Forum
InformatikerInnen für
Frieden und gesellschaftliche
Verantwortung e.V.

Fachhochschule
Brandenburg
University of
Applied Sciences

Ingo Ruhmann

NSA, IT-Sicherheit und die Folgen:
Mitten im Cyberwar - was sind unsere Optionen?

GI SECMGT-Workshop

Frankfurt, 9.05.2014

1. Was macht die NSA (und ihre Kollaborateure)?
2. War das wirklich neu?
3. Exkurs: Information Warfare – definitorisches
4. Schlussfolgerungen

*Hinweis: Als **geheim** markierte Slides wurden aus rechtlichen Gründen entfernt, können aber im Internet gefunden werden.*

1. Was machen „die NSA“ und ihre Kollaborateure?

1. Rekonstruktion von Kommunikationsnetzen und -inhalten
2. „DNI Exploitation“ := Manipulation von Computersystemen

Slide „What is XKEYSCORE?“ (entfernt)
*-> 1. **DNI Exploitation System***

Siehe Folie auf Seite 2 (externer Link):
http://upload.wikimedia.org/wikipedia/commons/4/48/XKeyscore_presentation_from_2008.pdf

3. Entschlüsselung und Auswertung der Inhalte

Slide „Technology Detection“ (entfernt)
-> … all the VPN startups … decrypt …

Siehe Folie auf Seite 16 (externer Link):
http://upload.wikimedia.org/wikipedia/commons/4/48/XKeyscore_presentation_from_2008.pdf

4. Manipulation von Daten, IT-Systemen, Unterbinden von Kommunikation

Seit 1998 hackt sich das „**Office of Tailored Access Operations“ (TAO)** der NSA in IT-Systeme ein, oder weist Agenten bzw. Militärs vor Ort an, Systeme mit Hilfe „*physischen Zugangs*“ zu manipulieren.

Stuxnet

Zur Erinnerung.....

- Beobachtet seit 2009
- Umfangreiche Software (1,5 MB)
- Ziel sind SIMATIC Programmierbare Logik Controller (PLCs) der Fa. Siemens
- Erstverbreitung über **USB-Stick,** Weiterverbreitung im LAN bis ein Zielsystem und ein Web-Zugang gefunden sind
- Ausgeklügelte Installations- und Aktionsmechanismen mit gestohlenen Zertifikaten
- Ausnutzung von zwei Zero-Day-Exploits zur Installation
- Rootkit-Funktion auf dem Zielrechner
- Erreicht Ende Sept. 2010 eine Ausbreitung von ca. 100.000 Systemen
- Gegenmaßnahmen erschwert durch Hard-Coding von Passworten, Defiziten in Authentisierungsmechanismen

http://www.aisec.fraunhofer.de/content/dam/sitmuc/en/pdf/studien/studie_stuxnet.pdf
http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf

Zur Erinnerung....

Flame

- Toolkit für Angriffe, Backdoor-Trojaner
- Entdeckt 2012, **entwickelt seit 2008**
- Verbreitet sich nach Erstinfektion über das lokale Netz
- **Verbreitungsmodul identisch zu Stuxnet**
- Nutzt Windows Update und **gefälschte Zertifikate** zur Verbreitung
- Zweck: Mitschneiden von Netzverkehr, Eingaben, Daten, etc.

miniFlame

- Entdeckt 2012
- Zielgerichteter **Trojaner** (vergleichbar zu „Staatstrojaner“) **gegen Einzelziele**, etabliert eine Backdoor auf dem Zielsystem
- Basiert auf Flame

Duqu

- Beobachtet seit Sept. 2011
- Ausgeklügelte Installations- und Aktionsmechanismen mit gestohlenen Zertifikaten
- Ausnutzung von Zero-Day-Exploits zur Installation
- Zweck: Datensammlung (Dateisammlungen, Keylogger)
- Command & Control-Server von Duqu auch in Deutschland

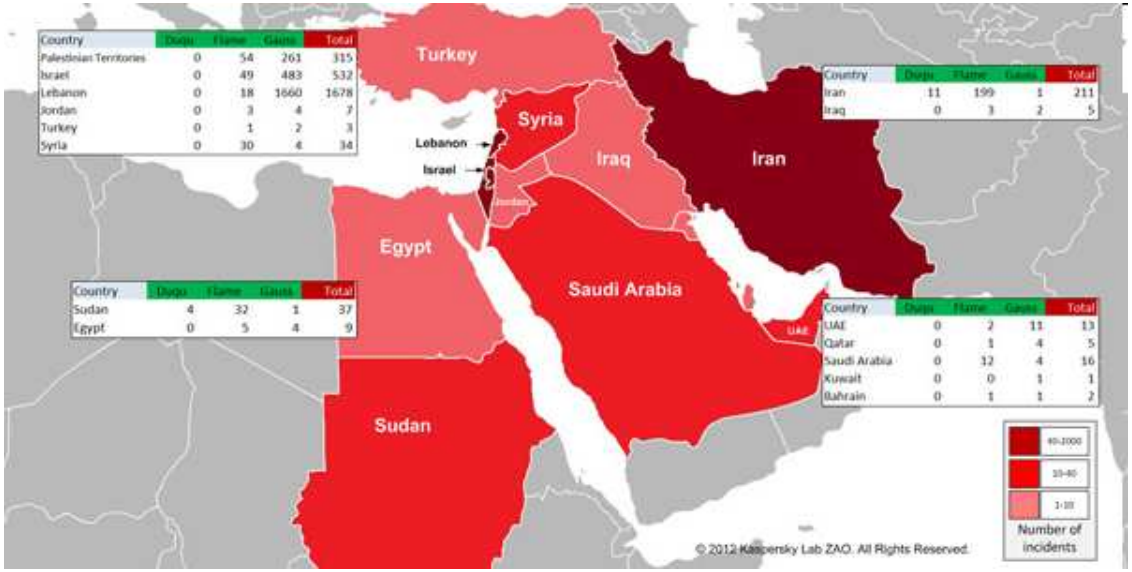
Wiper

- Beobachtet April 2012
- Zweck: Löschen von Daten und sich selbst - es liegen so gut wie keine Spuren des Programms vor

http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf

CyberWar-Werkzeuge im Einsatz

2012: Stuxnet wurde nach eigenen Angaben von der U.S.-Administration entwickelt und eingesetzt.



Nach Analysen von Kasperski Labs sind **mehrere** mit Stuxnet eng „verwandte“ Trojaner und Würmer (d.h. mit teilw. identische Source-Blöcken) vorwiegend im arabischen Raum verbreitet

Name	Number of incidents	Approx. number of incidents
Stuxnet	Over 100 000	Over 300 000
Gauss	~ 2500	~10 000
Flame	~ 700	~5000-6000
Duqu	~20	~50-60
miniFlame	~10-20	~50-60
Summe (nach späteren Zahlen):		mind. **350.000 infizierte Systeme**

http://www.securelist.com/en/analysis/204792257/Kaspersky_Security_Bulletin_2012_Cyber_Weapons

Hinweis für Insider: Ermittlungen ganz ohne Folgen?

12/14/2009

Print | E-Mail | Feedback

FROM THE MAGAZINE

DER SPIEGEL

Find out how you can reprint this DER SPIEGEL article in your publication.

RELATED SPIEGEL ONLINE LINKS

Nuclear Dispute: Germany, EU Increasingly Ready to Impose Tough New Sanctions on Iran (08/17 /2009)

Landmark Court Decision: Will Germany Loosen Trade Embargo with Iran? (06/16/2009)

SPIEGEL 360: Our Full Coverage of Iran

EUROPEAN PARTNERS

Presseurop

Eurozone | European disco (International Herald Tribune, Paris)

Italy | Italian waters still dragged by illegal nets (La Repubblica, Rome)

Siemens High Tech for Tehran

German Government Probes Shipments to Iran

AFP

Some fear that German technology is finding its way into Iranian weapons systems.

The German government is currently investigating whether engineering giant Siemens violated export control laws by shipping high tech equipment to companies in Iran. Siemens says its business in Iran is purely civilian, but some fear the equipment could be used for Tehran's missile or nuclear programs.

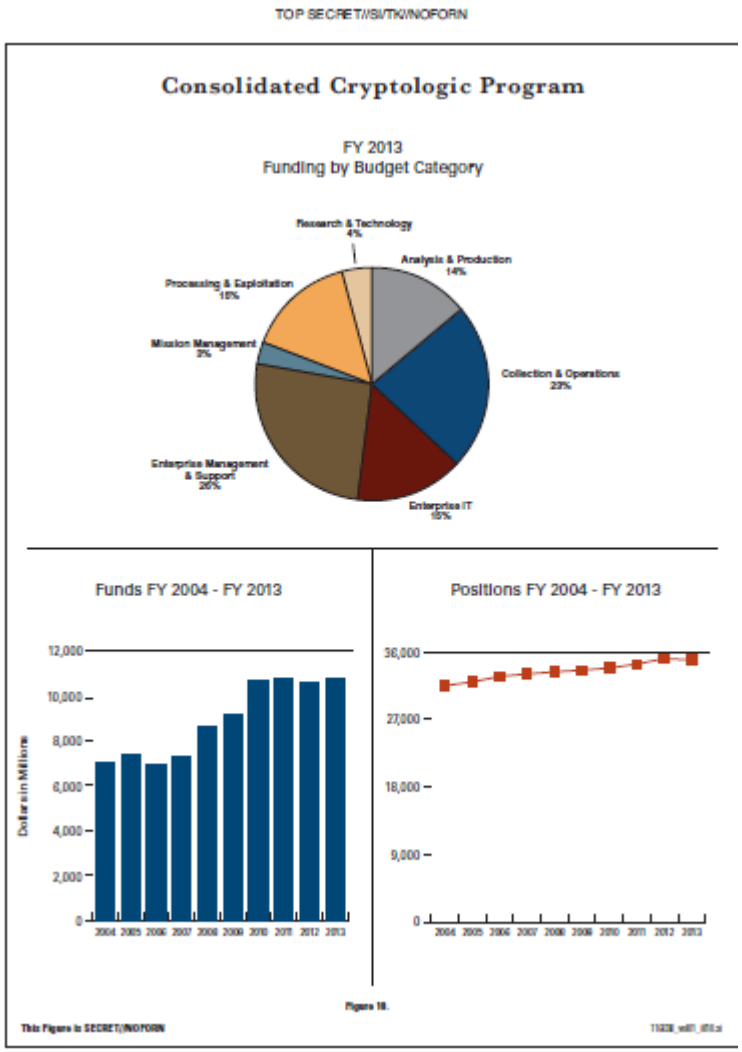
http://www.spiegel.de/international/world/0,1518,666900,00.html

Ressourceneinsatz

Das Budget der NSA für Cyber Warfare in 2013 (Auszüge):

- 652 Mio. Dollar für ein Programm zur Schadsoftware-Verbreitung
- 10 Mrd. Dollar für das „Gemeinsame Kryptologische Programm“ für „bahnbrechende kryptoanalytische Fähigkeiten […], um den Internetverkehr auszuwerten“

In Summe über *12 Mrd. US-$* für Internet-Überwachung, Entschlüsselung und Angriffswerkzeuge (lt. Budgetentwurf 2013 der NSA für den US-Kongress)



Bekannte Sicherheitslücken

SSL: in 2010 – also *vor* der *Programmierung* von Heartbleed 2011 – erklärte die NSA, es sei ihr durch spezielle Zugänge zu Unternehmen und Manipulation von Softwarelösungen gelungen, die SSL-Verschlüsselung auszuhebeln. Außerdem sei ihr das Brechen der Verschlüsselung älterer, gesammelter Daten gelungen.

Bemerkung: Der Heartbleed-Bug verdeckt die Untersuchung, welche Kryptoverfahren schon kompromittiert waren und sind

VPN: Denselben Dokumenten zufolge existieren Schwachstellen in der Verschlüsselung mehrerer VPN-Produkte.

Werkzeuge: RSA warnt dem eigenen Software-Entwicklungswerkzeug „BSafe“: das enthaltene Kryptoverfahren mit von der NSA entwickelten Elliptischen Kurven sei unsicher und kompromittiert.

Bekannte Sicherheitslücken

Zertifikate: Der FLAME-Trojaner nutze zum Nachladen von Schadcode die Update-Funktion mit gefälschten Microsoft-Zertifikate - lt. Microsoft-Bulletin wegen „ älterer Kryptographie-Algorithmen“

Mögl. Sicherheitslösung: IP-Nummern-Prüfung ausweiten

Anonyme Internet Services: Wichtiges NSA-Programm ist die Aushebelung anonymer Services – unklar ist, ob das TOR-likes Routing meint oder Methoden zur Nutzeridentifikation

Telekommunikation: NSA arbeitet an der Aushebelung der Verschlüsselung der 4G-Mobilfunkkommunikation, liest die verschlüsselte Datenübermittlung von Blackberry-Smartphones mit und hat durch manipulierte Apps Zugriff auf iPhones von Zielpersonen

Weitere Sicherheitslücken und Angriffspfade

XKeyScore und add-ins wie „Constant Web“: Sicherheitslücken werden in constant web seit den 1990er Jahren gesammelt; mit Hilfe XKeyScore wird versucht, Lücken automatisch zu nutzen

„Quantum (theory)“: Die NSA kapert IP-Verbindungen (z.B. von Admins) und lenkt diese auf gefälschte und mit Schadcode versehen Ziele um

Special Embedded Systems: Für harte Fälle bietet die NSA-“Haustechnik“ Zwischenstecker mit Keylogger plus Sender, und diverse andere Standard-Technik zur Etablierung verdeckter Kanäle per Netz oder Funk (*als Idee wirklich nicht neu…*)

Offene Fragen: Wie werden bekannte Schwachstellen bei embedded systems (diverse Seitenkanalangriffe) genutzt, was tut sich bei TEMPEST?

Zusammenfassung

NSA und kollaborierende Dienste

- Unterhalten seit 1998 mit dem TAO und als Teil des U.S. Cyber Commands personalstarke Hacker- und Cyberwar-Einheiten
- Entwickeln seit 2005 automatisierte Aufklärungs- und Angriffswerkzeuge für Cyberwarfare
- Wenden derzeit jährlich mind. 12 Mrd. US-$ für Cyberwar-Werkzeuge auf
- Haben mit Stuxnet und „verwandter Software“ Cyberwar-Waffen eingesetzt
- Operieren gegen Freund und Feind: im arabischen Raum gegen Banken („Flame“) ebenso wie in Belgien gegen EU-KOM oder in Deutschland gegen Siemens („Stuxnet“)
- Haben durch gesetzliche Befugnisse und zusätzliche Einflussnahme Zugriff auf Betriebsinterna von IT-Unternehmen, die auch zur Schwächung von IT-Sicherheitsfeatures genutzt wird.

2. War das wirklich alles neu?

IW: Datensammlung - „konventionell“

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 sabotage 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 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 a 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,"

DEFENSE IMAGE

U.S. troops field-testing some portable hardware

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

„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

IW: Datensammlung - „konventionell“

What Goes There?

Cybersentries block access to crucial systems

David Fulghum Netanya, Israel

Computer networks that control crucial industrial and manufacturing processes, and vital energy and water utilities, were once considered immune to cyberattack, because in theory they were "air-gapped," with no physical connection to the worldwide Internet. But that notion has died as researchers have found obscure Internet connections in virtually every automated system.

"These Scada (supervisory control and data acquisition) networks are becoming more and more connected to corporate networks [that are in turn] connected to the Internet," says Eyal Udassin, chief technical officer of C4 Security, a company acquired a year ago by Elbit to expand the parent company's cybercapabilities. "The assumption that Scada networks are iso... was never true."

Scada systems monitor and co... large-scale processes that often ... multiple sites and long distance... cluding the production and dist... tion of oil, gas, electricity and ... supplies. If they are connected t... Internet, cyberattackers can use... a pathway into the industry's co... center.

Such connections have multi... with innocent intentions. Smart... sors and automated control sys... have been attached to remote... cated valves and switches, to re... the need for costly on-the-spot m... nance and adjustment. Linking d... across the Internet or with wi... technology is far cheaper than ...

Key targets for a cyberwar might be computer-controlled industrial processors such as electric, water, gas or oil pipelines, and nuclear facilities like this power plant at Bushehr, Iran.

CYBER

has penetrated the control system, malicious commands can be used to allow component loads, speeds and pressures to exceed design levels. For example, abruptly closing a valve can create a pressure pulse that bursts pipes. Stuxnet commanded Iran's uranium-enrichment centrifuges to overspeed.

In November 2011, fears exploded that a water plant in Springfield, Ill., had been attacked from an Internet site in Russia. It turned out to be an employee trying to make repairs while on vacation, but system defenses reported it as a cyberattack.

That crystallizes the problem with Scadas, say researchers. They were not designed with security in mind, so most do not feature a security-focused monitoring system.

Israeli researchers say that is exactly what has to be done. In the Illinois incident, analysts had to be flown in from all over the U.S. to examine the event. It was never reported how much it cost to conduct the investigation.

If operators could have done "a quick check to see if someone sent any commands to start or stop the pumps from some remote or unauthorized location, the crisis would have been over in five minutes," Udassin says.

Another weak spot is in the Netherlands, where Scada systems connected to the Internet control gates and sluices in the dams that keep below-sea-level parts of the country dry.

In Lodz, Poland, in early 2008, a 14-year-old noticed that track-switching of the neighborhood tramway tracks were controlled by radio signals, in another incident cited by Udassin. He found the control frequency and built a device that could control switches. He switched the tracks from outside the Scada system and caused several derailments.

"This is being an easy target and that's a very dangerous thing," Udassin says. "These systems are too important [to leave defenseless]."

C4 started confronting the Scada problem by taking on the role of the aggressor, launching attacks in a controlled environment to find soft spots. The researchers repeatedly found that Scada networks are never monitored.

"Once you are in the network, you are never challenged because of the communications protocols used in those systems," Udassin says. "You can do whatever you want. There is implicit trust among all the elements of the network. If I control a power generator, all someone has to do to start or stop it is to send me a message. No one tells me who it is or what location it's from and it doesn't require encryption, authentication or authorization."

Such systems were the target of the Stuxnet and Flame viruses that delayed the Iranian uranium enrichment program for years.

"There was a lot of bashing of Siemens [company and equipment] for being infected by the cybermalware, but it just happened that they were the first to suffer a major attack," Udassin says. "The other vendors are not much better off. You can't expect them to solve all their problems within six months. There is just too much code."

"If we can break into just one of these stations, we can disconnect any instrument connected to the network, connect our equipment and instantaneously we are in the network. It is the most cost-effective way to gain [illegal] access."

C4's first solution was called Fides, the Greek goddess of trust. Researchers placed sensor boxes in the Scada network that tap into the communications. Because it is completely passive, it introduces no latency or other effects that jeopardize Scada operations—an important issue for utility owners and control engineers.

"When you introduce new equipment, you have to know it won't disturb the ongoing process," Udassin says. The same principle underlies a C4 product that is being developed to protect a major airport's computer-controlled baggage handling systems. Researchers built a model of how the baggage system should work. When anything in the system does not meet the security profile, it gives an alert. In normal operation, the system should never show anything.

"We don't define what something suspicious should look like," Udassin says. For example, "our profile says the [customer's] system is only allowed to report information. It is not allowed to initiate communications or send commands. We analyze all the communications layers from the networking down to the specific applications. If anything else comes out of it, I want to know."

Another C4 Security product, called Insight, is designed to avert the type of incident that occurred in the Illinois water plant.

"We don't filter or define, we just collect all of the transmissions in an analytical manner," he says. "We not only analyze the communications networking information and data volume, but we also understand the content and the application. We have the capability of storing millions and millions of transmissions—virtually limitless—and we enable forensics based on that," says Udassin.

"If we have a pump malfunctioning, let's see the commands that were sent to it in the last 24 hours. You can bluff your way through logs and do housekeeping to hide your presence. But if you want a pump to operate, you have to send it a command. This is a very unhampered source of information."

More tools are being developed to defend against Stuxnet-generation threats. C4 Security rolled out a new field device in August called Change Management Monitoring (CMM) that would have detected Stuxnet.

CMM provides an alternative "safety valve" check on any industrial process, using a completely different code base, so it can still trigger an alert even if the malware circumvents the vendor's built-in defenses. A pilot project using CMM is looking at companies that manufacture Food and Drug Administration regulated products, including medication for pharmaceutical companies. They use completely automated production lines, so they need to know if something has been tampered with.

"Our device spots an unmonitored or uncontrolled change," Udassin says. "It asks, Did you do it?" ●

If we can break into just one of these stations, we can disconnect any instrument connected to the network, connect our equipment and instataneously, we are in the network. It is the most cost-effective way to gain [illegal] access “

AW&ST, 19.11.2012

Netz- und Schwachstellenanalyse

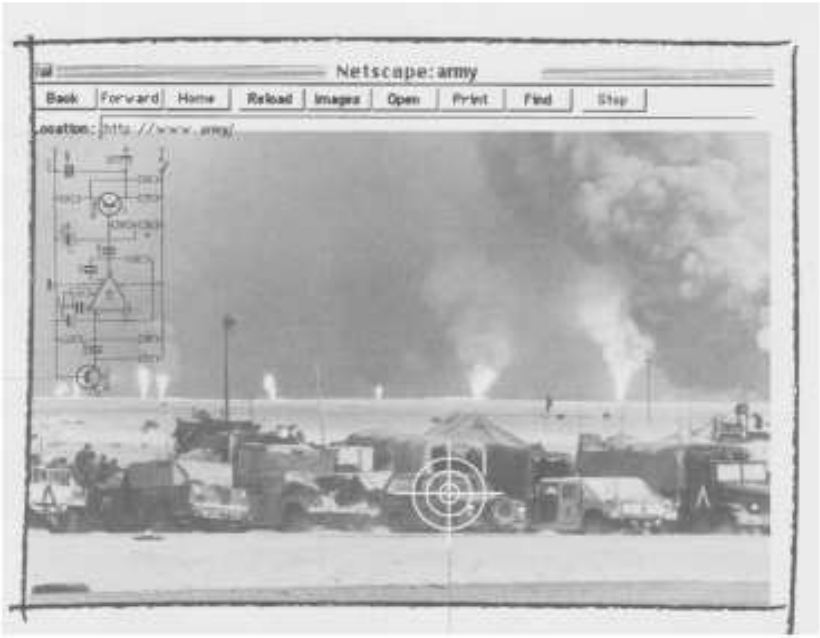
Schwachstellendatenbank Constant Web, heute „plug-in“ für XKeyscore

1997

W & F

Wissenschaft und Frieden

Dossier Nr. 24



Der digitale Feldherrnhügel

Military Systems: Informationstechnik für Führung und Kontrolle

von Ute Bernhardt, Ingo Ruhmann

W&F in Zusammenarbeit mit dem Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung

FIfF

ist das Ausschalten des irakischen C³I-Systems in der ersten Angriffswelle alliierter Luftstreitkräfte im Golfkrieg, das die Iraker unwissend über die alliierten Aktionen und damit wehrlos ließ.

und Informationen in "near-real-time", also fast in Echtzeit. Die Echtzeitanforderung dient der Steigerung der Operationsgeschwindigkeit. Das zentrale Ziel ist die Informations-Dominanz[70], die aufgefächert wird in die bereits bekannten Forderungen

- situational awareness,
- top-sight und vor allem
- die erhebliche Verbesserung der Leistung des C³I-Systems.

Zu dem mit dem C³I-System technisch möglich gewordenen Überblick entstand damit das passende operative Modell.

Diesem Modell entsprechend wurden in den USA bereits einige militärische Einheiten reorganisiert, um auf die Bedürfnisse von Information Warfare besser reagieren zu können. Seit 199' verfügt die U.S. Air Force über ein Air Force Information Warfare Center[71], das DoD über ein Joint Command and Control Warfare Center[72], das mit Aufgaben der psychologischen Kriegsführung, operativen Sicherheit und (C³I-) Destruktion betraut ist. Dort werden auch alle verfügbaren Daten über Waffen- und C³I-Systeme potentieller Gegner und deren Schwachstellen gesammelt. Diese Constant Web-Datenbank zu gegnerischen C³I-Systemen ist auf einem Netzwerk in 67 Ländern verteilt realisiert[73].

Die große Abhängigkeit moderner Industrienationen von informationstechnischen Systemen macht sie anfällig für Störungen durch verschiedene Ursachen. Obwohl Ausfälle von Computersystemen vor allem durch fehlerhafte Software und andere systemimma-

war, wird heute davor gewarnt, es gäbe keine Frontlinie mehr. Die Informationsinfrastruktur in den USA könnte jederzeit ebenso Opfer eines Angriffs werden wie Computersysteme auf dem Schlachtfeld[74]. Eine derartige Bedrohung verlangt nach einer permanenten Wachsamkeit.

In den USA wird zur konzeptionellen Differenzierung von Information Warfare daher folgerichtig zwischen Netwar und Cyberwar getrennt. Während Cyberwar im herkömmlichen Sinne kriegerische Aktivitäten gegen die Informationsinfrastruktur eines Gegners bedeutet, werden unter Netwar Aktivitäten außerhalb bewaffneter Auseinandersetzungen verstanden, bei denen die Sabotage der Infrastruktur zur permanenten Bedrohung wird. Erweitert wird überdies der Kreis jener, die als Gegner in einem Netwar gesehen werden. Zu den möglichen Konfliktparteien werden nun auch Umwelt- oder Menschenrechtsgruppen gezählt[75].

Information Warfare hat damit die Phase reiner Begrifflichkeit verlassen. Militärische Organisationen sind mit Kernelementen der Definition betraut, entwickeln entsprechende Konzepte und Techniken und üben diese bereits. Bei diesen Übungen wurden überdies neue Ziele von Information Warfare erkennbar. Das erste Manöver der "voll digitalisierten" EXFOR-Truppe im Sommer 1994 hinterließ dank der für C³I-Zwecke stark verbesserten Visualisierungstechnik den Eindruck, ein für potentielle Aggressoren zur Abschreckung taugliches Kriegsspiel sein zu können. Der Kommandeur des Joint Command and Control Warfare Centers sieht in der Abschrek-

2006: William Arkin listet in der Washington Post über 500 Softwarewerkzeuge, Datenbanken und „DNI“-Tools der NSA für Überwachung und Cyberangriffe auf, neben „Trailblazer“ auch „Constant Web“.

Arkin publiziert 2010 nach zwei Jahren Recherche für die Washington Post „**Top Secret America**“ als Online-Landkarte der Einrichtungen der U.S.-Geheimdienste.

GlobalResearch
Centre for Research on Globalization
globalresearch.ca / globalresearch.org

Notre site en Français : mondialisation.ca
Español Italiano Deutsch Português srpski العربية

About | Contact | Membership | Online Store | Donate

Font-size: A Print:

Latest News / Top Stories

- A New State Secrecy Law for Japan? The Abe Proposal
- Freedom Rider: Food Stamp Corporate Welfare, "Poverty is Good for Business"
- Who Sank Detroit – the "Hip Hop Mayor" or Wall Street?
- "Economic Repression": Obama, Democrats offer Deeper Social Cuts in New Budget Talks
- Social Inequality and the Impacts of Austerity Budgets: Nearly Half of US Public School Children are Poor
- "De-Americanize": The Man Who Usurped The Constitution
- For the Love of Money, "Wealth and Compassion": Who are the One

All Articles

and Security — Did Part of SEAL Team Six Die in a Helicopter Explosion During the Osama Bin Laden Raid?

Telephone Records are just the Tip of NSA's Iceberg

By William M Arkin
Global Research, May 14, 2006
Washington Post 14 May 2006

Region: USA
Theme: Police State & Civil Rights

Share 0 | Like | Tweet 0 | Email 0 | +1 0 | ShareThis 47

The National Security Agency and other U.S. government organizations have developed hundreds of software programs and analytic tools to "harvest" intelligence, and they've created dozens of gigantic databases designed to discover potential terrorist activity both inside the United States and overseas.

These cutting edge tools — some highly classified because of their functions and capabilities — continually process hundreds of billions of what are called "structured" data records, including telephone call records and e-mail headers contained in information "feeds" that have been established to flow into the intelligence agencies.

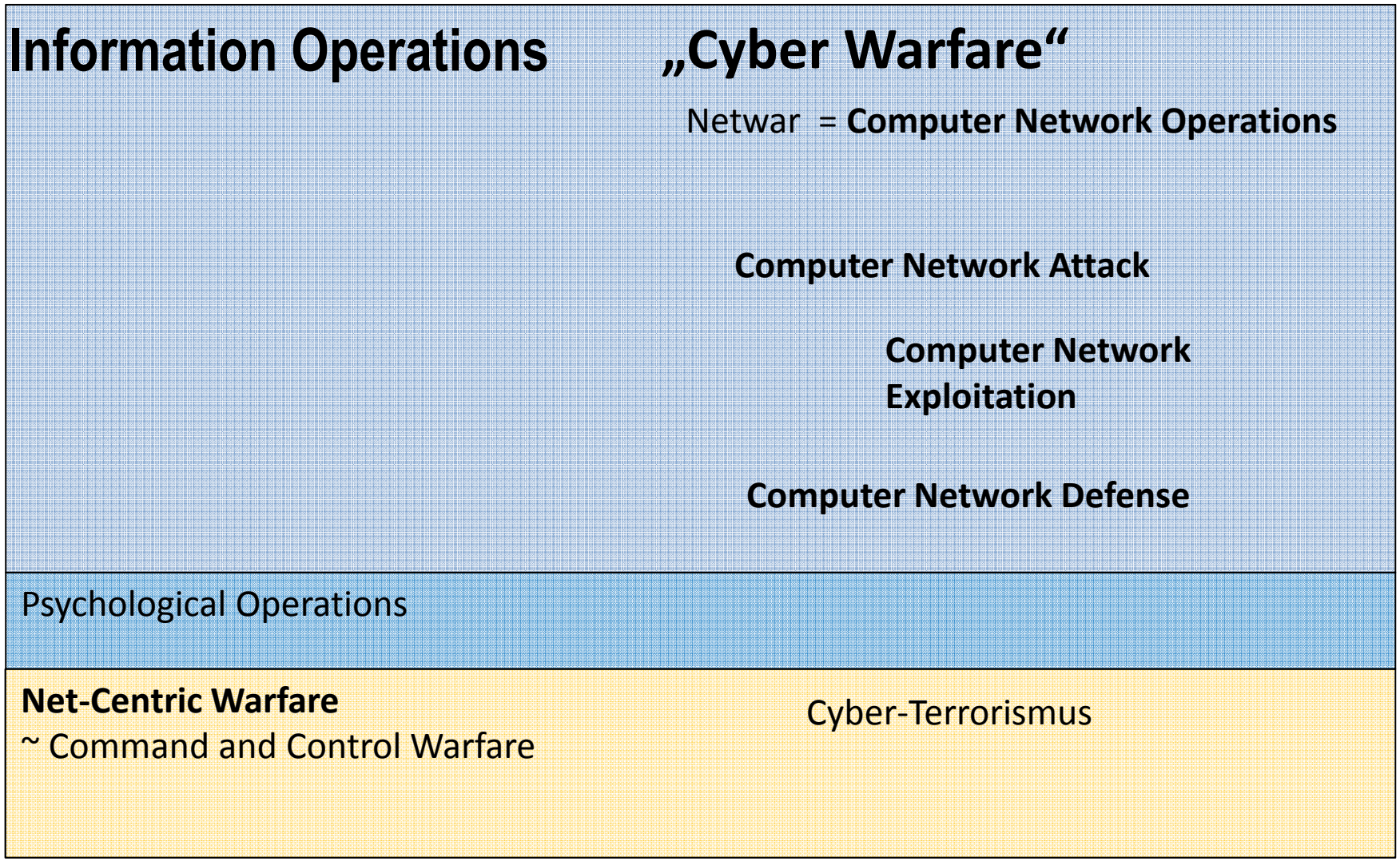
2007: Allein 2005-2007 wandte die NSA **2 Mrd**. US.$ auf für die Projekte

- "**Trailblazer**" zur massiven Datensammlung und
- "**Turbulence**" zur selektiven Kontrolle von Internet-Knotenpunkten, Web Traffic Überwachung und selektiven Modifikation von Datenpakten

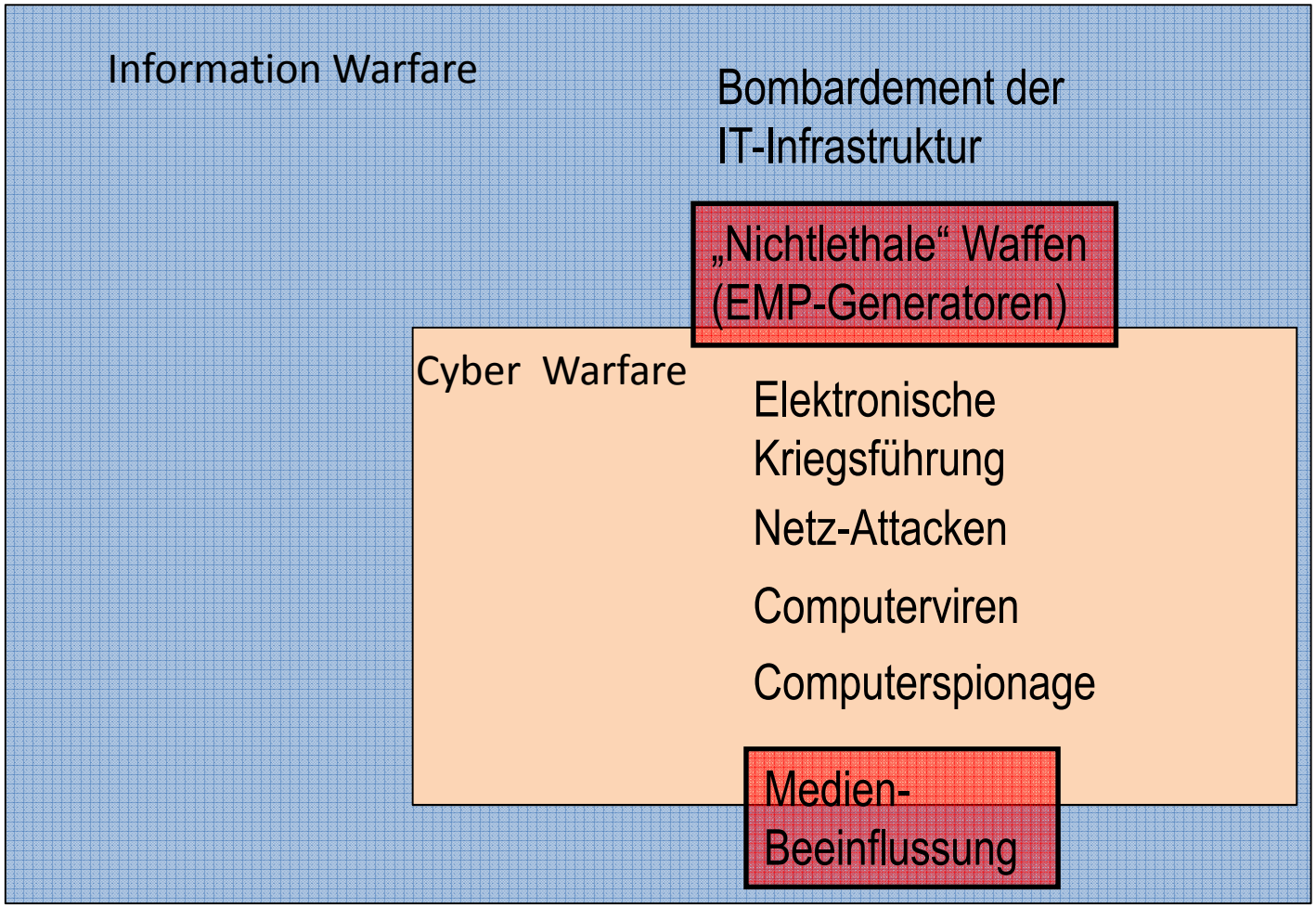
Die Projekte wurden abgebrochen, Teile für PRISM / XKeyScore etc. adaptiert

Wer bedroht uns eigentlich?

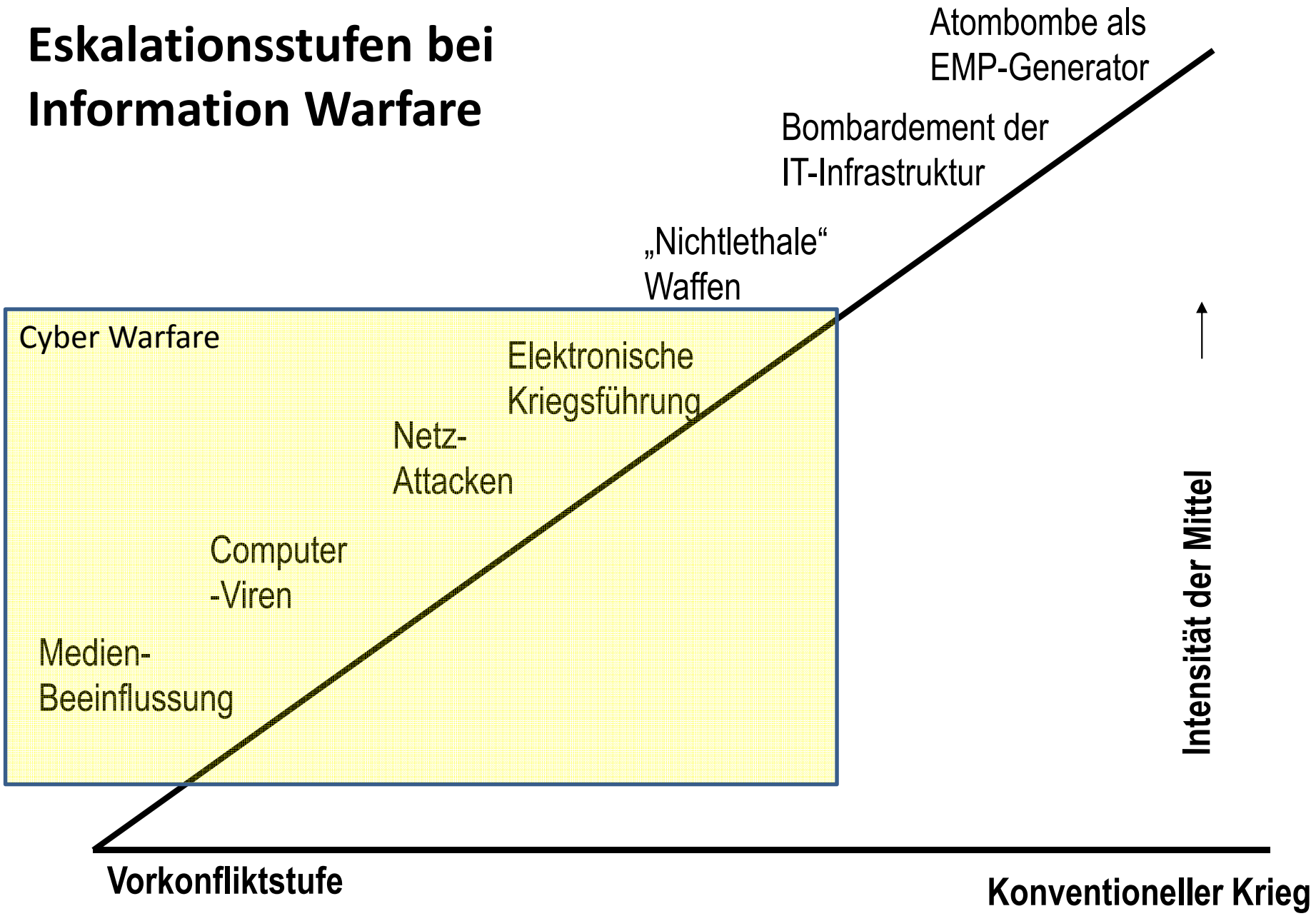
3. Exkurs: Information Warfare



Begriffe und damit verbundene Mittel



Eskalationsstufen bei Information Warfare



Warum dieser Exkurs?

Department of Defense

DIRECTIVE

NUMBER 5100.20
January 26, 2010

DA&M

SUBJECT: National Security Agency/Central Security Service (NSA/CSS)

References: S

1. PURPOSE
Code (U.S.C.)
Security Direc
(DoDDs) 514
(Reference (h
functions, rela

5. ORGANIZATION AND MANAGEMENT

a. NSA/CSS is a Defense Agency. The Secretary of Defense exercises authority, direction, and control over NSA/CSS, pursuant to References (a) through (e), Presidential Memorandum (Reference (j)), and other applicable authorities. The USD(I) exercises the authority, direction, and control of the Secretary of Defense over the DIRNSA/CHCSS, pursuant to Reference (f) and the responsibilities and authorities of the Secretary of Defense in References (a), (c), (d), and (e), and in coordination with the ASD(NII)/DoD CIO concerning IA.

b. NSA/CSS is designated a Combat Support Agency of the Department of Defense pursuant to Reference (a) and Secretary of Defense Memorandum (Reference (k)). NSA/CSS performs combat support activities, pursuant to References (a) and (j), and Secretary of Defense Memorandums (References (k) and (l)), in a manner consistent with DoDD 3000.06 (Reference (m)). These activities are also defined in Acting Chairman of the Joint Chiefs of Staff Memorandum (Reference (n)).

http://www.dtic.mil/whs/directives/corres/pdf/510020p.pdf

Wir sollten nicht übersehen …

- Jeder NSA-Direktor ist zugleich Kommandeur des U.S. Cyber Commands – d.h. Kommandeur der "information operations units" in NSA, Army, Air Force, Navy und Marine Corps.
- Die NSA ist zugleich Geheimdienst und Kampftruppe.
- Aufgabe der NSA ist nicht allein die Spionage, sondern ebenso die Computersabotage – genauer: Information Warfare in allen elektronischen und digitalen Formen.

Schlussfolgerung

- NSA und kollaborierende Dienste sind die bei weitem ressourcenstärkste Hackertruppe weltweit
- Sie haben wesentliche IT-Sicherheitsmittel umfassend kompromittiert. Gewissheit über die Sicherheit von IT-Sicherheitswerkzeugen kann es derzeit nicht geben.
- nach eigener Definition führen die USA uneingeschränkten Cyberkrieg gegen Freund und Feind.
- Datenschutz kann nur Teil in einer Debatte sein über „Cyberwar unter Freunden“

Die Debatte um IT-Sicherheit „nach Snowden“ hat noch gar nicht begonnen!

To Do‘s für die IT-Sicherheit:

- Welche IT-Sicherheitsmechanismen sind noch sicher, welche sind kompromittiert?
- Wer hat dazu den Überblick? Und welche staatliche Stelle ist noch vertrauenswürdig?
- Welche Systeme, Anwendungen und Werkzeuge sind von kompromittierten Bausteinen betroffen?
- Welche alternativen und sicheren IT-Sicherheitswerkzeuge sind anwendbar in Fällen einer Kompromittierung?
- Wer haftet für die Sicherheitslücken?
- Wo sind neue IT-Sicherheitswerkzeuge verfügbar / in Arbeit?
- ….. und noch sehr viel mehr Arbeit …..

Vielen Dank!

Cyberterrorismus – militärisches oder strafrechtliches Problem?

Computermanipulationen im engeren Sinne

- Ausspähung von Daten (202aStGB)
- Computerbetrug (§263a StGB)
- Fälschung technischer Aufzeichnungen (§268 StGB)
- Fälschung beweiserheblicher Daten (§269 StGB)
- Datenveränderung (§303a StGB)
- Computersabotage (§ 303b StGB)
- Bruch des Fernmeldegeheimnisses (§206 StGB)

Zusätzlich in Betracht kommende Straftatbestände

- Herbeiführung einer Explosion durch Kernenergie, Freisetzung ionisierender Strahlung, Vorbereitungsdelikte (§310b ff StGB),
- Störung von Fernmeldeanlagen (§317 StGB)
- ...

Computerstraftaten lassen sich *als Terrorismusdelikt* nach §129a StGB werten bei Angriffen auf IT-Systeme, sofern es sich um gemeingefährliche Straftaten handelt nach

- §305a StGB - Zerstörung wichtiger Arbeitsmittel
- §315 StGB - Gefährliche Eingriffe in den Bahn-, Schiffs- und Luftverkehr
- §316b StGB - Störung öffentlicher Betriebe (Bahn, Post, Versorgung mit Wasser, Licht, Wärme, Kraft)

Basis der Informationskriegführung

Datensammlung

Emitter Lokalisierung

Signaturenermittlung

Rekonstruktion von Kommunikationsnetzen

Entschlüsselung, Auswertung der Inhalte

Schutzmaßnahmen

Tarnen und Täuschen

Physische Sicherheit (Anlagen etc.)

Operative Maßnahmen der Informationskriegsführung

Psychologische Einflussnahme, Medienbeeinflussung

Manipulation von Daten

Manipulation von Computersystemen

Unterbinden von Kommunikation und Datenaustausch

Gegenspionage, Gegensabotage

Zerstörung von IT-Systemen

Die Kollateralschäden sind zivile IT-Systeme