SATW

Schweizerische Akademie der Technischen Wissenschaften
Académie suisse des sciences techniques
Accademia svizzera delle scienze tecniche
Swiss Academy of Engineering Sciences

Mitglied der
Akademien der Wissenschaften Schweiz

Cyber-Überwachung: Technische Möglichkeiten und Grenzen

Bernhard M. Hämmerli mit Unterstützung von Eirik Bae

Thesis: Cyber Surveillance Architectures: What is behind the curtain?

Master thesis under supervision of Prof. Hämmerli

Student: Eirik Bae

Career at Gjøvik University College:

Bachelor of Science in Information Security	(2009 - 2012)
Master in Information Security	(2012 - 2014)

Content

Part I: Basic technical attack options by

Software, Development Kit, Tools, Hardware, Updates, any Combination
Transferring Data

Part II: Attacks in action

A: Without supplier support

Vulnerabilities, Attack Cycle

B: With supplier support

Terms & Condition, Server Access, “Lawful Interception”

Mitigation and impact on common attack categories

Part III: Information superiority and “Qui Bono”

understanding the current situation …

Appendix

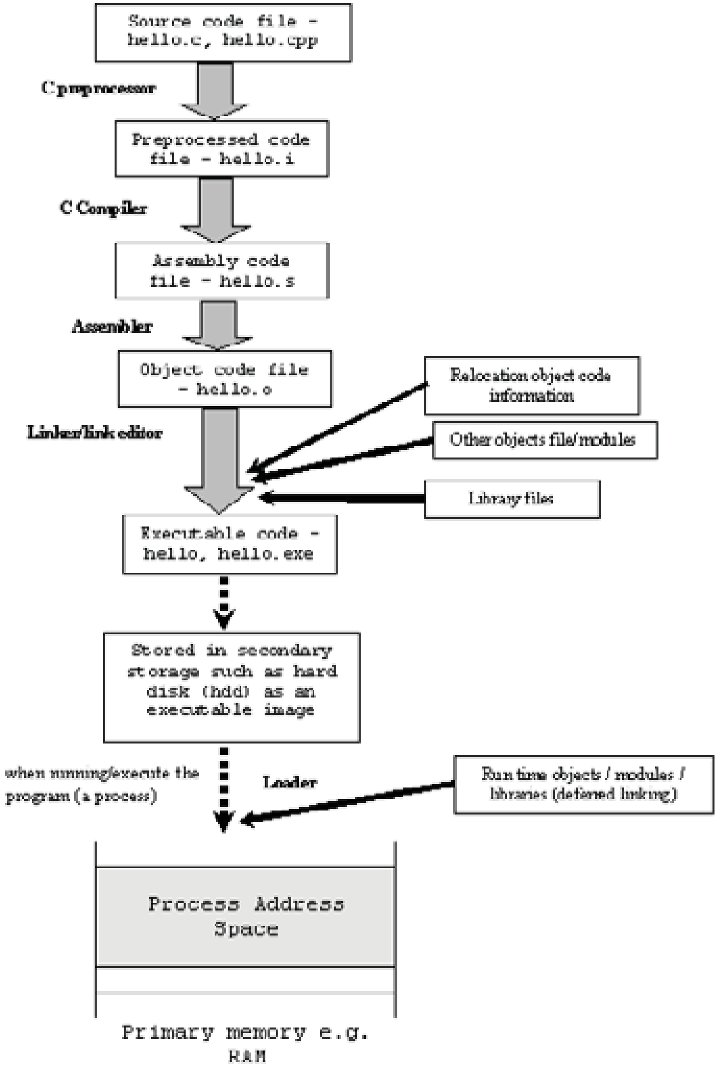
Part I: Basic technical attack options

Software Attack

- Apps and Application (these are most vulnerable)
- Middleware
- Virtualization
- Hardware abstraction
- Operation System OS
- Drivers (of OS and of peripherals)
- Firmware

➔ Believers in software audit reviews: Attention!!!

Path from code to Executable: another option to inject malware

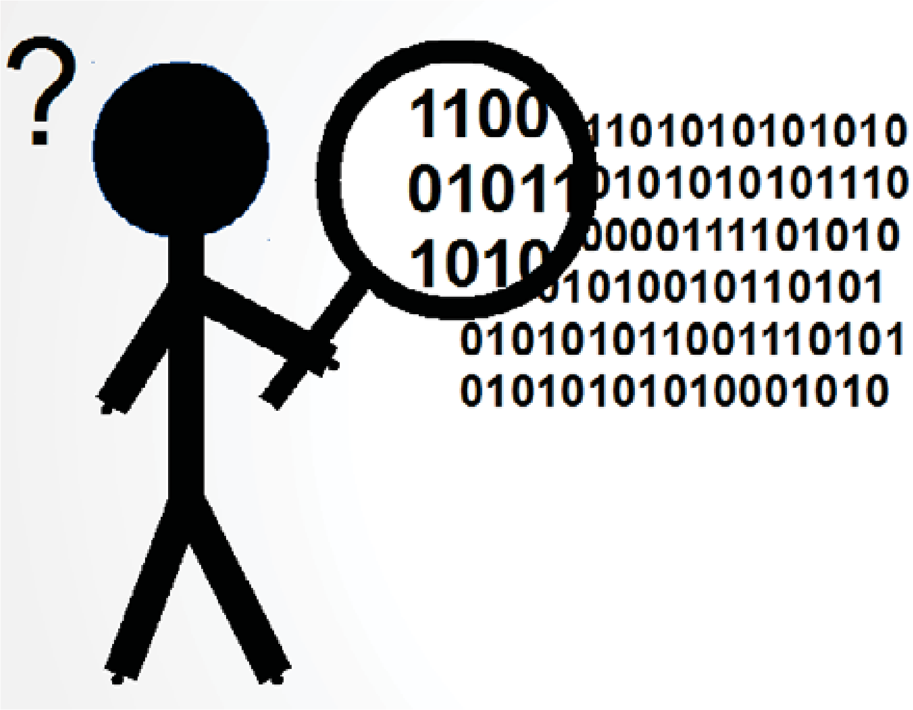

Source code file - hello.c, hello.cpp
C preprocessor
Preprocessed code file - hello.i
C Compiler
Assembly code file - hello.s
Assembler
Object code file - hello.o
Relocation object code information
Linker/link editor
Other objects file/modules
Library files
Executable code - hello, hello.exe
Stored in secondary storage such as hard disk (hdd) as an executable image
when running/execute the program (a process)
Loader
Run time objects / modules / libraries (deferred linking)
Process Address Space
Primary memory e.g. RAM

What happens if you change?

- C pre-processor
- C Compiler (*Ken Thompson, 1984)
- Assembler
- Linker
- Loader

(Image: Tenouk), *ACM: http://dl.acm.org/citation.cfm?id=358210

Deceptive Software assessments:
Are tools clean?



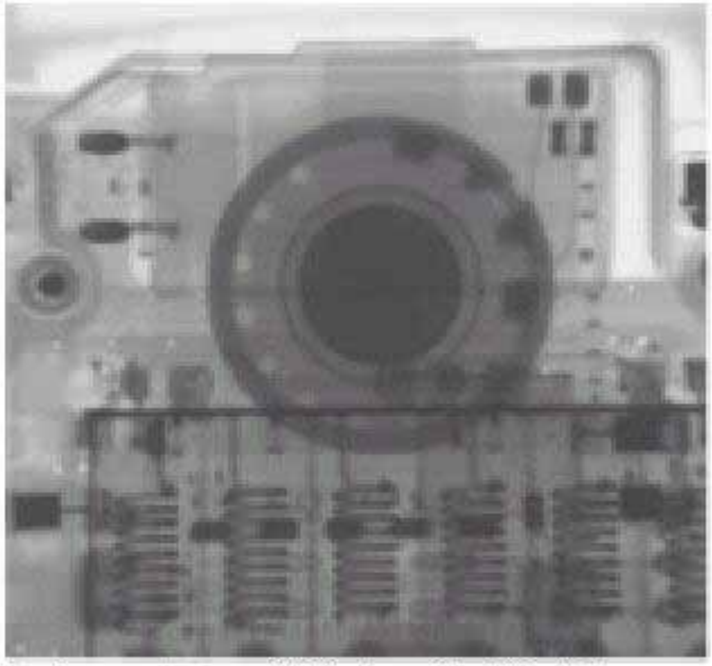
- Source code audit: King’s way?
  - A lot of work
  - Unclear: Did we find everything?
- A lot of tools are used for the assessment:
  - Task manager
  - Debugger
  - Source code analysis tools
  - Source code navigators
  - Binary navigation tools
  - Fuzz testers
  - Sandboxing

The Syria attack

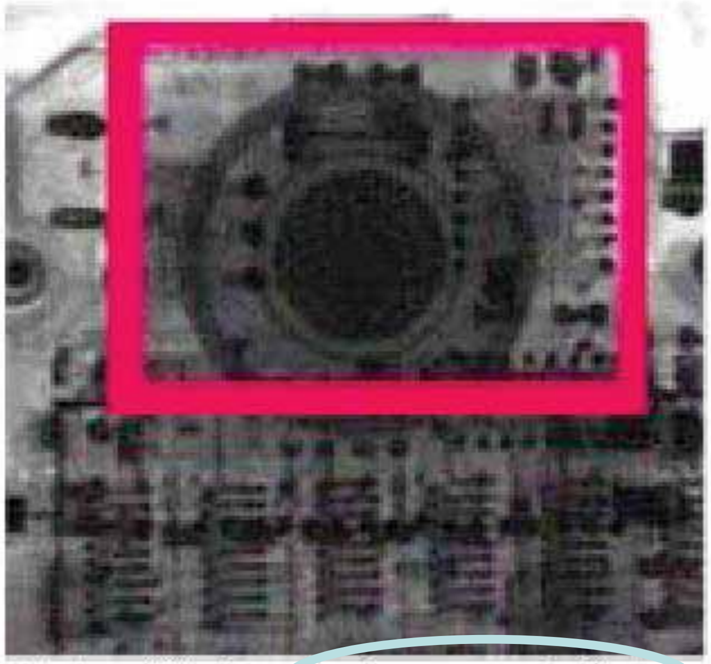
As an example of monitoring tool manipulation

**Syria nuclear plant (bomb production) should be bombed
not loosing too many airplanes …
how to protected against strong air defense weapons?**

Add-on Hardware für Zusatzfunktionalität



Referenzröntgenbild eines Mobiltelefons (Teilansicht)



Röntgenbild eines hardware-manipulierten Mobiltelefons (Teilansicht)

Bild: Euroforum 2006: Wilfried Karden, NRW Abwehr von Wirtschaftsspionage

Air Gap Security I

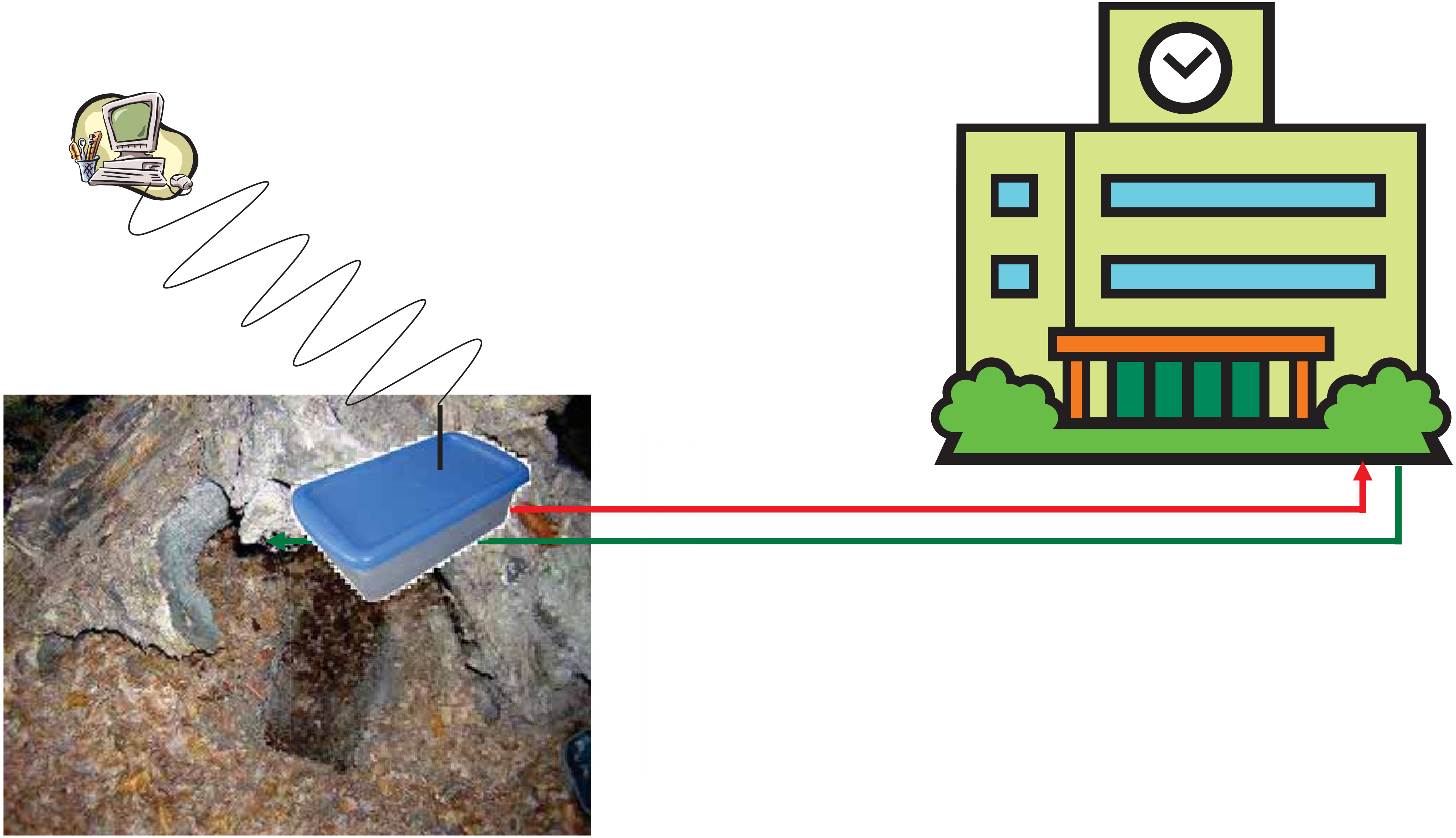
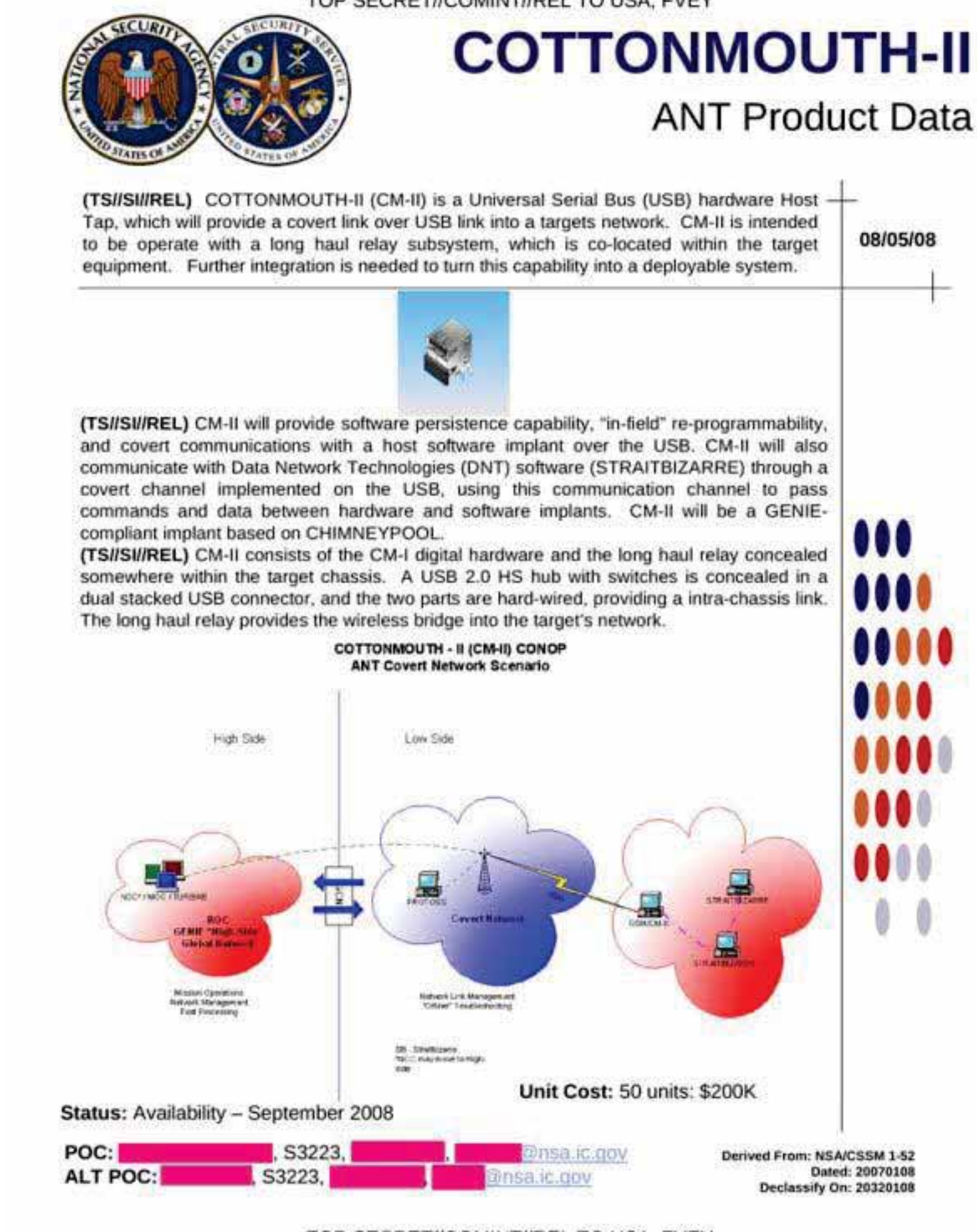


Bild: Euroforum 2006: Wilfried Karden, NRW Abwehr von Wirtschaftsspionage



TOP SECRET//COMINT//REL TO USA, FVEY

COTTONMOUTH-II

ANT Product Data

(TS//SI//REL) COTTONMOUTH-II (CM-II) is a Universal Serial Bus (USB) hardware Host Tap, which will provide a covert link over USB link into a targets network. CM-II is intended to be operate with a long haul relay subsystem, which is co-located within the target equipment. Further integration is needed to turn this capability into a deployable system.

08/05/08

(TS//SI//REL) CM-II will provide software persistence capability, "in-field" re-programmability, and covert communications with a host software implant over the USB. CM-II will also communicate with Data Network Technologies (DNT) software (STRAITBIZARRE) through a covert channel implemented on the USB, using this communication channel to pass commands and data between hardware and software implants. CM-II will be a GENIE-compliant implant based on CHIMNEYPOOL.

(TS//SI//REL) CM-II consists of the CM-I digital hardware and the long haul relay concealed somewhere within the target chassis. A USB 2.0 HS hub with switches is concealed in a dual stacked USB connector, and the two parts are hard-wired, providing a intra-chassis link. The long haul relay provides the wireless bridge into the target's network.

COTTONMOUTH - II (CM-II) CONOP
ANT Covert Network Scenario

Unit Cost: 50 units: $200K

Status: Availability – September 2008

POC: [redacted], S3223, [redacted], [redacted]@nsa.ic.gov
ALT POC: [redacted], S3223, [redacted], [redacted]@nsa.ic.gov

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

TOP SECRET//COMINT//REL TO USA, FVEY

Air Gap Security II

NSA's ANT Division Catalogue of Exploits for Nearly Every Major Software / ...

Page 48 of 52

Hardware covert channel out of air gaped network

Inside hardware chip

- *Gaming consoles*
  - *High focus on software security*
  - *Preventing the consoles from running pirated games*
  - *http://dl.acm.org/citation.cfm?id=777347*
  - *http://www.cs.arizona.edu/~collberg/Teaching/466-566/2013/Resources/presentations/2012/topic1-final/slides.pdf*
- *Backdoor in military chip*
  - *Found backdoor*
  - *Able to extract encryption keys*
  - *http://link.springer.com/chapter/10.1007%2F978-3-642-33027-8_2*
  - *http://defensetech.org/2012/05/30/smoking-gun-proof-that-military-chips-from-china-are-infected/*
- Hardware backdooring is practical
  - “[..] an attacker can use the underlying hardware to circumvent the software countermeasures.” ➔ detection just via hashed firmware: Malware Protection checks only Software
  - https://www.youtube.com/watch?v=yRxDvkKBMTc : Very good!
  - http://www.toucan-system.com/research/blackhat2012_brossard_hardware_backdooring.pdf

Picture: http://images.defensetech.org/wp-content/uploads/2012/05/actel-proasic31.jpg

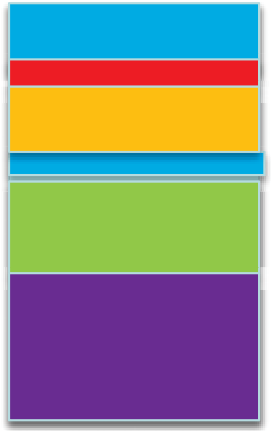
Updates

- Signed driver with vulnerability installs unsigned virtual box driver for installing / updating malware
  - Installing and exploiting vulnerability in (trusted) signed VirtualBox-driver as step-stone to install its malicious unsigned drivers. (SNAKE 2014 http://info.baesystemsdetica.com/rs/baesystems/images/snake_whitepaper.pdf)
  - Performing Man-In-The-Middle attack:
    - Pretend to be the update server and provide fake Flash / iTunes / Firefox
      - http://www.spiegel.de/international/germany/troublesome-trojans-firm-sought-to-install-spyware-via-faked-itunes-updates-a-799259.html
      - http://www.bbc.com/news/technology-22372027
      - http://blogs.wsj.com/digits/2011/11/21/surveillance-company-says-it-sent-fake-itunes-flash-updates-documents-show/
    - Inject malicious code to benign executables that are passing through the network in control of the attacker.

Combination

- Multiple pieces of code makes little or no meaning, but together they make up the malicious code.

- Can be distributed in two or more of the following ways:
  - Operating system software
  - Be a part of popular applications or an additional application
  - Added in development process
  - Added into hardware or added as extra hardware
  - Sent through updates from trusted vendors*
  - …



*Requires either to “collaborate with” or “hack” a vendor, or ”inject an undercover employee”.

➔ Combination makes the attack almost impossible to detect ...
Ideal: stealth & untraceable, immune to malware detection: see appendix A1

To whom we should trust …

- Find a trusted supplier and consider complete **supply chain for security**
- ➔ Nationalisation of IT: software, hardware, legal framework

See: www.lancom-systems.de/presse/pressemitteilung/pressemitteilung/cebit-2014-kanzlerin-merkel-informiert-sich-bei-lancom-systems-ueber-hochsichere-router-made-in-germany/

- To whom we should not trust:
  Alike many other states: 250 million dollar / year NSA fund to weaken security products*

  *"The third is the deliberate sabotaging of security. The primary example we have of this is the **NSA's BULLRUN** program, which tries to "insert vulnerabilities into commercial encryption systems, IT systems, networks and endpoint communication devices." This is the worst of the NSA's excesses, because it destroys our trust in the Internet, weakens the security all of us rely on and makes us more vulnerable to attackers worldwide. "*

*www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security

Eindringen in jedes Computer System, ZDF World Wide War

Data in Transition: Transferring Data to the Attacker

- **Technical options:**
  - Transferring Data over the Internet
    - Plain or using encryption (for hiding purposes) to “normal” names
    - During Updates
    - Embedded into unused fields in protocols
    - Embedded into maintenance Protocol
    - Hiding origin by using many proxies
      - TOR
      - Hidden Collection Infrastructure (Information) (CitizenLab, 2014) https://citizenlab.org/2014/02/mapping-hacking-teams-untraceable-spyware/
  - **Transferring Data without connect to internet**
    - Employee using USB-stick
    - Physically collect data (HW maintenance)
    - Locally connected PC without internet using “proxy server”
    - Radio access (COTTONMOUTH http://leaksource.files.wordpress.com/2013/12/nsa-ant-cottonomouth-iii.jpg)

Part II
Attacks in action

A: Without supplier support

Step 1: Identifying Vulnerabilities

- **Published vulnerabilities** (Patch available, Attack suite available ➔ Script kiddies)

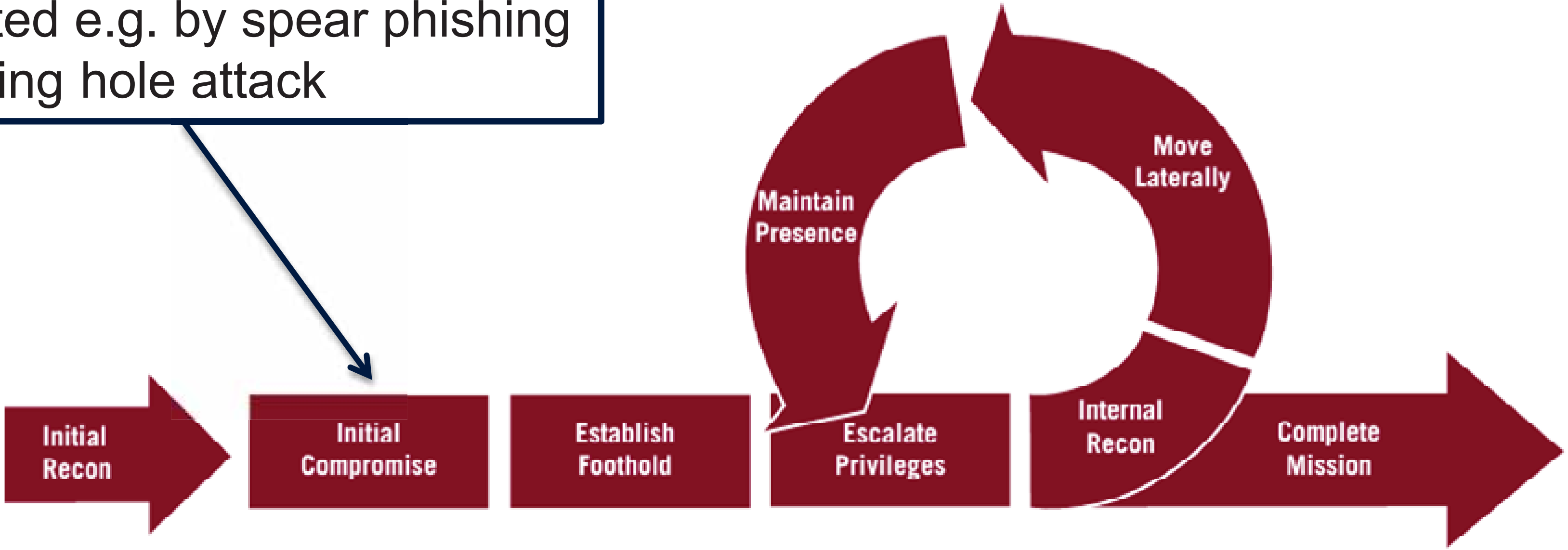
- **Vulnerability market** buy or rent a vulnerability
  as service to governments
  - Commercial companies as e.g. VUPEN for zero day exploits
  - Providing "lawful interception" e.g. (Hacking Team, Gamma International, Blue Coat etc.)
  as service to criminals (crimeware as a service, no ethical conduct)
  - black market: zero exploits
  - crime as a service. With explicit business conditions *

- Self-researched **vulnerability by engaged hacker team** (in-house or any others …)

* (2007 / 2) MELANI International Journal of Critical Infrastructure Protection 6 (2013) 28-38)
https://www.sciencedirect.com/science/article/pii/S1874548213000036?np=y (crimeware as a service)

Mandiant attack cycle

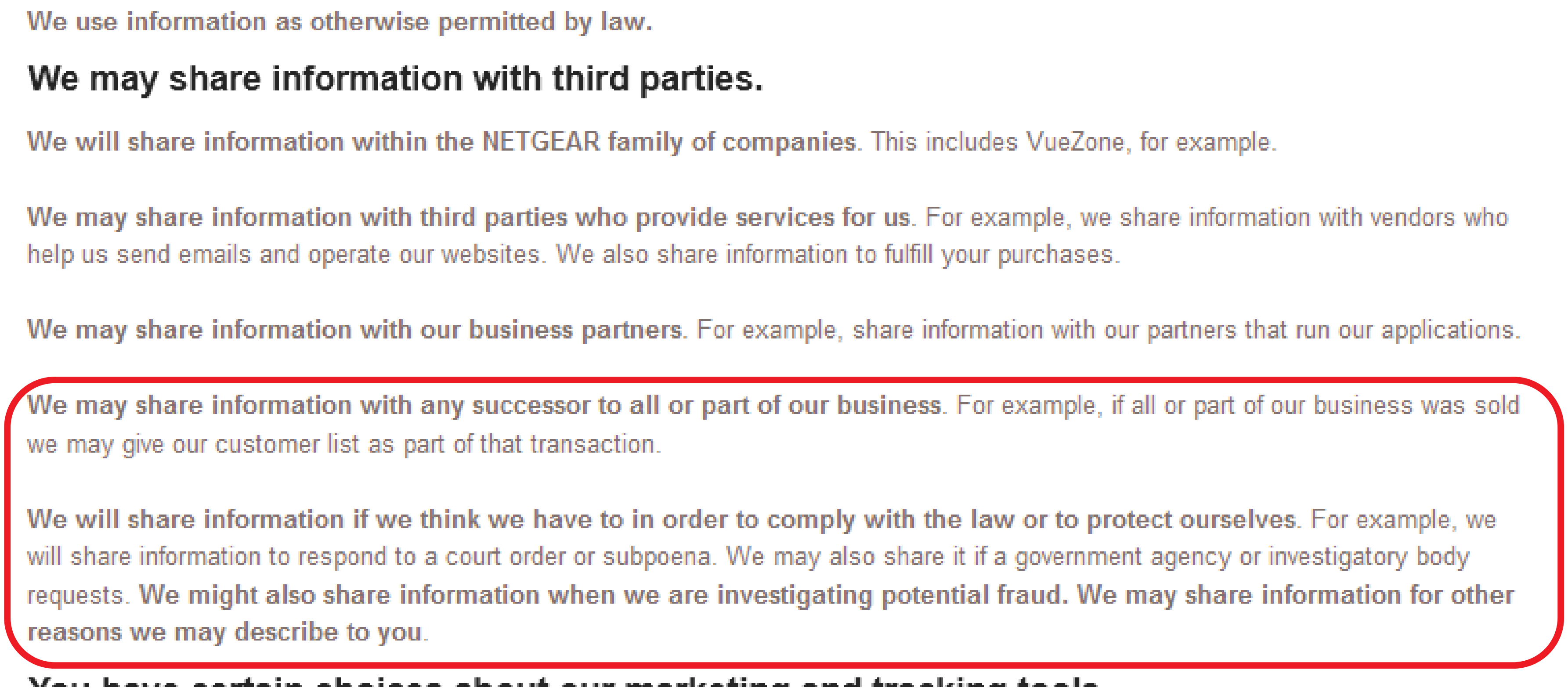
- Exploited vulnerability
- Distributed e.g. by spear phishing or watering hole attack



(Image: Mandiant APT1 Report 2013, https://community.norton.com/t5/Ask-Marian/Cyber-Security-Term-Watering-Hole-Attack/ba-p/1004915)

B: With supplier support

Accessing data with legitimation by Terms & Conditions



We use information as otherwise permitted by law.

We may share information with third parties.

We will share information within the NETGEAR family of companies. This includes VueZone, for example.

We may share information with third parties who provide services for us. For example, we share information with vendors who help us send emails and operate our websites. We also share information to fulfill your purchases.

We may share information with our business partners. For example, share information with our partners that run our applications.

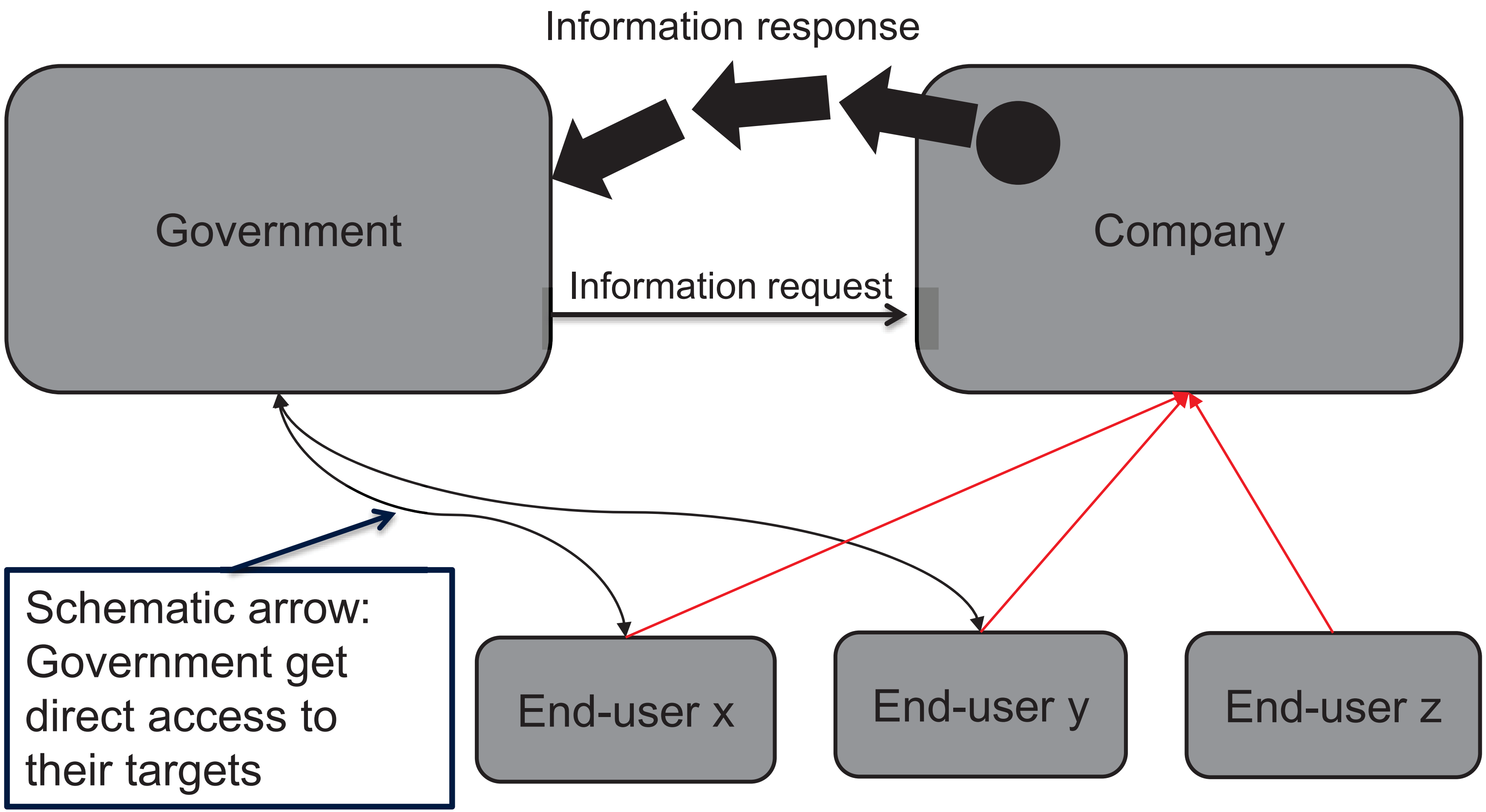
We may share information with any successor to all or part of our business. For example, if all or part of our business was sold we may give our customer list as part of that transaction.

We will share information if we think we have to in order to comply with the law or to protect ourselves. For example, we will share information to respond to a court order or subpoena. We may also share it if a government agency or investigatory body requests. **We might also share information when we are investigating potential fraud. We may share information for other reasons we may describe to you**.

You have certain choices about our marketing and tracking tools

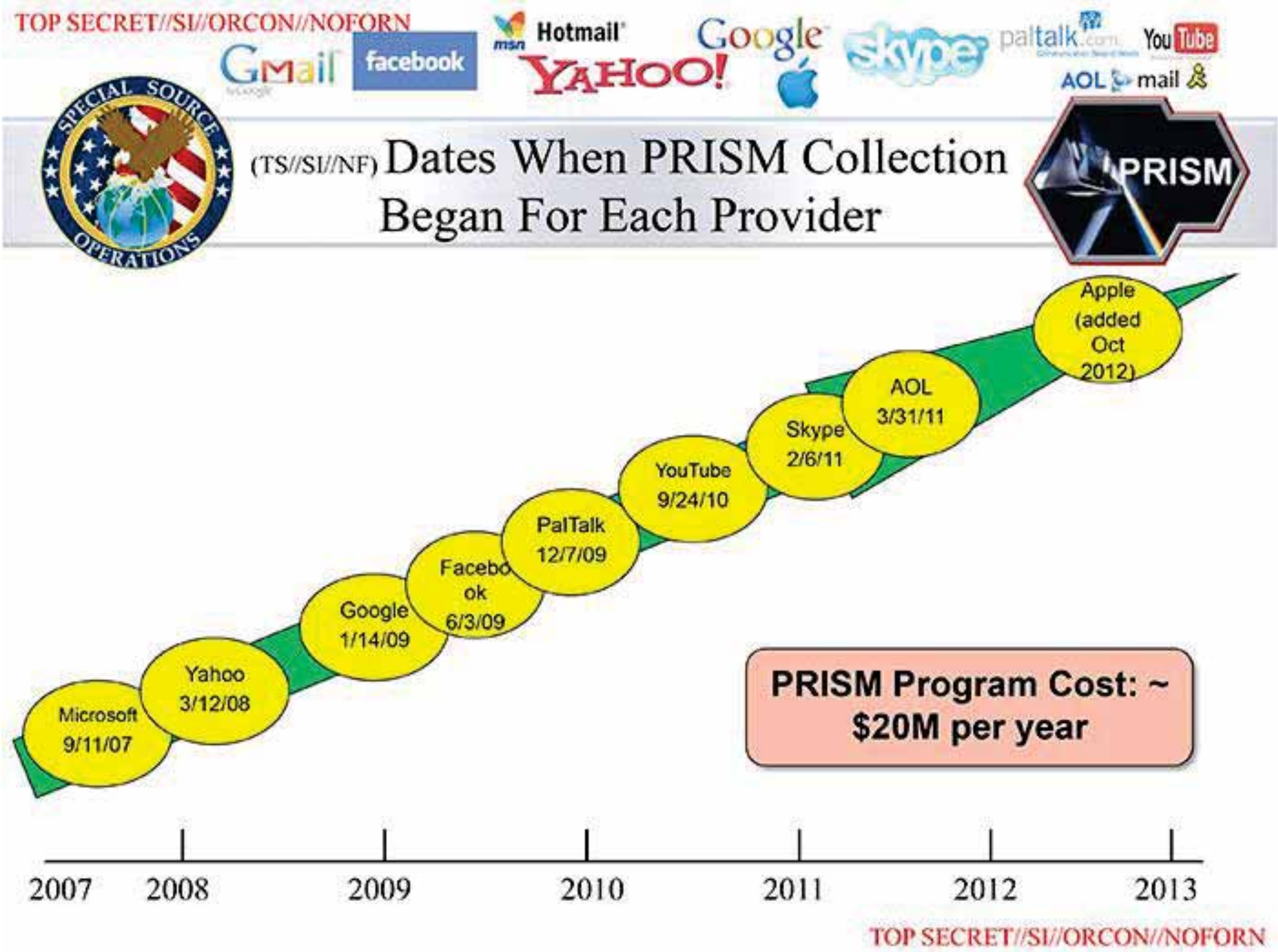
(Image: Netgear NAS, published Terms and Conditions, accessed March 31, 2014)

Service provider opens for government access to user data



Schematic arrow: Government get direct access to their targets

Collaboration with companies via PRISM (e.g. USA)



TOP SECRET//SI//ORCON//NOFORN

(TS//SI//NF) Dates When PRISM Collection Began For Each Provider

PRISM Program Cost: ~ $20M per year

TOP SECRET//SI//ORCON//NOFORN

Principally governments act along equal lines to perform their tasks.

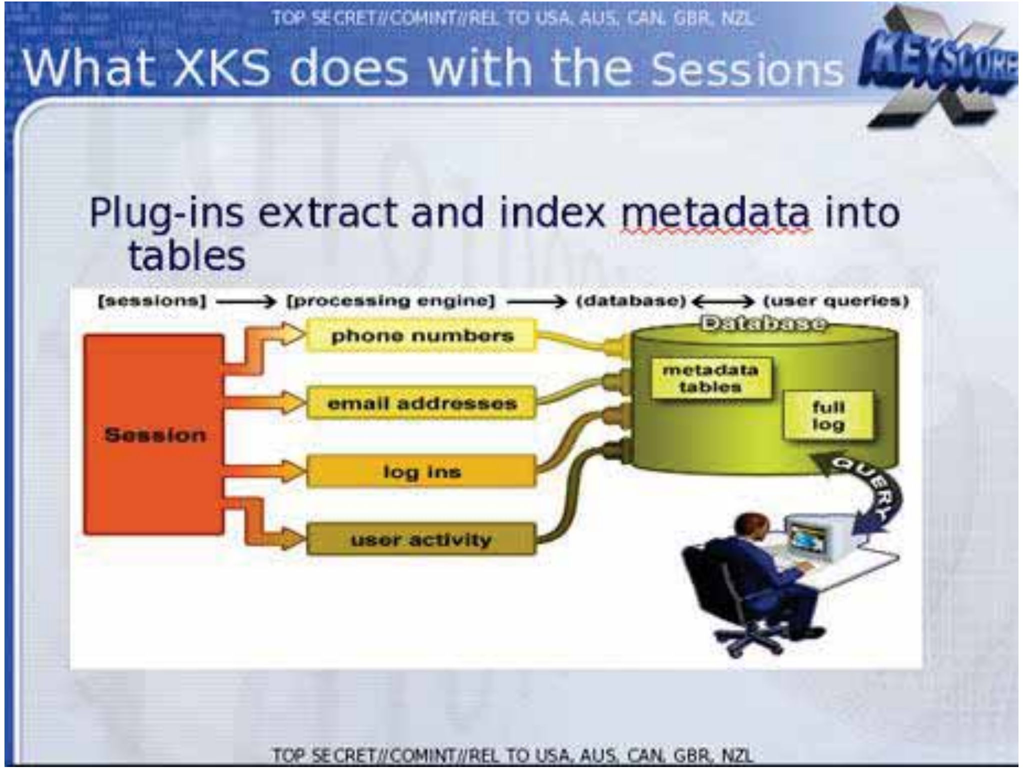
USA is in common with many other nations ...

(Image: The Guardian)

On big data analytics: Data & Metadata

e.g. NSA **X-keyscore**, dishfire (collection of millions of text messages), prefer

DNI = Digital Network Intelligence



TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

What XKS does with the Sessions

KEYSCORE

Plug-ins extract and index metadata into tables

[sessions] → [processing engine] → (database) ↔ (user queries)

Session

phone numbers

email addresses

log ins

user activity

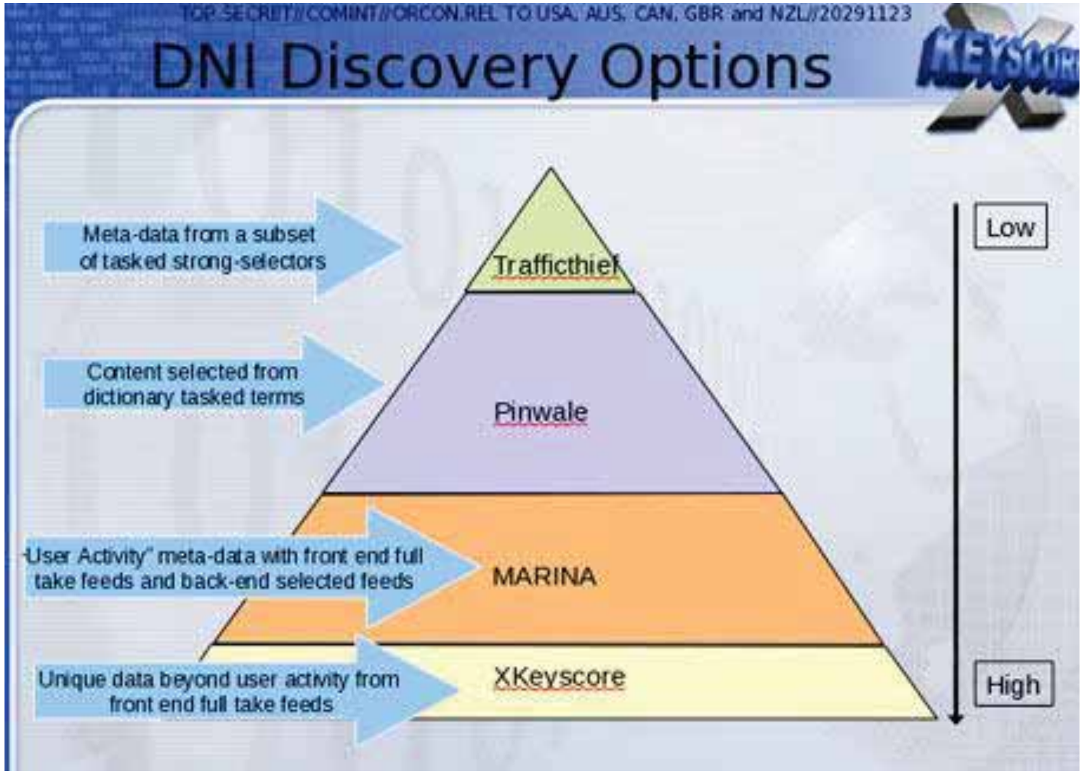
Database

metadata tables

full log

QUERY

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL



TOP SECRET//COMINT//ORCON,REL TO USA, AUS, CAN, GBR and NZL//20291123

DNI Discovery Options

KEYSCORE

Meta-data from a subset of tasked strong-selectors → Trafficthief

Content selected from dictionary tasked terms → Pinwale

User Activity" meta-data with front end full take feeds and back-end selected feeds → MARINA

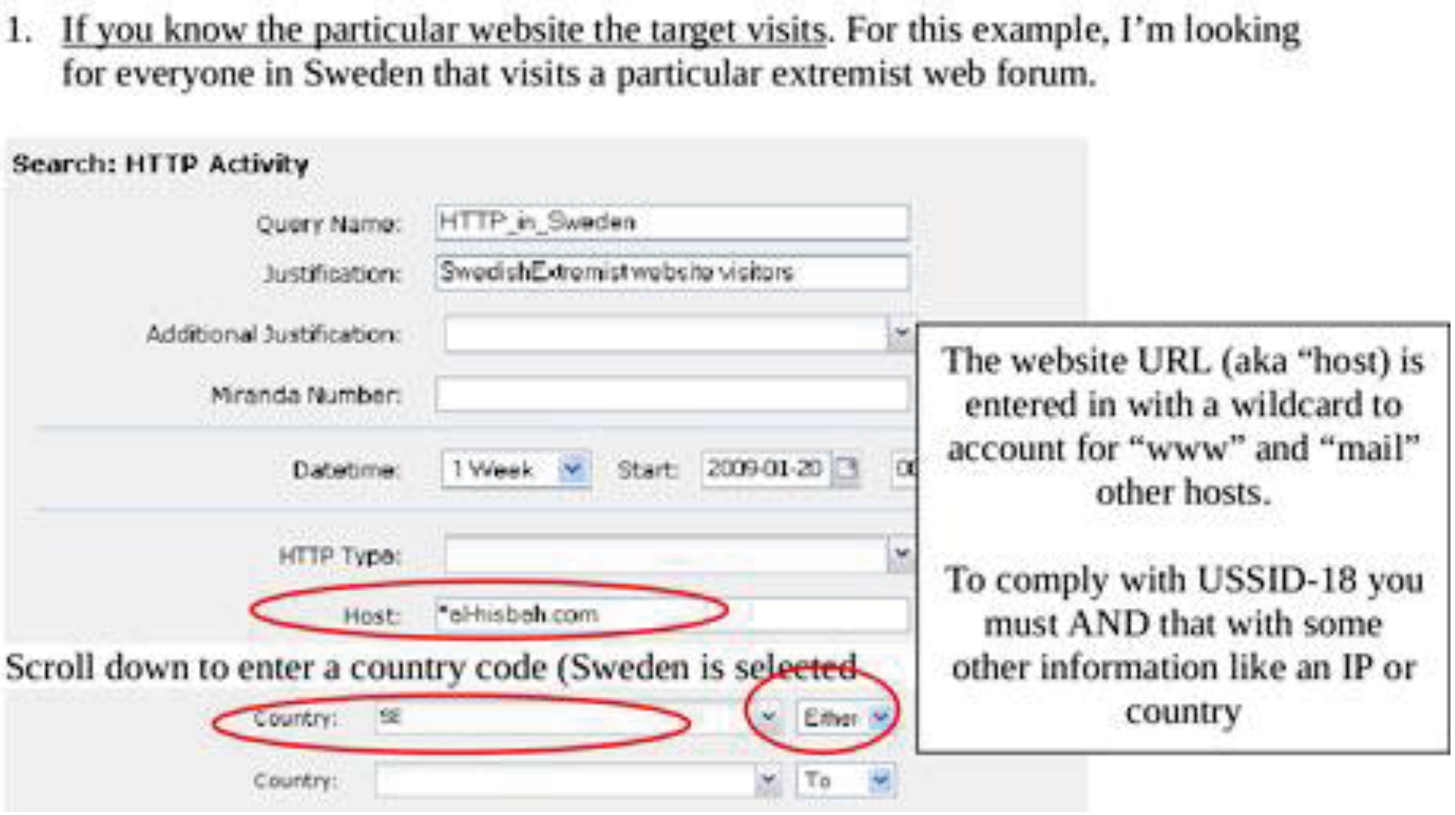
Unique data beyond user activity from front end full take feeds → XKeyscore

Low

High

www.theguardian.com/world/interactive/2013/jul/31/nsa-xkeyscore-program-full-presentation

NSA is more then "NCIS" or "Homeland"
New form of mining: data mining



1. If you know the particular website the target visits. For this example, I'm looking for everyone in Sweden that visits a particular extremist web forum.

Search: HTTP Activity

Query Name: HTTP_in_Sweden

Justification: SwedishExtremist website visitors

Additional Justification:

Miranda Number:

Datetime: 1 Week Start: 2009-01-20 00

HTTP Type:

Host: *alHisbah.com

Scroll down to enter a country code (Sweden is selected

Country: SE Either

Country: To

The website URL (aka "host) is entered in with a wildcard to account for "www" and "mail" other hosts.

To comply with USSID-18 you must AND that with some other information like an IP or country

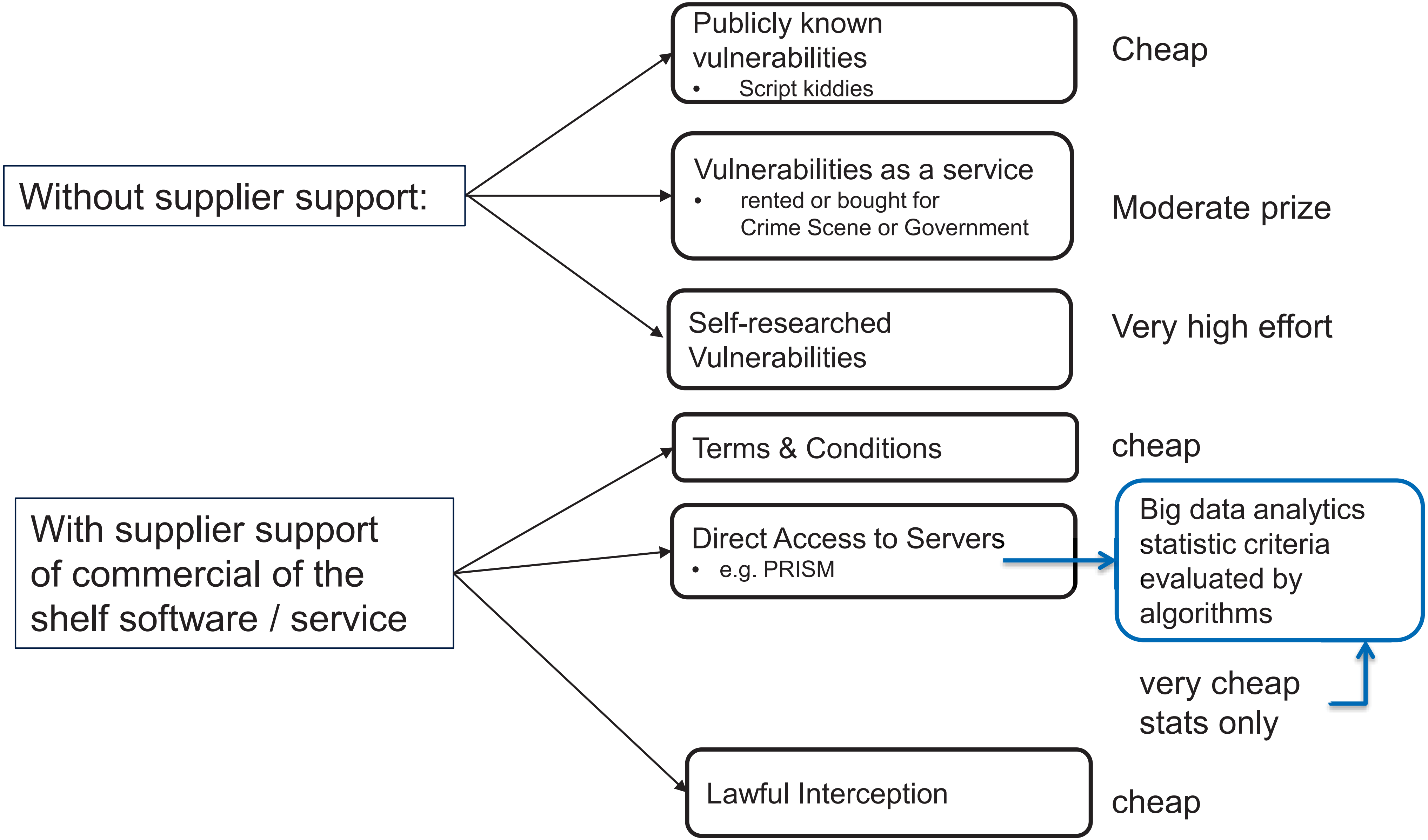
http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data

Government code in products for “lawful interception”

- Technical principle
  - Add government access option in products
    e.g. using nation-state sponsored algorithms and program code, e.g. NSA key
  - Giving the government information on undisclosed vulnerabilities
  - Allowing governments targeted access based on identifiers
    to specific customer information, using company software components (e.g. updates providing access as e.g. Trojan horse, team viewer)

References not have been found for each case

Technical options for attacks



Without supplier support:

Publicly known vulnerabilities
- Script kiddies

Cheap

Vulnerabilities as a service
- rented or bought for
  Crime Scene or Government

Moderate prize

Self-researched Vulnerabilities

Very high effort

With supplier support of commercial of the shelf software / service

Terms & Conditions

cheap

Direct Access to Servers
- e.g. PRISM

Big data analytics statistic criteria evaluated by algorithms

very cheap
stats only

Lawful Interception

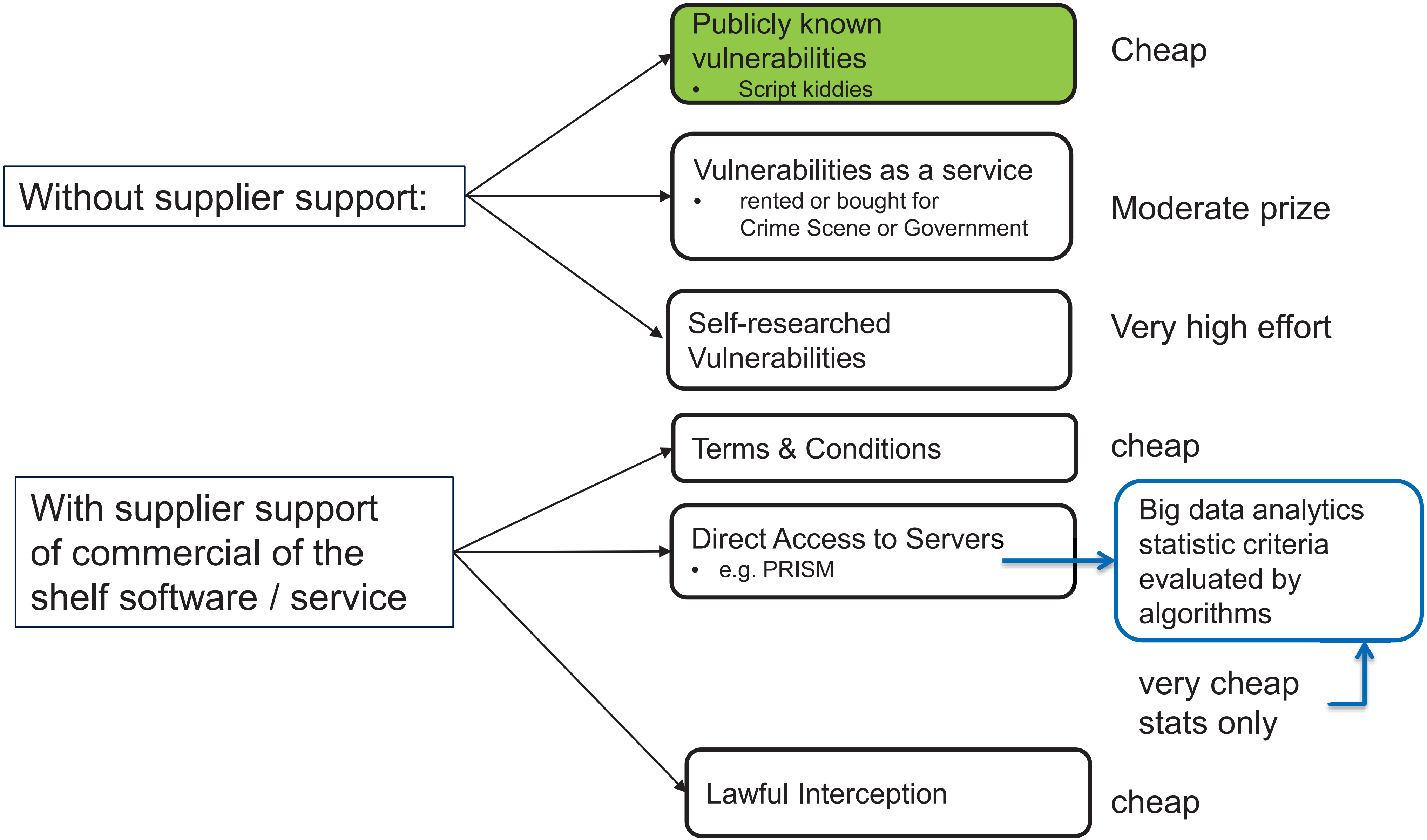
cheap

Mitigation I

- Regularly patch your operating system and applications.

- Always update to the newest anti-virus definitions.
  - Be aware that some anti-virus vendors might decide to not detect surveillance software used for lawful interception by governments in their country of origin.

Technical options for attacks



Without supplier support:

Publicly known vulnerabilities
- Script kiddies

Cheap

Vulnerabilities as a service
- rented or bought for Crime Scene or Government

Moderate prize

Self-researched Vulnerabilities

Very high effort

With supplier support of commercial of the shelf software / service

Terms & Conditions

cheap

Direct Access to Servers
- e.g. PRISM

Big data analytics statistic criteria evaluated by algorithms

very cheap
stats only

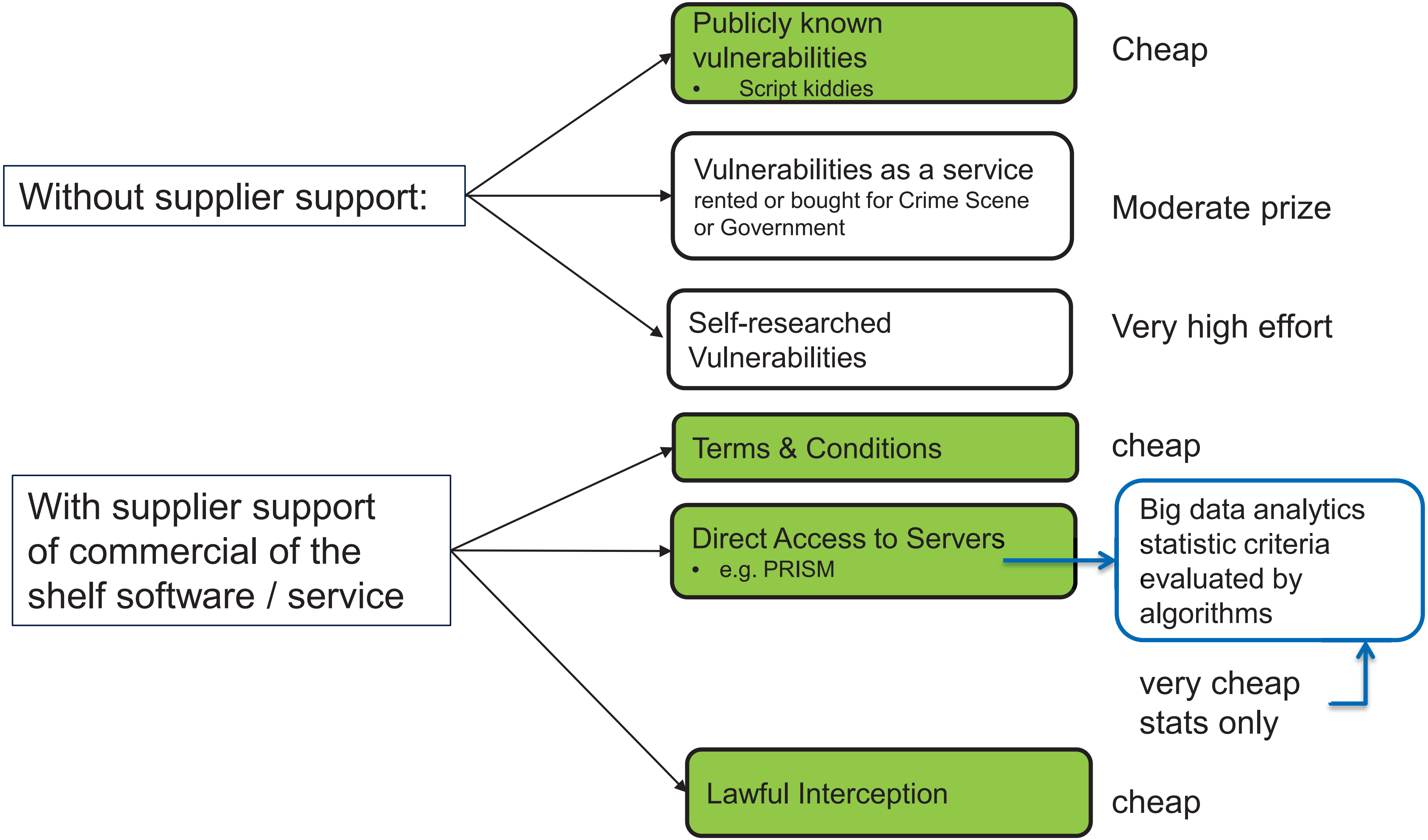
Lawful Interception

cheap

Mitigation II

- Mitigation I + :
- Exclusively use software and hardware from vendors you trust, including services
  - You need to trust all steps of their Supply Chain (feasible? If production is worldwide distributed)
  - Even one single untrusted product could harm your whole system (zero tolerance)

Technical options for attacks



Without supplier support:

Publicly known vulnerabilities
- Script kiddies

Cheap

Vulnerabilities as a service
rented or bought for Crime Scene or Government

Moderate prize

Self-researched Vulnerabilities

Very high effort

With supplier support of commercial of the shelf software / service

Terms & Conditions

cheap

Direct Access to Servers
- e.g. PRISM

Big data analytics statistic criteria evaluated by algorithms

very cheap
stats only

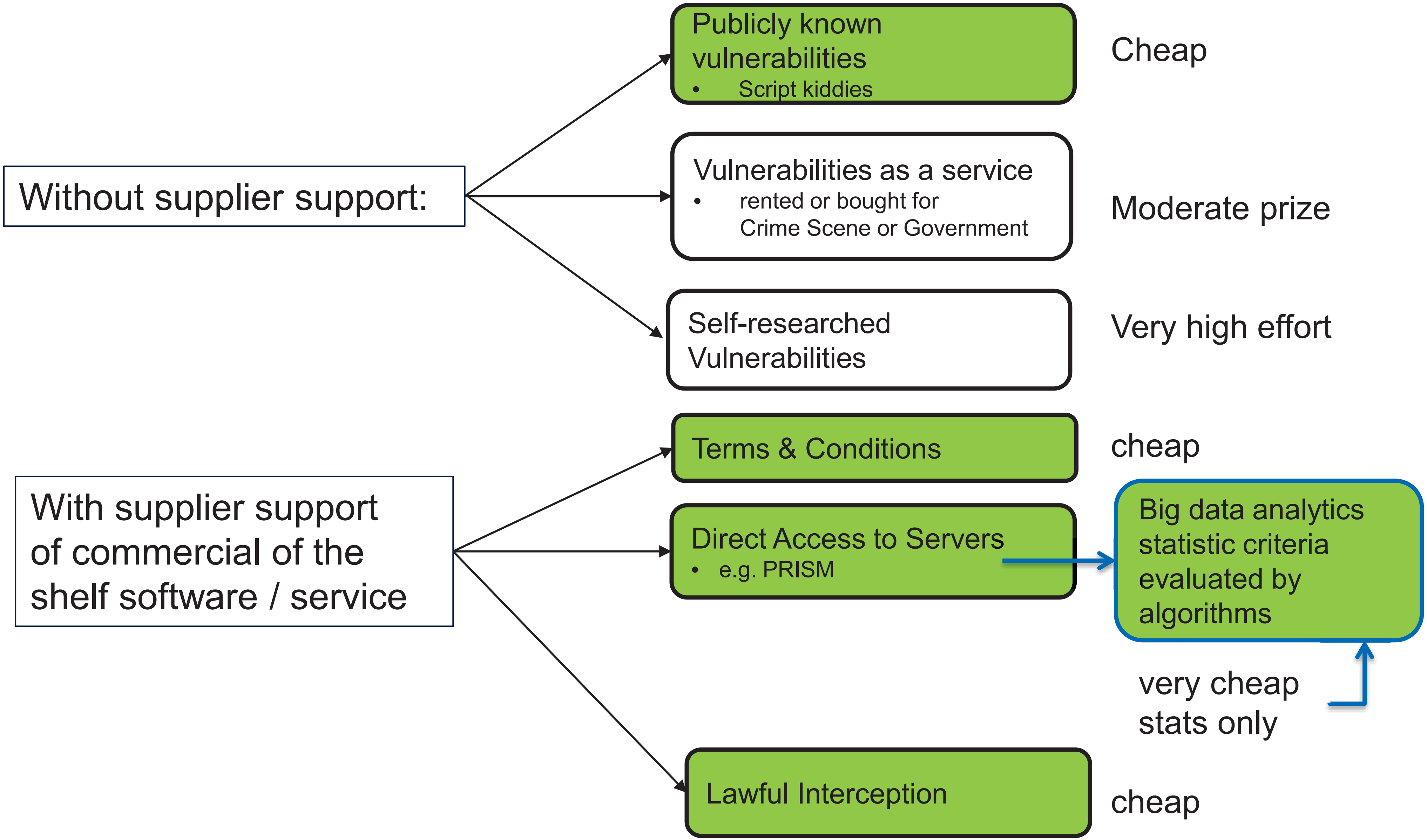
Lawful Interception

cheap

Mitigation III

- Mitigation II + :
- Use strong encryption only and
  avoid proprietary encryption solutions, e.g. BitLocker.
  (B. Schneier 2013)
- Note: Any plain information sent through the internet will most likely be collected and analyzed: **Be aware!**

Technical options for attacks



Without supplier support:

Publicly known vulnerabilities
- Script kiddies

Cheap

Vulnerabilities as a service
- rented or bought for Crime Scene or Government

Moderate prize

Self-researched Vulnerabilities

Very high effort

With supplier support of commercial of the shelf software / service

Terms & Conditions

cheap

Direct Access to Servers
- e.g. PRISM

Big data analytics statistic criteria evaluated by algorithms

very cheap stats only

Lawful Interception

cheap

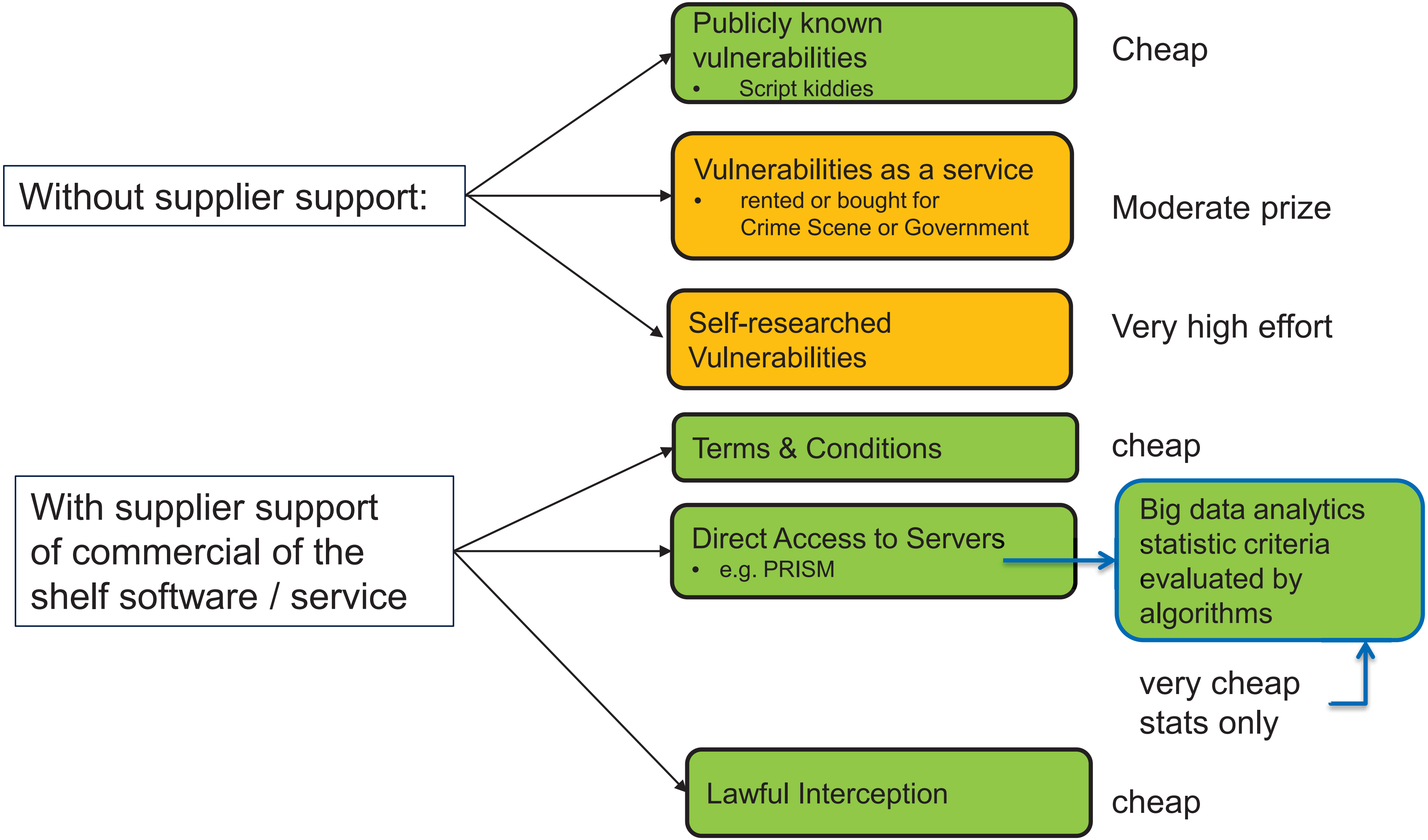
Mitigation IV

- Mitigation III + :
- Use trusted sophisticated professional security services,
  including monitoring, intrusion detection / prevention, statistical analysis,
  zero day exploit disclosure, sandboxing (for malware code detection)
  for the entire network.

Mitigation V: Data in transition

- Mitigation IV + :
- Use strong encryption for communication (VPN, HTTPS, etc.)
  ➔ protects against content monitoring
- + Use proxy chains with TOR or equivalent services
- ➔ traceability of the endpoints is made costly
  ➔ big data analytics on connection data is made costly

Technical options for attacks
Blue Eye Version:
What we want to see



Without supplier support:

Publicly known vulnerabilities
- Script kiddies

Cheap

Vulnerabilities as a service
- rented or bought for Crime Scene or Government

Moderate prize

Self-researched Vulnerabilities

Very high effort

With supplier support of commercial of the shelf software / service

Terms & Conditions

cheap

Direct Access to Servers
- e.g. PRISM

Big data analytics statistic criteria evaluated by algorithms

very cheap
stats only

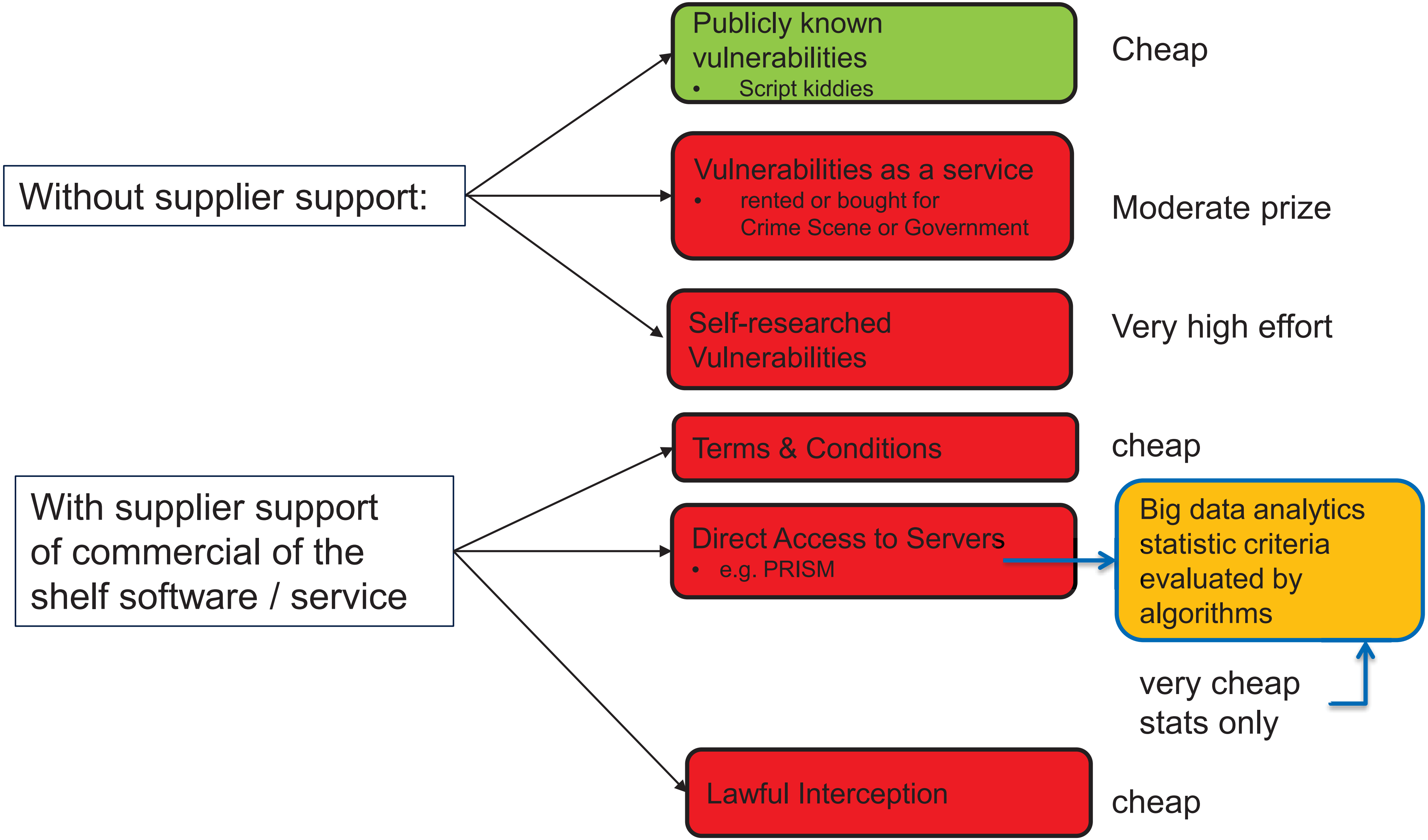
Lawful Interception

cheap

Other Assumptions

- All governments do their job i.e.
  there is **no trusted supplier**
- In spite of all security expertise and prevention there is **no relevant successful protection against zero day exploits** and **full professional target software attacks: Advanced Persistent Threats (APT)**.
- Big data analytics can be avoided by strong encryption on both: data at rest and data in transition.
  However, most common applications do not support encryption, like social media, web, etc.
  i.e. the wish for visibility supports big data analytics
  Is Facebook or the Facebook user the product?

Technical options for attacks
Realistic Version today:
What we hate to see



Without supplier support:

Publicly known vulnerabilities
- Script kiddies

Cheap

Vulnerabilities as a service
- rented or bought for Crime Scene or Government

Moderate prize

Self-researched Vulnerabilities

Very high effort

With supplier support of commercial of the shelf software / service

Terms & Conditions

cheap

Direct Access to Servers
- e.g. PRISM

Big data analytics statistic criteria evaluated by algorithms

very cheap stats only

Lawful Interception

cheap

Part III
Information Superiority and "Qui bono"

Qui bono

- Economical interest for hackers (& states)
- Hacktivist are politically driven … difficult to estimate
- Information superiority
  - Richard Clarke on Trust
  - Chinese “We do everything to …

Chinas Absichten: Wir werden die Dominanz einer Nation im Cyber Space nicht zulassen

US-Cyber-Guru: «Eure Daten sind nirgends sicher»

Wer meint, seine Daten seien in einer Schweizer Cloud sicher, ist naiv. Dies meint zumindest Richard Clarke, der langjährige IT-Security-Berater und Anti-Terrorismus-Expert für das Weisse Haus.

Wird IT nationalisiert?

oder

Können wir weiterhin von der weltweiten internationale

Bei der Speicherung von Daten in lokalen Clouds, wie etwa in der Schweiz, gehe es nur ums Geschäft, nicht um den Schutz der Informationen, ist Richard Clarke, langjähriger Berater des Weissen Hauses, überzeugt.

Quelle: Computerworld, Von Jens Stark , 25.02.2014 11:00.

Final Thoughts I

- If a nation-state wants to hack you, they will succeed to do so.
  (B. Schneier 2013)
- **Internet is and always will be public space!**
  - Do not let it stop you, but be aware of the problem
  - Don’t think, because you know, you should completely change your behavior.
  - Use it for public and publicity purposes!

Final Thoughts II

Richard Clarke: Drei Gesetze zur Cyber-Sicherheit:

1. Kaufe keinen Computer! Aber wenn Du wirklich eine kaufen musst …
2. Schalte den Computer nicht ein! Aber wenn Du ihn wirklich einschalten musst …
3. Schliesse den Computer nicht ans Netz an!

Und wie sollen wir uns verhalten?

1. Die Tatsache, dass man die Sache besser versteht, ändert nichts am täglichen Leben.
2. Für viele Bereiche ist es irrelevant, ob jemand mithört.
3. Auswertungen sind kostspielig und werden meistens begründet gemacht!
4. Grosse Sorge: Unser Daten bleiben lebenslange zugreifbar …
   (jederzeit kann nachuntersucht werden) ➔ **Seien Sie datensparsam!!!**
5. Für wirklich Vertrauliches: Wenden Sie die drei Gesetze an!

Nächste Präsentationen

- **Prof. Dr. Jürg Gutknecht (ETHZ und designierter Präsident SI)** macht seine Ausführungen zum Thema «Was kann im Betriebssystem und in der Hardware versteckt werden?».
- **Andreas Wuchner (CTO Strategy Group, HP Enterprise Security Services)** zeigt auf, wie hochsichere System funktionieren, unter anderem am Beispiel einer sicheren Videokonferenz.
- **Prof. Dr. Donald Kossmann (Institut für Informationssysteme, ETHZ)** führt u.a. aus, wie mit Hardware Sicherheit erzeugt werden kann.
- **Dr. Jan Camenisch (IBM Research Lab Zürich)** befasst sich mit Privatsphäre und Überwachung sowie den dazugehörigen technologischen Schutzmöglichkeiten.

Appendix

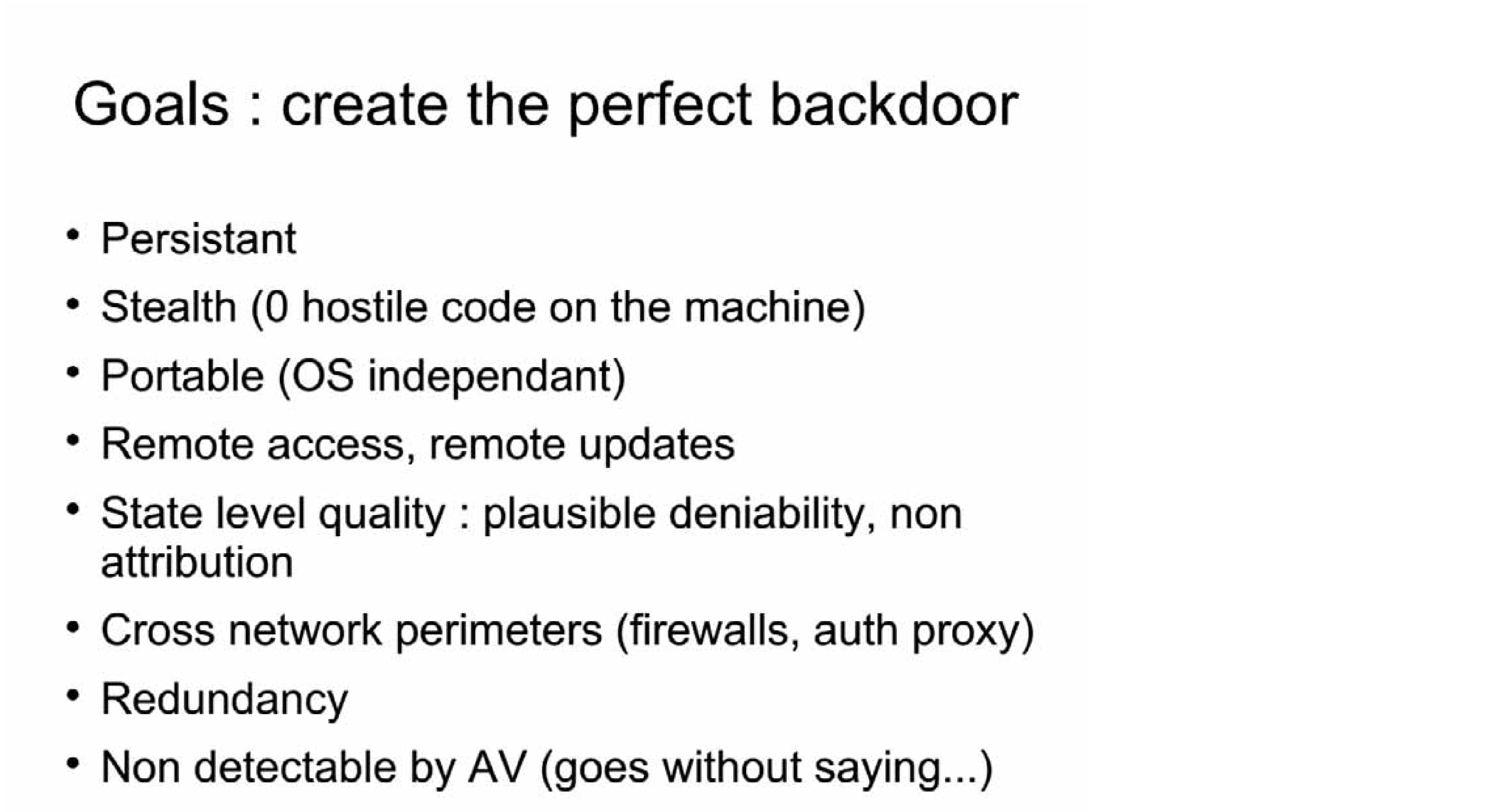
Additional Readings

- Companies were aware of that NSA was collection information from them
  - http://www.theguardian.com/world/2014/mar/19/us-tech-giants-knew-nsa-data-collection-rajesh-de
- Schneier on NSA spying
  - http://bigdata.csail.mit.edu/node/154
- Mandiant attack cycle
  - http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf
- When companies became a part of PRISM
  - http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/

Video References

- Commercialized surveillance software for governments: http://www.hackingteam.it/index.php/remote-control-system

A1: Hidden Collection Infrastructure:
https://citizenlab.org/2014/02/mapping-hacking-teams-untraceable-spyware/



Goals : create the perfect backdoor

- Persistant
- Stealth (0 hostile code on the machine)
- Portable (OS independant)
- Remote access, remote updates
- State level quality : plausible deniability, non attribution
- Cross network perimeters (firewalls, auth proxy)
- Redundancy
- Non detectable by AV (goes without saying...)

Any information you send can be collected

- Anything in plaintext that passes through central points of a network (e.g. telephone or Internet) can be collected and stored for a very long time.
  - Location information
  - Messages containing sensitive information
  - Web-camera images
    - *"[..] the program saved one image every five minutes from the users' feeds, partly to comply with human rights legislation, and also to avoid overloading GCHQ's servers."*
    - Captures also sexually explicit images

  (http://www.theguardian.com/world/2014/feb/27/gchq-nsa-webcam-images-internet-yahoo)

- Encryption can protect the confidentiality
  - Some data can still be read
    - Who are talking to whom (Connection data)
    - Encrypted data can be deciphered if it has been used weak- or intentionally flawed encryption algorithms.
    - In most cases it can not be deciphered, but can be stored if it is of high importance.

  - In order to circumvent encryption can the government instead compromise the endpoint (e.g. computer, or mobile device).
    - *Video: http://www.hackingteam.it/index.php/remote-control-system*