NSA: Teufel oder Sicherheitsbehörde für die Demokratie?

Virgil Gligor
Carnegie Mellon University
Pittsburgh, PA 15213

Swiss Cyber Risk Research Conference

Swiss Tech Convention Center - EPFL
Lausanne, Schweiz
20. Mai 2016

Offenlegungserklärung

1. Ich habe:
   - *keine direkte oder indirekte Finanzierung durch die NSA* für Forschung oder andere Zwecke erhalten
   - in der vergangenen 7 Jahren *sehr wenige Kontakte* mit der NSA-Führung (z.B. Direktor/stellvertretender Direktor, CTO) *gehabt* und in der näheren Zukunft sind auch *keine solchen Kontakte geplant*…

2. Ich habe *nur öffentliche Informationen* verwendet
   - keine Informationen, die eine *Sicherheitsfreigabe* erfordern, *keine* Leaks ☺

3. Ich spreche für keine Organisation, mit der ich direkt oder indirekt verbunden bin, und alle hier geäusserten Ansichten und Fehler sind *meine eigenen*.

NSA: Teufel oder Sicherheitsbehörde für die Demokratie?

Antwort: Beides

… gemäss gewissen (z.B. nicht religiösen) Definitionen von Teufel und Demokratie

Überblick

- Was tut ein Teufel im Bereich Cyber-Sicherheit und wie tut er es? Beispiel: eine andauernde Präsenz in einem Netzwerk aufbauen – ***nicht NSA****-spezifisch*

- 3 Dilemmas für die vernetzte Welt

- Mögliche Lösungen: Das Beispiel der ***NSA***

Teufel (im Bereich Cyber-Sicherheit): ein Gegner

baut eine *dauerhafte Präsenz* in einem Netzwerk eines Verteidigers auf, indem er:

- *Kosten & Unannehmlichkeiten* von massgeschneiderten Sicherheits- & Nischensystemen,
- die *grundlegende Unsicherheit* von Commodity-Systemen & -Netzwerken und
- die *Schwächen der Menschen* – z.B. durch Methoden wie Käuflichkeit, Bestechung und Erpressung – ausnutzt.

Teufel (im Bereich Cyber-Sicherheit): ein Gegner

baut eine *dauerhafte Präsenz* in einem Netzwerk eines Verteidigers auf, indem er:

- *Kosten & Unannehmlichkeiten* von massgeschneiderten Sicherheits- & Nischensystemen,
- die *grundlegende Unsicherheit* von Commodity-Systemen & -Netzwerken und
- die *Schwächen der Menschen* – z.B. durch Methoden wie Käuflichkeit, Bestechung und Erpressung – ausnutzt.

Demokratie (z.B. im Sinne der westlichen Welt): ein politisches System, in dem die Bürgerinnen und Bürger

- die Regierung durch Wahlen bestimmen und ersetzen; keine Revolutionen oder Staatsstreiche,
- am politischen und bürgerlichen Leben teilnehmen $\rightarrow$ ihre Rechte müssen geschützt werden,
- sich auf die Rechtsstaatlichkeit verlassen; d.h. das Gesetz gilt für alle gleichermassen.

$\Rightarrow$ ***öffentliche Rechenschaftspflicht der Regierung***

Teufel (im Bereich Cyber-Sicherheit): ein Gegner

baut eine *dauerhafte Präsenz* in einem Netzwerk eines Verteidigers auf, indem er:

- *Kosten & Unannehmlichkeiten* von massgeschneiderten Sicherheits- & Nischensystemen,
- die *grundlegende Unsicherheit* von Commodity-Systemen & -Netzwerken und
- die *Schwächen der Menschen* – z.B. durch Methoden wie Käuflichkeit, Bestechung und Erpressung – ausnutzt.

Demokratie (z.B. im Sinne der westlichen Welt): ein politisches System, in dem die Bürgerinnen und Bürger

- die Regierung durch Wahlen bestimmen und ersetzen; keine Revolutionen oder Staatsstreiche,
- am politischen und bürgerlichen Leben teilnehmen → ihre Rechte müssen geschützt werden,
- sich auf die Rechtsstaatlichkeit verlassen; d.h. das Gesetz gilt für alle gleichermassen.

⇒ ***öffentliche Rechenschaftspflicht der Regierung***

Ein Nachrichtendienst in einer Demokratie:

⇒ ein Teufel für ausländische Gegner, die die Institutionen & Lebensweise der Demokratie bedrohen

Drei Dilemmas

1) **Für eine Demokratie**: *öffentliche* Rechenschaftspflicht für *geheime* Operationen?
   - *keine nachrichtendienstlichen Informationen* für Spione, ausländische Gegner, Terroristen
   - *keine Verletzung der Persönlichkeitsrechte* unter dem Deckmantel der Geheimhaltung

2) **Für einen Nachrichtendienst**: Wie können im Cyberspace *ausländische Gegner, aber keine Bürgerinnen und Bürger* ins Visier genommen werden? Was ist erfolgsversprechend?
   - *Überwachung nur von Ausländern?*
   - *Überwachung nur zu nachrichtendienstlichen Zwecken?*
   - *Freund-Feind-Erkennung?*

3) **Für Bürgerinnen und Bürger**: Wie können wir darauf vertrauen, dass unser eigener Nachrichtendienst *uns nicht ausspioniert*?
(Freunde und Alliierte: Teilen wir immer noch die gleiche Vision von Demokratie?)

Dilemma 1: Alternative Mittel zur Erfüllung der Rechenschaftspflicht?

General Counsel der NSA (*Georgetown University Law School*, 27. Februar 2013):

«In einer Demokratie gibt es keinen perfekten Ersatz für öffentliche Transparenz.»

«… wir müssen uns weitgehend auf […] alternative Mittel zur Erfüllung der Rechenschaftspflicht abstützen.»

Dilemma 1: Alternative Mittel zur Erfüllung der Rechenschaftspflicht?

Exekutive

DoD (1952) + ODNI (2004)

UnderSec (Nachrichten-dienst)

AsstSec (Überblick)

Gen Counsel

IG (vom Kongress ernannt)

Gen Counsel

IG (vom Kongress ernannt)

IG (vom Kongress ernannt)

Civil Liberties Protection Officer

Legislative

Repräsentatenhaus & Senat (1952)

Ausschüsse:
Intelligence
Judiciary
Armed Services
Homeland Security usw.

Judikative

11 Richter am Bundesbezirksgericht FISC (ernannt durch den Supreme Court), eingeführt 1978

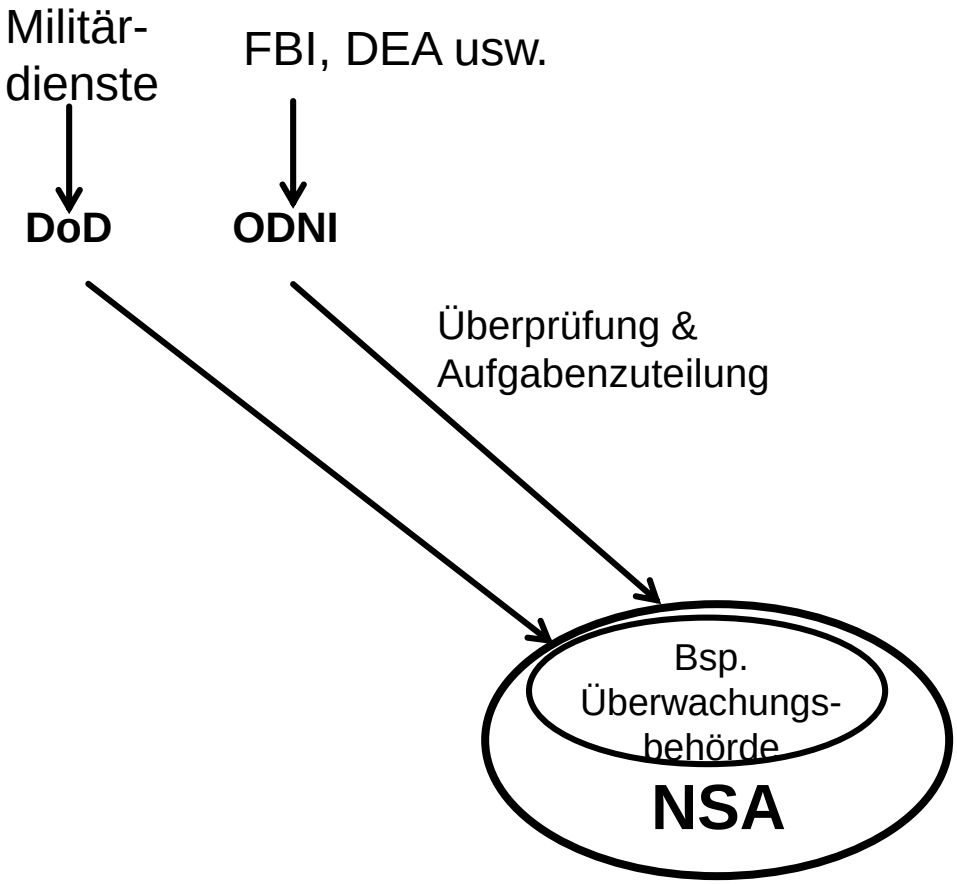
Unabhängiges Gremium Privacy & Civil Liberties Oversight Board (PCLOB)

2004 – 2006 im Executive Office?
2007 – 2012 --
2013 – Neuer Vorsitz (Jan.)
2014 – Bericht über Private Act, Abschnitt 215
2014 – Bericht über Private Act, Abschnitt 702
2016 – Assessment Report

Intern

Compliance-Schulung, Audit, Zugangskontrollen

Dilemma 2: Genehmigte Überwachung?



Ziel: ***Nicht-US*-Person *ausserhalb der USA***

⇒ *nicht «bewusst» ins Visier genommen:*

- *jeder in der USA;* US-Person *ausserhalb der USA (Ausländer, der in die USA zieht → US-Person);*
- keine rein inländische Überwachung;
- kein sogenanntes «reverse targeting» von *ausserhalb der USA;*
- «Minimierungsverfahren»
- *darf nicht gegen das 4th Amendment der US-Verfassung verstossen*

Zweck: nur nachrichtendienstliche Informationen

Überwachung von Nicht-US-Person?

USA ratifizierte 1966 den Zivilpakt ICCPR (1992)

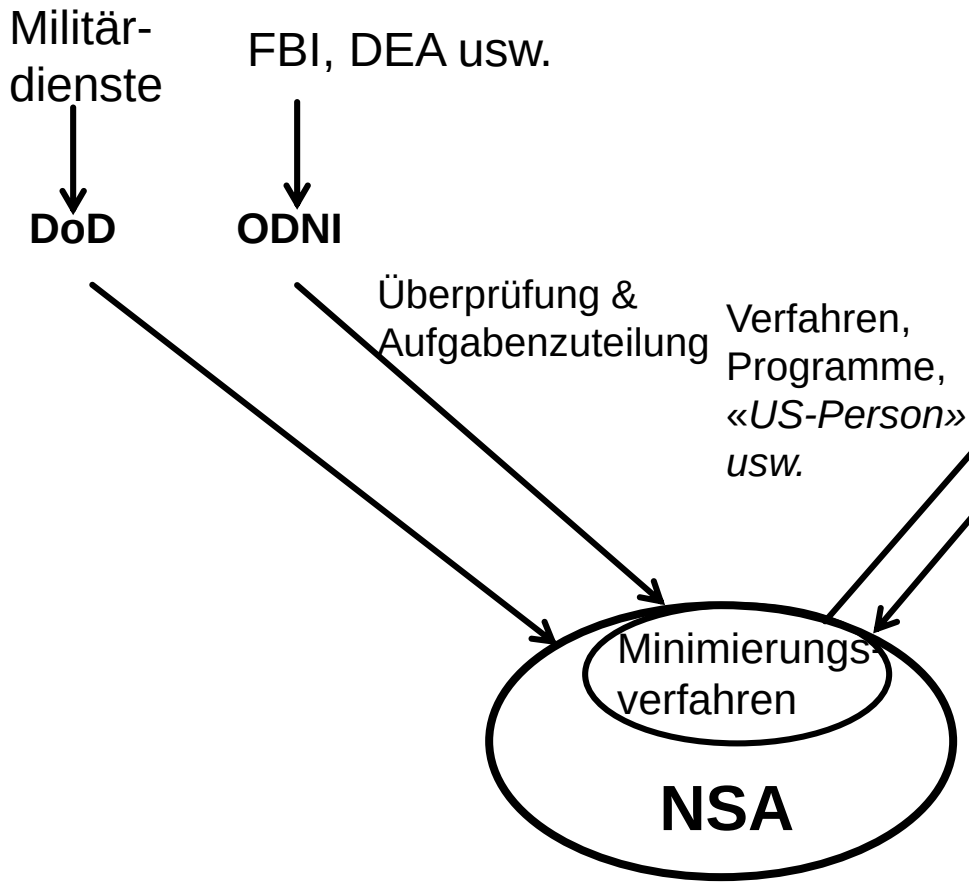
- Presidential Policy Directive 28 (2014) *beschränkt* die Informationsbeschaffung, *gleiche «Minimierungsverfahren» wie innerhalb der USA*

1. Ex. Order 12333
(ausserhalb der USA, 1981)

2. Abschnitt 215 des Patriot Act
(in der USA, «Telefonaufzeichnungen», 2001)

3. Abschnitt 702 FISA
(in der USA, 2008 geändert)

Dilemma 2: Korrekte Überwachung?



FISC – Gibt OK zu Revisionen der NSA 2012

z.B. 198 Genehmigungen für US-Personen
9500 Anfragen zu US-Personen
89 138 allgemeine Ziele (2013)

Abschnitt 702 FISA

1) PRISM ← spezifische ISP-Kommunikation
tiefe Fehlerquote (0,4%–1,5%) im Jahr 2013

2) «upstream» ← Backbone-Kommunikation
nicht von spezifischem «an/von/über-Selektor»
FISC: Mitschneiden von mehreren zusammen-hängenden Kommunikationssträngen (Multi Communication Transactions, MCTs) verstösst gegen das 4th Amendment (2008–2011)

unbeabsichtige Datensammlung; z.B. via MCT ~7000–8000 US-Personen, 97 000–140 000 wissen von nichts
keine routinemässige sofortige Löschung

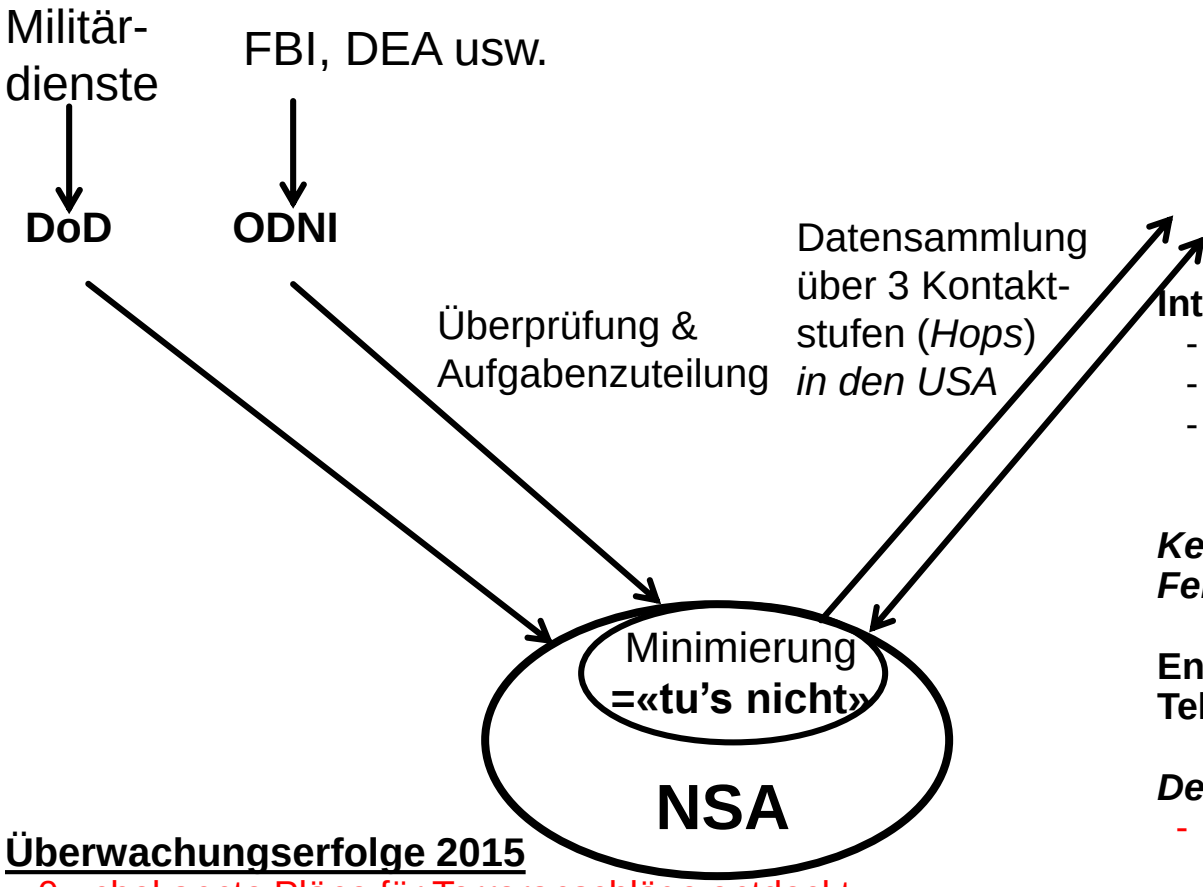
Executive Order 12333

1) Internes NSA-Audit fand & meldete
13 vorsätzliche Verstösse in einem Jahrzehnt

702 FISA Targeting Success

> 100 Verhaftungen wegen Terrorismusvorwürfen
z.B. 15 Fälle von geplanten Anschlägen in den USA,
40 Fälle von solchen in anderen Ländern, Waffenhandel usw.

Dilemma 2: Korrekte Überwachung?



Überwachungserfolge 2015

- 0 unbekannte Pläne für Terroranschläge entdeckt
- 0 Terroranschläge entdeckt
- 1 unter Umständen unbekannter Terrorist gefunden (kein Anschlag geplant)
- weitere Hinweise auf Kontakte mit Vedächtigen, die dem FBI bekannt sind
- Vermeidung von Falschmeldungen, spart FBI-Ressourcen

Patriot Act, Abschnitt 215

Alle 3 Monate vom FISC überprüft

Interpretation der NSA von Abschnitt 215

- gesetzliche Grundlage fehlt
- verstiess gegen ECPA 1986
- führte zu Bedenken bezüglich dem 1st & 4th Amendment der US-Verfassung

Kein Beweis für Arglist oder Fehlverhalten der NSA

Ende der massenhaften Sammlung von Telefondaten

Der FISC fehlt es an:

- gegensätzlichen Standpunkten & spezialisierten Anwälten
- Möglichkeiten einer Überprüfung eines Entscheids durch nächsthöheres Gericht (*Appellate Review*)
- technischer & externer rechtlicher Unterstützung

Freigabe & stat. Offenlegungen

Dilemma 3: Wie vertrauen wir?

Erst mit Enthüllungen der freien Presse & Insider-«Leaks» beginnen ☺

New York Times (Dez. 2005): NSA belauscht ohne Befugnis
New York Times (Feb. 2006): NSA sammelte 1,9 Billionen Gesprächsaufzeichnungen

- Bedeutende politische Veränderungen zwischen 2006 und 2012
- Enthüllungen von Snowden (Juni 2013) beschleunigten die Debatte
    - Tröpfchenweise Leaks tragen aber dazu bei, dass viele *falsche Mythen* über die NSA entstehen.

Danach auf starker Rechenschaftspflicht und gesetzgeberischen Massnahmen bestehen…

Unabhängiges PCLOB – die meisten Empfehlungen wurden von der US-Regierung angenommen.

Z.B. 1. Juni 2015: Ablauf von Abschnitt 215 des Patriot Act – keine weitere massenhafte Sammlung von Telefondaten durch die NSA

Gesetzgeberische Massnahmen: z.B. Email Privacy Act (H.R. 699), 27. April 2016

Neu braucht es u.a. einen gerichtlichen Beschluss, um

- *E-Mails* von *Providern zu sammeln* und
- die *Geo-Positionsdaten* eines Nutzers zu erhalten.

Dilemma 3: Wie vertrauen wir?

Man kann sich immer darauf verlassen, dass die Amerikaner das Richtige tun – aber erst, nachdem sie alles andere ausprobiert haben.»

Anonyme Anpassung (1970) eines Zitats von Abba Eban (1967)
(fälschlicherweise Winston Churchill zugeschrieben)

Und schliesslich debattieren, bis alle Alternativen ausgeschöpft sind…

z.B. abschreckende Wirkungen... oder doch nur Wechselwirkungen?

- Veränderungen im Internet-Browsing-Verhalten nach den Enthüllungen von Snowden, z.B. Pew Research Center (2013), Matthews and Tucker (2015), Jonathon Penney (2016)

- Selbstzensur beim Surfen über Themen im Zusammenhang mit Terrorismus?
  ODER veränderte Suche nach «skandalträchtigeren» Themen, z.B. Enthüllungen von Snowden?
  ODER beides?

- US-Bundesrichter weist Wikimedia-Klage gegen das Upstream-Programm der NSA ab (Oktober 2015)
  … keine Beweise dafür, dass die NSA das Internet «voll» überwacht.

Fakt: *91% der Internet-Kommunikation wird mit PRISM und nicht «upstream» überwacht.*

Gewonnene Erkenntnisse

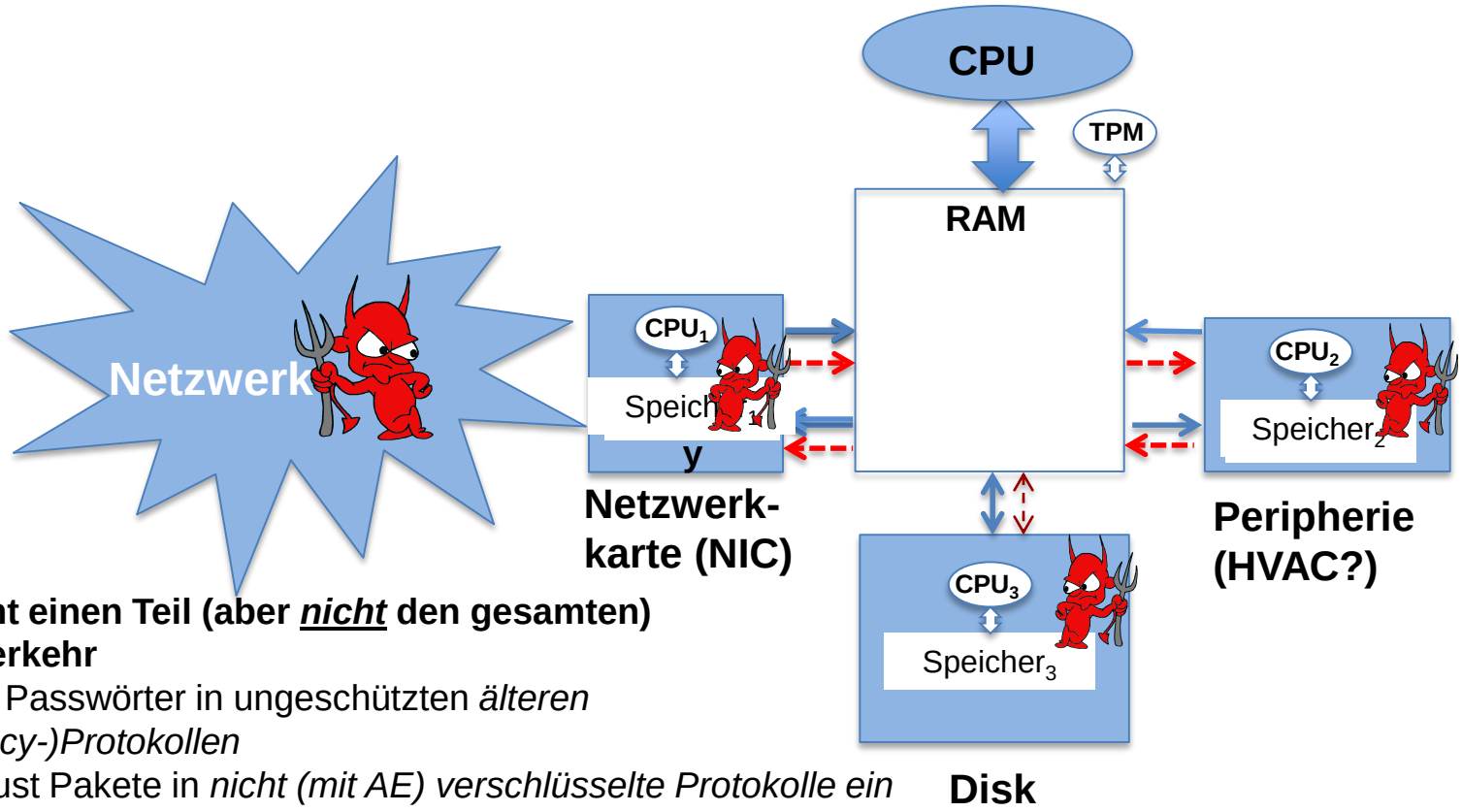
1. **Absolutes Fehlen von Transparenz (z.B. «Nie etwas sagen») hat vorhersehbare Konsequenzen.**
   - führt zu *falschen Mythen*; z.B. über ein Dutzend über die NSA
   - untergräbt letztlich das *Vertrauen in die Regierung*

2. **Bei der Überprüfung von Genehmigungen müssen die Gerichte auch einen Verteidiger des Teufels und nicht nur die Befürworter der Sache (d.h. Nachrichtendienst) anhören.**
   - Die Gerichte müssen den Eindruck vermeiden, die Entscheide seien bereits im Vorfeld gefallen.

3. **Gesetze und Regierungspolitik müssen mit der Technologie Schritt halten.**
   - Nachrichtendienstliche Genehmigungen müssen öfter als alle 10 Jahre neu geprüft werden.
   - Unabhängig davon, wie gebildet sie sind: Richter brauchen Hilfe, um die neue Technologie zu verstehen.

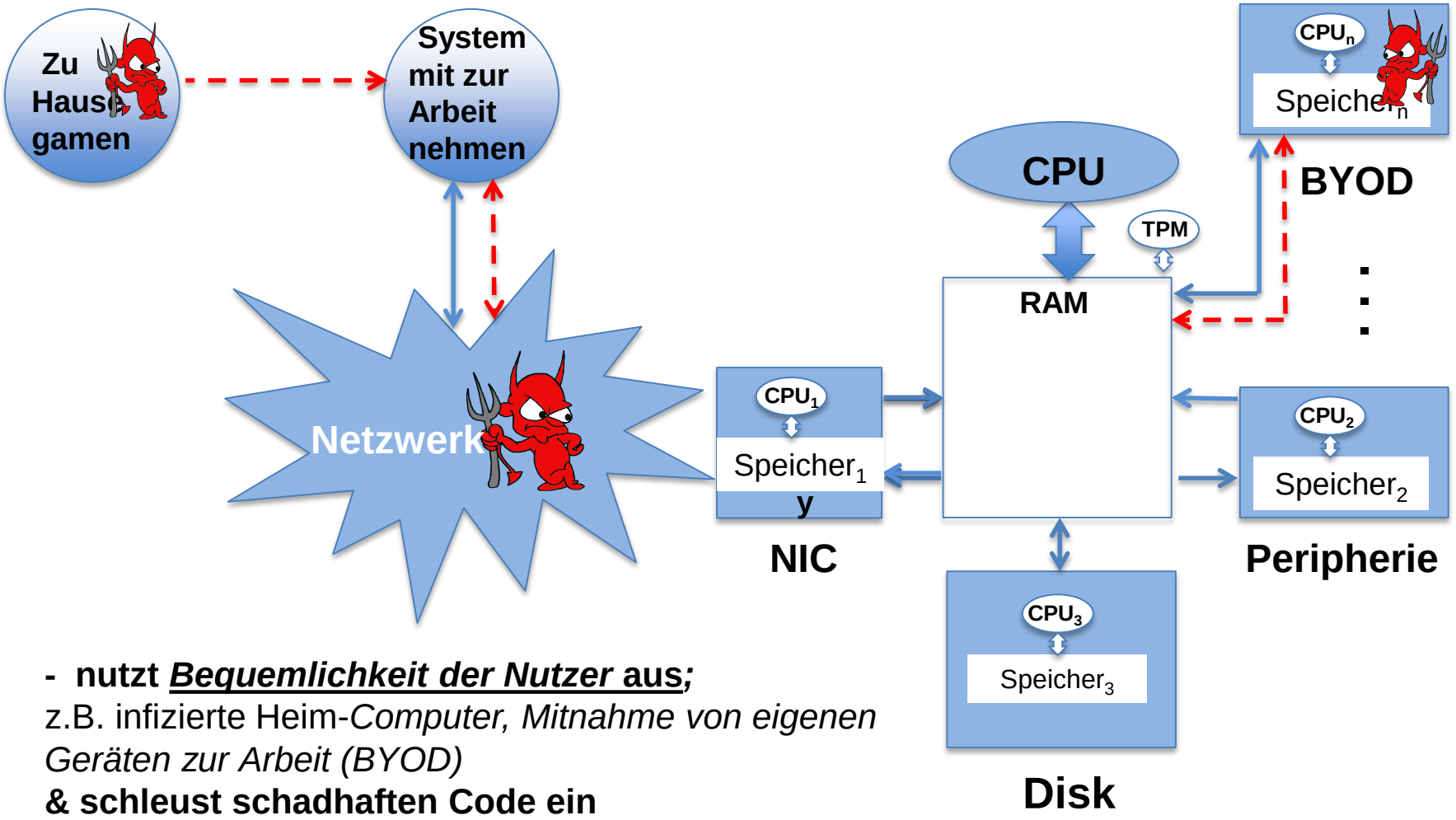
Beispiele:
Was tut ein Teufel im Bereich Cyber-Sicherheit & wie tut er es?

Dauerhafte Präsenz in einem Netzwerk – Kein NSA-Beispiel



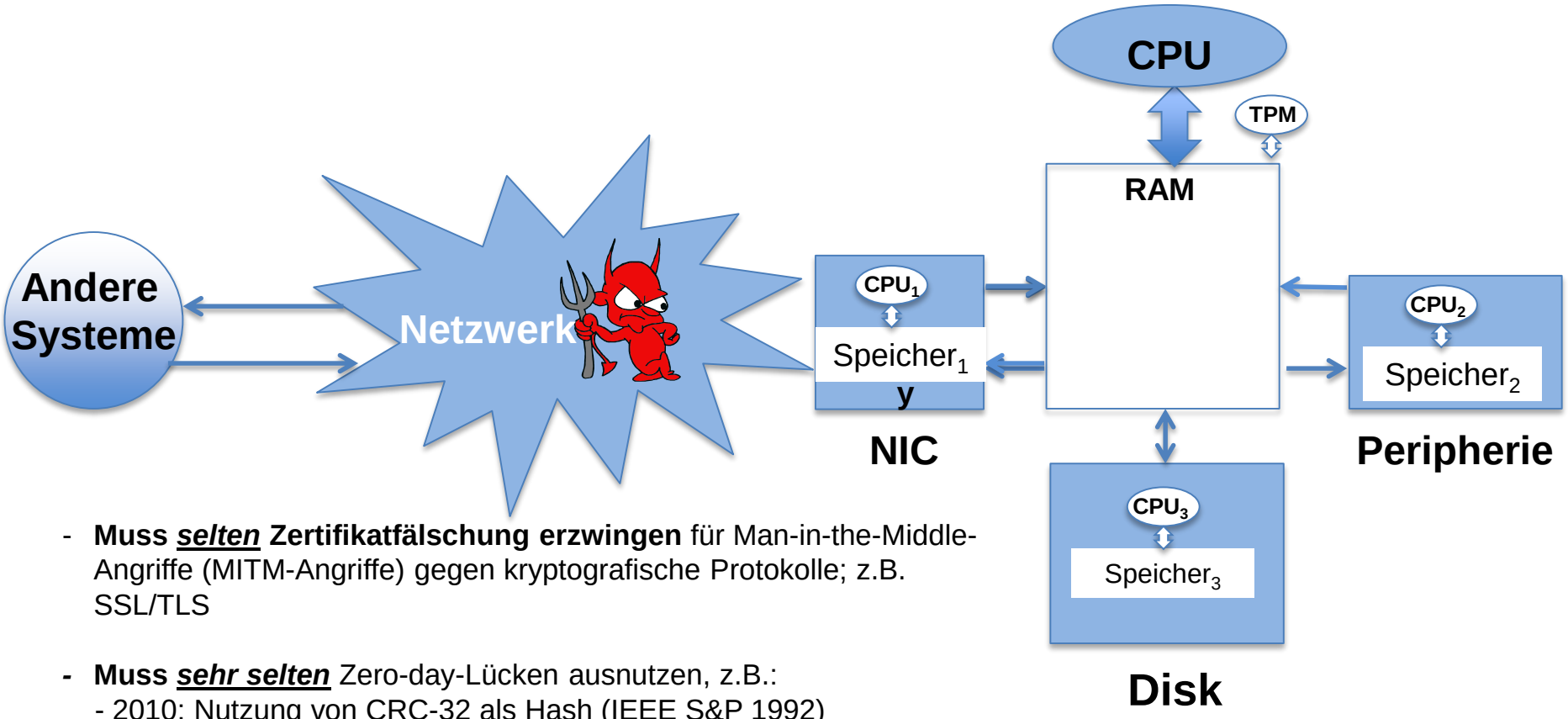
- **Überwacht einen Teil (aber *nicht* den gesamten) Internetverkehr**
  - findet Passwörter in ungeschützten *älteren (Legacy-)Protokollen*
  - schleust Pakete in *nicht (mit AE) verschlüsselte Protokolle ein* **& fügt schadhaften Code an unerwarteten Stellen ein**

Dauerhafte Präsenz in einem Netzwerk – Kein NSA-Beispiel



- **nutzt *Bequemlichkeit der Nutzer* aus;**
z.B. infizierte Heim-*Computer, Mitnahme von eigenen Geräten zur Arbeit (BYOD)*
& schleust schadhaften Code ein

Dauerhafte Präsenz in einem Netzwerk – Kein NSA-Beispiel



- **Muss *selten* Zertifikatfälschung erzwingen** für Man-in-the-Middle-Angriffe (MITM-Angriffe) gegen kryptografische Protokolle; z.B. SSL/TLS

- **Muss *sehr selten*** Zero-day-Lücken ausnutzen, z.B.:
  - 2010: Nutzung von CRC-32 als Hash (IEEE S&P 1992)
  - 2012: Chosen-Prefix-Kollisionen mit MD-5 (2006–2008 TUE - EPFL)

Sichere Netzwerkadministration: Kosten (3x) & Unannehmlichkeiten

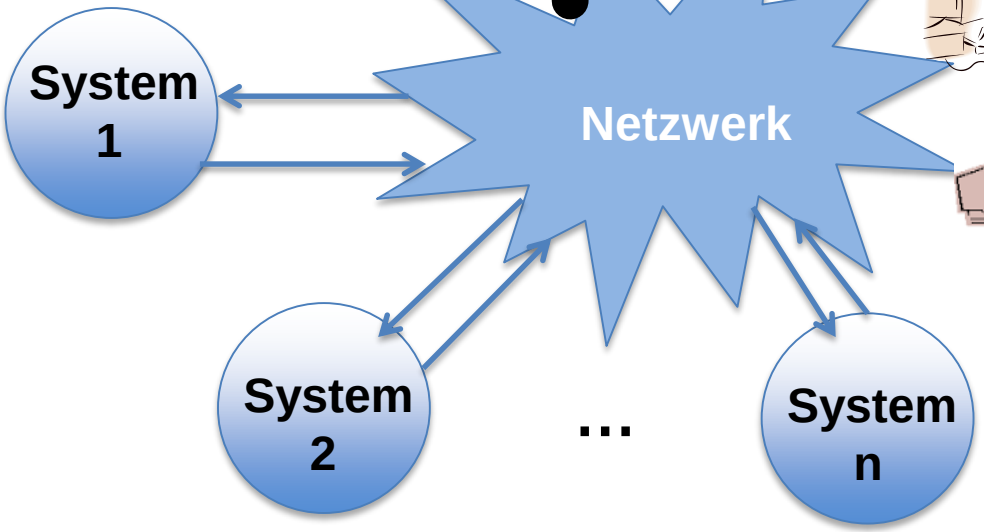
Ein einziger voll vertrauenswürdiger Systemadministrator

Strikte Aufgabentrennung

Auditor

Admin. für Systemsicherheit

nicht vertrauenswürdiger Administrator/Anwender



Mögliche Lösung:

Sichere Netzwerkadministration über interne Clouds skalieren

Grundlegende Unsicherheit von Commodity-Betriebssystemen/Anwendungen

Commodity-Software-Märkte

→ **Rasche Innovation**

-> **Kaum/nicht gesicherte Software**

Merkmale

Einführungskosten ≈ **0**
Regulierung ≈ **0**
Haftung ≈ **0**

Hersteller

- hohe Produktivität; z.B. viele Software-Funktionen, Apps
- wenige Barrieren, um den Code von andern zu benutzen

⇒ Software-«**Giganten**»

Konsumenten

- Zugang zu vielen Funktionen und Apps
- tiefer Preis

Hohe Sicherung/Sicherheit

- hohe Latenzzeit, Opportunitäts-kosten
- strikte Herkunftsprüfung
  ⇒ nicht verifizierter Code von andern kann nicht verwendet werden

⇒ wenige Funktionen; d.h. **WIMPs**

- hohe Kosten, z.B. für Produktion & Unterhalt

Nischen-Software-Märkte

z.B. wenige kleine Segmente der Raumfahrt-, Verteidigungs- und Atomindustrie