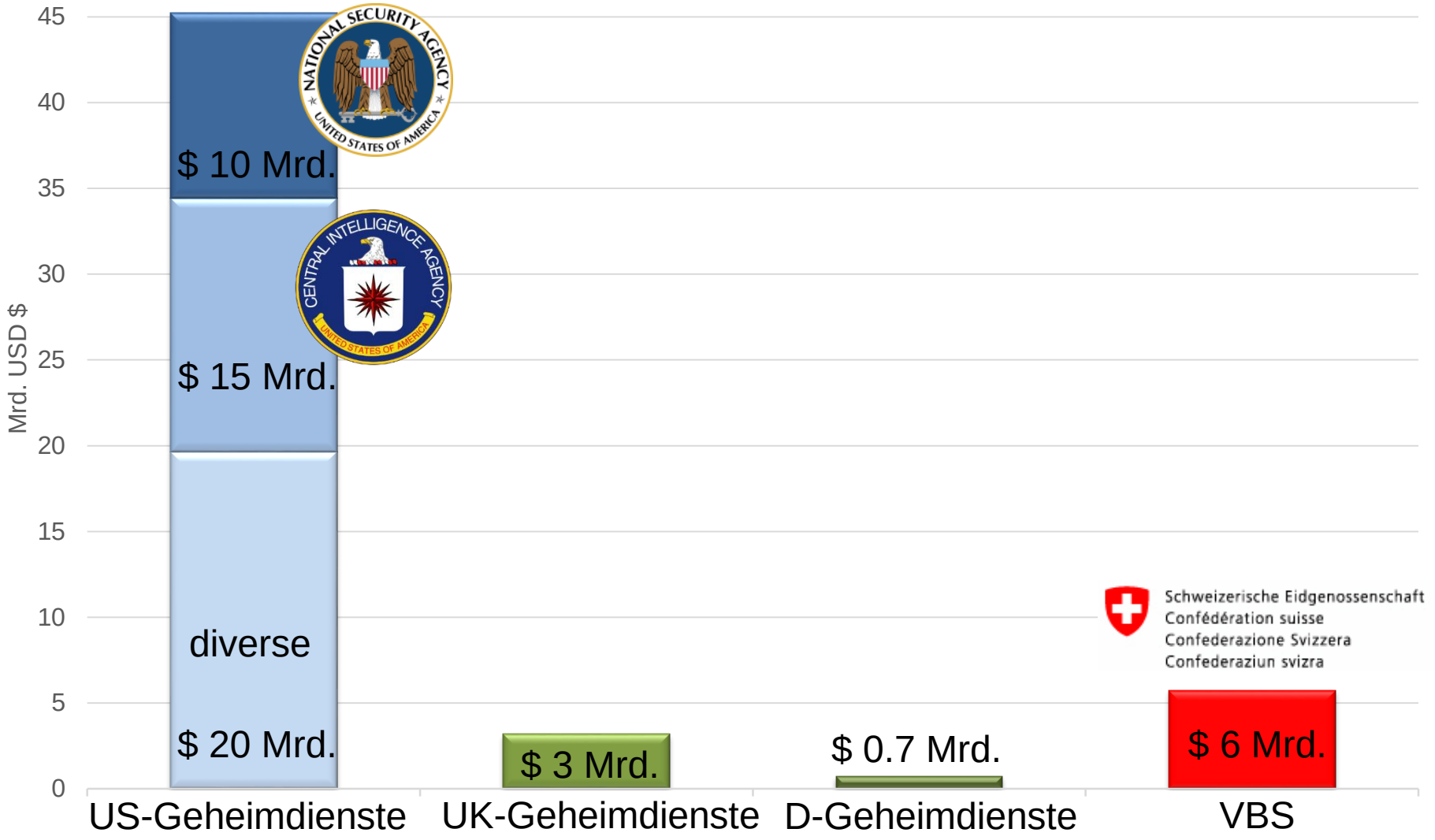
Cnlab / CSI Herbsttagung 2014

WER KANN SICH GEGEN DEN GEHEIMDIENST SCHÜTZEN?

Schlagwörter

- «Jeder Bürger landet im Netz der NSA»
- «Gegen die NSA kann man sich nicht schützen»
- «Das kann die NSA sowieso brechen»
- «Die NSA weiss alles über mich»

Budgets im Vergleich



Die grossen Programme von NSA und GCHQ

Angriffe auf Computer übers Internet

QUANTUM

PRISM

Firmen mit grossen Datenzentren werden gerichtlich zur Datenherausgabe gezwungen

Riesiges Rechenzentrum

Utah Data center

Brechen / Umgehen von Verschlüsselung, durch:
- Cryptanalysis
- Backdoors

BULLRUN
EDGEHILL

Abhören von Datenlinks zwischen grossen Datenzentren (Google, Yahoo, etc.)

MUSCULAR

Katalog mit ca. 50 Angreif-Produkten

ANT-Katalog
JTRIG-Katalog

NSA-Programm
GCHQ-Programm

Gesetzliche Grundlage elektronischer Überwachung (USA) (1/2)

Früher	Jetzt
Verfassung	**Verfassung** (aufgeweicht durch Verordnungen)
US-Verfassung (Fourth Amendement)	**F**oreign **I**ntelligence **S**urveillance **A**ct 1978 **U**niting and **S**trengthening **A**merica by **P**roviding **A**ppropriate **T**ools **R**equired to **I**ntercept and **O**bstruct **T**errorism Act 2001 **P**rotect **A**merica **A**ct 2007 (temporär) **F**ISA **A**mendment **A**ct 2008

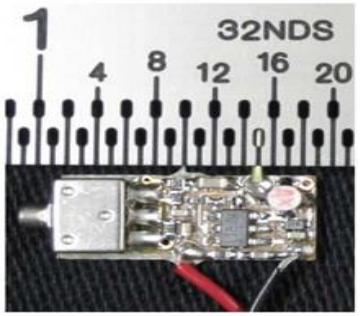
Gesetzliche Grundlage elektronischer Überwachung (USA) (2/2)

Früher	Jetzt
• Hinreichender Verdacht einer Straftat	• Wahrscheinlichkeit des Ziels ein «agent of a foreign power» zu sein – Non-US-Person – US-Person + Straftat – Ausl. Regierungsorganisation – Interessengruppen aus mehrheitlich non-US-Personen – Internationale Terrororganisation
• Durchsuchungsbeschluss eines Gerichts	• Mit/ohne Durchsuchungsbeschluss eines geheimen Gerichts • Gerichtsentscheid (2014): Geographischer Ort der Datenträger ist irrelevant

ANT-Katalog

Angriffe auf Router und Firewall

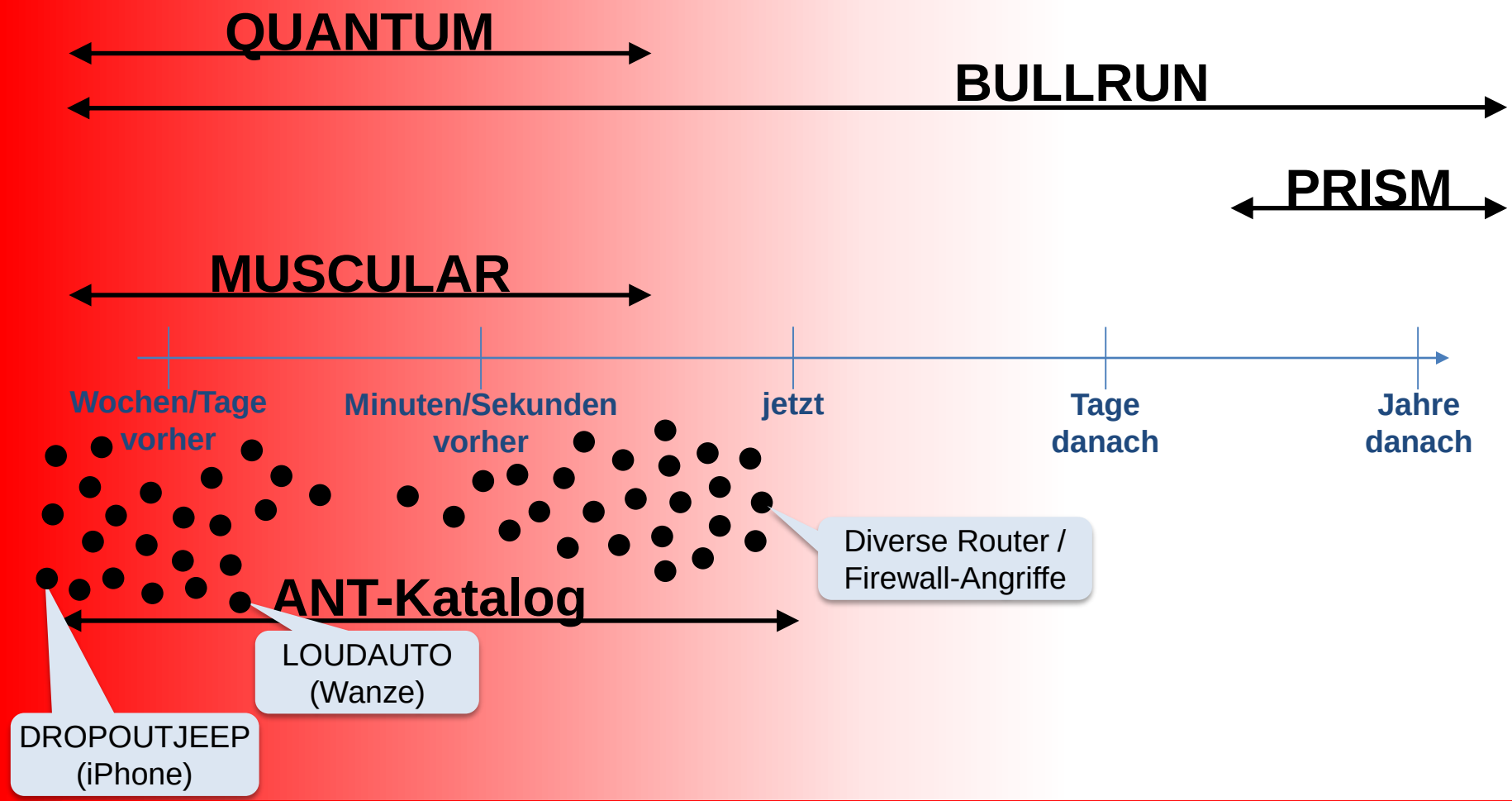
LOUDAUTO: Wanze



DROPOUTJEEP: iPhone-Spyware
Ferngesteuertes Herauf- und Herunterladen von Dateien, SMS, Kontaktlisten, Telefonbeantworternachrichten, Ort; Wanzenfunktion, Kamera-bilder auslösen, Ort des Funkturms.
Kontrolle per SMS oder Datenverbindung

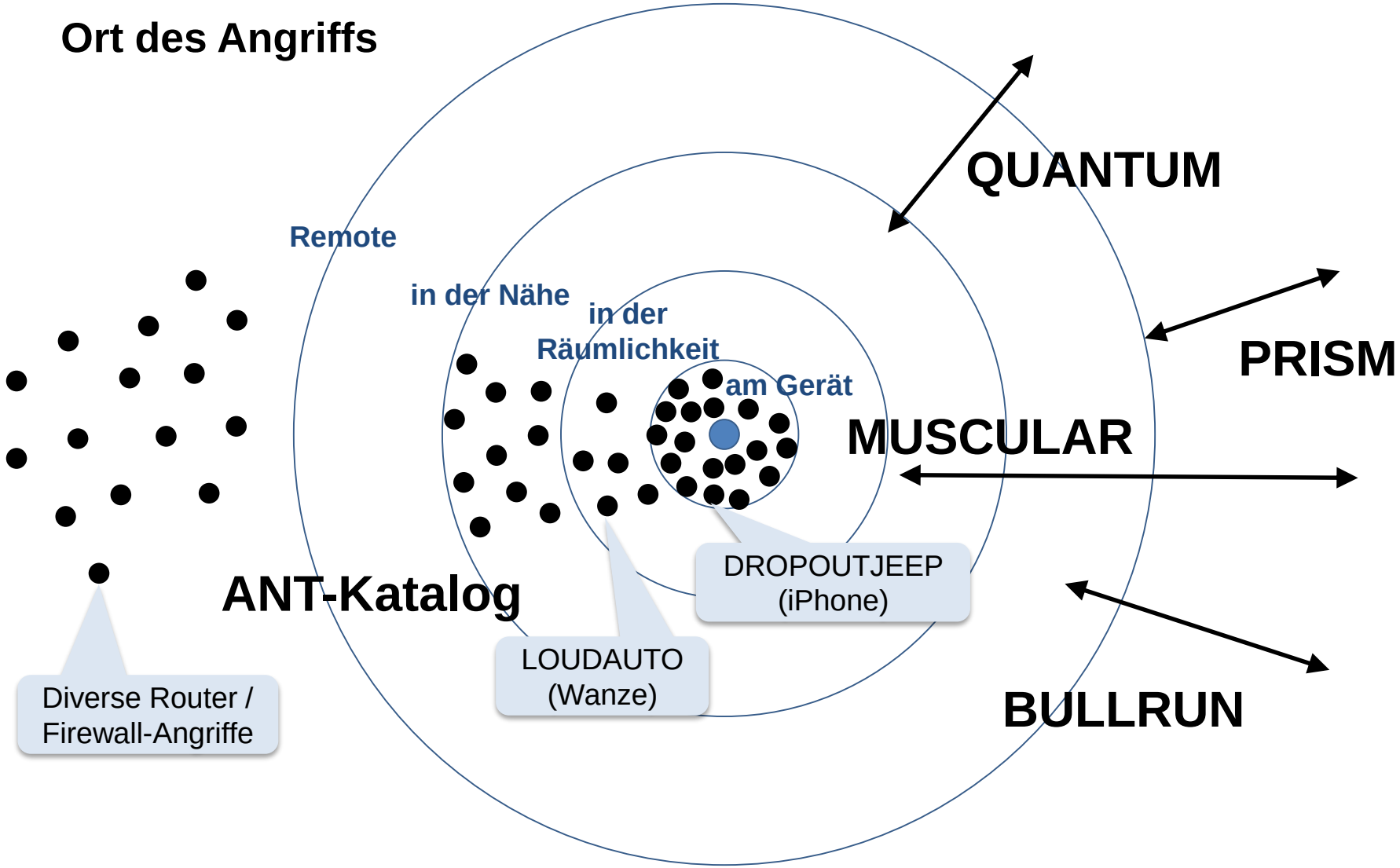
Name	Cost	Hardware / Software	Short description	Target System	prep. required	phys.acc. to device for prep.	phys.acc. to location for prep.	phys.acc. to device during event	phys.acc. to location during event
DEITYBOUNCE	0	Software	Persist other attack	Dell PowerEdge serv	yes	no	no	no	no
IRONCHEF	0	Software	Persist other attack	HP server	yes	yes	no	no	no
FEEDTROUGH	0	Software	Persist other attack	Juniper Netscreen fir	yes	(no)	no	no	no
GOURMETTROUGH	0	Software	Persist other attack	Juniper firewalls	yes	(no)	no	no	no
HALLUXWATER	0	Software	Persist other attack	Huawei Eudemon fire	yes	(no)	no	no	no
JETPLOW	0	Software	Persist other attack	Cisco, ASA firewalls	yes	no	no	no	no
SOUFFLETROUGH	0	Software	Persist other attack	Juniper firewalls	yes	no	no	no	no
HEADWATER	0	Software	Persist other (backdoor) attack	Huawei routers	yes	no	no	no	no
SCHOOLMONTANA	0	Software	Persist other (DNT implant) attack	Juniper router	yes	(no)	no	no	no
SIERRAMONTANA	0	Software	Persist other attack	Juniper	yes	(no)	no	no	no
STUCCOMONTANA	0	Software	Persist other attack	Juniper	yes	(no)	no	no	no
CTX4000	na	Hardware	tragbare Radarstation	-	yes	no	yes	no	yes
LOUDAUTO	30	Hardware	Wanze	-	yes	no	yes	no	yes
NIGHTSTAND	na	Hardware	Wireless Abhör- und Injectiontool, insbesondere a	IE 5-6	yes	no	yes	no	yes
NIGHTWATCH	na	Hardware	PC zum Darstellen von Video (zB zum darstellen vo	-	yes	no	no	no	yes
PHOTOANGLO	40000	Hardware	tragbare Radarstation (Nachfolger von CTX4000)	-	yes	no	yes	no	yes
SPARROW ii	6000	Hardware	Wireless Abhörsystem	-	yes	no	yes	no	(no)
TAWDRYYARD	30	Hardware	Radar-Reflektor zum Orten des Geräts	-	yes	yes	no	no	yes
GINSU	0	Software	Persist other attack (BULLDOZER). Triggered reboot	Microsoft Windows	yes	yes	no	no	no
HOWLERMONKEY	750	Hardware	Funkstation. Wird zusammen mit einem "digital core" zum Abhören ver		yes	yes	no	no	yes
IRATEMONK	0	Software	Persist other attack	Western Digital, Seag	yes	no	no	no	no
JUNIORMINT	na	Hardware			yes	yes	no	no	no
MAESTRO ii	3500	Hardware			yes	yes	no	no	no
SOMBERKNAVE	50000	Software	Wireless software implant, provides covert interne	Windows XP	yes	(yes)	no	no	no
SWAP	0	Software	software application persistence	Windows, Linux, Free	yes	no	no	no	no
TRINITY	6250	Hardware		-	yes	yes	no	no	no
WISTFULTOLL	0	Software	Plugin um forensische Infos zu extrahieren	Microsoft Windows 2	yes	no	no	no	no
SURLYSPAWN	30	Hardware	radar-retroreflektor, liest z.B. die Verbindung von der Tastatur und kann		yes	yes	no	no	yes
DROPOUTJEEP	0	Software	iPhone software implant: remotely pull/push files	iPhone	yes	yes	no	no	no
GOPHERSET	0	Software	Telefon- und Kontaktdaten Spyware für Smartphone über SIM Toolkit		yes	no	no	no	no
MONKEYCALENDAR	0	Software	Geolocation-Daten Spyware für Smartphone via Sim-Tool-kit		yes	no	no	no	no
PICASSO	2000	Hardware	Abgeändertes Mobiltelefon. Mikrophon abhören, l	Eastcom, Samsung	yes	yes	no	no	no
TOTECHASER	na	Software	GPS, GSM Geolocation, call log, contact list etc Date	Thuraya 2520 phone	yes	yes	no	no	no
TOTEGHOSTLY 2.0	0	Software	Windows Phone software implant: remotely pull/p	Windows Mobile	yes	yes	no	no	no
CANDYGRAM	40000	Hardware	fake cell tower	-	yes	no	no	no	yes
CROSSBEAM	40000	Hardware	GSM communications module: receive GSM voice, record voice data, tra		yes	yes	no	no	no
CYCLONE Hx9	70000	Hardware	Network in a box system		yes	no	no	no	yes
EBSR	40000	Hardware	GSM base station		yes	no	no	no	yes
ENTOURAGE	70000	Hardware	Direction finding application, line of bearing for GSM/UMTS/CDMA2000/		yes	no	no	no	yes
GENESIS	15000	Hardware	Mobiltelefon für Netwerküberwachung und -aufzeichnung, Handset loc		yes	no	no	no	yes
NEBULA	250000	Hardware	Base station router, network in a box		yes	no	no	no	yes
TYPHON HX	na	Hardware	GSM base station router, network in a box: find fix and finish targeted ha		yes	no	no	no	yes
WATERWITCH	na	Hardware	Hand held finishing tool: geolocation of targeted handsets in the fields		yes	no	no	no	yes
COTTONMOUTH-I	20300	Hardware	USB hardware implant: wirelss bridge into target network, load exploit s		yes	yes	no	no	no
COTTONMOUTH-II	4000	Hardware	USB hardware implant: covert lin into targets network		yes	yes	no	no	no
COTTONMOUTH-III	24960	Hardware	USB hardware implant: wirelss bridge into target network, load exploit s		yes	yes	no	no	no
FIREWALK	10.74	Hardware	Ethernet network implant: collect ethernet network traffic, inject ether		yes	yes	no	no	yes
RAGEMASTER	30	Hardware	RF retro-reflector in a VGA-cable: shows what is displayed on the monit		yes	yes	no	no	yes

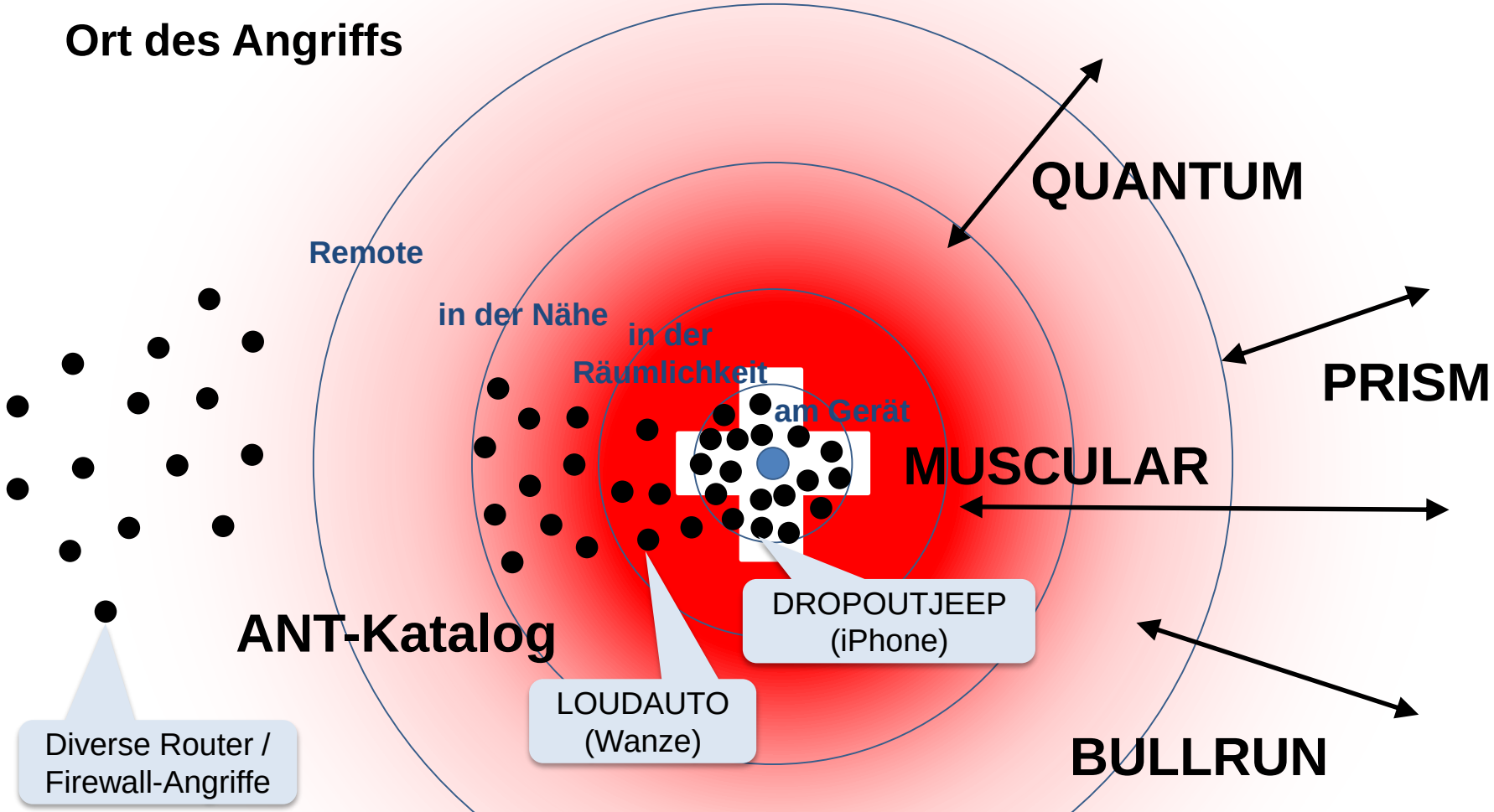
Zeitpunkt des Angriffs



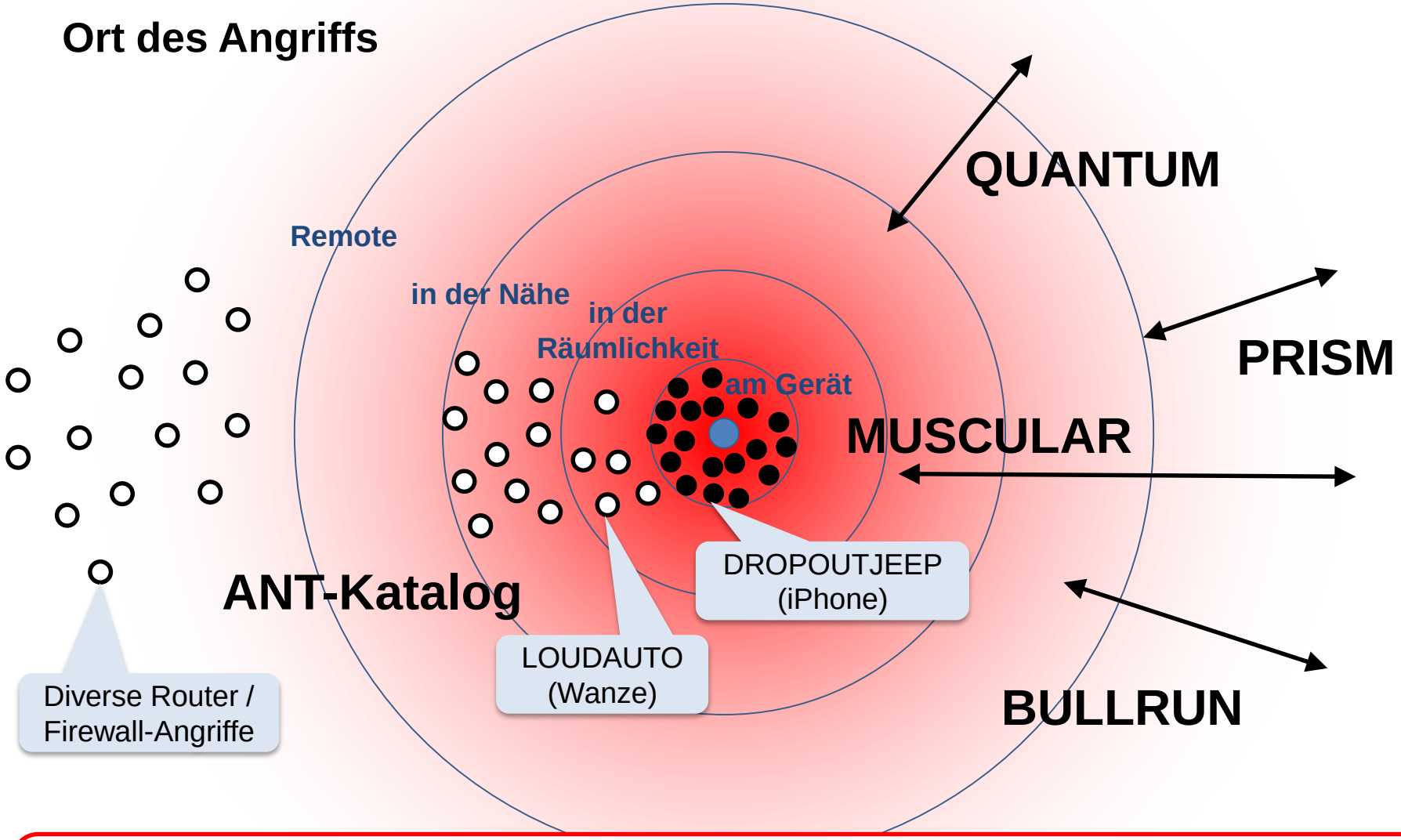
- Angriffe welche Vorbereitung benötigen, sind kostspieliger
- Alle «Produkte» des ANT-Katalogs benötigen Vorbereitung

Ort des Angriffs





- Angriffe welche Zugang zum Gerät / Location benötigen, sind kostspieliger
- Cloud → Verschiebung des Ortes → Kostenverschiebung
- «Ort» der Cloud ist wichtig



- Herstellungsort → Verschiebung des Ortes für Vorbereitung → Kostenverschiebung
- «Ort» der Herstellung ist wichtig

Gute Crypto hält

- Snowden «Gute Crypto hält»
- Anerkannte Standard-Algorithmen (z.B AES, RSA) und genügend lange Schlüssel
  (http://www.keylength.com: z.B. 128 Bit AES und 2’048 Bit RSA)

- Marginale Crypto: kann nicht als sicher angenommen werden
- Aber: Crypto-Systeme können «bypassed» werden
  Beispiel: ungeeignete Wahl von EC, schlechte Random Number Generatoren

Wie kann man sich schützen? (1/2)

Was kann die NSA nicht?

- Unbeschränkte Mittel einsetzen (Finanzen, Rechenleistung, Man-Power)
- «Gute» Crypto brechen

Welche Massnahmen sind wirksam?

- HW und SW von vertrauenswürdigen Herstellern
- Geeignete geografische Positionierung der Systemteilnehmer
- Geeignete geografische Positionierung der Datenspeicher
- «gute» Crypto (Datenspeicherung, Datenübertragung)
- Starke Authentisierung
- Starker Perimeter-Schutz (Netzwerk- und Anwendungsstufe)

Wie kann man sich schützen? (2/2)

- Komplexe Gesamtsysteme können immer angegriffen werden, es ist nur eine Frage des Aufwandes.
- Teilsysteme zu sichern lohnt sich, der Aufwand für die Geheimdienste wird dadurch erhöht.

Danke

Christian Birchler
christian.birchler@cnlab.ch
+41 55 214 33 33

Esther Hänggi
esther.haenggi@cnlab.ch
+41 55 214 33 36