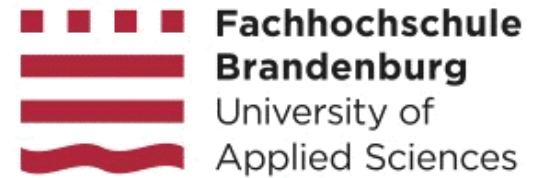




Forum
InformatikerInnen für
Frieden und gesellschaftliche
Verantwortung e.V.



Ingo Ruhmann

New Approaches to Arms Control in Cyber Conflicts

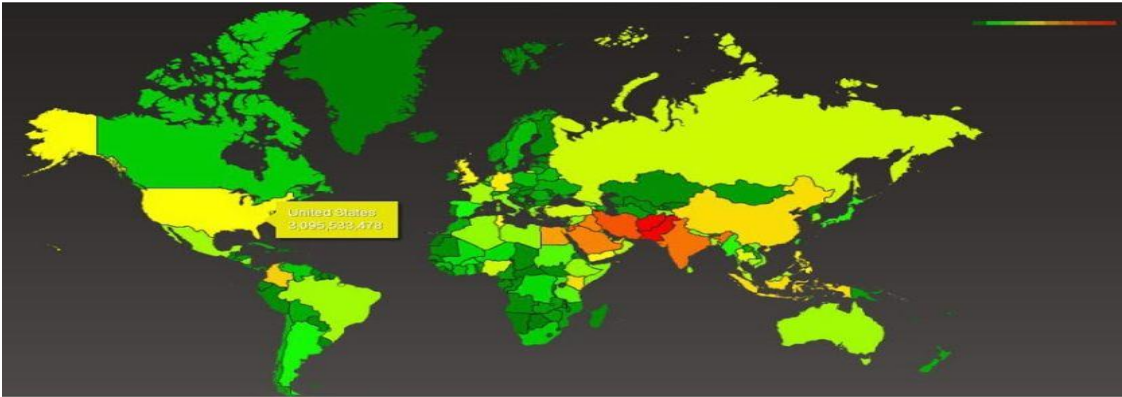
International Pugwash Workshop
Berlin, 24th Oct. 2015

- 1. Lesson from the „Snowden Revelations“**
- 2. Cyber Arms – from Noticing to Detection**
- 3. Comprehensive Sourcing**
- 4. Applying Established Mechanisms of Arms Control**

The reception: a surveillance debate



- 1. Surveillance of telecommunications: globally, automated, attempting a „full take“
- 2. Co-operation with agencies and commercial players (service providers – based on compensation, by law or unwittingly)
- 4. Monitoring metadata and content; organization in elaborate data bases
- 5. Against friend and foe



The fact: Revelation of Cyber War tools

1. „Digital Network Intelligence Exploitation“ := Manipulation of Computer Systems

What is XKEYSCORE?




1. **DNI Exploitation System**/Analytic Framework
2. Performs strong (e.g. email) and soft (content) selection
3. Provides real-time target activity (tipping)
4. "Rolling Buffer" of ~3 days of ALL unfiltered data seen by XKEYSCORE:
 - Stores full-take data at the collection site – indexed by meta-data
 - Provides a series of viewers for common data types
1. Federated Query system – one query scans all sites
 - Performing full-take allows analysts to find targets that were previously unknown by mining the meta-data

Attack functionality of XKeyScore was first recognized in Report PE 474.405 by the EU-KOM, Sept. 2013.

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

Technology Detection



- Show me **all the VPN startups** in country X, and give me the data so I can **decrypt** and discover the users
 - These events are easily browsable in XKEYSCORE
 - **No strong-selector**
 - XKEYSCORE extracts and stores authoring information for many major document types – can perform a retrospective survey to trace the document origin since metadata is typically kept for up to 30 days
 - **No other system** performs this on raw unselected bulk traffic, **data volumes prohibit forwarding**

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

Noticing Cyber Arms

We recognize prehistoric weapons systems and defense installations.
Do we recognize cyber arms?



Source: wikipedia.de

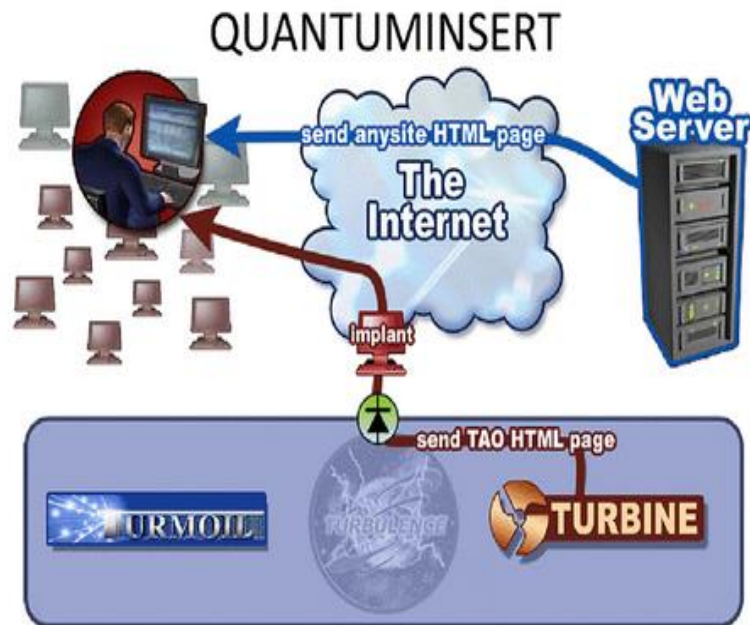


XKeyScore – an automated intelligence and attack system

- Agents scan data base for communications properties - language, location, communications medium
- Automatic background analysis of properties and weaknesses of the target system
- Uses „Plug-Ins“
 - **Constant Web data base** for known weaknesses and exploits
 - Tools to **decrypt** communication (VPN)
 - Automated tools for **malware insertion**
- Collects attack paths by collecting **Windows Error Reports** of target system
- Continuous addition of automated attack tools

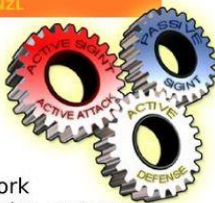
XKeyScore is the core of an integrated cyber weapon along the cycle of reconnaissance – decision – operation – damage assessment

TS//REL



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

QUANTUMTHEORY



- (TS//SI//REL) Extremely powerful CNE/CND/CNA network effects are enabled by integrating our passive and active systems:
 - Resetting connections (QUANTUMSKY)
 - Redirecting targets for exploitation (QUANTUMINSERT)
 - Taking control of IRC bots (QUANTUMBOT)
 - Corrupting file uploads/downloads (QUANTUMCOPPER)
- (TS//SI//REL) QUANTUMTHEORY dynamically injects packets into a target's network session to achieve CNE/CND/CNA network effects.
 - Detect:** TURMOIL passive sensors detect target traffic & tip TURBINE command/control.
 - Decide:** TURBINE mission logic constructs response & forwards to TAO node.
 - Inject:** TAO node injects response onto Internet towards target.
- (TS//SI//REL) The propagation delay from tip-to-target determines the success rate of the network effect. **Less Latency = More Success!**

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

XKeyScore is one attack tool amongst many

Others scan communication content (**TURMOIL**) and modify data transmissions (**TURBINE**)

Quantumtheory

Elaborate tool set for „man in the middle“-attacks: Rerouting of data traffic to implant malware

The BELGACOM attack (of GCHQ)

- Customized attack on data communication of BELGACOM system administrators by rerouting them to faked web sites
- Inserting malware (trojan, key logger)
- Stealing password and system data
- Exploiting the data in attacks on IT systems of the EU-Commission

2005-2007 alone, the NSA spent \$ **2 bn.** for projects named

- **“Trailblazer”** for bulk data collection and
- **“Turbulence”** for selective control of Internet intersections, web traffic surveillance and selective modification of data packets

Project work was redirected and has since been adapted for PRISM / XKeyScore

The screenshot shows a web browser window with multiple tabs. The active tab is titled 'Turbulence Nsa | Costly NSA initiative ha...'. The address bar shows the URL 'articles.baltimoresun.com/2007-02-11/news/0702110034_1_turbulence-cyberspace-nsa'. The page features the Baltimore Sun logo and a navigation menu with links to HOME, NEWS, LOCAL, SPORTS, RAVENS, BUSINESS, ENTERTAINMENT, LIFE, HEALTH, OPINION, MARKETPLACE, and SERVICES. Below the menu, a breadcrumb trail reads 'Home → Collections → Cyberspace'. The main headline is 'Costly NSA initiative has a shaky takeoff' in a large, bold, blue font. Below the headline, a sub-headline reads 'Vexing snags for cyberspace tool 'Turbulence' Sun Exclusive'. The byline, 'February 11, 2007 | By Siobhan Gorman | Siobhan Gorman, Sun Reporter', is circled in red. The article text begins with 'WASHINGTON -- An expensive National Security Agency initiative to search the world's communication networks for security threats is hitting early but significant snags, prompting intelligence officials and lawmakers to raise questions about its funding and its future.' and continues with 'Dubbed "Turbulence," the NSA's ambitious effort is part bloodhound and part attack dog. It attempts to continuously troll cyberspace to sniff out threats from terrorists and others, then rapidly tip off analysts who can mobilize defenses. With the potential to be a powerful anti-terror weapon, it has become NSA Director Lt. Gen. Keith B. Alexander's top priority.'

The NSA files | World news | The Guardian x Turbulence Nsa | Costly NSA initiative ha... x +

articles.baltimoresun.com/2007-02-11/news/0702110034_1_turbulence-cyberspace-nsa

Google

THE BALTIMORE SUN

HOME NEWS LOCAL SPORTS RAVENS BUSINESS ENTERTAINMENT LIFE HEALTH OPINION MARKETPLACE SERVICES

Home → Collections → Cyberspace

Costly NSA initiative has a shaky takeoff

Vexing snags for cyberspace tool 'Turbulence'
Sun Exclusive

February 11, 2007 | By Siobhan Gorman | Siobhan Gorman, Sun Reporter

WASHINGTON -- An expensive National Security Agency initiative to search the world's communication networks for security threats is hitting early but significant snags, prompting intelligence officials and lawmakers to raise questions about its funding and its future.

Dubbed "Turbulence," the NSA's ambitious effort is part bloodhound and part attack dog. It attempts to continuously troll cyberspace to sniff out threats from terrorists and others, then rapidly tip off analysts who can mobilize defenses. With the potential to be a powerful anti-terror weapon, it has become NSA Director Lt. Gen. Keith B. Alexander's top priority.

f Like

Submit

„physical access “ to enemy computers - a tactic with a long history

Spying and Sabotage by Computer

The U.S. and its adversaries are tapping data bases—and spreading viruses

BY JAY PETERZELL

In early 1981, National Security Agency officials working at an intelligence facility in suburban Washington made an alarming discovery: someone had made off with a sizable haul of classified information. The thief did not jimmy open a window at the well-guarded site; instead, he gained access to a "secure" cable leading into the facility and was able to trespass electronically. NSA officials believed the breach was the work of an East bloc spy agency.

If so, it was not the only one. A previously undisclosed series of high-tech espionage coups have been achieved by both sides. "Foreign intelligence services have gained access to classified information in U.S. computers by remote means," a former senior Government computer expert told TIME. "And we have done the same thing to them."

Last week the U.S. arrested and then expelled a Soviet military attaché for allegedly trying to steal details of computer-security programs. The incident, as well as the arrest earlier this month of three West German computer hackers suspected of spying for the Soviet Union, highlighted the extent to which rival intelligence agencies are scrambling to devise ways to penetrate one another's security systems.

A number of current or former officials say U.S. intelligence agencies have had considerable success in penetrating classified military computer systems in the Soviet Union and other countries. The rule, explains one expert, is that "any country whose sensitive communications we can read, we can get into their computers." Breaches of some Soviet computers were done not by cracking codes but by physically breaking into Soviet military facilities, sources said.

Both the NSA and CIA have also "experimented" with the disruption of other nations' computers by infecting them with viruses and other destructive programs, according to some sources. But there is said to be concern in the intelligence community that these disruption operations could go too far and lead to retaliation.

The military's growing reliance on linked computer networks for battle management and command and control increases the danger of catastrophic sabo-

tage by a hostile insider. That's why some U.S. security officials lie awake at night imagining scenarios like these:

► An enemy agent in the Pentagon sends a computer virus through the World-Wide Military Command and Control System, which U.S. commanders would rely on in wartime for information and coordination. The virus sits undetected. When hostilities begin, the agent sends a message that triggers the



U.S. troops field-testing some portable hardware

A series of high-tech espionage coups have been achieved by both sides

virus erasing everything in the system. A different virus is introduced into NATO's logistics computers. Triggered just as the Soviet army marches into West Germany, the virus alters messages so that all allied supplies are sent to the wrong places. By the time the mistake is corrected a day or two later, key parts of NATO's defense line have collapsed.

Officials differ about the likelihood that such sabotage could be carried off. But the damage that can be caused by a virus was dramatically illustrated last November, when computer hacker Robert Morris injected a bug into an unclassified

Defense Department computer network, Arpanet. The virus reproduced wildly and brought research computers nationwide to a halt. "If someone at NORAD [North American Aerospace Defense Command] wanted to do what Robert Morris did at Arpanet, he could cause a lot of damage," says Stephen Walker, former Pentagon director of information systems. A retired senior military computer-security expert goes even further: "The potential for offensive use of viruses is so great that I would have to view the power and magnitude as comparable with that of nuclear or chemical weapons."

With all this in mind, the Government has in recent years stepped up efforts to ensure that all sensitive computers that have links to other systems are adequately protected by encoding equipment. In addition to guarding against assaults by hostile intelligence agencies, this improved encryption program appears to have ended, at least for now, the ability of amateur computer hackers to breach secure military systems.

The KGB does, however, consider hackers an asset in its search for weak points. The West German hackers arrested last month are believed to have broken into some 30 unclassified U.S. defense computers and tried to enter 420 others. According to Clifford Stoll, a computer expert at Harvard who followed their activities for almost a year, they seemed to be assembling a "map" of links between U.S. defense computers and systematically seeking out "unauthorized gateways" into classified systems. Such gateways are created when a computer user has access to both secure and unclassified networks and is careless about keeping them separate. The hackers never did get access to classified information. The reconnaissance

they gave the Soviets cannot be fully exploited until the KGB recruits an insider with access to a computer at one of the installations on the hacker's map.

In other words, as in *Reilly: Ace of Spies*, there is no substitute for man on the scene. The relative success of computer-security officials in frustrating outside attacks has turned attention to the more serious threat from insiders—people who have authorized access to defense computers and who sell their services to a foreign government. Such an agent could do enormous damage, either as a spy or a saboteur. "There is a threat, and it's real,"

„Breaches of some Soviet computers were done not by cracking codes but by physically breaking into Soviet military facilities“

„Both the NSA and CIA have also „experimented“ with the disruption of other nation's computers by infecting them with viruses or other destructive programs.“

TIME, 20.03.1989

SPIEGEL ONLINE **POLITIK**

Login | Registrierung

Nachrichten > Politik > Deutschland > XKeyscore > BND und BfV setzen NSA-Spähprogramm XKeyscore ein

Schnüffelsoftware XKeyscore: Deutsche Geheimdienste setzen US-Spähprogramm ein



BND-Zentrale in Pullach: "Fleißigster Partner" der US-Geheimdienste

REUTERS

Angela Merkel und ihre Minister wollen erst aus der Presse von den Spähprogrammen der US-Regierung erfahren haben. Doch nach Informationen des SPIEGEL nutzen deutsche Geheimdienste eines der ergiebigsten NSA-Werkzeuge selbst.

1 Samstag, 20.07.2013 – 18:00 Uhr

Drucken | Senden | Merken

Nutzungsrechte | Feedback

Kommentieren | 835 Kommentare

Hamburg - Der deutsche Auslandsgeheimdienst BND und das im Inland operierende Bundesamt für Verfassungsschutz (BfV) setzen eine Spähsoftware der amerikanischen NSA ein: XKeyscore. Das geht aus geheimen Unterlagen des US-Militärgeheimdienstes hervor, die der

Ignorance or concealment?

XKeyScore, a tool in German hands

The nuclear disarmament debate

- in 1958 civil physicists began to elaborate ways to verify an atomic test ban
- In 1976, an expert group was tasked with developing verification mechanisms for a nuclear test ban treaty , producing results in 1989
- In 1996 the test ban treaty was ratified
- In 1999 a verifications regime made of 170 seismic stations was installed

In Cyber Warfare

- since 1989 has seen a steady refinement of cyber attack tactics
- since 2007 explicitly and since 2013 in detail specific cyber weapons have been reported – without them being classified as such
- civilian IT security experts collect data on cyber arms and infrastructures; however, the analytic frame is lacking
- it is only debated about proliferation and containment of IT security tools instead of cyber arms
- will there possibly be a verification regime in 2029 – after 40 years of debate???

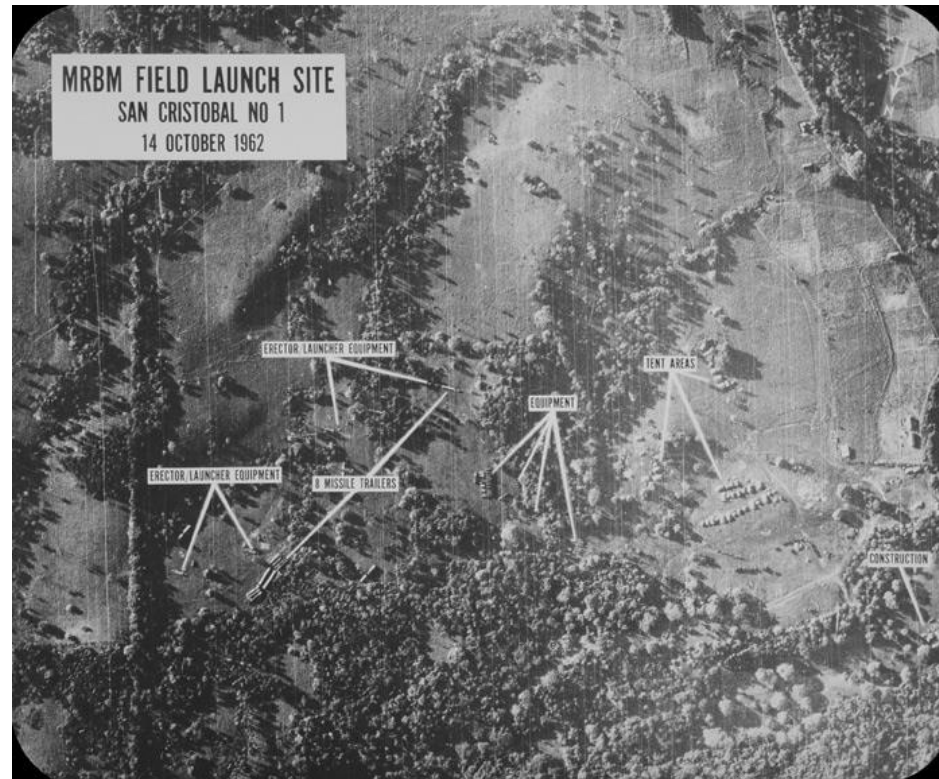
... we seem to have a perception deficit!

Comprehensive Sourcing

For conventional arms, we have highly developed reconnaissance tools at our disposal. Where are those for cyber arms?

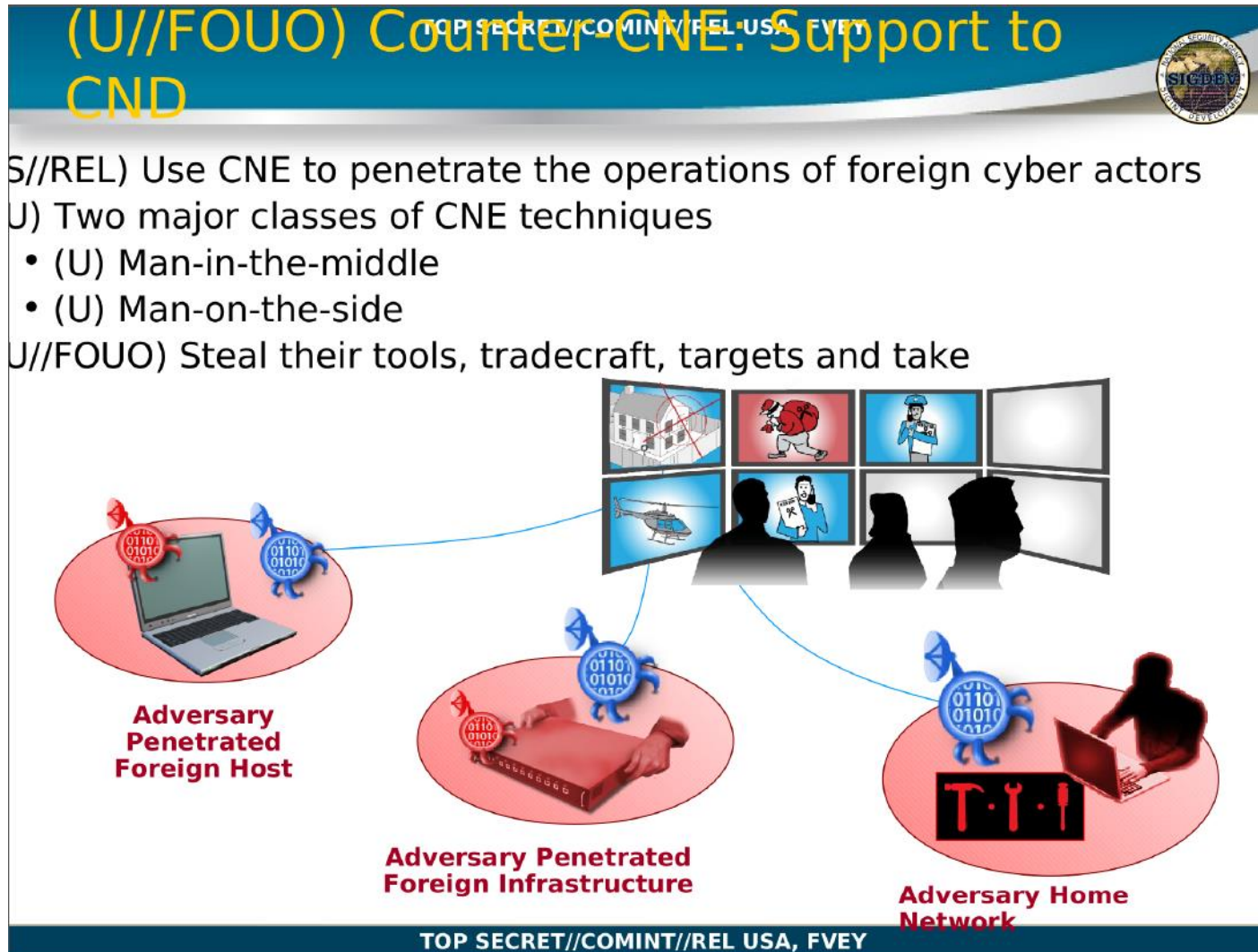
Are all available data and information used and exploited?

Which reconnaissance systems for cyber arms are under development?



Aerial reconnaissance in Cuba crisis
Source: wikipedia.de

Counter espionage: TRANSGRESSION, 3rd und 4th Party Collection



TRANSGRESSION is a program with specialized tools to penetrate an adversary's IT systems to collect and falsely plant data on these IT systems.

Whoever runs the program needs detailed knowledge on an adversary's

- Departement structure
- Tasks
- Infrastructures
- Access paths

3rd und 4th Party Collection: TRANSGRESSION



XKEYSCORE:

A Critical TRANSGRESSION Tool



- Over 50 daily workflows
 - SIGINT and POLARSTARKEY (NetDef)
- Fingerprints and Microplugins
- GUI Workflows and Webservice

TOPSECRET//COMINT//REL TO USA, FVEY

Transgression

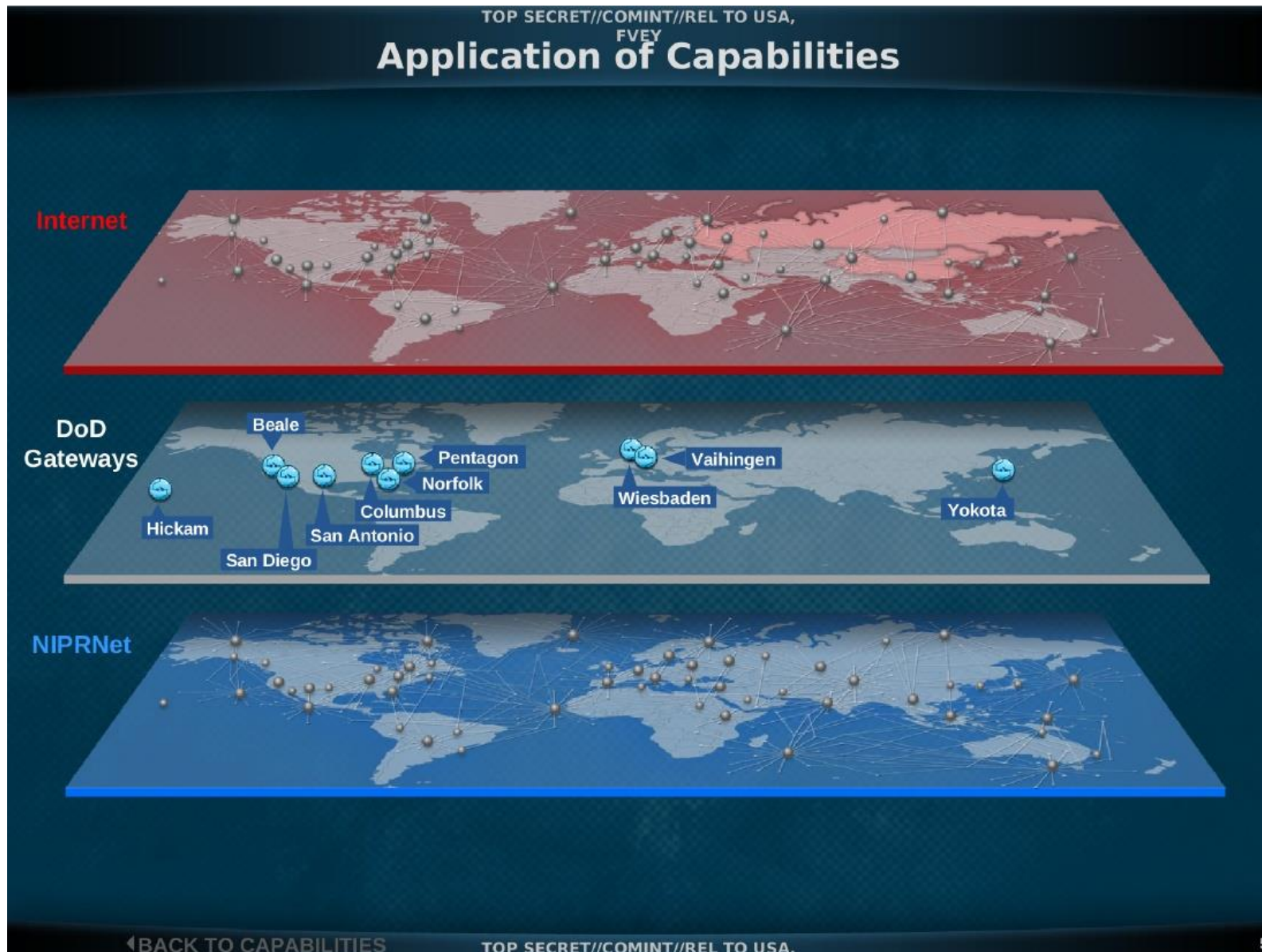
Collects espionage results from adversaries especially about IT systems, the adversary has "reaped" for

- a) Counter espionage (knowledge about one's own weaknesses)
- b) Espionage on 3rd, 4th and 5th party
- c) Dumping compromising data, to produce false leads and redirect suspicion

Result:

Active knowledge on the cyber war infrastructures and tactics of many actors

3rd und 4th Party Collection: Gateways in Germany



Vast amounts of data pass through three sites outside the US.

Lesson 1

Cyber war actors are no phantoms (to each other)!

The knowledge of cyber warfare actors about their counterparts suffices to attack, steal data and lay false leads.

Lesson 2

Cyber warfare actors are dependent on infrastructures:

- a) public systems to intercept and manipulate,
- b) their own special infrastructures for special tasks.

All these infrastructures and their add-ons are visible to the (civilian) expert, who only lacks the know how and experience to interpret them.

1. Conclusion

In civil life there are sufficient hints for cyber warfare infrastructures. The services collect as much as knowledge as possible on cyber warfare structures of other actors.

Arms control has always rested on the comprehensive and systematic use of various kinds of knowledge resources.

Export controls – just a political instrument?

„Crypto Wars“

U.S. Export Administration Act

In 1983 restricting the delivery of UNIX software to Germany because of crypto algorithms

Wassenaar

- Crypto products still are dual use items
- Expanded export controls on strong cryptography (> 64 Bit, “for mass market use”).

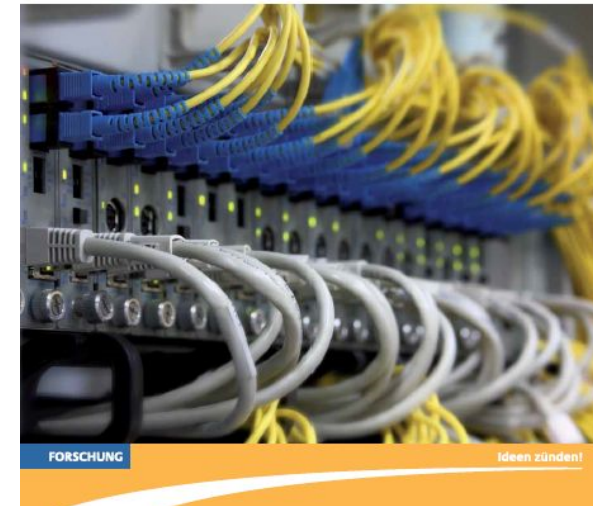
Problem: Timeliness

Export restricted are

- „**digital computers**“ with a peak performance of 0,75 TFLOPs (Nr. 4A003 b) – an ATI Radeon HD 3870 X2 graphics card performs at ~ 1 TFlop
- „**network equipment**“ with transmission rates of over 1,25 GByte/s“ (=10GBit) (Nr. 4A003 g) – 10 GBit network cards cost ca. 50 €
- Every single case of a **guest scientists’s work on super computers** has to comply with export control rules and may need authorization by the export control administration – otherwise may lead to criminal prosecution.



Supercomputer und Exportkontrolle
Hinweise zu internationalen wissenschaftlichen
Kooperationen



Export control – a political steering mechanism

Wassenaar export controls cover

- since 2012 surveillance systems,
- since 2013 also surveillance systems for IP networks and „Intrusion Software“ (like trojans).

„Controlled Exports“ equal exports under control of public authorities - leaving leeway in decision making as seen in conventional arms trade.

Lesson 3

Export control is a cumbersome instrument. Apparently however, it is deemed possible to classify cyber arms and subordinate them to a proliferation control.

WA-LIST (14) 2*
25-03-2015

THE WASSENAAR ARRANGEMENT

ON

EXPORT CONTROLS FOR CONVENTIONAL ARMS

AND

DUAL-USE GOODS AND TECHNOLOGIES

LIST OF DUAL-USE GOODS AND TECHNOLOGIES

AND

MUNITIONS LIST

* This version is a second corrigendum to the Control Lists (WA-LIST (14) 1 Corr.), to incorporate the amendment to ML10. Note 2 in the Munitions List.

Analysing Resources

NSA budget in 2013 for cyber warfare (excerpt from the budget proposal for US congress, incl. payment to third parties):

- **\$ 652 Mill.** for a program on **malware distribution**
- **\$ 10 Mill.** For the “**common cryptologic program**” on „groundbreaking crypto analytic capabilities [...], to exploit internet traffic“

In sum over \$ 12 bn. for internet surveillance, decryption and cyber attack tools

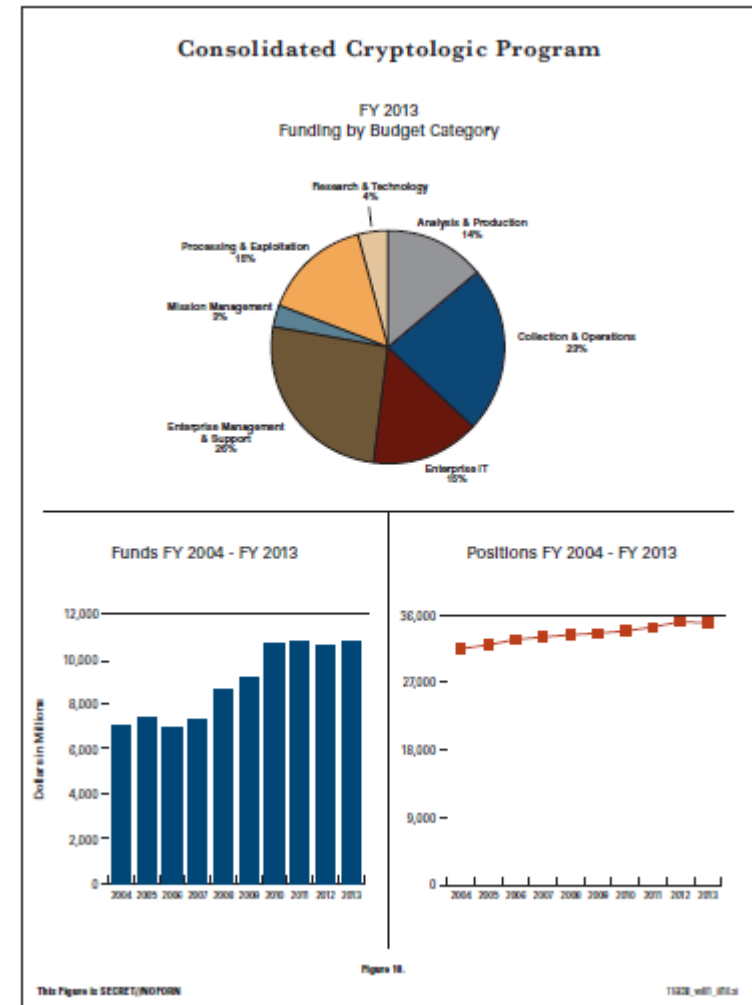
Personnell

NSA: > 35.000 employees

U.S. Cyber Command - from 2015 on: surge of 8.000 further soldiers and employees

FBI: 750 Cybercrime agents

TOP SECRET//SI//TK//NOFORN



Germany: broad view of the actors on cyber warfare

Personnel	genuine	additional (by new law)
State and national police	360	
State and national domestic Intelligence services	unavailable	175
IT Security and Crypto systems (BSI)	600	175
Of this:		
IT Security Monitoring Center (BSI):	„1 Expert 24 h on call “	
Cyber Defense Center (9 to 5 hours)	10	
21 CERTs (in the CERT network incl. CERTBw)	<150	
<u>Common activities (personnel is used in double roles – cannot be counted twice)</u>		
GIZ – Common Internet Center	51	
GTAZ - Internet Content monitoring on terror defense		
National authorities	198	
State authorities	31	

The “Defense” (including CERTBw, without doubles): Now to come

Internet Content Monitoring	280 + X (intell.)	
Civilian IT specialists	~ 1.000	1.250

The “Offensive side”

KSA	6.000	
-----	-------	--

Fin. Ressources

IT security
research
30 Mio. p.a.

BND upgrade
300 Mio.
(attack tools,
0-day Exploits)

Lesson 4

IT systems are „Force Multipliers“ – especially in cyber war. Data on force strength, financial and technical resources are at least as valuable for cyber war forces as with regard to conventional forces.

Lesson 5

Data on cyber war forces have been published since the 1990ies – a systematic accounting has so far been lacking.

Lesson 6

The “attack side” of government agencies have 6 to 10 times the resources at their disposal compared to the civilian “defense side”. With these force relations, “defenders” in cyber attacks have no chance.

2. Conclusion

Disarmament should take all cyber war resources into account.

Final Conclusion

Data and documents available today are a rich source for new approaches to arms control and disarmament in cyberspace. A consolidated approach of IT and arms control experts to monitor cyber war actors and their activities can lead to results similar to the limitations in nuclear, biological, and chemical weapons.

To Do's:

International Security Policy

- Conventions on civil co-operation without limits on behalf of intelligence and military
- Outlaw „cyber weapons“; no first use
- Expansion of emergency links between US, Russia (2013) and China (2015) into a multilateral framework
- Export control regulations and arms control conventions; verification by international bodies (“Cyber War Prevention CERTs” analog to CTBTO etc.)
- Limiting spying on and compromising of IT systems and their security mechanisms
- Systematic analysis of cyber war resources (analog to SIPRI data on conventional arms)

Technical

- Baseline study of compromised IT systems
- Resources for intensive development of IT security tools and systems
- Expansion of IT security centers (CERTs and others)
- Expand auditing of selected sectors (infrastructures)

Thank you for your attention!

Wer bedroht uns eigentlich?

3

