AUSTRIAN INSTITUTE OF TECHNOLOGY

Die Waffen der NSA

Unsere IT wird abgehört - wie funktioniert das eigentlich?

Thomas Bleier

Dipl.-Ing. MSc zPM CISSP CEH CISM
Thematic Coordinator ICT Security
Safety & Security Department
AIT Austrian Institute of Technology GmbH

Warnhinweis

- Die Inhalte basieren auf Open-Source Quellen und Berichten in öffentlichen Medien
- Der Fokus liegt auf der Erklärung der technischen Hintergründe, nicht auf politischen oder gesellschaftlichen Aspekten
- Empfehlungen basieren tlw. auf spekulativen Annahmen - für die Richtigkeit der Angaben wird keine Haftung übernommen - insbesondere nicht für den garantierten Schutz für Angriffen :-)
- Das Nachdenken über die in diesem Vortrag präsentierten Techniken und Technologien kann zu übertriebener Paranoia führen
- Zu Risiken und Nebenwirkungen fragen Sie ihren IT-Sicherheitsbeauftragten oder den lokalen Nachrichtendienst

Abhören, Spionage - Warum?

NSA spied on foreign leaders at the G20 summit in Canada.
CBC, November 27, 2013

NSA spied on OPEC.
Der Spiegel, November 11, 2013

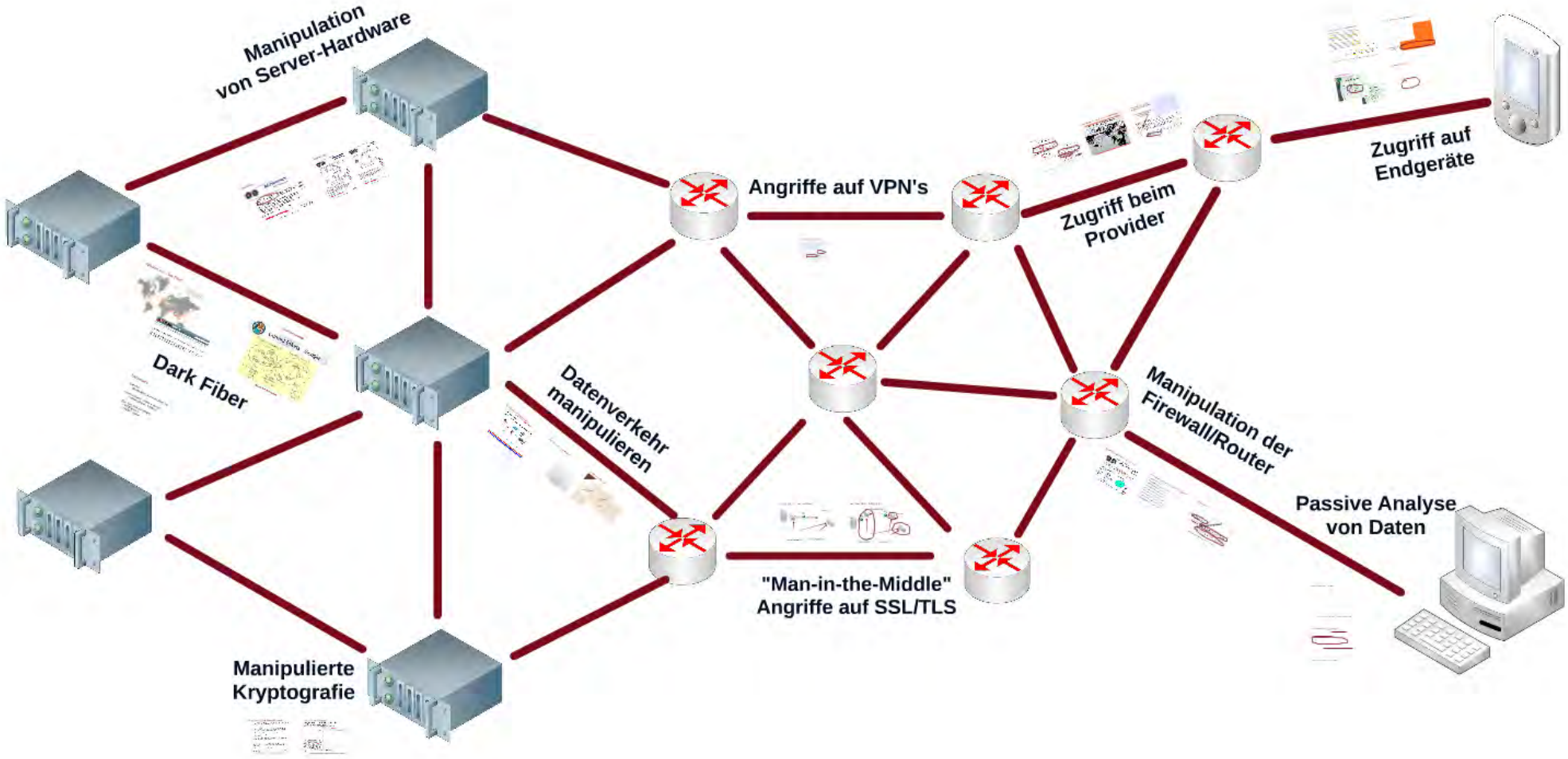
Französische Internet-Überwachung - Das "böse Reich" der Wirtschaftsspionage
Süddeutsche Zeitung, October 30, 2013

"PRISM auf Steroiden": Totalüberwachung der Olympischen Spiele in Sotschi geplant
heise online, October 6, 2013

NSA targeted Tor network, relied upon by dissidents and activists for anonymous communication.
The Guardian, October 4, 2013

Verfassungsschutz besorgt über Cyberspionage aus China
heise online, October 4, 2013

Trojaner aus China bedrohen deutsche Stromnetze
Die Welt, July 21, 2009



Content-/Dienste-Anbieter

(Google, Microsoft, Yahoo, etc)

"Das Netzwerk"

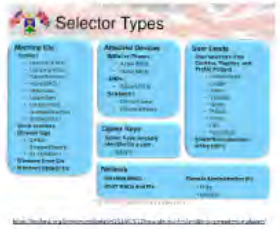
(Backbone Provider, Access Provider)

Endgerät

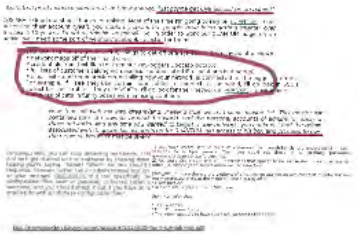
(User)

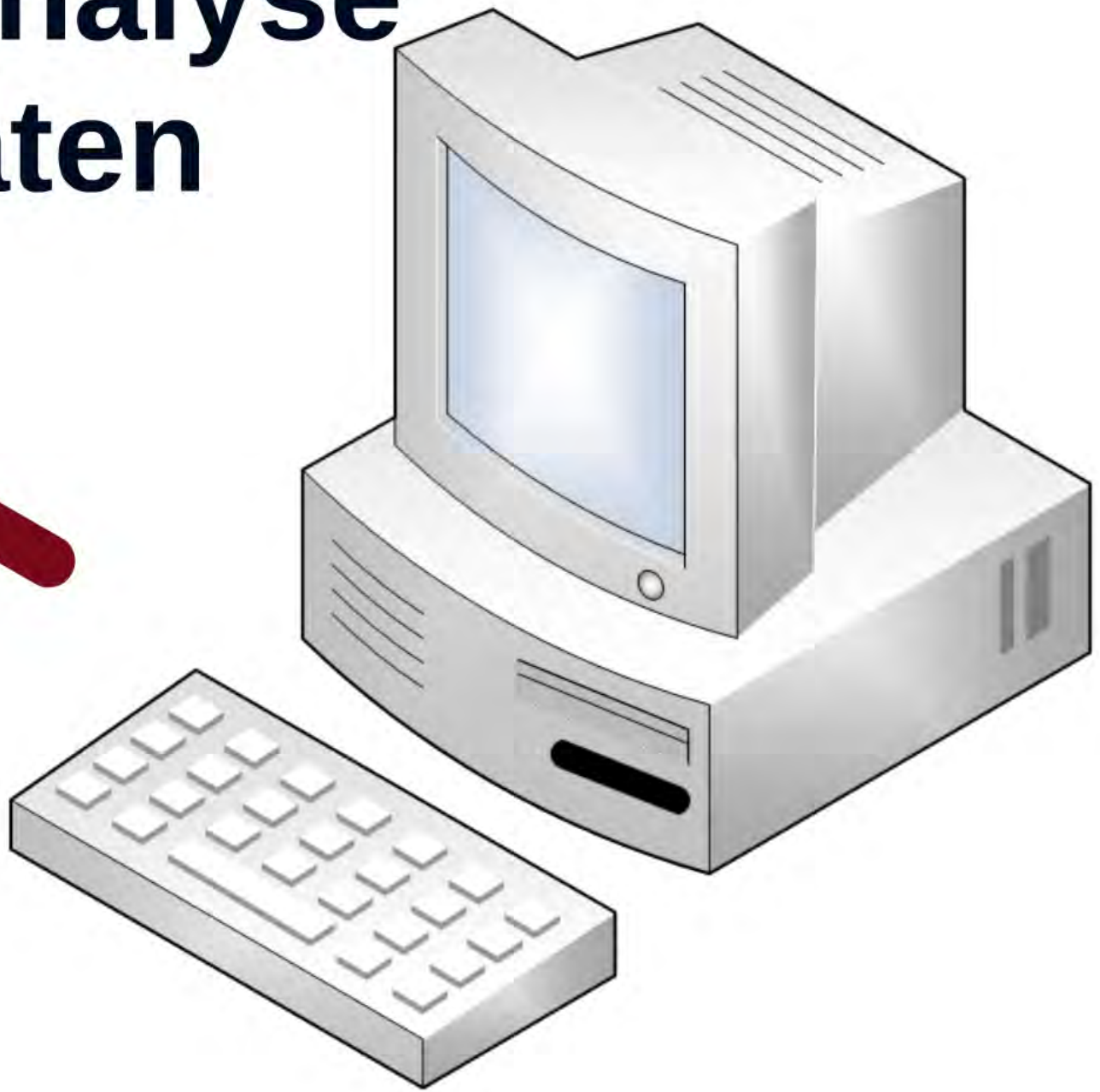
Passive Analyse von Daten

Identifizierung von "Targets"

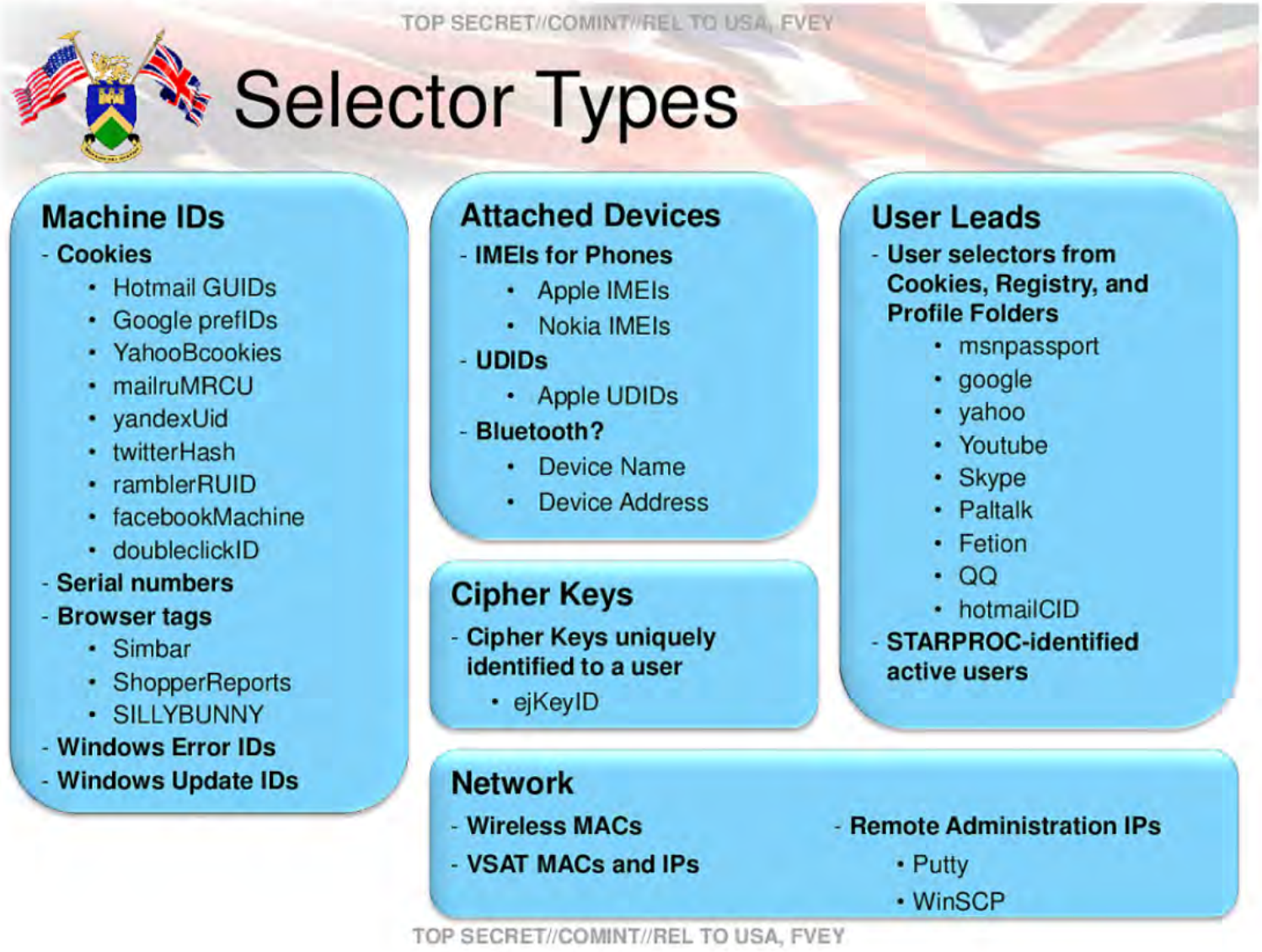


Identifizierung von "SysAdmins"





Identifizierung von "Targets"



https://firstlook.org/theintercept/article/2014/03/12/nsa-plans-infect-millions-computers-malware/

Identifizierung von "SysAdmins"

"*Yeah, that pretty much makes sense, but how are you 'just gonna get CNE access' on an admin?*"

(S/SI//REL) Good question, thanks for asking. Most of the time I'm going to rely on QUANTUM to get access to their account *(yeah, you could try spam, but people have been getting smarter over the last 5-10 years...it's not as reliable anymore)*. So, in order to work our QUANTUM-magic on an admin, we'll need some sort of webmail/facebook selector for them.

(S/SI//REL) Other fun (read:useful) things to get off of a sys admin (from my point of view):
* network maps off of their hard drive
* credentials from text files (or from our key-loggers...potato potato)
* full lists of customers (along with associated dedicated IP allocations is a bonus)
* e-mail with upstream providers detailing how your network is connected to the bigger internetz. For example, if I see they use certain fiber cables to connect to the world, I'll go look in SSO's collect for their traffic. If they use VSAT's, I'll go look for their network in FORNSAT's environment.
* pictures of cats in funny poses with amusing captions

Now, fade off with me into dream-land. Pretend that we had some master list. This master list contained tons of networks around the world, and the personal accounts of admins for each of those networks. And any time you wanted to target a new network, you could just find the admin associated with it, queue his accounts up for QUANTUM, get access to his box and proceed to pwn the network. Wouldn't that be swell?

(S/SI//REL) Well, you can stop dreaming my friends, I thi
And we'll get started on this endeavor by chasing down
hoping you're saying, "Telnet? Telnet?! No one should s
response, however, telnet (as an administrative tool on
so alive and well, DISCOROUTE is a tool specifically de
configuration files seen in passively collected telnet s
awesome, and you should check it out if you have at le
shall we do with all of these configuration files?

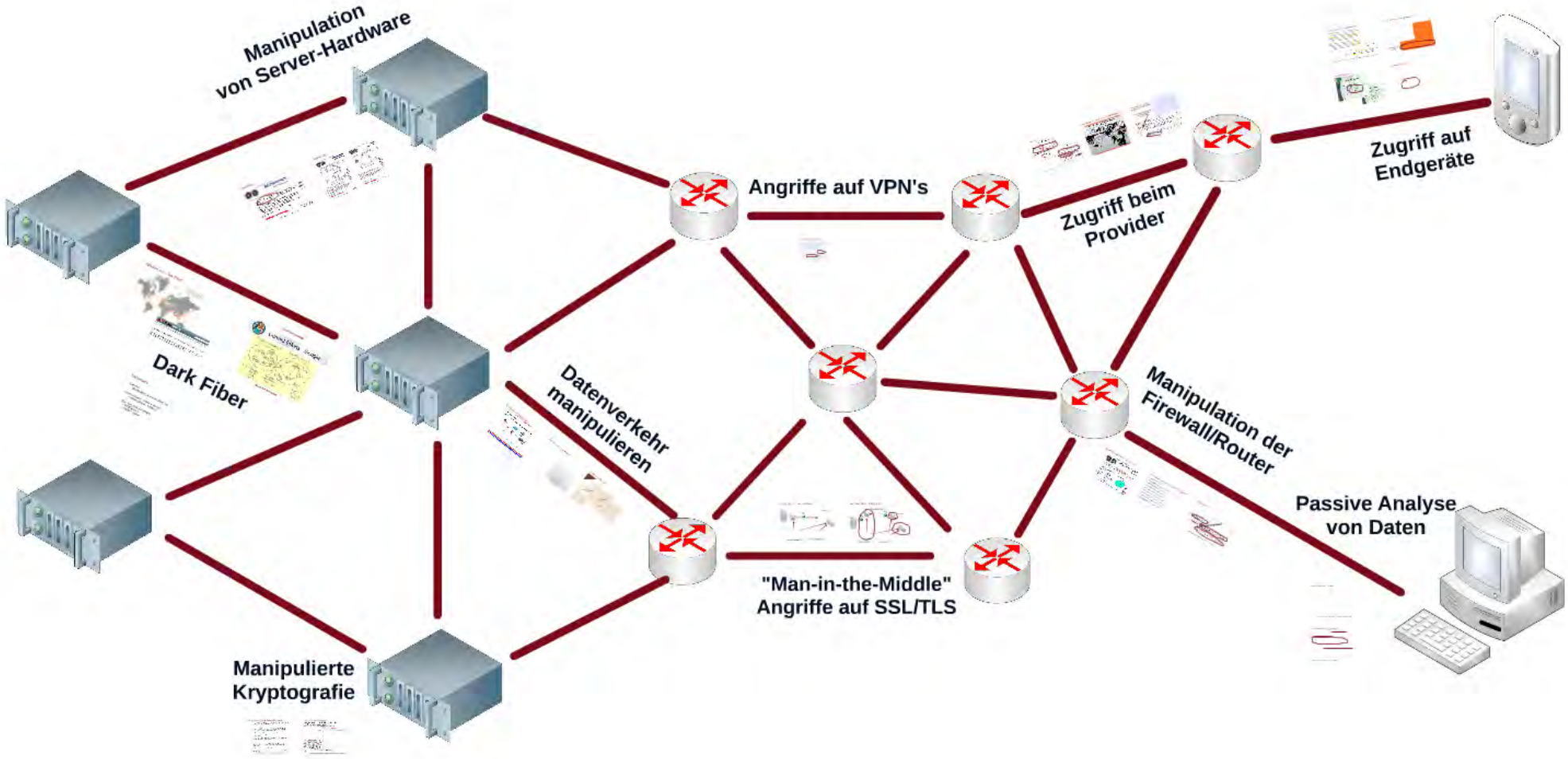
1) You could create lists of client IP addresses that **consistently** are unsuccessful in SSH sessions to multiple servers. Then you could put these in a, "probably password guessers/probably brute forcers" list.
2) You could also create lists of IP addresses that appear to be successful in having access to other IPs. *(ahhhh yeah, here's where we can have fun)*

(S//SI//REL) I'm sure there are a plethora of other things you can do with that sort of data, but I'm really interested in #2 at the moment. Based purely off of:
* FROM port 22
* session size is greater than 1500 bytes

then I can infer that:

* To IP = admin
* From IP = server/router
* The admin appears to have successful access to the server

http://freesnowden.is/wp-content/uploads/2014/03/i-hunt-sys-admins.pdf



Content-/Dienste-Anbieter

(Google, Microsoft, Yahoo, etc)

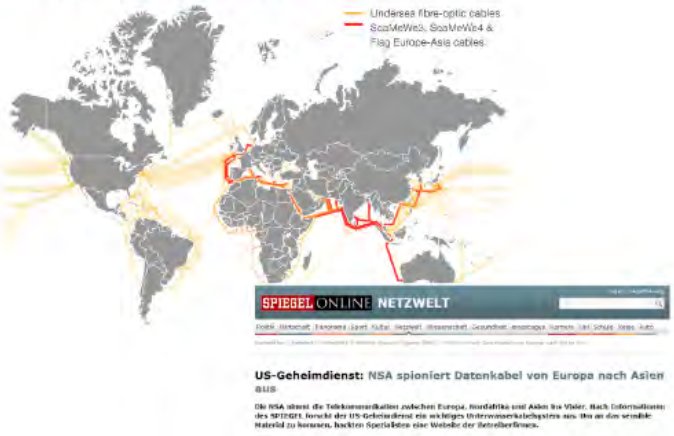
"Das Netzwerk"

(Backbone Provider, Access Provider)

Endgerät

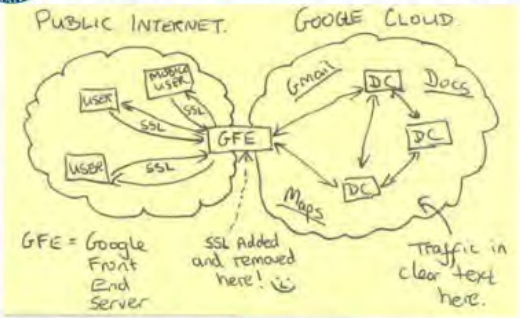
(User)

Abhören von "Dark Fiber"



TOP SECRET//SI//NOFORN

Current Efforts - Google



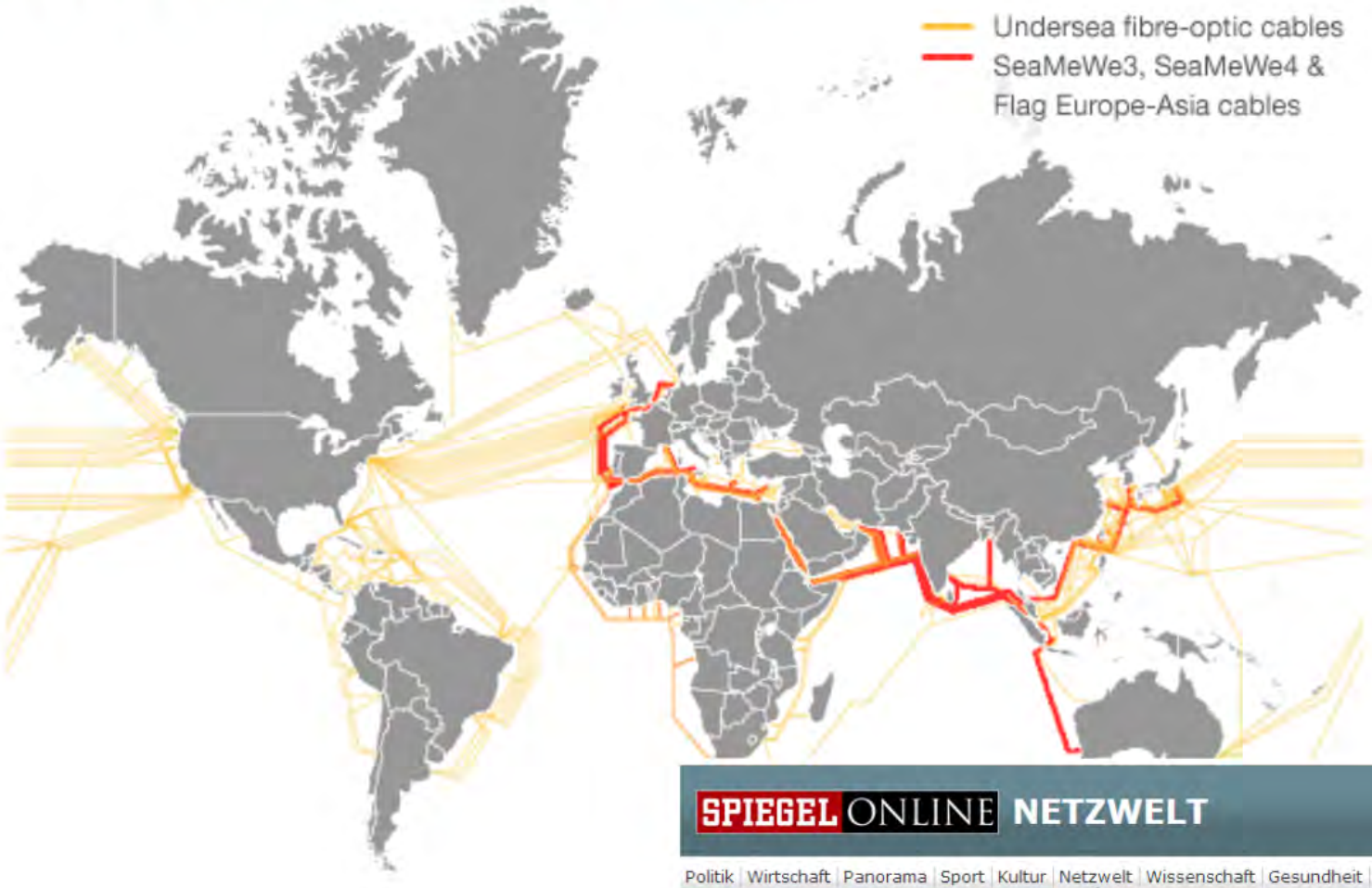
TOP SECRET//SI//NOFORN

Dark Fiber

Takeaway's

- Identifier
  - WLAN MAC, Bluetooth MAC, etc.
- Verschlüsseln - immer & überall
  - Volltextsuche vs. Aufwand
- Was geht über die Leitung?
  - VM Migration
  - DRBD / Cluster

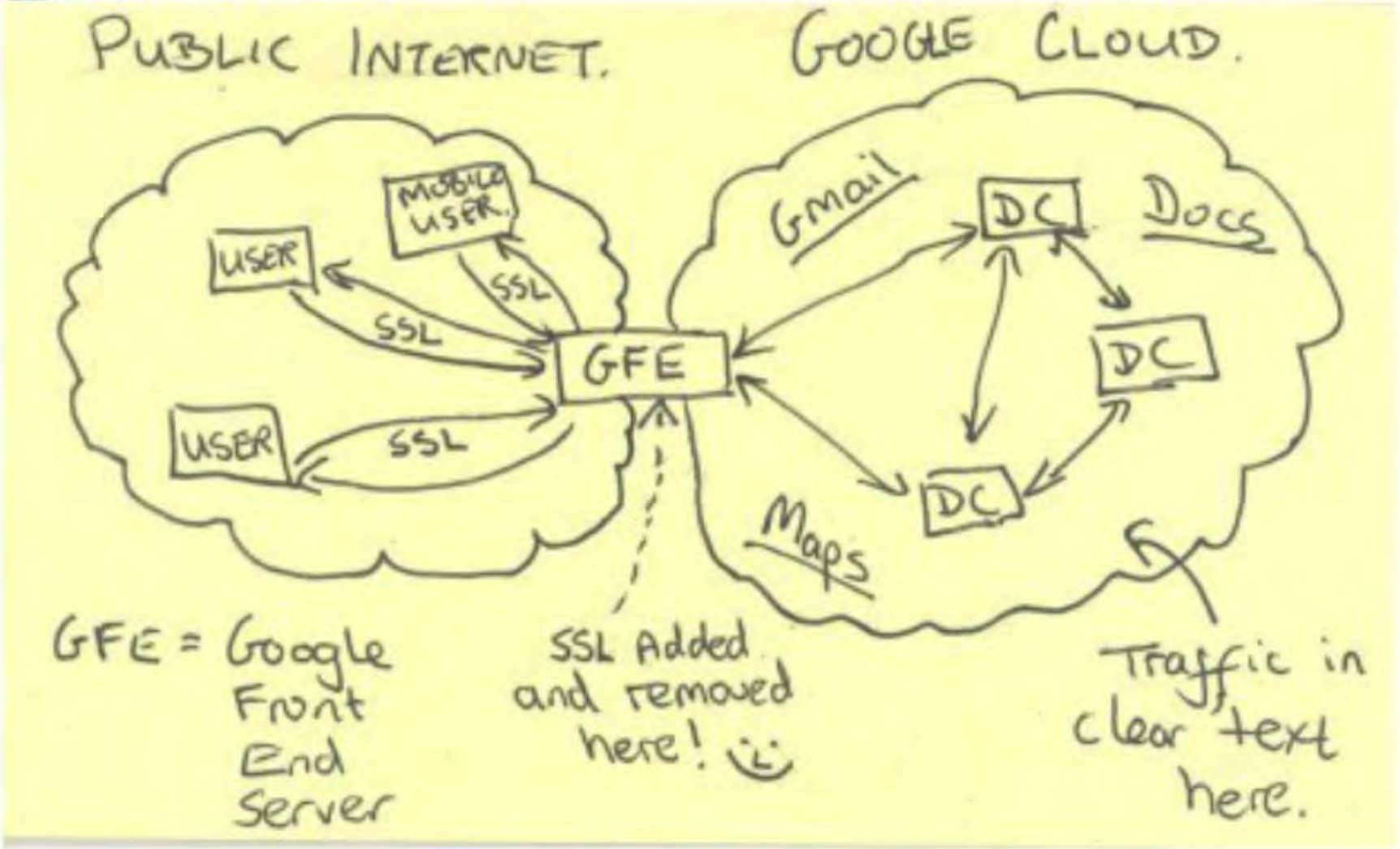
Abhören von "Dark Fiber"



US-Geheimdienst: NSA spioniert Datenkabel von Europa nach Asien aus

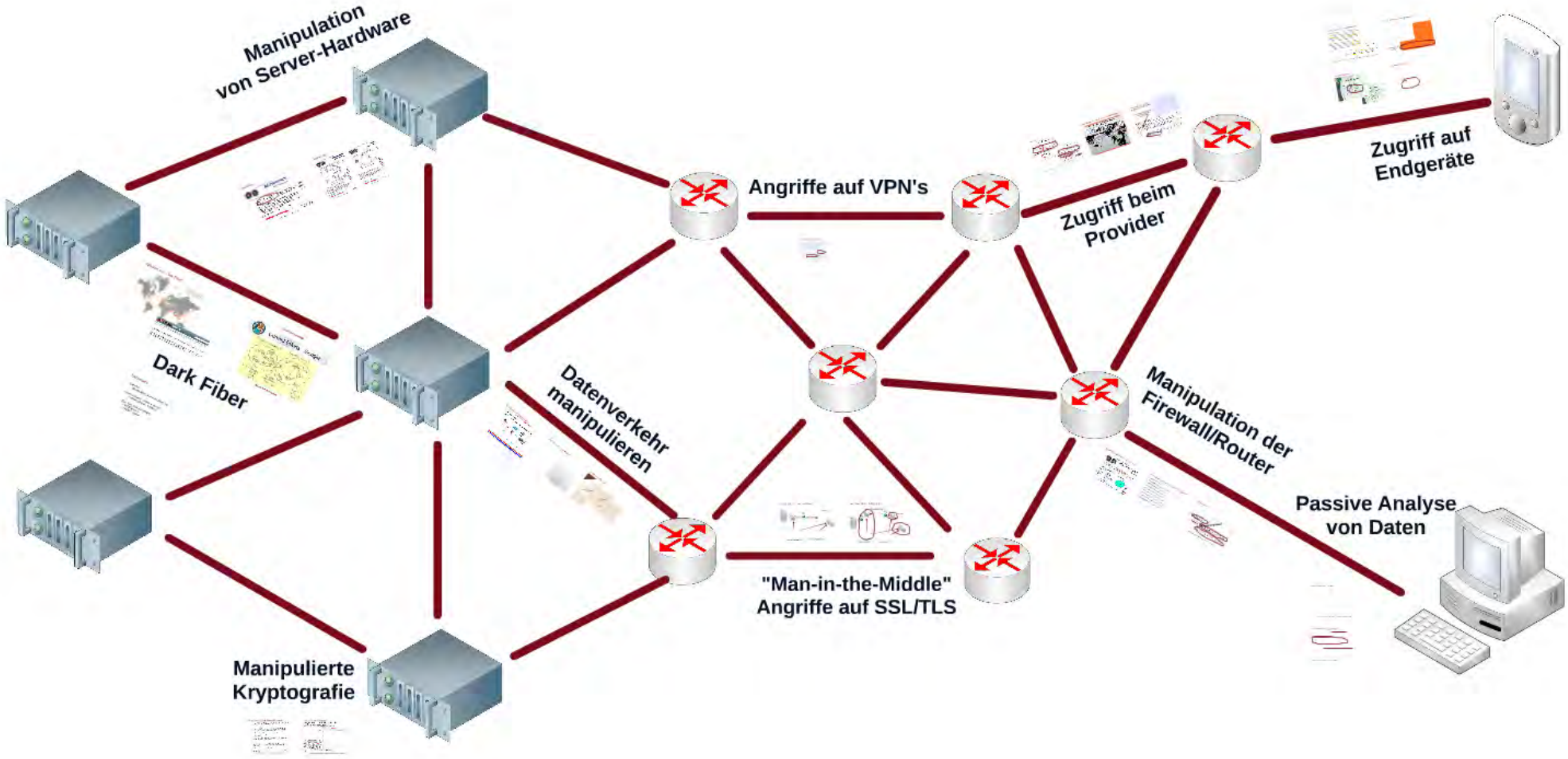
Die NSA nimmt die Telekommunikation zwischen Europa, Nordafrika und Asien ins Visier. Nach Informationen des SPIEGEL forscht der US-Geheimdienst ein wichtiges Unterwasserkabelsystem aus. Um an das sensible Material zu kommen, hackten Spezialisten eine Website der Betreiberfirmen.

Current Efforts - Google



Takeaway's

- Identifier
  - WLAN MAC, Bluetooth MAC, etc.
- Verschlüsseln - immer & überall
  - Volltextsuche vs. Aufwand
- Was geht über die Leitung?
  - VM Migration
  - DRBD / Cluster



Content-/Dienste-Anbieter

(Google, Microsoft, Yahoo, etc)

"Das Netzwerk"

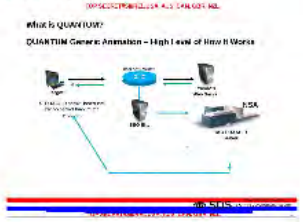
(Backbone Provider, Access Provider)

Endgerät

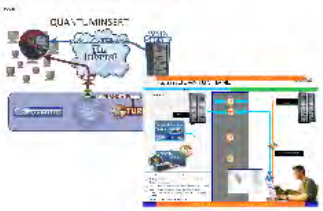
(User)

Datenverkehr manipulieren

"Man on the side" Attacke im WAN



Manipulation des Netzwerktraffics

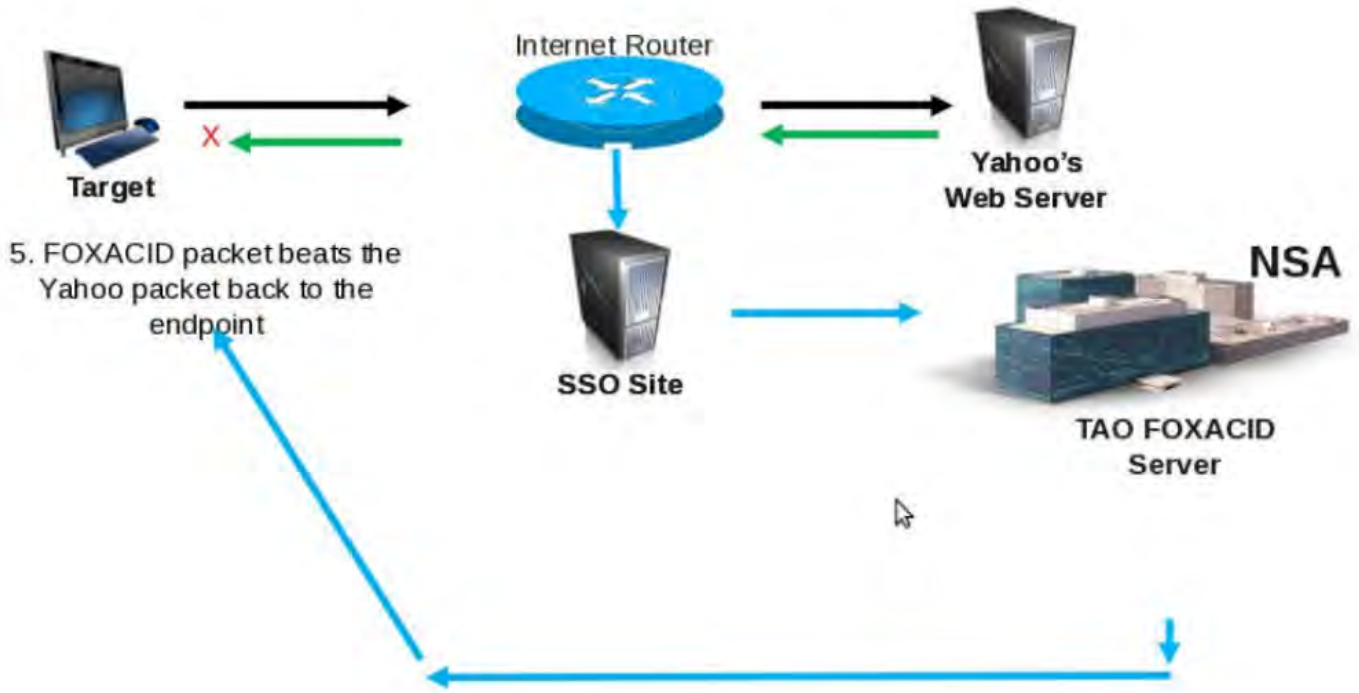


Verfügbare Technologien

"Man on the side" Attacke im WAN

What is QUANTUM?

QUANTUM Generic Animation – High Level of How It Works



Manipulation des Netzwerktraffics

TS//REL

Verfügbare Technologien

TOP SECRET//COMINT//REL TO USA, FVEY//20320108

(C) Legacy QUANTUMTHEORY techniques

- (TS//SI//REL) QUANTUMINSERT
  - HTML Redirection
- (TS//SI//REL) QUANTUMSKY
  - HTML/TCP resets
- (TS//SI//REL) QUANTUMBOT
  - IRC botnet hijacking

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

TOP SECRET//COMINT//REL TO USA, FVEY//20320108

(U) New Hotness

- (TS//SI//REL) QUANTUMBISCUIT
  - Redirection based on keywork
  - Mostly HTML Cookie Values
- (TS//SI//REL) QUANTUMDNS
  - DNS Hijacking
  - Caching Nameservers
- (TS//SI//REL) QUANTUMBOT2
  - Combination of Q-BOT/Q-BISCUIT f
    Command and controlled botnets

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

TOP SECRET//COMINT//REL TO USA, FVEY//20320108

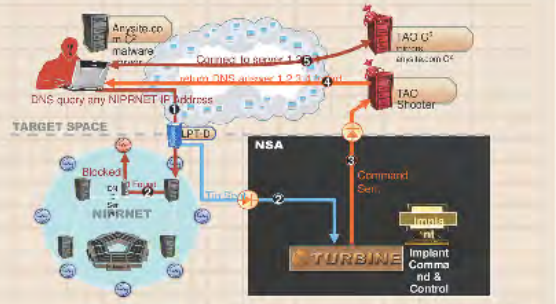
(U) Experimental

- (TS//SI//REL) QUANTUMCOPPER
  - File download disruption
- (TS//SI//REL) QUANTUMMMUSH
  - Virtual HUFFMUSH / Targeted Spam Exploitation
- (TS//SI//REL) QUANTUMSPIM
  - Instant Messaging (MSN chat, XMPP)
- (TS//SI//REL) QUANTUMSQUEEL
  - Injection into MySQL persistent database connections
- (TS//SI//REL) QUANTUMSQUIRREL
  - Truly covert infrastructure, be any IP in the world

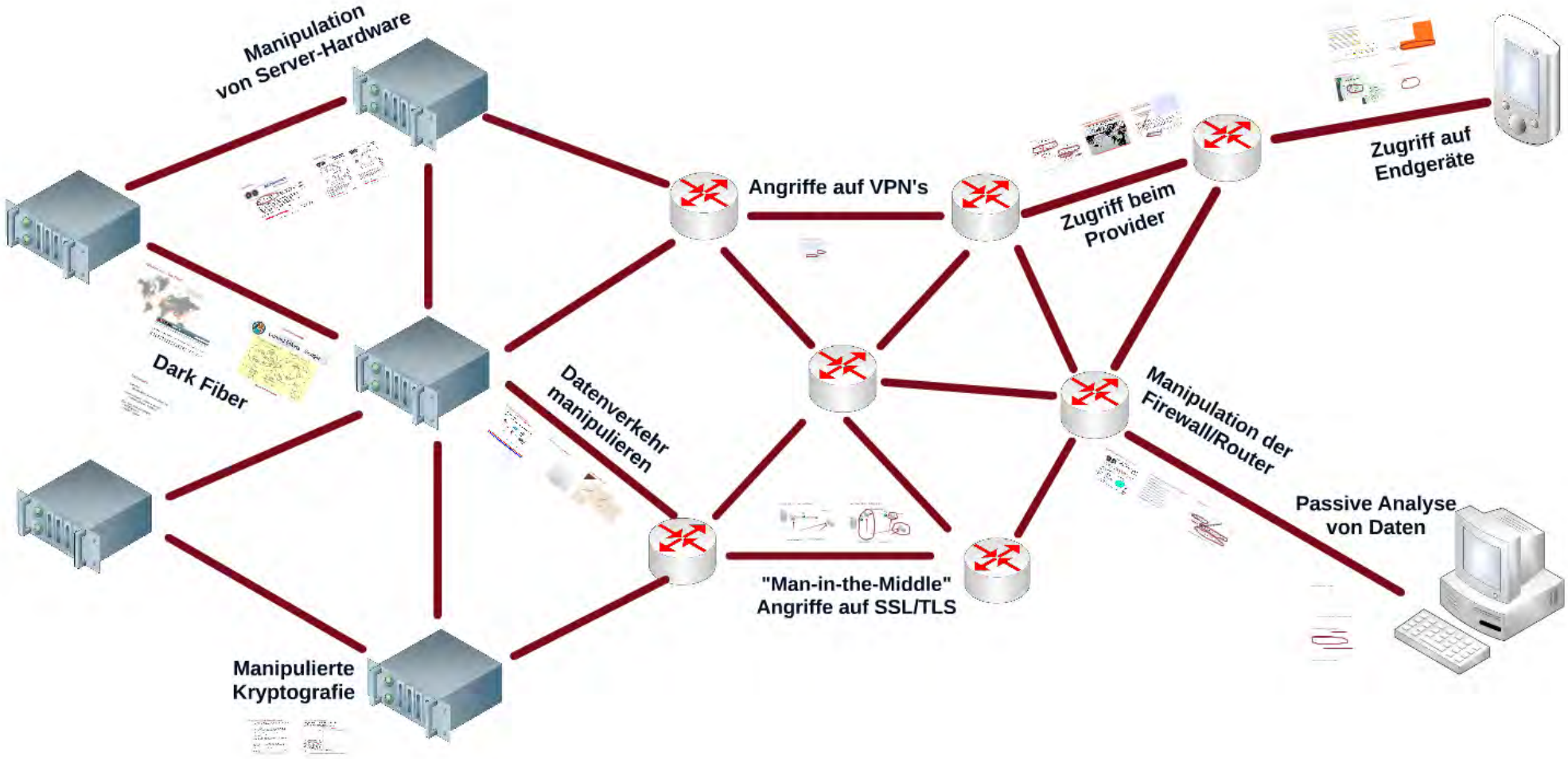
TOP SECRET//COMINT//REL TO USA, FVEY//20320108

TOP SECRET//COMINT//REL TO USA, FVEY//20320108

(U//FOUO) QUANTUMDEFENSE



TOP SECRET//COMINT//REL TO USA, FVEY//20320108



Content-/Dienste-Anbieter

(Google, Microsoft, Yahoo, etc)

"Das Netzwerk"

(Backbone Provider, Access Provider)

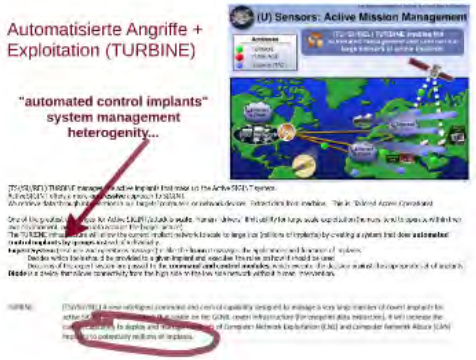
Endgerät

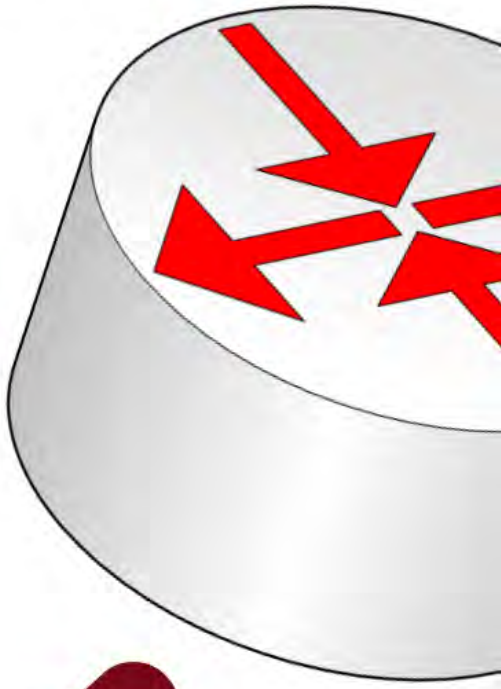
(User)

Belgacom

Systematische Infiltration von Providern/Netzwerken

Automatisierte Angriffe + Exploitation (TURBINE)





Zugriff beim Provider

Belgacom

TOP SECRET STRAP 2

One Month Later – OP SOCIALIST

- Scoping session conducted – main focus to be on enabling CNE access to **BELGACOM GRX Operator**
- **Ultimate Goal – enable CNE access to BELGACOM Core GRX Routers from which we can undertake MiTM operations against targets roaming using Smart Phones.**
- Secondary focus – breadth of knowledge on GRX Operators
- Operations Manager assigned, team assembles

bics
a belgacom company

NAC NETWORK ANALYSIS CENTRE

TOP SECRET STRAP 2

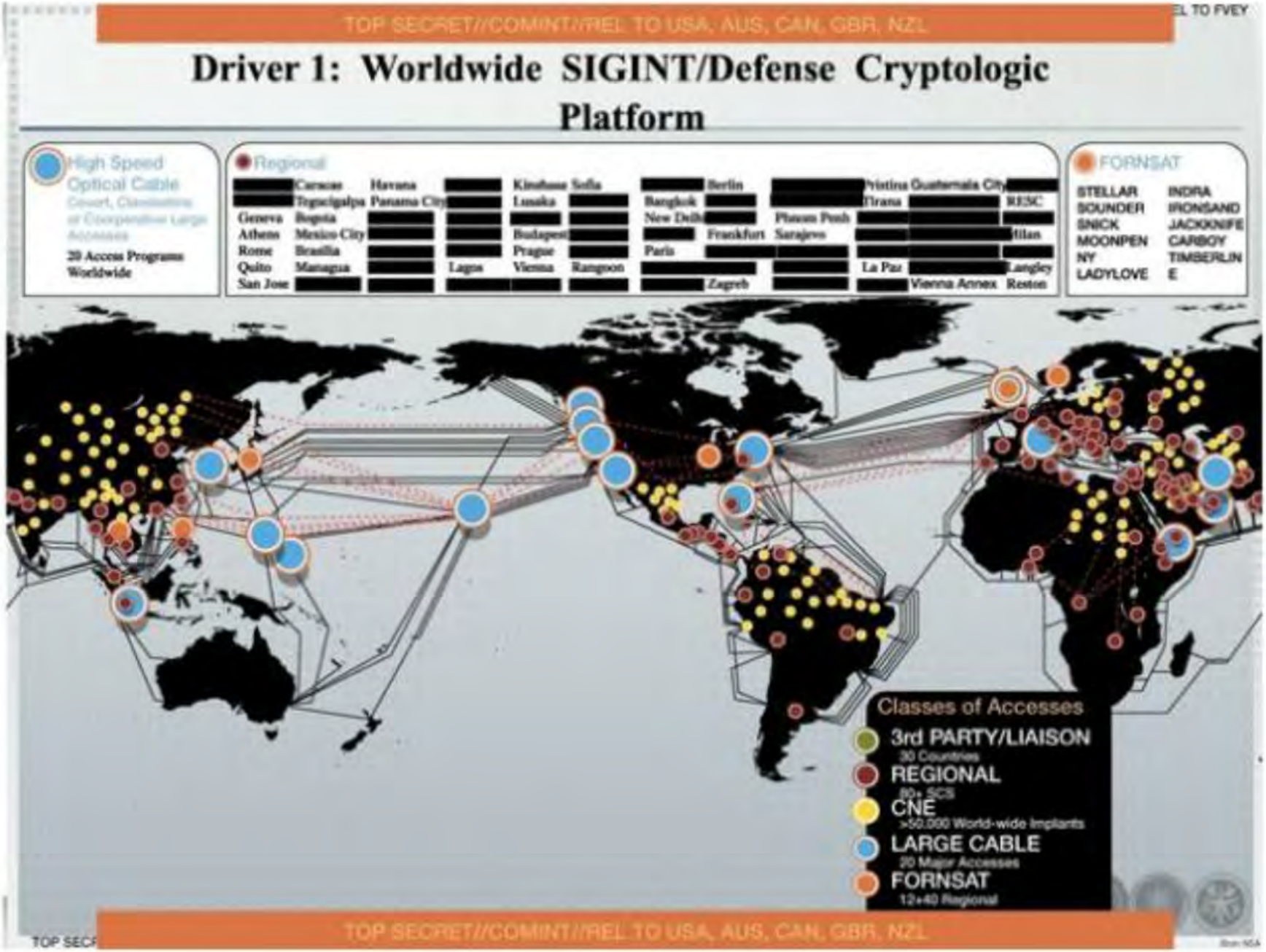
OP SOCIALIST Outcome

- In MyNOC:
  - CNE Access to BELGACOM – MERION ZETA – 6 endpoints into Engineer/ support staff IP range
  - 2 endpoints into BELGACOM DMZ (from prep VA work)
  - Optimal Bearers identified providing good access to BELGACOM proxy
- Post MyNOC:
  - Optimal Bearers continue to allow CI against BELGACOM engineers/proxy
  - Internal CNE access continues to expand – getting close to access core GRX Routers – currently on hosts with access
  - NAC continue to support with Network Analysis of internal networks, network understanding research on credentials and identification of engineers/system administrators and their specific roles.

NAC NETWORK ANALYSIS CENTRE

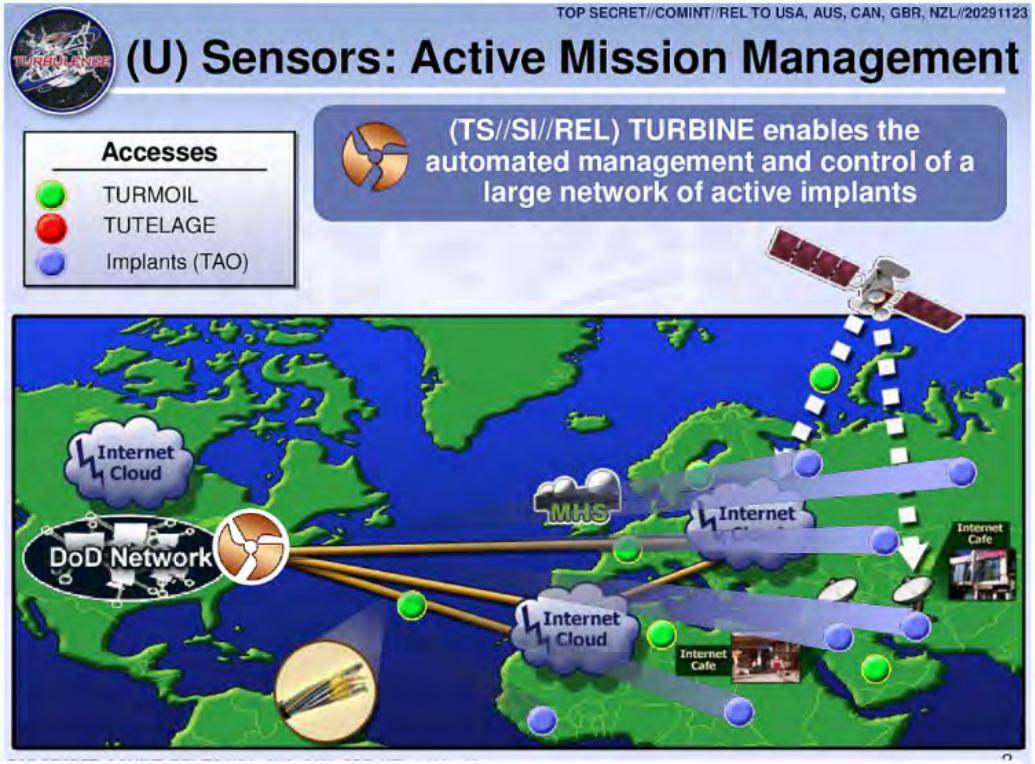
http://www.spiegel.de/netzwelt/web/belgacom-geheimdienst-gchq-hackte-belgische-telefongesellschaft-a-923224.html

Systematische Infiltration von Providern/Netzwerken



Automatisierte Angriffe + Exploitation (TURBINE)

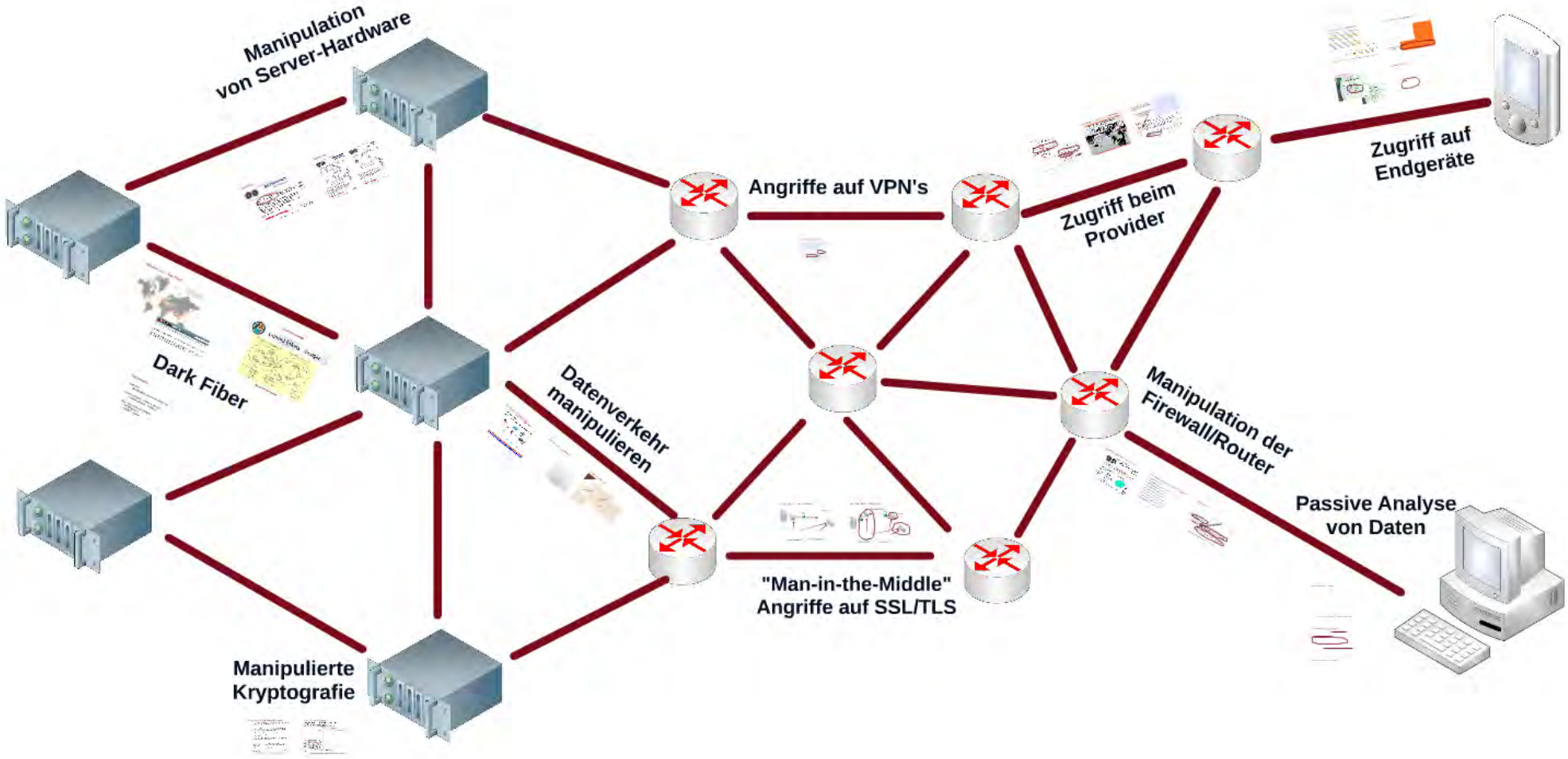
"automated control implants" system management heterogenity...



(TS//SI//REL) TURBINE manages the active implants that make up the Active SIGINT system.
Active SIGINT offers a more **aggressive** approach to SIGINT.
We retrieve data through intervention in our targets' computers or network devices. Extract data from machine. This is: Tailored Access Operations!

One of the greatest challenges for Active SIGINT/attack is **scale**. Human "drivers" limit ability for large-scale exploitation (humans tend to operate within their own environment, not taking into account the bigger picture)
The TURBINE infrastructure will allow the current implant network to scale to large size (millions of implants) by creating a system that does **automated control implants by groups** instead of individually.
Expert System (resource and operations manager) is like the **brain** it manages the applications and functions of implants.
Decides which tools should be provided to a given implant and executes the rules on how it should be used
Decisions of the expert system are passed to the **command and control modules**, which execute the decision against the appropriate set of implants.
Diode is a device that allows connectivity from the high side to the low side network without human intervention.

TURBINE	(TS//SI//REL) A new intelligent command and control capability designed to manage a very large number of covert implants for active SIGINT and active Attack that reside on the GENIE covert infrastructure (for endpoint data extraction). It will increase the current capability to deploy and manage hundreds of Computer Network Exploitation (CNE) and Computer Network Attack (CAN) implants to potentially millions of implants.



Content-/Dienste-Anbieter

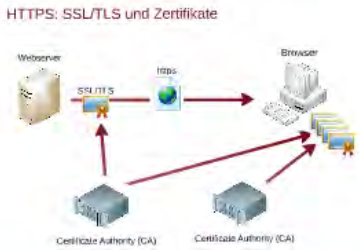
(Google, Microsoft, Yahoo, etc)

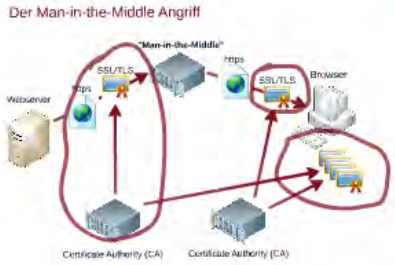
"Das Netzwerk"

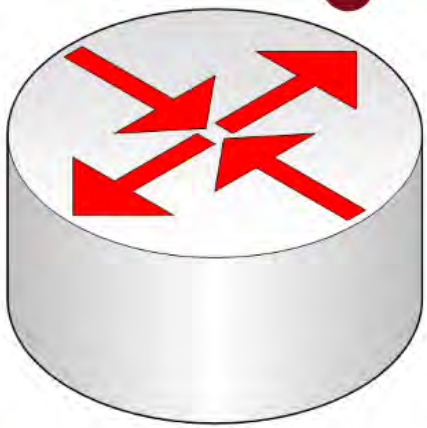
(Backbone Provider, Access Provider)

Endgerät

(User)

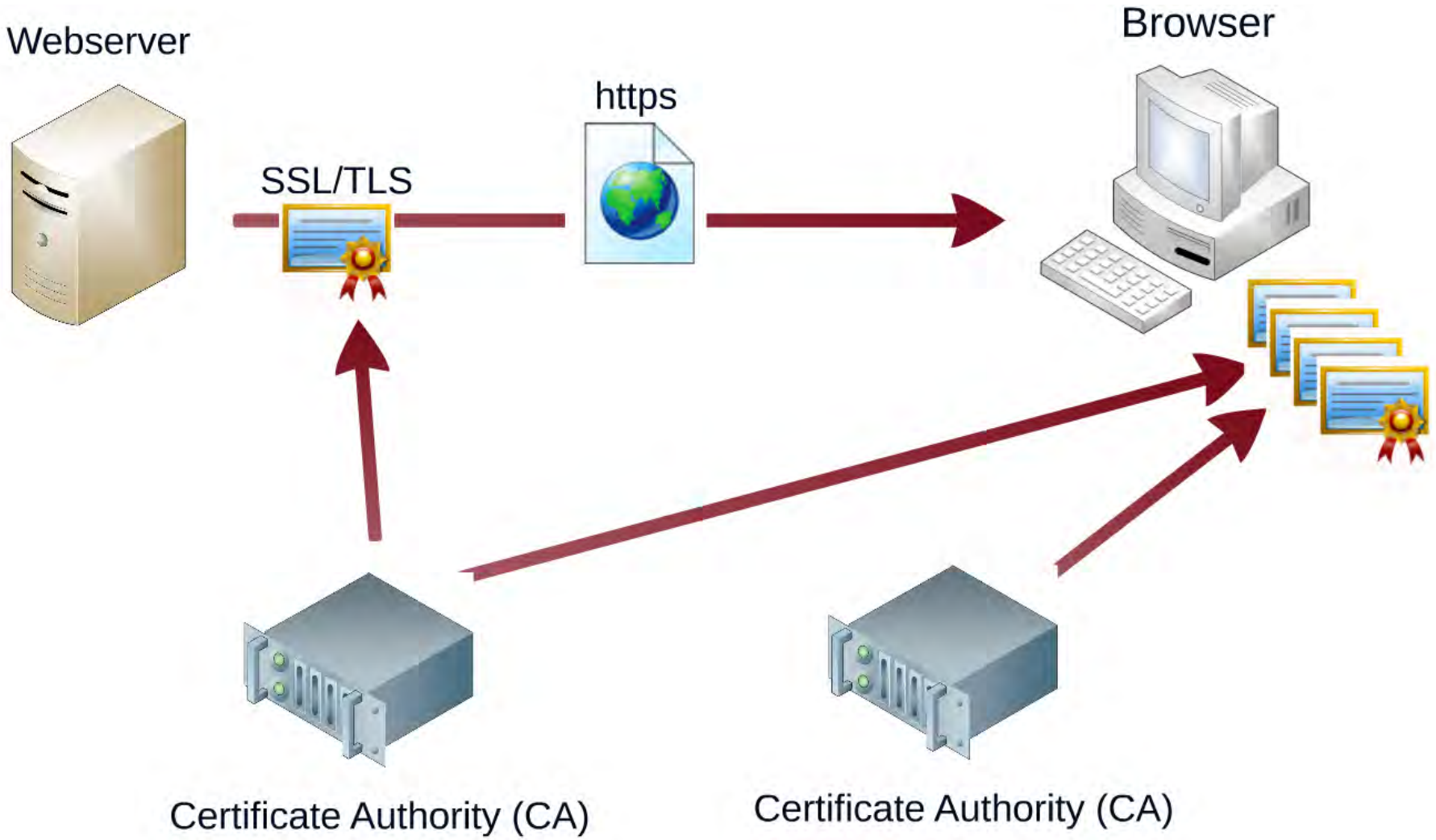




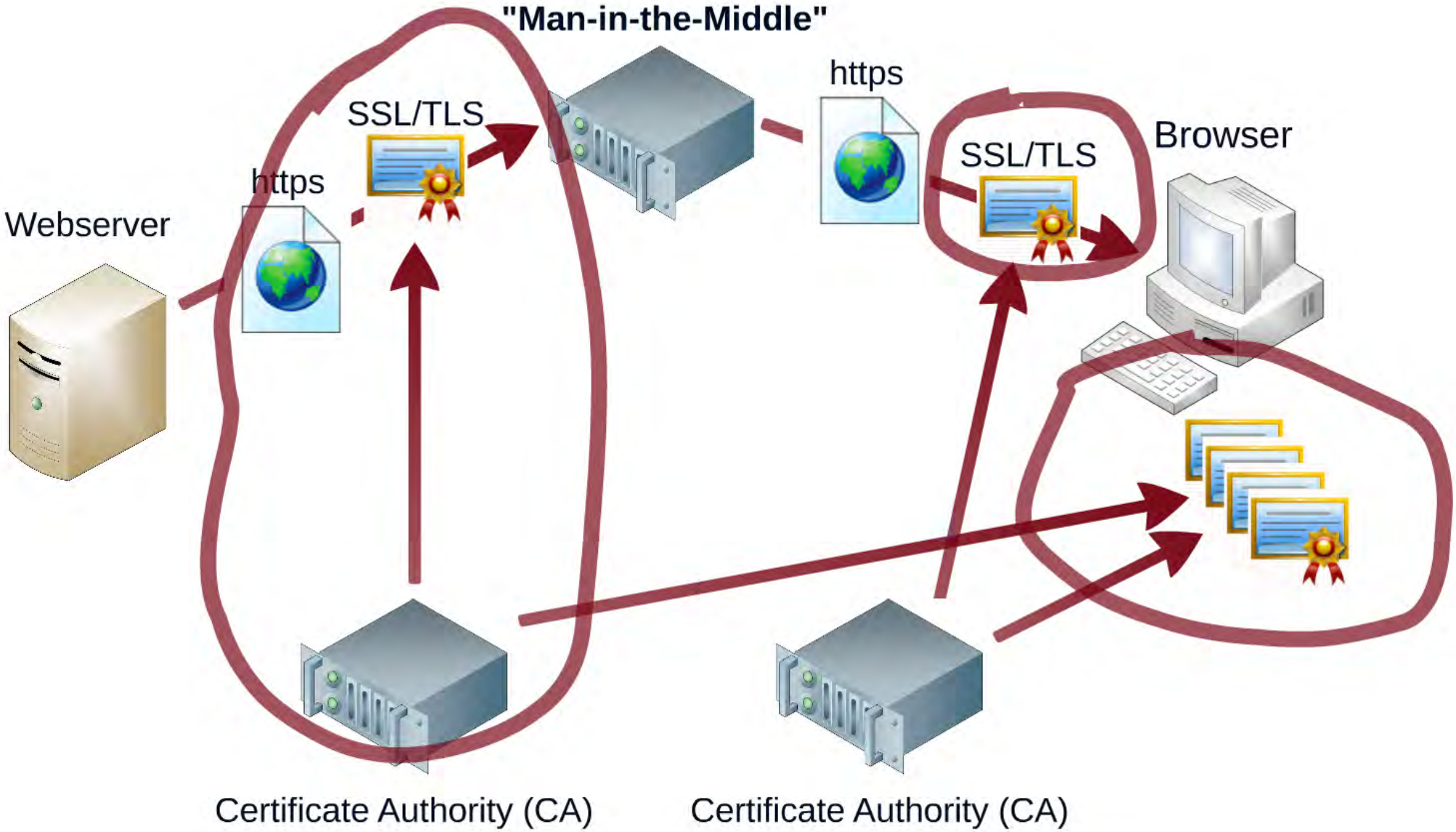


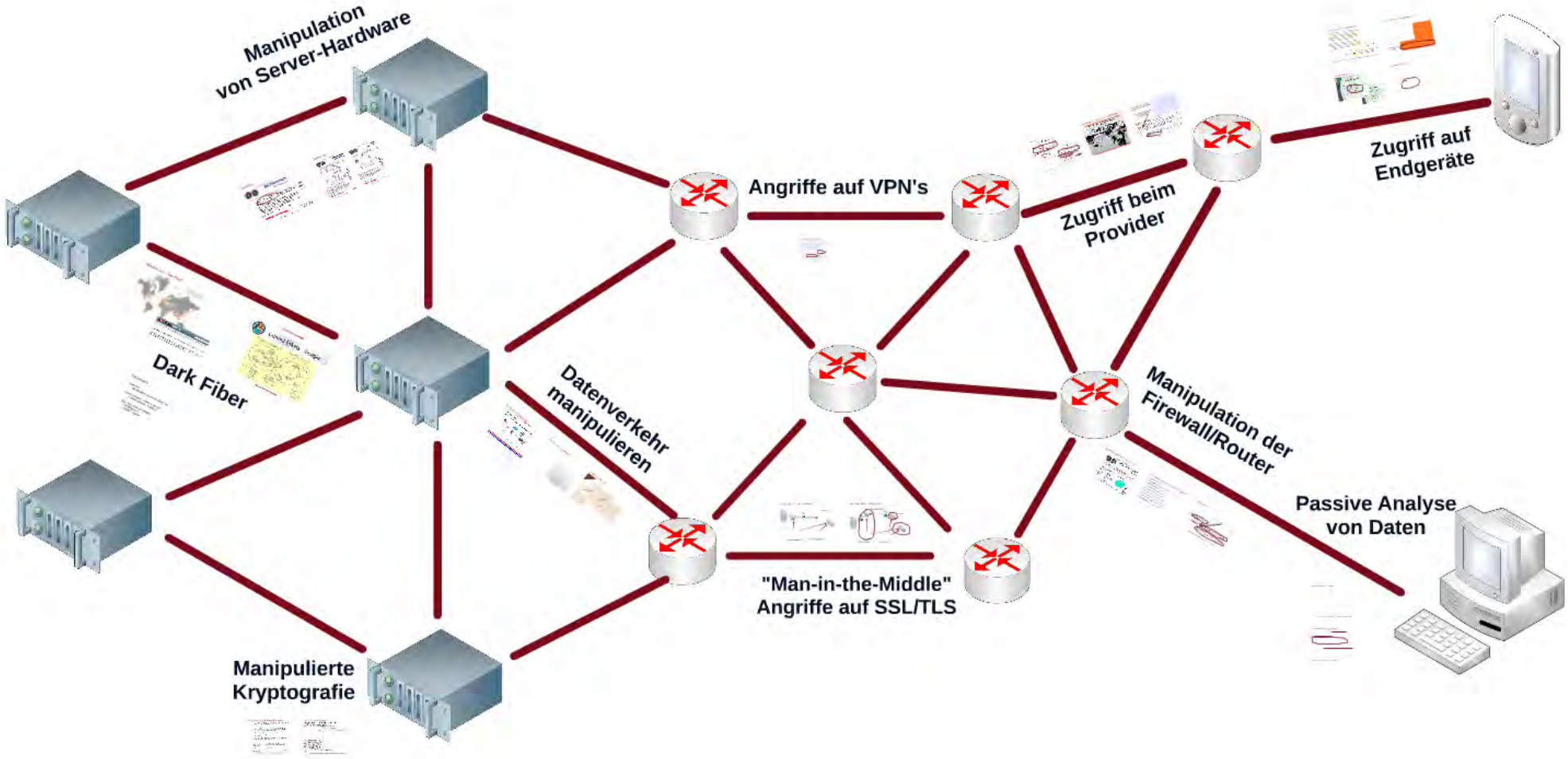
"Man-in-the-Middle" Angriffe auf SSL/TLS

HTTPS: SSL/TLS und Zertifikate



Der Man-in-the-Middle Angriff





Content-/Dienste-Anbieter

(Google, Microsoft, Yahoo, etc)

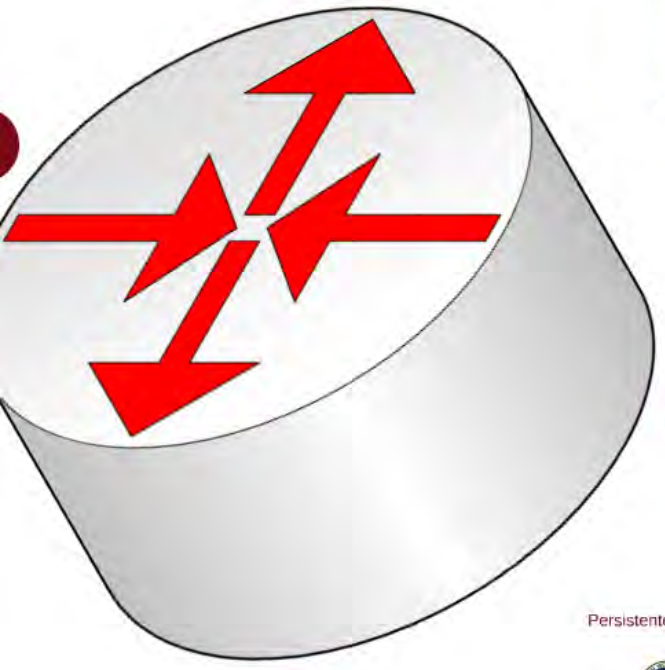
"Das Netzwerk"

(Backbone Provider, Access Provider)

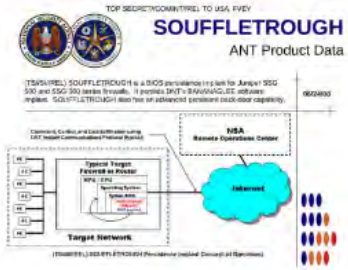
Endgerät

(User)

Manipulation der Firewall/Router

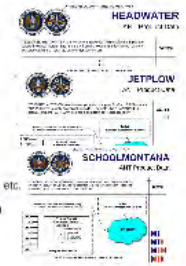


Persistente Schadsoftware in der Firmware



Stand 2008 verfügbar für eine Reihe von Modellen

HEADWATER: Huawei Router
SCHOOLMONTANA: Juniper J-Series router
SIERRAMONTANA: Juniper M-Series router
STUCCOMONTANA: Juniper T-Series router
JETPLOW: Cisco PIX und ASA firewalls
HALLUXWATER: Huawei Eudemon firewalls
FEEDTROUGH: Juniper Netscreen firewalls
GOURMETTROUGH: Juniper nsg5t, ns50, ns25, etc.
SOUFFLETROUGH: Juniper SSG 500, SSG 300



Gängige Praxis...

Persistente Schadsoftware in der Firmware

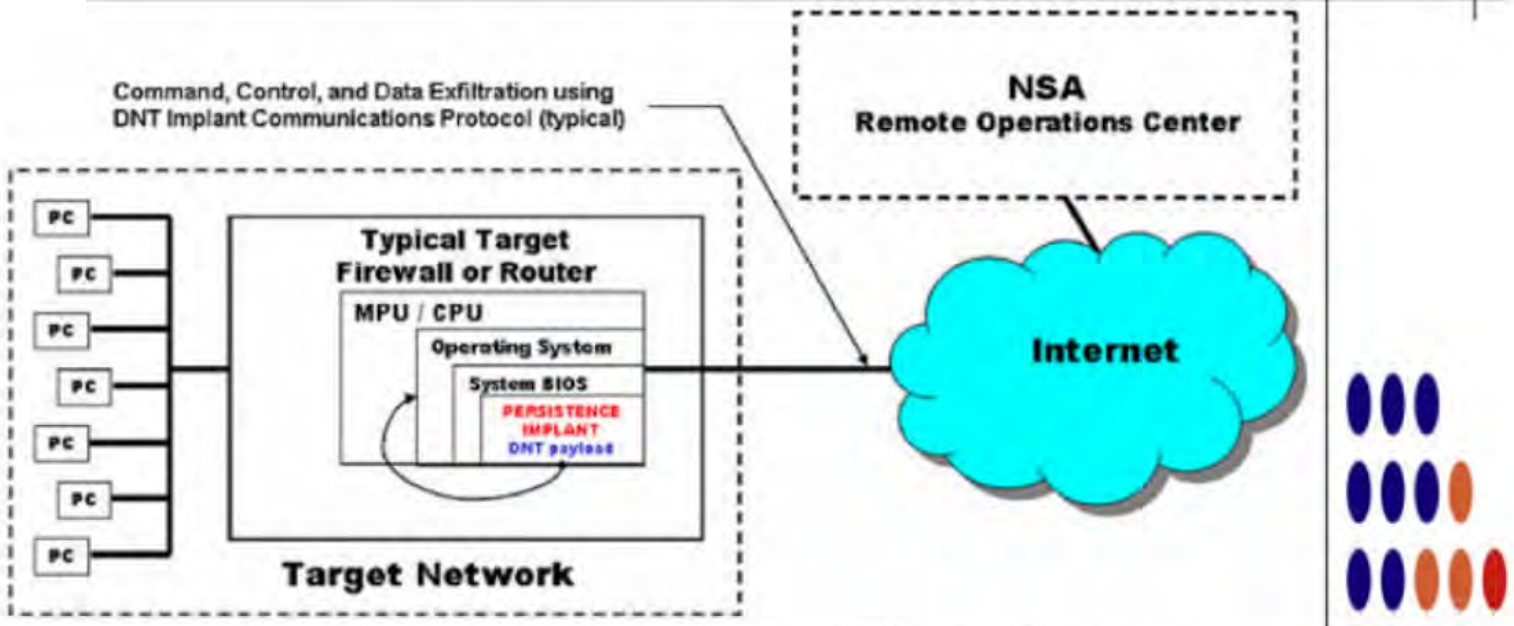
TOP SECRET//COMINT//REL TO USA, FVEY

SOUFFLETROUGH

ANT Product Data

(TS//SI//REL) SOUFFLETROUGH is a BIOS persistence implant for Juniper SSG 500 and SSG 300 series firewalls. It persists DNT's BANANAGLEE software implant. SOUFFLETROUGH also has an advanced persistent back-door capability.

06/24/08



(TS//SI//REL) SOUFFLETROUGH Persistence Implant Concept of Operations

Stand 2008 verfügbar für eine Reihe von Modellen

HEADWATER: Huawei Router

SCHOOLMONTANA: Juniper J-Series router

SIERRAMONTANA: Juniper M-Series router

STUCCOMONTANA: Juniper T-Series router

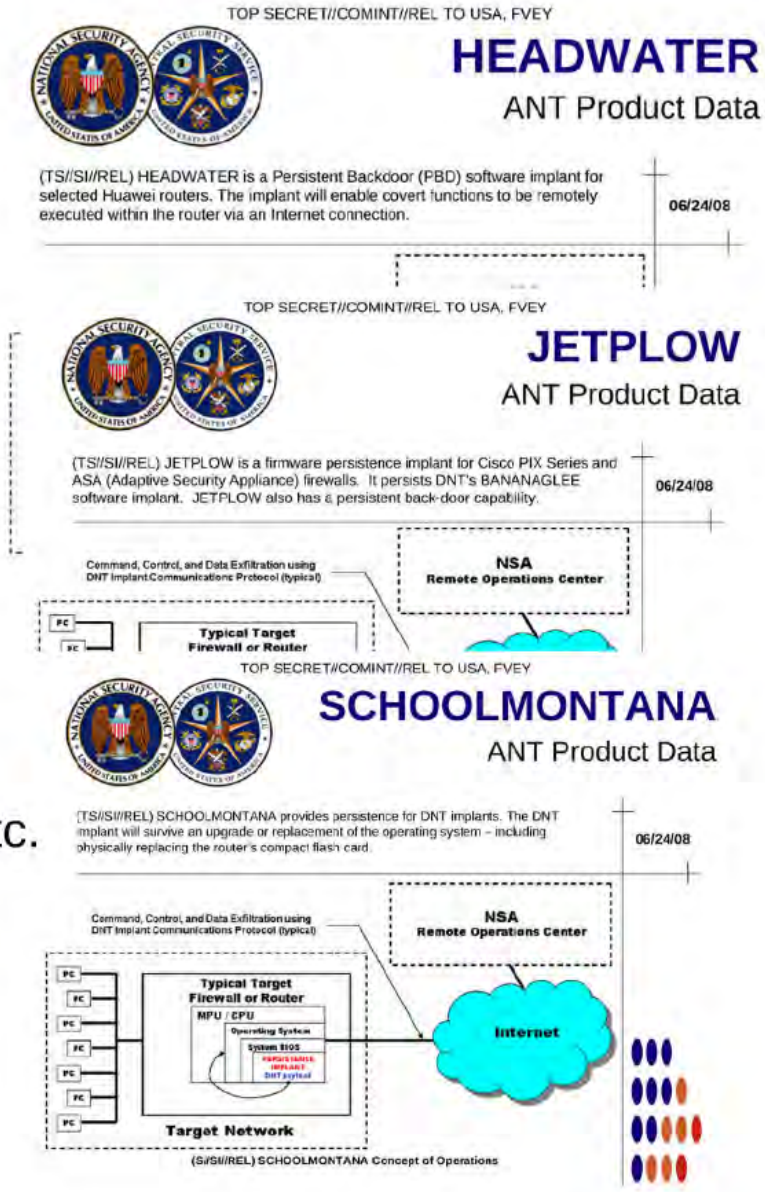
JETPLOW: Cisco PIX und ASA firewalls

HALLUXWATER: Huawei Eudemon firewalls

FEEDTROUGH: Juniper Netscreen firewalls

GOURMETTROUGH: Juniper nsg5t, ns50, ns25, etc.

SOUFFLETROUGH: Juniper SSG 500, SSG 300



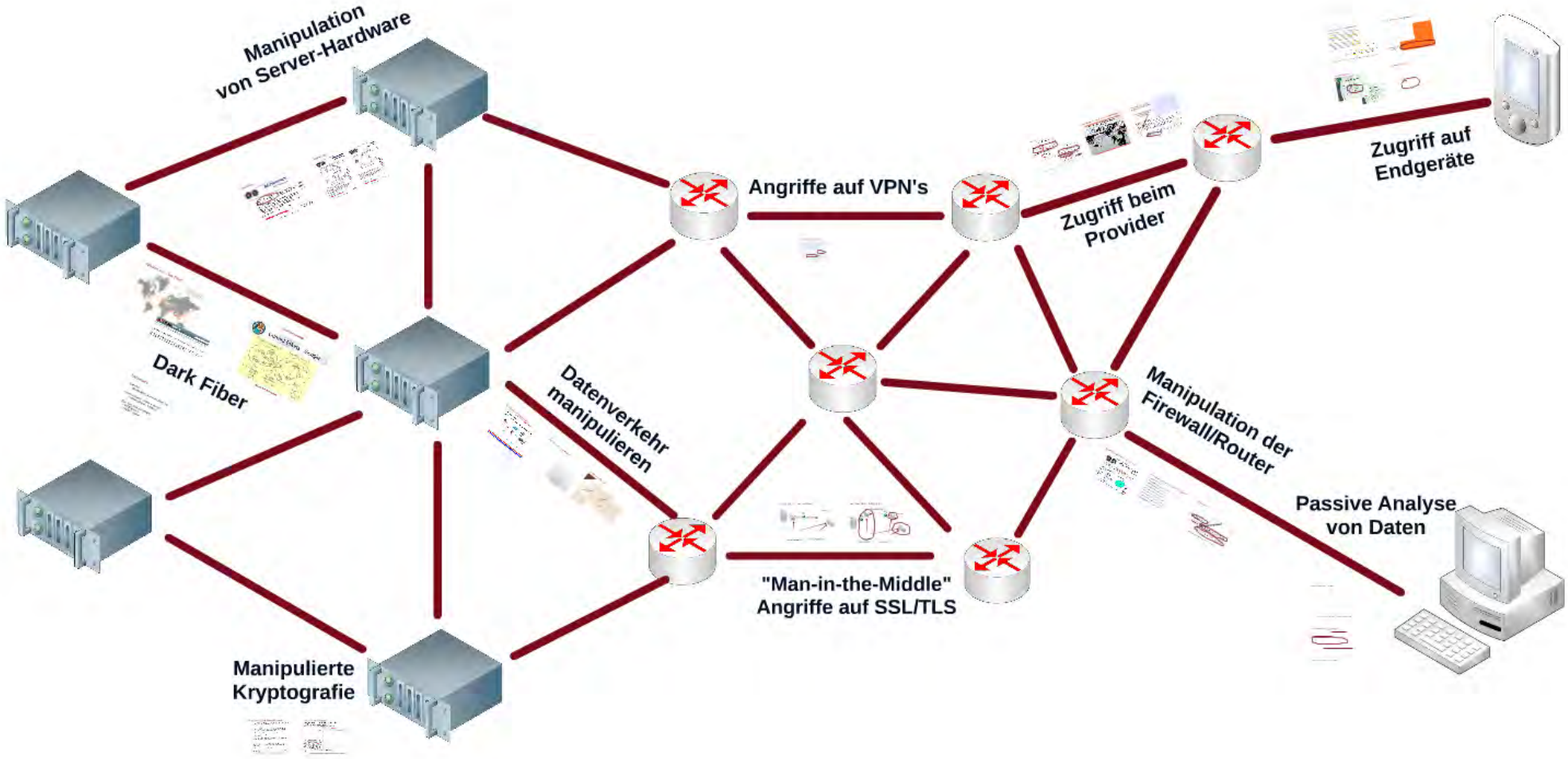
Gängige Praxis...

(TS//SI//REL) Happy Friday my esteemed and valued Intelligence Community colleagues! There has been a topic of conversation that has started to rumble beneath the surface of the Cyber-scene lately, it's about router hacking(for this post, I'm not talking about your home ADSL router, I'm talking about bigger routers, such as Ciscos/Junipers /Huaweis used by ISPs for their infrastructure). Hacking routers has been good business for us and our 5-eyes partners for some time now, but it is becoming more apparent that other nation states are honing their skillz and joining the scene. Before I get into it too much, let's go over some of the things that someone could do if they hack a router:

* You could add credentials, allowing yourself to log in any time you choose
* You could add/change routing rules
* You could set up a packet capture capability...imagine running Wireshark on an ISP's infrastructure router...like a local listening post for any credentials being passed over the wire(!)
* You could weaken any VPN encryption capabilities on the router, forcing it to create easily decryptable tunnels
* You could install a dorked version of the Operating System with whatever functionality you want pre-built in

Zoning-Konzepte?

https://firstlook.org/theintercept/article/2014/03/12/nsa-plans-infect-millions-computers-malware/



Content-/Dienste-Anbieter

(Google, Microsoft, Yahoo, etc)

"Das Netzwerk"

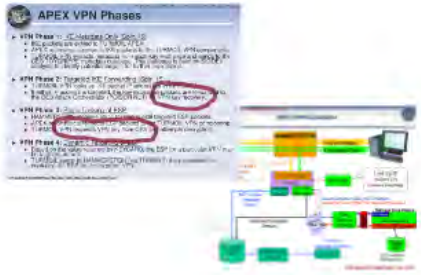
(Backbone Provider, Access Provider)

Endgerät

(User)

Angriffe auf VPN's

Zugriff auf (IPSec) VPN's



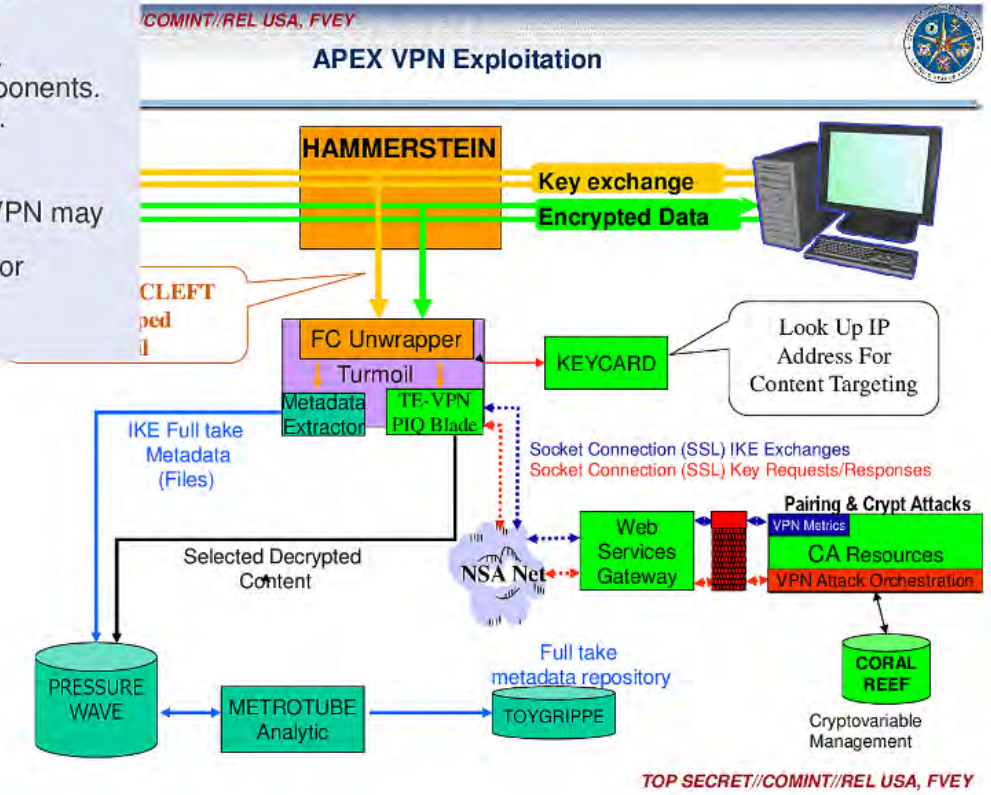
Zugriff auf (IPSec) VPN's

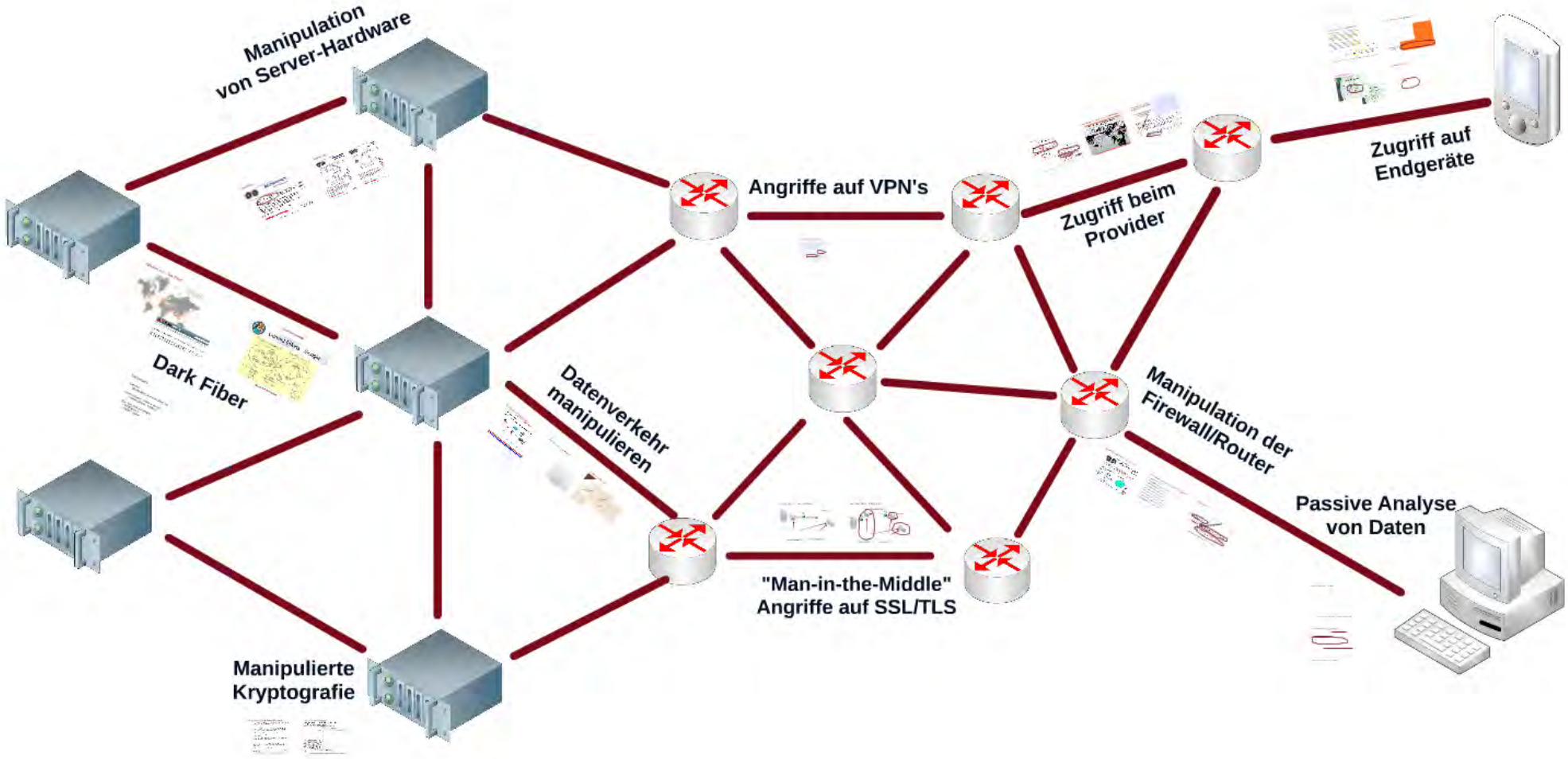
TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL//20291123

APEX VPN Phases

- **VPN Phase 1:** IKE Metadata Only (Spin 15)
  - IKE packets are exfiled to TURMOIL APEX.
  - APEX reconstructs/reinjects IKE packets to the TURMOIL VPN components.
  - TURMOIL VPN extracts metadata from each key exchange and sends to the CES TOYGRIPPE metadata database. This database is used by SIGDEV analysts to identify potential targets for further exploitation.
- **VPN Phase 2:** Targeted IKE Forwarding (Spin 15)
  - TURMOIL VPN looks up IKE packet IP addresses in KEYCARD.
  - If either IP address is targeted, the key exchange packets are forwarded to the CES Attack Orchestrator (POISON NUT) for VPN key recovery.
- **VPN Phase 3:** Static Tasking of ESP
  - HAMMERSTEIN receives static tasking to exfil targeted ESP packets.
  - APEX reconstructs/reinjects ESP packets to the TURMOIL VPN components.
  - TURMOIL VPN requests VPN key from CES and attempts decryption.
- **VPN Phase 4:** Dynamic Targeting of ESP
  - Based on the value returned by KEYCARD, the ESP for a particular VPN may be targeted as well.
  - TURMOIL sends to HAMMERSTEIN (via TURBINE) the parameters for capturing the ESP for the targeted VPN.

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





Content-/Dienste-Anbieter

(Google, Microsoft, Yahoo, etc)

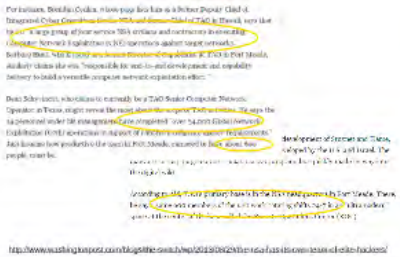
"Das Netzwerk"

(Backbone Provider, Access Provider)

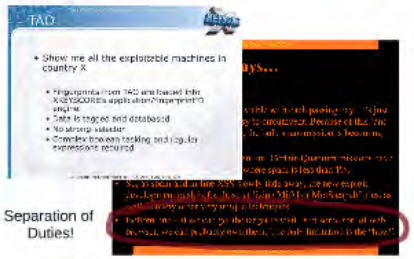
Endgerät

(User)

TAO - "Taylored Access Operations"

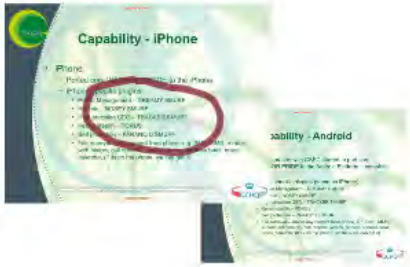


TAO - "Taylored Access Operations"



Separation of Duties!

Malware-Implantate



Malware-Implantate

Zugriff auf Endgeräte

TAO - "Taylored Access Operations"

For instance, Brendan Conlon, whose page lists him as a former Deputy Chief of Integrated Cyber Operations for the NSA and former Chief of TAO in Hawaii, says that he led "a large group of joint service NSA civilians and contractors in executing Computer Network Exploitation (CNE) operations against target networks." Barbara Hunt, who is listed as a former Director of Capabilities at TAO in Fort Meade, similarly claims she was "responsible for end-to-end development and capability delivery to build a versatile computer network exploitation effort."

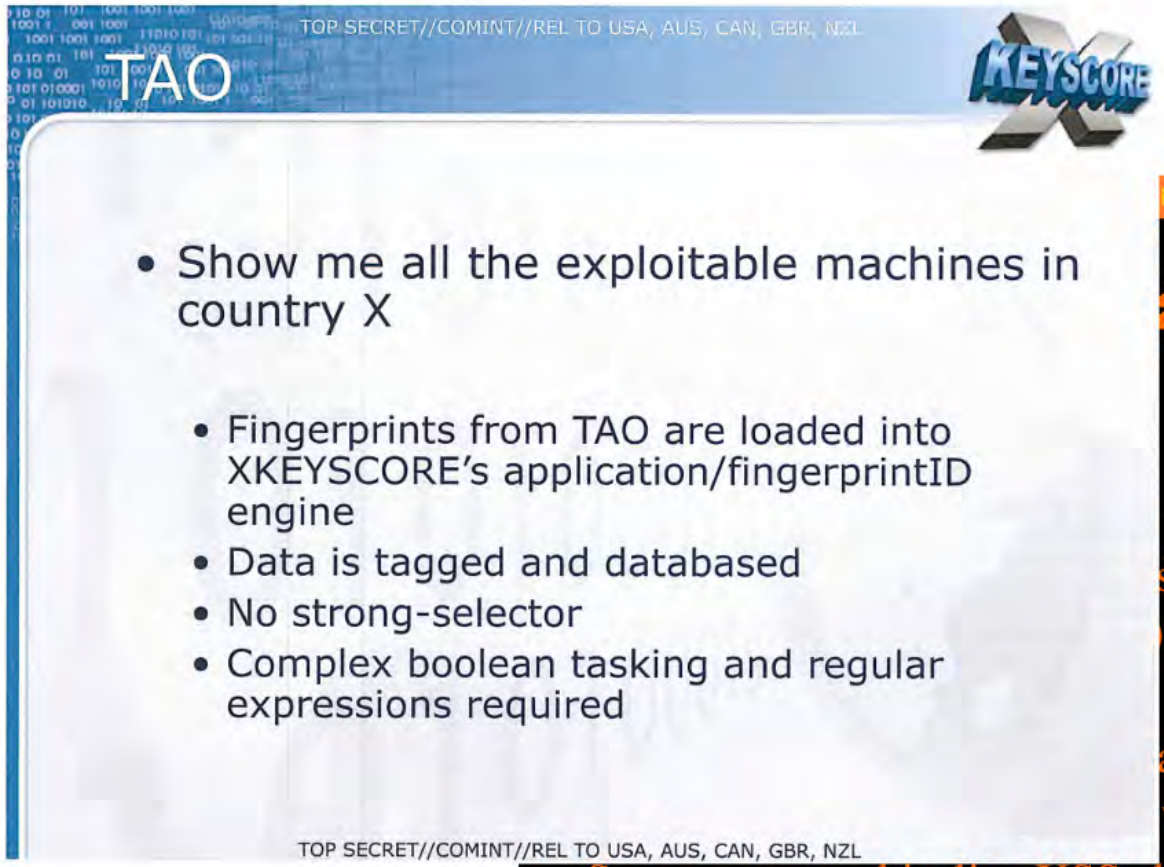
Dean Schyvincht, who claims to currently be a TAO Senior Computer Network Operator in Texas, might reveal the most about the scope of TAO activities. He says the 14 personnel under his management have completed "over 54,000 Global Network Exploitation (GNE) operations in support of national intelligence agency requirements." Just imagine how productive the team in Fort Meade, rumored to have about 600 people, must be.

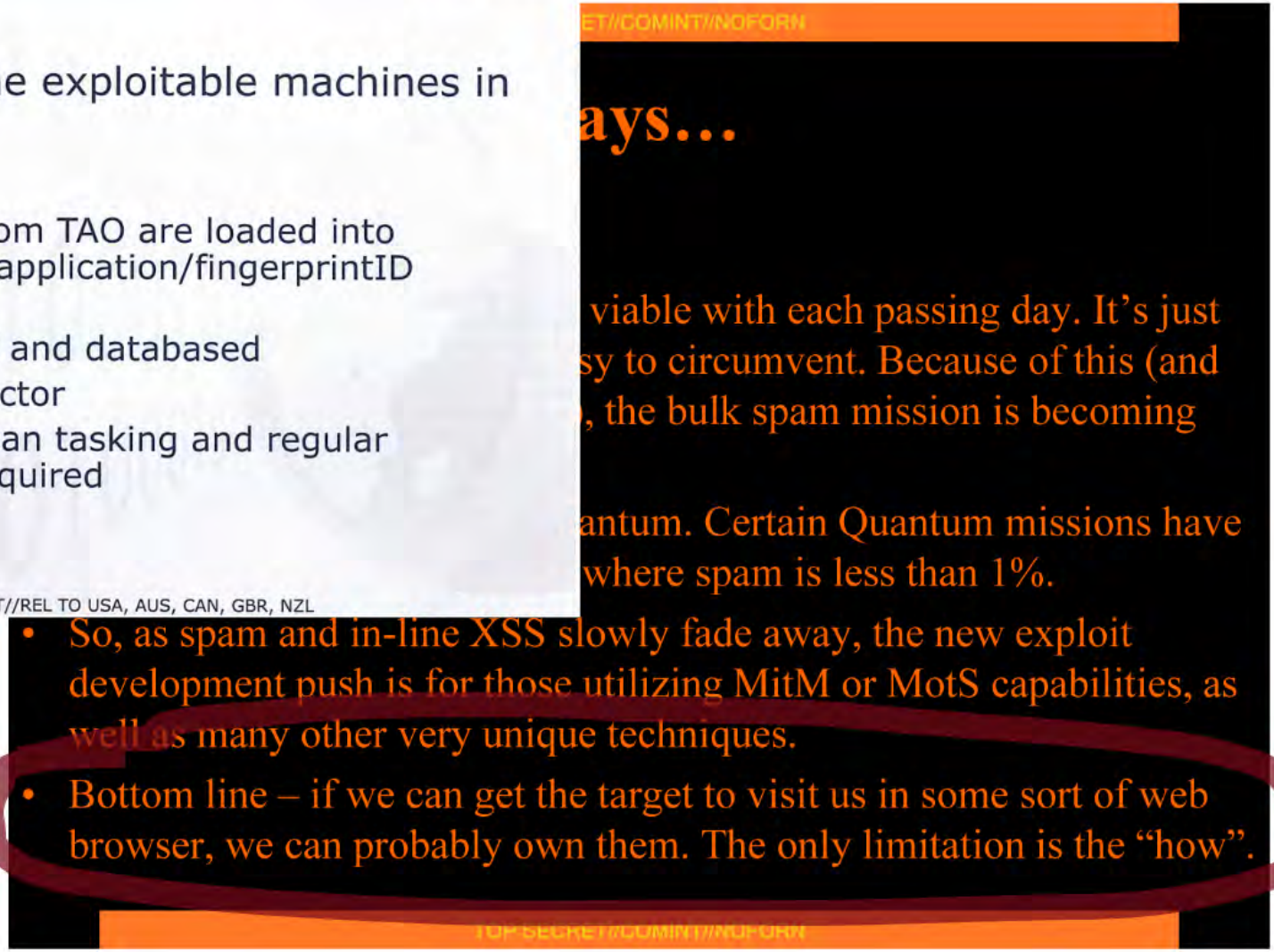
development of Stuxnet and Flame, veloped by the U.S. and Israel. The malware initially targeted the Iranian nuclear program, but quickly made its way into the digital wild.

According to Aid, TAO's primary base is in the NSA headquarters in Fort Meade. There, he says some 600 members of the unit work rotating shifts 24-7 in an "ultramodern" space at the center of the base called the Remote Operations Center (ROC).

http://www.washingtonpost.com/blogs/the-switch/wp/2013/08/29/the-nsa-has-its-own-team-of-elite-hackers/

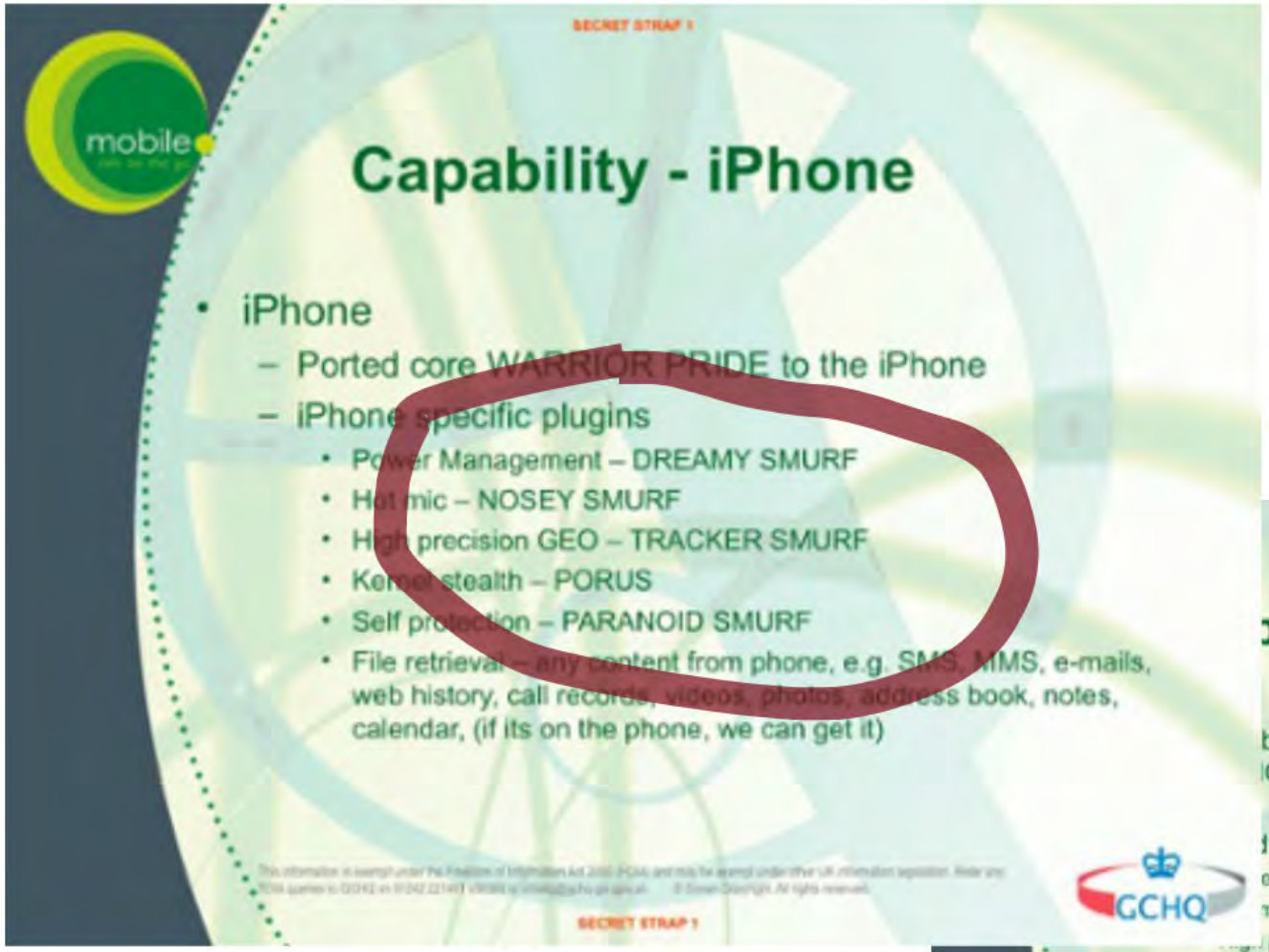
TAO - "Taylored Access Operations"

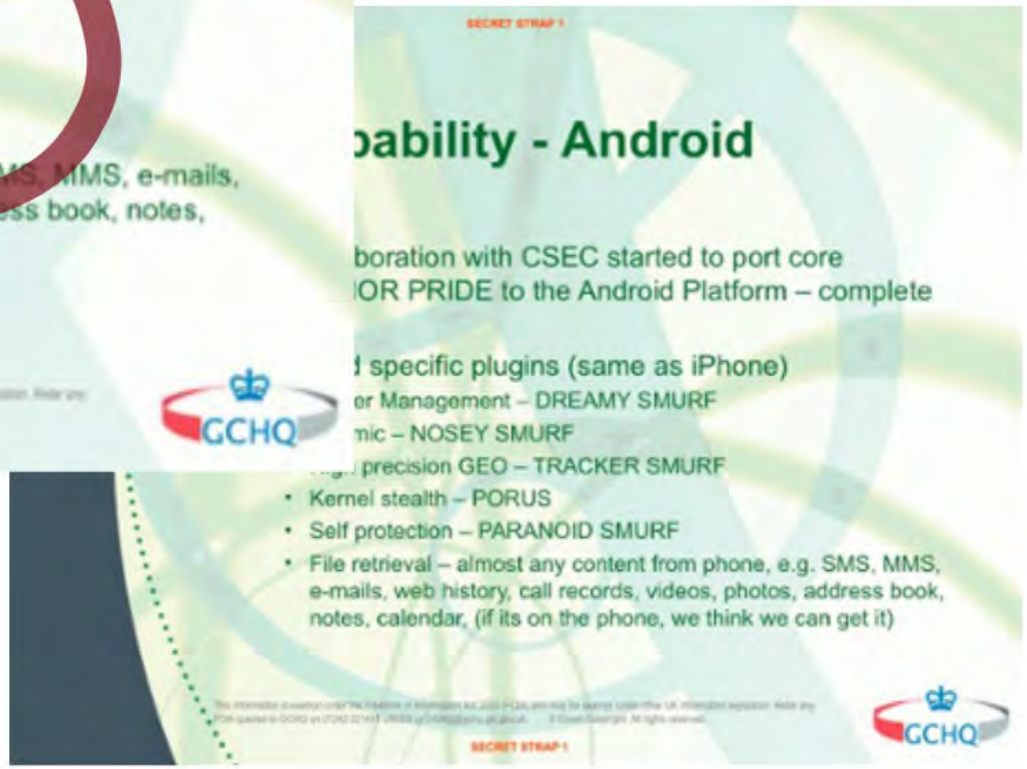




Separation of Duties!

Malware-Implantate





Malware-Implantate

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

NIGHTSTAND

Wireless Exploitation / Injection Tool

(TS//SI//REL) An active 802.11 wireless exploitation and injection tool for payload/exploit delivery into otherwise denied target space. NIGHTSTAND is typically used in operations where wired access to the target is not possible.

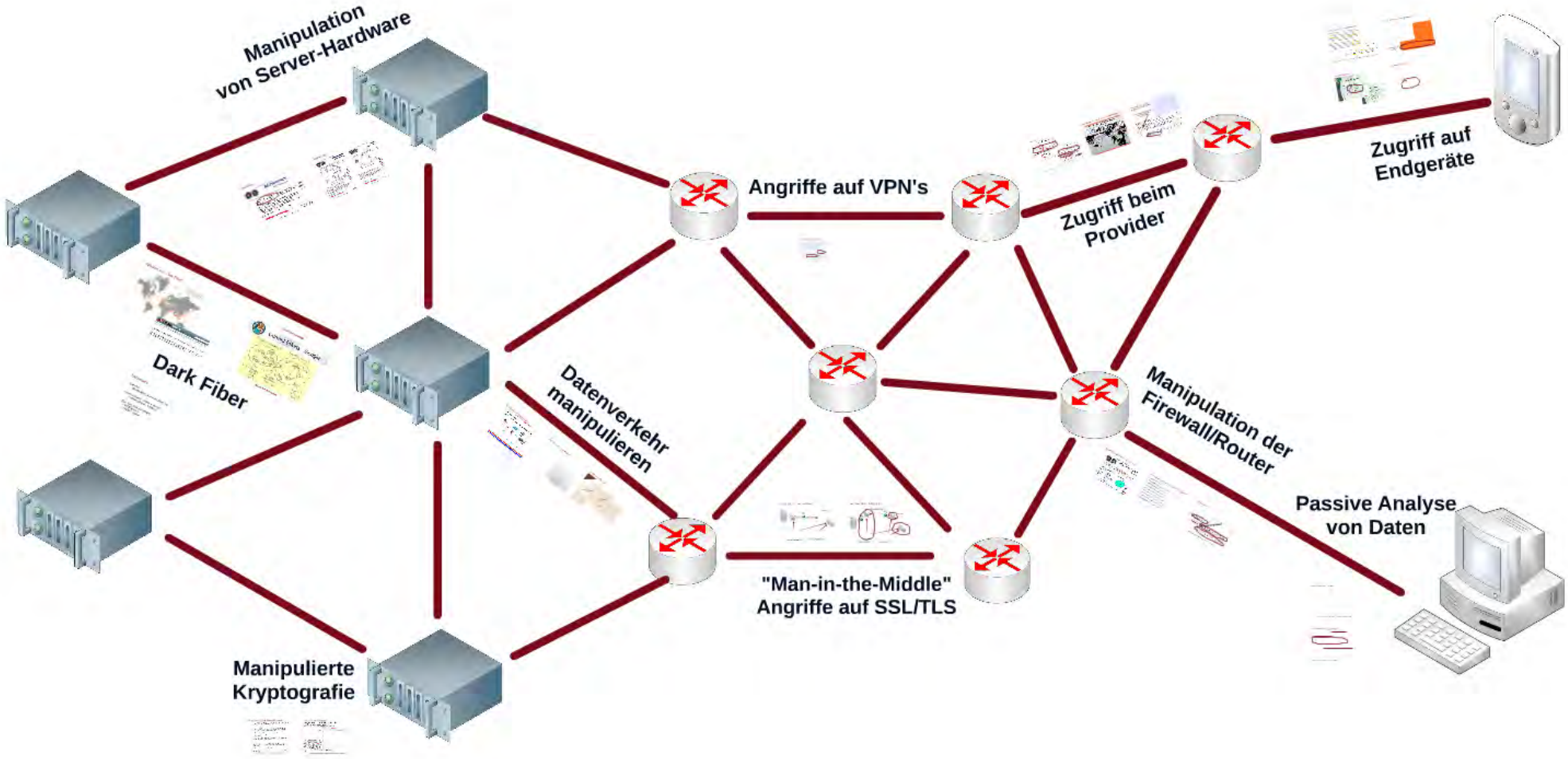
07/25/08

(TS//SI//REL) **NIGHTSTAND** - Close Access Operations • Battlefield Tested • Windows Exploitation • Standalone System

System Details

- (U//FOUO) Standalone tool currently running on an x86 laptop loaded with Linux Fedora Core 3.
- (TS//SI//REL) Exploitable Targets include Win2k, WinXP, WinXPSP1, WINXPSP2 running internet Explorer versions 5.0-6.0.
- (TS//SI//REL) NS packet injection can target one client or multiple targets on a wireless network.
- (TS//SI//REL) Attack is undetectable by the user.

NIGHTSTAND Hardware



Content-/Dienste-Anbieter

(Google, Microsoft, Yahoo, etc)

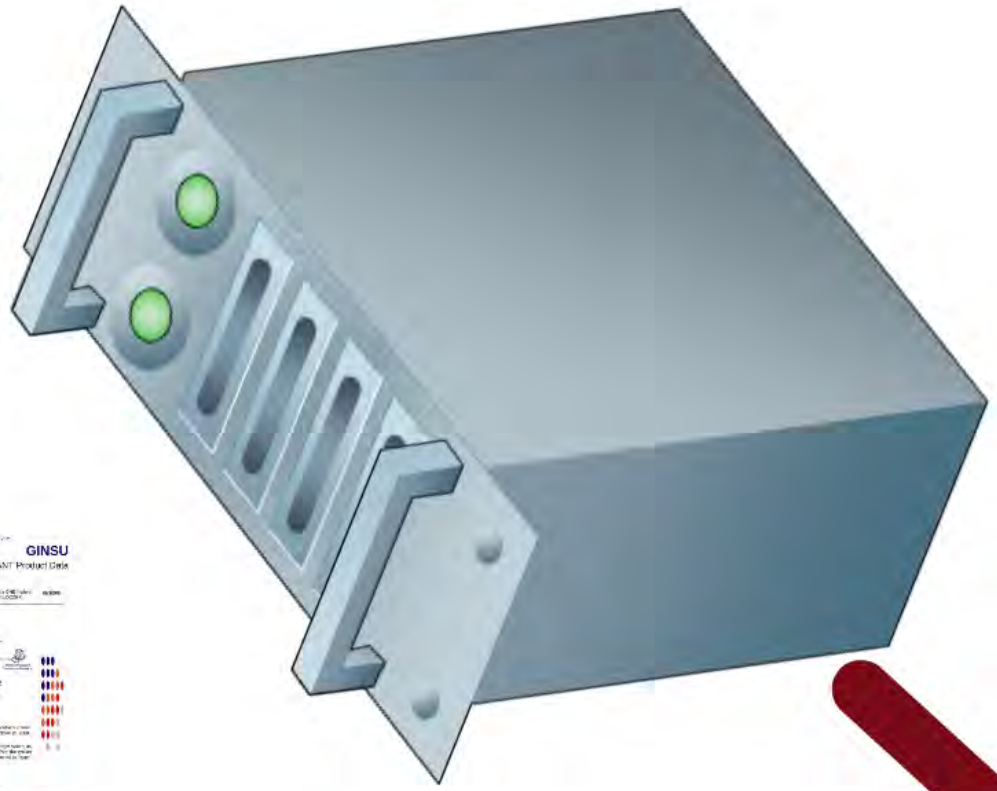
"Das Netzwerk"

(Backbone Provider, Access Provider)

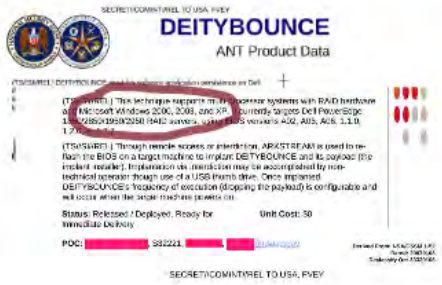
Endgerät

(User)

Manipulation von Server-Hardware



"Implantate"



SECRET//COMINT//REL TO USA, FVEY

DEITYBOUNCE

ANT Product Data

(TS//SI//REL) This technique supports the [redacted] processor systems with RAID hardware and Microsoft Windows 2000, 2003, and XP. Currently targets Dell PowerEdge [redacted] servers using BIOS versions A02, A05, A06, 1.1.0, 1.7.0, [redacted]

(TS//SI//REL) Through remote access or interdiction, ARKSTREAM is used to re-flash the BIOS on a target machine to implant DEITYBOUNCE and its payload (by insider/ retailer). Implantation via interdiction may be accomplished by non-technical operator though use of a USB thumb drive. Once implanted, DEITYBOUNCE's frequency of execution (dropping the payload) is configurable and will occur when the target machine powers on.

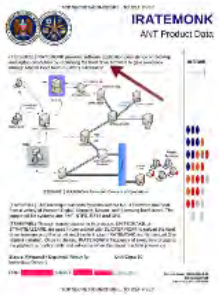
Status: Released / Deployed. Ready for Immediate Delivery

Unit Cost: 50

POC: [redacted] S32221, [redacted], [redacted]

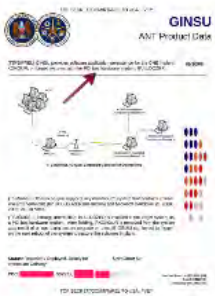
SECRET//COMINT//REL TO USA, FVEY

"Implantate"



IRATEMONK

ANT Product Data



GINSU

ANT Product Data

"Implantate"

SECRET//COMINT//REL TO USA, FVEY

DEITYBOUNCE

ANT Product Data

(TS//SI//REL) DEITYBOUNCE provides software application persistence on Dell P
M
I

(TS//SI//REL) This technique supports multi-processor systems with RAID hardware and Microsoft Windows 2000, 2003, and XP. It currently targets Dell PowerEdge 1850/2850/1950/2950 RAID servers, using BIOS versions A02, A05, A06, 1.1.0, 1.2.0, or 1.3.7.

(TS//SI//REL) Through remote access or interdiction, ARKSTREAM is used to re-flash the BIOS on a target machine to implant DEITYBOUNCE and its payload (the implant installer). Implantation via interdiction may be accomplished by non-technical operator though use of a USB thumb drive. Once implanted, DEITYBOUNCE's frequency of execution (dropping the payload) is configurable and will occur when the target machine powers on.

Status: Released / Deployed. Ready for Immediate Delivery

Unit Cost: $0

POC: [redacted], S32221, [redacted], [redacted]@nsa.ic.gov

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

SECRET//COMINT//REL TO USA, FVEY

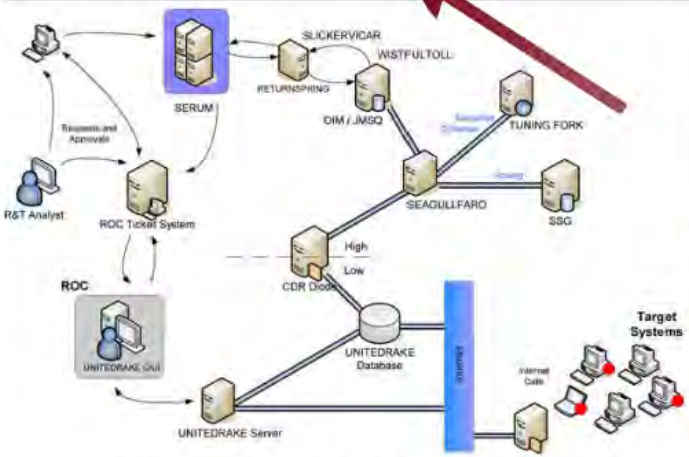
"Implantate"

IRATEMONK

ANT Product Data

(TS//SI//REL) IRATEMONK provides software application persistence on desktop and laptop computers by implanting the hard drive firmware to gain execution through Master Boot Record (MBR) substitution.

06/20/08



(TS//SI//REL) IRATEMONK Extended Concept of Operations

(TS//SI//REL) This technique supports systems without RAID hardware that boot from a variety of Western Digital, Seagate, Maxtor, and Samsung hard drives. The supported file systems are: FAT, NTFS, EXT3 and UFS.

(TS//SI//REL) Through remote access or interdiction, UNITEDRAKE, or STRAITBAZZARE are used in conjunction with SLICKERVICAR to upload the hard drive firmware onto the target machine to implant IRATEMONK and its payload (the implant installer). Once implanted, IRATEMONK's frequency of execution (dropping the payload) is configurable and will occur when the target machine powers on.

Status: Released / Deployed. Ready for Immediate Delivery

Unit Cost: $0

POC: [redacted], S32221, [redacted], [redacted]@nsa.ic.gov

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

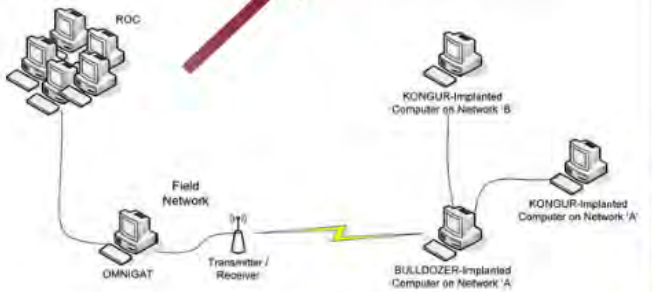
TOP SECRET//COMINT//REL TO USA, FVEY

GINSU

ANT Product Data

(TS//SI//REL) GINSU provides software application persistence for the CNE implant, KONGUR, on target systems with the PCI bus hardware implant, BULLDOZER.

06/20/08



(TS//SI//REL) GINSU Extended Concept of Operations

(TS//SI//REL) This technique supports any desktop PC system that contains at least one PCI connector (for BULLDOZER installation) and Microsoft Windows 9x, 2000, 2003, XP, or Vista.

(TS//SI//REL) Through interdiction, BULLDOZER is installed in the target system as a PCI bus hardware implant. After fielding, if KONGUR is removed from the system as a result of an operating system upgrade or reinstall, GINSU can be set to trigger on the next reboot of the system to restore the software implant.

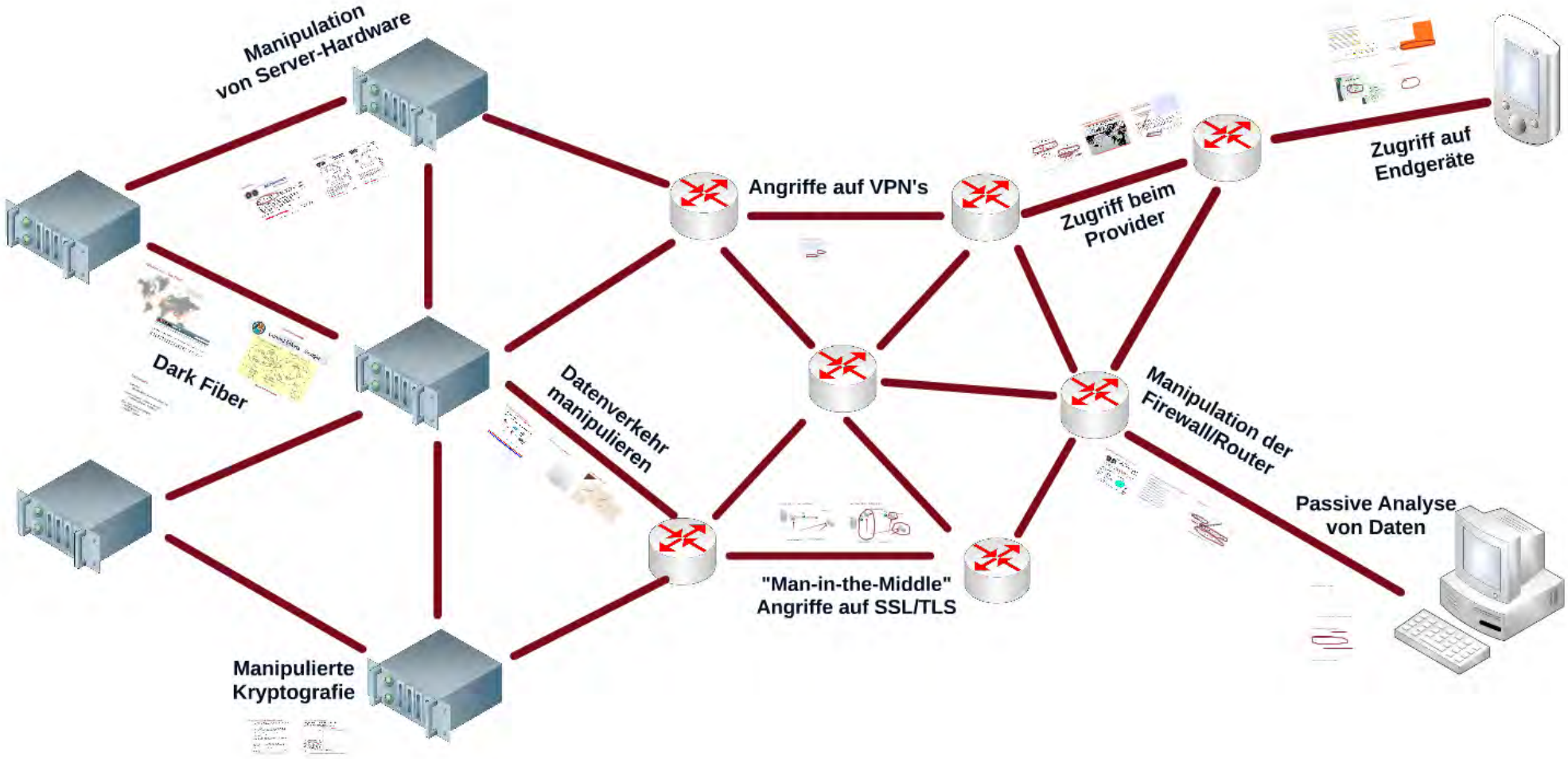
Status: Released / Deployed. Ready for Immediate Delivery

Unit Cost: $0

POC: [redacted], S32221, [redacted], [redacted]@nsa.ic.gov

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

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



Content-/Dienste-Anbieter

(Google, Microsoft, Yahoo, etc)

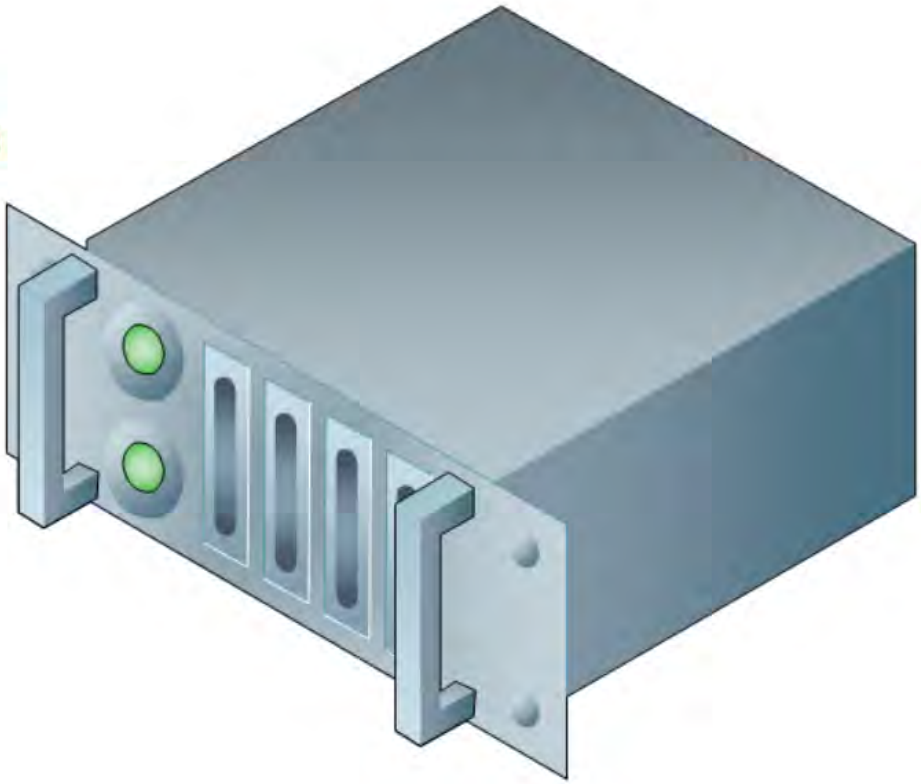
"Das Netzwerk"

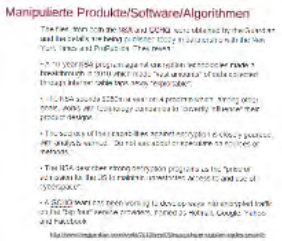
(Backbone Provider, Access Provider)

Endgerät

(User)

Manipulierte Kryptografie





Manipulierte Produkte/Software/Algorithmen

The files, from both the NSA and GCHQ, were obtained by the Guardian, and the details are being published today in partnership with the New York Times and ProPublica. They reveal:

• A 10-year NSA program against encryption technologies made a breakthrough in 2010 which made "vast amounts" of data collected through internet cable taps newly "exploitable".

• The NSA spends $250m a year on a program which, among other goals, works with technology companies to "covertly influence" their product designs.

• The secrecy of their capabilities against encryption is closely guarded, with analysts warned: "Do not ask about or speculate on sources or methods."

• The NSA describes strong decryption programs as the "price of admission for the US to maintain unrestricted access to and use of cyberspace".

• A GCHQ team has been working to develop ways into encrypted traffic on the "big four" service providers, named as Hotmail, Google, Yahoo and Facebook.

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

Standards mit "Hintertüren"

New York Times provides new details about NSA backdoor in crypto spec

The paper points a finger definitively at the long-suspected Dual_EC_DRBG algorithm.

by **Megan Geuss** - Sept 11 2013, 5:00am WEDT

HACKING PRIVACY 85

Today, the *New York Times* reported that an algorithm for generating random numbers, which was adopted in 2006 by the National Institute of Standards and Technology (NIST), contains a backdoor for the NSA. The news followed a *NYT* report from last week, which indicated that the National Security Agency (NSA) had circumvented widely used (but then-unnamed) encryption schemes by placing backdoors in the standards that are used to implement the encryption.

In 2007, cryptographers Niels Ferguson and Dan Shumow presented research suggesting that there could be a potential backdoor in the Dual_EC_DRBG algorithm, which NIST had included in Special Publication 800-90. If the parameters used to define the algorithm were chosen in a particular way, they would allow the NSA to predict the supposedly random numbers produced by the algorithm. It wasn't entirely clear at the time that the NSA had picked the parameters in this way; as Ars noted last week, the rationale for choosing the particular Dual_EC_DRBG parameters in SP 800-90 was never actually stated.

A.1.1 Curve P-256

p = 115792089210356248762697446949407573530086143415290314195533631308867097853951

n = 115792089210356248762697446949407573529996955224135760342422259061068512044369

b = 5ac635d8 aa3a93e7 b3ebbd55 769886bc 651d06b0 cc53b0f6 3bce3c3e 27d2604b

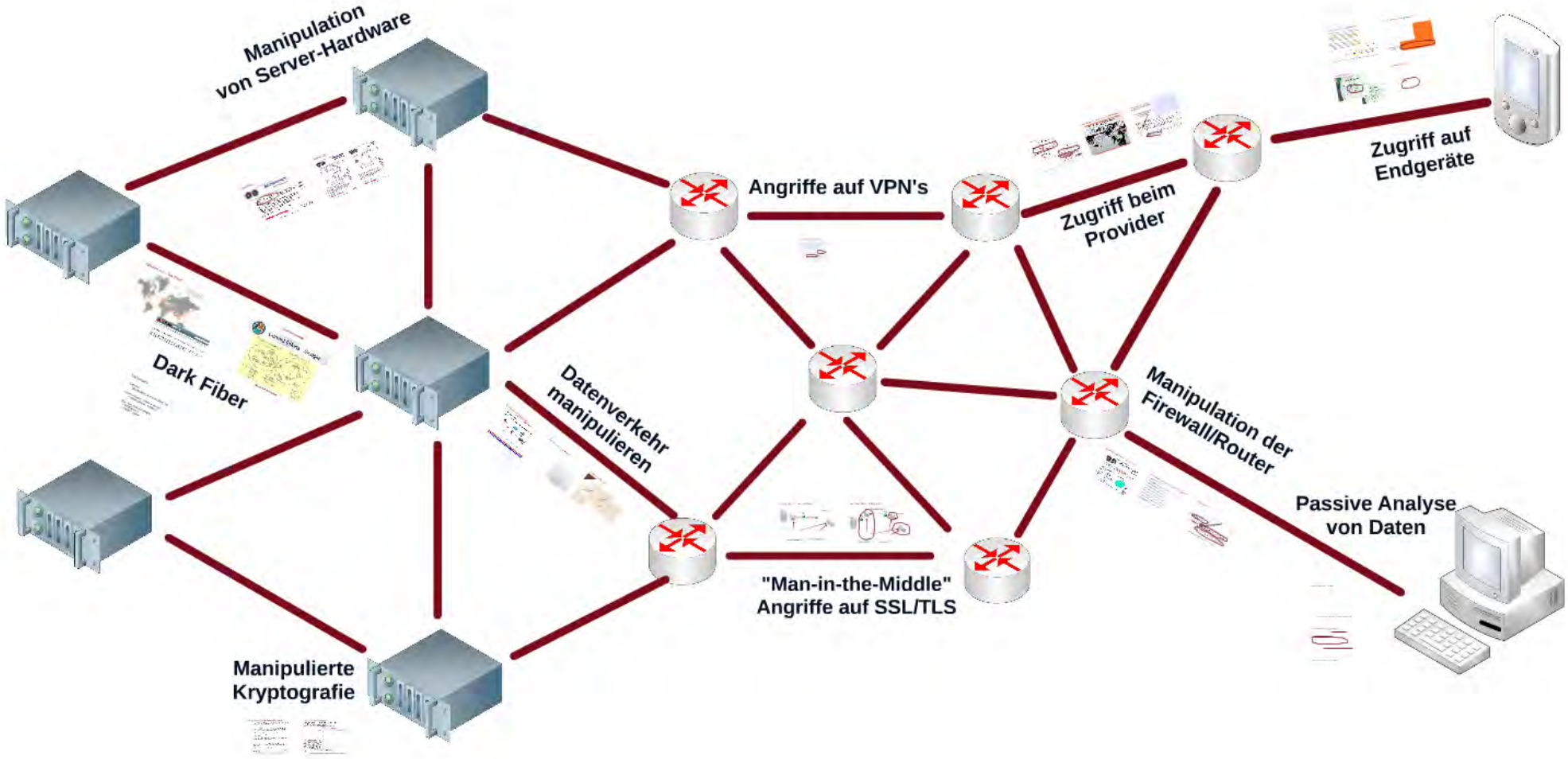
Px = 6b17d1f2 e12c4247 f8bce6e5 63a440f2 77037d81 2deb33a0 f4a13945 d898c296

Py = 4fe342e2 fe1a7f9b 8ee7eb4a 7c0f9e16 2bce3357 6b315ece cbb64068 37bf51f5

Qx = c97445f4 5cdef9f0 d3e05e1e 585fc297 235b82b5 be8ff3ef ca67c598 52018192

Qy = b28ef557 ba31dfcb dd21ac46 e2a91e3c 304f44cb 87058ada 2cb81515 1e610046

http://arstechnica.com/security/2013/09/new-york-times-provides-new-details-about-nsa-backdoor-in-crypto-spec/



Content-/Dienste-Anbieter

(Google, Microsoft, Yahoo, etc)

"Das Netzwerk"

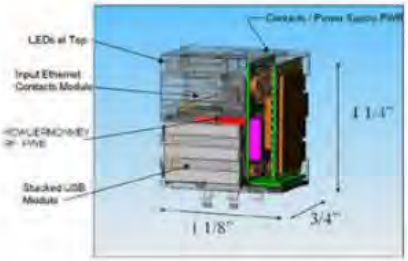
(Backbone Provider, Access Provider)

Endgerät

(User)

War das alles? - Leider nein...

- Manipulierte Bildschirmkabel für das "Mitlesen" der Bildschirminhalte via Radar
- SIM Toolkit Malware
- Abhören von GSM/UMTS Sprach- und Datenverkehr über Base-Station etc.
- Audio-Wanzen mit Exfiltration über Radar-Signale
- USB Keylogger über Radar ansteuerbar in der Tastatur, im Kabel oder USB-Port
- Ethernet-Wanzen im Ethernet-Port
- und noch einiges mehr...



Conclusio

Kein System ist 100% sicher
Aber auch kein physisches...

Jedes System kann gehackt werden
Der Aufwand macht den Unterschied...

Dark Fiber != automatisch sicher
Verschlüsselung auch bei internen Verbindungen

MitM Angriffe im großen Maßstab sind keine Theorie
Problematik Zertifikatsstrukturen / Root-CA's

"Big Data" ist auch für Angreifer ein Problem
Aber es existieren bereits erstaunliche Lösungsansätze

Angriffe auf Hardware/Router/etc. sind gänge Praxis
Insbesondere bei Providern als Basis weiterer Operationen

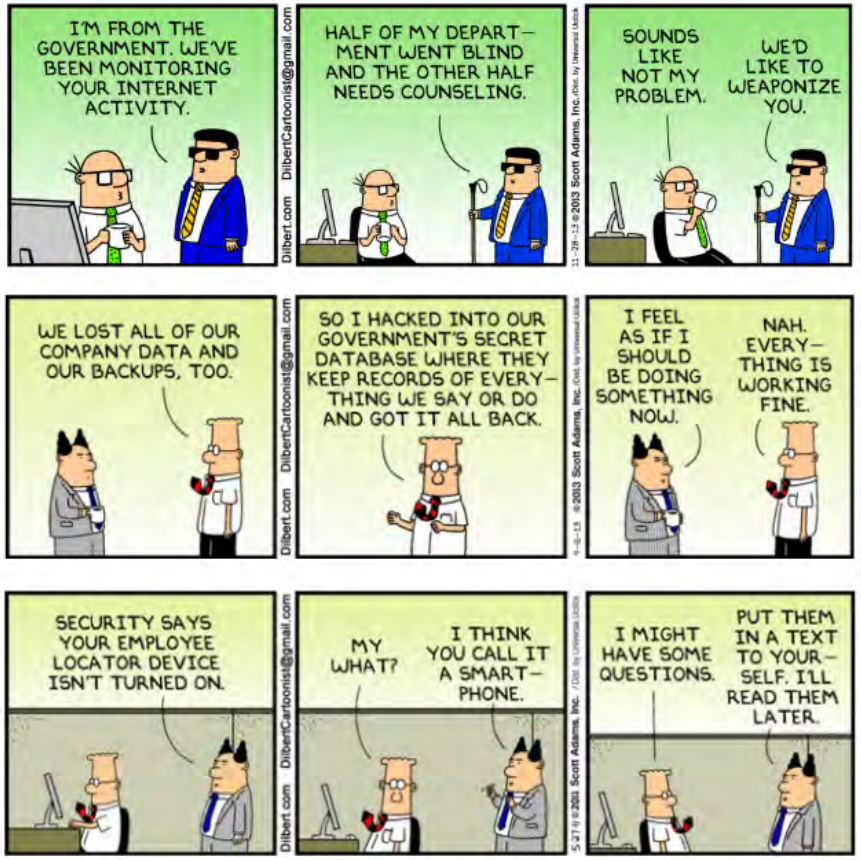
Danke für die Aufmerksamkeit!

Fragen?

Thomas Bleier

Dipl.-Ing. MSc zPM CISSP CEH CISM
Thematic Coordinator ICT Security
Safety & Security Department

thomas.bleier@ait.ac.at | +43 664 8251279
www.ait.ac.at/ict-security



http://www.dilbert.com/