie täglich ausgesetzt sind.

- Personelle Verstärkung der Cyber-Expertise in der Bundesverwaltung
  - **28** zusätzliche Stellen für Cyber-Schutz-Experten und -Expertinnen werden geschaffen
- Handeln in Eigenverantwortung, dezentrale Umsetzung der Strategie
- Nationale Zusammenarbeit zwischen der Wirtschaft und den Behörden
- Kooperation mit dem Ausland

Melani

www.melani.admin.ch

- Die im EFD und im VBS angesiedelte **Melde- und Analysestelle Informationssicherung Melani** erfülle eine zentrale Rolle bei der Umsetzung der Strategiemassnahmen

- **Informations-Drehscheibe** zur fortlaufenden Koordination, Auswertung und Weiterleitung des Informationsflusses

- Mit Abschluss der Umsetzung Ende 2017 soll Melani eine **Leit- und Koordinationsfunktion** im operativen Bereich übernehmen

MELANI richtet sich an **private Computer- und Internetbenutzer**, sowie an **kleinere und mittlere Unternehmen (KMU)** der Schweiz.

- Informationen über Gefahren im Internet
- Lageberichte
- Meldeformular

Cloud Computing

- Die NSA-Affäre kostet die US-Cloud-Anbieter in den nächsten drei Jahren zwischen **21,5 und 35 Milliarden US-Dollar**

- **Schweizer Daten-Clouds** werden davon profitieren

    - Mount10, SecureSafe, Greenbyte, SafeSwissCloud,..

Verschlüsselung

- Datenverschlüsselung ist notwendig
  - Für alle Dienste (E-Mail, Web, FTP, ...)
  - Verschlüsselungs-Algorithmen „Made in Europe“
  - OpenSource-Verschlüsselung (TrueCrypt, PGP,..)
  - Für Mobiltelefone (Secure-Voice, EMail, Apps, ..)

Papstwahl 2005 – Quelle: spon, AP

Papstwahl 2013 – Quelle: spon, AP

Hochsicherheits-Handy

- SiMKo 3 (BSI zertifiziert)
- Daten der Geheimhaltungsstufe VS-NfD (Verschlusssache - Nur für den Dienstgebrauch)
- Wurde von D Telekom in Zusammenarbeit mit der TU Dresden und den beiden deutschen Startups Kernkonzept und Trust2Core entwickelt
- Kern soll aus überschaubaren "wenigen 10.000 Zeilen Programmcode“
- Eigenständiger Krypto-Chip
  - Sichere E-Mails, Kontakte, Termine, SMS, Fotos, Tonaufnahmen und Telefonate

Weitere Sicherheits-Smartphones

- Blackphone
  - Privatsphären-Firma, die ein Smartphone entwickelt
  - u.a. von Phil Zimmermann (PGP)
  - PrivateOS, basiert auf Android

Feature	Android Default	PrivatOS Enhancement
Search	Trackable	Anonymous
Bundled Apps	Many, with privacy disabled by default	Few, and all privacy-enabled
Wi-Fi usage	Always on for geolocation and user tracking	Smart disabling of all Wi-Fi except trusted hotspots
App permissions	All-or-nothing	Fine-grained control in a single interface
Communications tools	Traceable dialer, SMS, MMS, browser. Vulnerable to spoofed cell networks and Wi-Fi.	Private calls, texting, video chat, file exchange up to 100MB, browsing, and conference calls
Updates	Supplied infrequently after carrier blessing	Frequent secure updates from Blackphone directly
Remote Wipe & Anti Theft	Requires use of centralized cloud account	Anonymous
Business Model	Personal data mining for tracking and marketing	Delivering privacy as a premium, valued feature

Hochsicherheits-Smartphone

Teopad

- Zwei gleichzeitig laufende, getrennte Umgebungen
- Patentierte „Sandbox“-Technologie
- Gesicherter Zugang zu Informationssystemen
- Gesicherte VoIP-Dienste
- Verschlüsselung lokaler Daten
- Starke Authentifizierung

Fazit

- NSA-Affäre hilft die IT-Sicherheit in den Blickpunkt der Öffentlichkeit zu stellen
- Im Fokus stehen nationale Strategien zur Minimierung der Cyberrisiken, sichere Daten-Cloud und die sichere Kommunikation
- Datenverschlüsselung aller Dienste wird notwendig
- Europäische Produkte und Standards werden durch die Affäre gestärkt