CORPORATE TRUST
business risk & crisis management

NSA Report

Systematische Analyse der Snowden-Dokumente zum Schutz der deutschen Wirtschaft

Begleitet durch: DR. HÖRTKORN VERSICHERUNGSMAKLER

Inhalt

Wir haben das Internet erfunden. [...] Und wenn Sie sich anschauen, was ISIS mit dem Internet macht, schlagen sie uns bei unserem eigenen Spiel. Also müssen wir sehr, sehr hart werden bei Cyber und Cyberkrieg.

Donald Trump, US-Präsident, 27.09.2016

Vorwort

Prof. Dr. Michael Meier
Inhaber des Lehrstuhls IT-Sicherheit
an der Universität Bonn und
Leiter der Abteilung Cyber Security
bei Fraunhofer FKIE

Sowohl in der digitalen als auch in der realen Welt basieren Sicherheitsmaßnahmen auf verschiedenen Annahmen. Hinsichtlich der Absicherung eines Hauses gehören zu diesen Annahmen beispielsweise, dass die Tür die einzige Zutrittsmöglichkeit ist und das Haus nicht durch die Fenster betreten werden kann, sowie dass die Hersteller, Lieferanten und Verkäufer der Türen, Schlösser und Schlüssel regelkonform agieren – keine dieser Parteien behält Duplikate der Schlüssel.

In vielen Situationen, die jeweils durch eine Interessenlage, ein Aufwand-Nutzenverhältnis aus Angreifersicht oder gegebene Fähigkeiten von Angreifern, charakterisiert sind, treffen diese Annahmen zu. In anderen Situationen ist dies nicht der Fall und das Versagen der Schutzmaßnahmen muss in Betracht gezogen werden. Zusätzliche Schutzmaßnahmen sind zu ergreifen, z. B. die Installation einer Alarmanlage oder die Beauftragung eines Wachdienstes. Bei hohen schutzwürdigen Werten ist die Absicherung der Außengrenzen des Hauses insgesamt nicht ausreichend. Auch im Inneren müssen Sicherheitsmaßnahmen ergriffen werden, z. B. werden auch die Zimmertüren mit Schlössern versehen, Wertgegenstände in verschlossenen Stahlschränken aufbewahrt sowie Bewegungsmelder installiert und mit der Alarmanlage gekoppelt.

In der digitalen Welt liegen der Absicherung unterschiedliche Annahmen zugrunde, z. B. hinsichtlich der Regelkonformität des Verhaltens von Herstellern und Lieferanten von IT-Systemen, oft aber auch eher implizite Annahmen zu technischen Gegebenheiten. Zum Beispiel veröffentlichte Robert T. Morris von den AT&T Bell Labs bereits 1985 eine Schwäche der Internetprotokollfamilie, die Grundlage für einen sogenannten Man-on-the-Side-Angriff ist. Hierbei sendet ein Angreifer manipulierte Antworten auf Anfragen eines Opfers, die das Opfer vor den legitimen Antworten des angefragten Servers erreichen.

Voraussetzung für den Erfolg des Angriffs ist das Vorhandensein eines Zeitvorteils für den Angreifer. Da dies eine exponierte Lage des Angreifers im Internet erfordert, die in der Vergangenheit als kaum erreichbar betrachtet wurde, erhielt diese Bedrohung kaum Aufmerksamkeit. Diese Annahme erwies sich als falsch, als 2013 im Zuge der Enthüllungen von Edward Snowden bekannt wurde, das Nachrichtendienste wie der GCHQ Untersee-Glasfaserkabel anzapfen und dass die NSA innerhalb ihres QUANTUM-Programms dedizierte Infrastrukturen betreibt, um mittels Man-on-the-Side-Angriffen gezielt ausgewählte Systeme mit Spionagesoftware zu infizieren.

Geschlussfolgert werden muss, dass explizit und implizit getroffene Annahmen regelmäßig auf ihre Tragfähigkeit überprüft werden müssen – der vorliegende Report von Corporate Trust liefert hierfür Ansatzpunkte. Dies gilt sowohl für die digitale als auch reale Welt, da zielgerichtete Cyberangriffe oftmals als Zusammenspiel in beiden Welten erfolgen. Das Wegfallen einzelner Annahmen und damit das Versagen von Schutzmechanismen ist einzukalkulieren und entsprechende Vorsorge durch zusätzliche Schutzmechanismen ist zu treffen.

Neben vielen grundsätzlichen Gemeinsamkeiten bei der Absicherung von digitalen und realen Werten existieren auch signifikante Unterschiede. In der digitalen Welt ist das Entdeckungsrisiko für Täter deutlich geringer. Gleichzeitig sind die Kenntnisse und Fähigkeiten zur Durchführung von Angriffen einfach vervielfältigbar und durch Programme automatisierbar.

Ein Unterschied ist mir unerklärlich: Opfer von Cyberangriffen verschweigen diesen Umstand oft schamhaft, weil sie fürchten, sonst werde ihr Ruf geschädigt. Warum schädigt dies den Ruf? In der realen Welt fürchtet kaum ein Einbruchsopfer um seine Reputation – zumindest nicht in diesem Maße. Mit Selbstverständlichkeit werden Einbrüche zur Anzeige gebracht (Etwa nur wegen Erfordernis für Versicherungsleistungen?) und sogar am Stammtisch ggf. als Warnung für die Nachbarn berichtet. In der Entwicklung einer neuen digitalen Fehlerkultur (nahe der in der realen Welt gelebten) sehe ich eine wichtige Voraussetzung für eine erfolgreiche Abwehr von Cyberangriffen. Die Offenheit von Thyssenkrupp zu den jüngst erfahrenen Cyberangriffen lässt mich hoffen.

Ihr

Michael Meier

Hintergrund und Methodik

Florian Oelmaier

Prokurist, Leiter Cyber-Sicherheit &
Computerkriminalität

Friedrich Wimmer

Leiter IT-Forensik &
Cyber Security Research

Seit dem Sommer 2013 sorgen die Enthüllungen Edward Snowdens für Wirbel. Der amerikanische Ex-Nachrichtendienstmitarbeiter hat der Öffentlichkeit detaillierte Einblicke in die stark abgeschirmte Arbeit der Nachrichtendienste gegeben.

Die Printmedien, mit denen er dabei kooperierte, haben vor allem versucht zu erklären, was die massiven Spionageprogramme für Politik, Staat und Privatpersonen bedeuten. Der Fokus unserer Auswertung liegt vielmehr darauf, was die Snowden-Erkenntnisse eigentlich für die deutsche Wirtschaft bedeuten. Das Ergebnis ist der vorliegende „NSA Report".

Corporate Trust beschäftigt sich seit fast zehn Jahren mit der Abwehr von Industriespionage. Wir halten es für unerlässlich, dass die Wirtschaft, als großer Know-how-Träger unserer Gesellschaft, versteht, wie staatliche und halbstaatliche Informationsbeschaffung funktioniert, damit sie sich davor schützen kann. Dies kann anhand der Snowden-Dokumente nun sehr viel besser eingeschätzt werden.

Die vorliegende Analyse soll die Welt der Geheimdienste für deutsche Firmen verständlicher machen. Nur wer seinen Angreifer kennt, kann ihn wirksam bekämpfen. Das Ausforschen von Unternehmen wird umso schwieriger, je genauer diese über die Vorgehensweise von Nachrichtendiensten Bescheid wissen. Nicht zuletzt aus diesem Grund operieren Nachrichtendienste unter strenger Geheimhaltung.

Auch wenn der Beginn der Snowden-Leaks bereits drei Jahre zurückliegt, hat der interessante Teil der Aufarbeitung gerade erst begonnen:

- Mehr und mehr Staaten rüsten ihre Geheimdienste mit Cyberfähigkeiten aus. Wie aber schützt man sich gegen solche Angreifer? Und wer muss sich überhaupt schützen?

- Teile der deutschen Wirtschaft sind explizit Aufklärungsziel von NSA & Co. Wer ist davon betroffen und wer nicht?

- Die organisierte Kriminalität übernimmt erfahrungsgemäß technische Möglichkeiten der Geheimdienste mit drei bis fünf Jahren Verzögerung. Welche neuen Schutzmaßnahmen sind nun für Firmen notwendig?

Der vorliegende Report basiert auf klassischer „Open Source Intelligence": Wir haben dazu Informationen aus öffentlich verfügbaren Quellen gesammelt, analysiert und neu zusammengesetzt. Naturgemäß sind viele Informationen über Geheimdienste nur aus einer einzelnen Quelle verfügbar und daher schwer zu verifizieren.

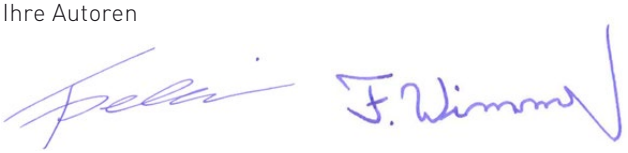
Auf Basis unserer Erfahrungen und Berufspraxis haben wir alle Informationen auf ihre Plausibilität überprüft. Darüber hinaus haben wir uns aber auch erlaubt, plausible Gerüchte und sinnvoll erscheinende Experteneinschätzungen miteinzubeziehen.

Die behördliche und geheimdienstliche Terminologie – die weitgehend in Englisch vorliegt – haben wir so weit wie möglich in Begriffe übersetzt, die in der deutschen Firmenlandschaft üblich und verständlich sind. Dabei können im Einzelnen Ungenauigkeiten entstanden sein, die wir aber um der besseren Lesbarkeit willen in Kauf genommen haben. Wir hoffen, dabei einen guten Kompromiss gefunden zu haben.

Auf den letzten Seiten findet sich zudem ein ausführliches Quellenverzeichnis, in dem alle verwendeten Quellen angegeben sind.

Der vorliegende Report soll den deutschen Unternehmen helfen, die Bedrohung der Spionage besser zu verstehen, um sich angemessen davor zu schützen. In diesem Sinne wünschen wir Ihnen bei der Lektüre viele neue Erkenntnisse!

Ihre Autoren



Florian Oelmaier und Friedrich Wimmer
im Januar 2017

Ergebnisse in Kürze

1 Aufklärungsziel Deutschland

- Betrachtet man die 90 größten Internetknoten und die 360 wichtigsten Unterseekabel, dann kann die NSA wohl mehr als 90% dieser Internet-Kapazitäten überwachen. Selbst in Russland oder China gibt es größere Installationen von Abhörtechnologie. Auf der Weltkarte mit den Standorten wird klar, wie nah die NSA ihrem erklärten Ziel ist, „global network dominance".

- In einer strategischen Liste von Spionagezielen wird im Januar 2007 Deutschland neben neun weiteren Ländern genannt, die allesamt „neu entstehende strategische Technologien" entwickeln und herstellen. Diese könnten „einen strategischen militärischen, wirtschaftlichen oder politischen Vorteil liefern", heißt es in dem NSA Dokument. Es ist davon auszugehen, dass die Bedeutung der deutschen Wirtschaft seitdem global eher zu als abgenommen hat, nicht zuletzt durch ihre wirtschaftliche Stärke innerhalb der EU und ihre Innovationskraft.

- Die NSA hatte in 2012 nachweislich den Auftrag, französische Angebote für internationale Aufträge, die 200 Mio. USD übersteigen, auszuspionieren. Warum sollte man glauben, dass deutsche Firmen nicht Ziel von NSA Spionage sind? Die Frage ist eher anders: Gibt es irgendeine Cybereinheit auf der Welt, die nicht mindestens eine deutsche Firma im Visier hat?

- Vor 10 Jahren waren Raumfahrt, Elektro-Optik, Nanotechnologie und energetischen Materialien auf der strategischen Missionsliste der NSA. Die Fallpraxis von Corporate Trust hat dies bestätigt. Heute sind bei geheimdienstlichen Spionageangriffen zusätzlich die Bereiche Biotechnologie, Getriebetechnologie und alternative Antriebe betroffen. Firmen, die solche Produkte entwickeln und produzieren, sowie deren Zulieferer und Dienstleister, werden gezielt von ausländischen Diensten ausgeforscht.

- Das Cyberwaffen-Arsenal der NSA ist flexibel einsetzbar und bereits heute brandgefährlich. In der Zukunft werden Cyberwaffen mit Industrie 4.0, selbstfahrenden Autos, computergesteuerten Stromnetzen und dem „Internet of Things" die Zerstörungskraft von Atomwaffen erreichen. Das lockt Diebe an. Und NSA Cyberwaffen in der Hand von Kriminellen oder anderen Geheimdiensten sind eine noch viel größere Bedrohung für die deutsche Wirtschaft. Erste Fälle gibt es bereits.

2 Herausforderung für die deutsche Wirtschaft

- Die Amerikaner geben mehr als 0,3% ihres Bruttoinlandsprodukts für die NSA aus. Der Gesamtetat von BND, BSI und Verfassungsschutz gesamt (nicht nur Cyber) beträgt weniger als 0,05% des deutschen BIP. Mit der derzeitigen finanziellen Ausstattung des Bundesamtes für Sicherheit in der Informationstechnik (BSI) und der Nachrichtendienste in Deutschland können die wirtschaftlichen Interessen des Landes nicht angemessen vor Spionage geschützt werden.

- Die Personalstärke der russischen Cybereinheiten (ca. 50.000) ist denen der Amerikaner (ca. 46.000) ebenbürtig. Die entsprechenden chinesischen Einheiten haben vermutlich fast dreimal so viel Personal (ca. 130.000). Das Vereinigte Königreich hat immerhin noch 6.500 Mann. Demgegenüber stehen wohl etwa 1.300 Stellen in Deutschland. Auch bei der Zahl der Mitarbeiter liegen die deutschen Sicherheitsbehörden im internationalen Vergleich also weit hinten. Unternehmen müssen aus eigenem Interesse selbst für die Abwehr von Spähangriffen sorgen.

- Die NSA (zuständig für Spionage und Cyberabwehr) hat 40.000 Mann, das United States Cyber Command (zuständig für Angriffe) 6.000. Damit die Zusammenarbeit reibungslos funktioniert, haben beide Einheiten per Dekret den gleichen Chef. In Deutschland verteilen sich die 1.300 Stellen auf die Cybereinheiten beim BND, das BSI, das Kommando digitale Kräfte bei der Bundeswehr sowie Cybermitarbeiter beim Bundesamt für Verfassungsschutz und den 16 Landesämtern für Verfassungsschutz und demnächst bei der neuen „Zentralen Stelle für Informationstechnik im Sicherheitsbereich". Dazu kommen noch das Bundeskriminalamt und die 16 Landeskriminalämter und einige Schwerpunktstaatsanwaltschaften. Selbst für Experten ist es schwer, den Durchblick zu behalten, wer in Deutschland für was zuständig ist.

- Das NSA Organigramm zeigt, die Spionageabteilung der NSA (Hauptabteilung S) ist organisiert wie ein Wirtschaftsunternehmen. Es gibt einen Vertrieb und Kundenkommunikation (S1), eine Produktion – in diesem Fall das Erstellen von Analysen in Form von „Produktlinien" (S2) – und eine Forschungs- und Entwicklungsabteilung (S3), die ständig verbesserte Methoden zum Sammeln von Daten entwickelt. Dieser effizienten Organisation können derzeit weder die deutschen Sicherheitsbehörden noch die IT-Abteilungen der Industrie etwas entgegensetzen.

3 Deutschland wird abgehängt

- Die amerikanischen Ausgaben für die staatlichen Cybereinheiten wirken wie ein Konjunkturprogramm für Cyber-Sicherheit. Es gibt international operierende deutsche Konzerne, die Ihre Sicherheitsabteilungen in den USA ansiedeln, weil man dort einfacher IT-Sicherheitsexperten rekrutieren kann.

- Die Fähigkeiten der NSA in den Snowden Dokumenten haben die Welt beeindruckt. Die meisten technischen Dokumente datieren aber auf 2007-2010. Dass die NSA ihre Technologien auf die seitdem hinzugekommenen Smartphones und Apps adaptiert hat, gilt als sicher. Es ist auch davon auszugehen, dass die NSA mittlerweile Cyberwaffen für Clouds, Internet of Things und Industrie 4.0 fertig entwickelt hat. Und auch ein Quantencomputer wird der NSA über kurz oder lang zur Verfügung stehen. Von solchen Fähigkeiten kann man in Deutschland nur träumen.

- Die NSA versteht sich als Werkzeug der Politik und des Militärs. Dazu gehört die Unterstützung bei Vertragsverhandlungen und internationalen Konferenzen. Kunden sind u.a. US Handelsvertretungen sowie das Finanz-, das Handels- und das Energieministerium. Die NSA ist ein sehr mächtiges Werkzeug in den Händen eines Präsidenten, der solche Machtoptionen zu nutzen weiß. Deutschland kann da kaum mithalten.

- In fast allen Ländern werden die Cybereinheiten vom Verteidigungsminister oder dem Regierungschef gesteuert. Die Doktrin dahinter ist, „nur wer weiß, wie man angreift kann sich verteidigen". Nur in Deutschland unterstehen mehr als die Hälfte der relevanten Cybereinheiten dem Innenminister. Während alle auf Angriff spielen, konzentriert sich Deutschland auf die Defensive.

- Die NSA orchestriert die Zusammenarbeit der westlichen Geheimdienste im Cyberraum nach dem Motto „quid pro quo". Wie die meisten westlichen Staaten braucht Deutschland die Technologien und Erkenntnisse der NSA zur Verteidigung und muss daher mitspielen. Gleichzeitig ist die NSA aber Teil des schwer kontrollierbaren und wenig transparenten US-amerikanischen militärisch-industriellen Komplexes, in dem die Interessen deutscher Firmen kaum eine Rolle spielen.

- Durch die weitreichenden Spionageaktivitäten anderer Staaten wird enormes Know-how in den Bereichen IT und speziell IT-Sicherheit aufgebaut. Deutschland verliert damit den Anschluss bei einer Schlüsseltechnologie und wird daher zunehmend von ausländischen Anbietern und deren Know-how abhängig sein.

Das Cybersicherheitsteam der Corporate Trust hat in den vergangenen Monaten die Snowden Dokumente, Wikileaks Informationen und weitere Open Source Quellen gesichtet und analysiert. Erstmals wurden die Dokumente der Whistleblower aus dem Blickwinkel ihrer Aussagekraft für die IT-Sicherheitslage in der deutschen Wirtschaft untersucht.

Zeitgleich arbeiteten die Spezialisten von Corporate Trust an der IT-forensischen Aufklärung zahlreicher Fälle von Datenspionage und Informationsabfluss bei deutschen Unternehmen. So konnten Analyseergebnisse der Dokumente teilweise gleich mit Fällen aus der Praxis abgeglichen werden.

Datengrundlage

Bis jetzt sind von den Snowden-Dokumenten erst weniger als drei Prozent veröffentlicht worden. Ein weiterer Erkenntnisgewinn in den nächsten Jahren ist zu erwarten. Dieser ist notwendig, da die NSA nicht der einzige Angreifer ist und unsere IT schutzloser ist denn je.

IT-Technologie durchdringt immer weitere Teile unserer Gesellschaft:

- Spezialisten leisten anderen Ärzten Hilfe via Telemedizin.
- Menschenleere Produktionsanlagen werden per Industrie 4.0 vernetzt und ferngesteuert.
- Heizungen, Türschlösser und Steckdosen unserer Häuser werden per „Smart Home" vom Urlaubsort aus gesteuert.
- Das „Smartgrid" kontrolliert mit intelligenten Stromzählern unsere Stromversorgung, damit wir die Energiewende umsetzen können.
- Autos erhalten Informationen aus der Cloud, um uns autonom an unser Ziel zu bringen.

Noch nie war unsere Gesellschaft so abhängig von einer einzigen Schlüsseltechnologie wie heute. Und es ist nicht absehbar, dass sich diese Abhängigkeit in Zukunft verringert.

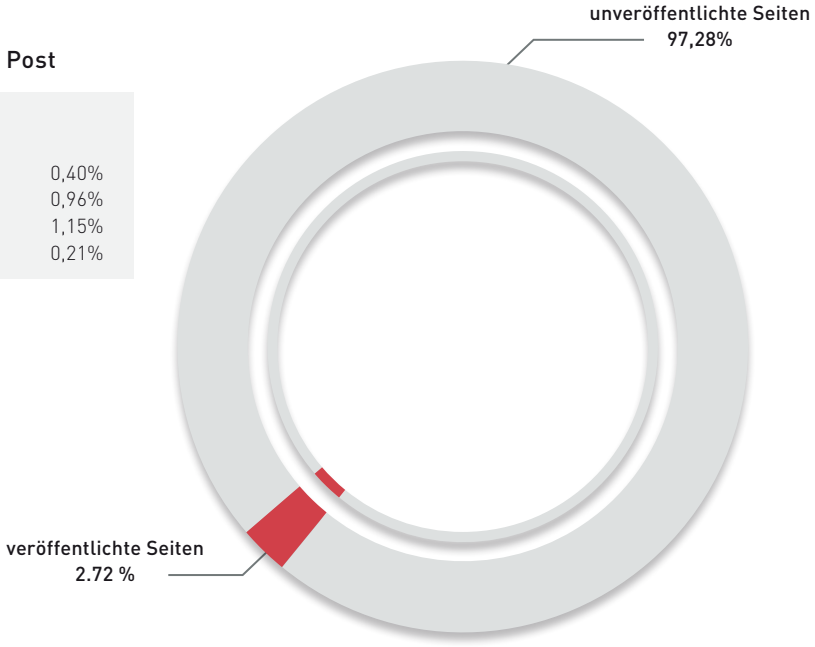
Gleichzeitig ist der Wohlstand auf der Welt ungerechter verteilt denn je und die Sicherheitslage dementsprechend schlecht. Zusätzlich stehen sich die großen Weltmächte wieder zunehmend feindlicher gegenüber.

In dieser Situation ist es nur logisch, dass die IT als Angriffsziel in Betracht gezogen wird. Dementsprechend muss die Verteidigung dieser Schlüsseltechnologie strategisch geplant werden. Erst die Veröffentlichungen von Edward Snowden haben eine breite Öffentlichkeit und die Führungseliten in Politik und Wirtschaft auf dieses Problem aufmerksam gemacht.

Seit Jahren werden Computer und Netzwerke zu Spionagezwecken genutzt. Dank Snowden wissen wir nun, wie dies organisiert und mit welchen Mitteln gearbeitet wird. Es gilt diese Informationen aufmerksam zu studieren und zu analysieren. Die Schwachstellen unserer IT, welche die NSA zur Informationsgewinnung nutzt, werden in den nächsten Jahren auch von weiteren Gegnern mit anderen Intentionen genutzt werden.

Snowden-Dokumente laut Washington Post

Gesamtumfang 250000		
Veröffentlichte Seiten in 2013	1008	0,40%
Veröffentlichte Seiten in 2014	2401	0,96%
Veröffentlichte Seiten in 2015	2880	1,15%
Veröffentlichte Seiten in 2016 (bis Juni)	521	0,21%



Quelle: Corporate Trust 2017

Edward Snowden war Systemadministrator bei der NSA. Angestellt war er bei einem Subunternehmer. Informationsabfluss durch interne Mitarbeiter ist nicht nur ein Problem der NSA.

Wie und wann Edward Snowden an die brisanten Dokumente gelangte, die er später an die Öffentlichkeit gab, ist bis heute ungeklärt. Es wird spekuliert, dass er zumindest einen Teil der Dokumente schon im April 2012 sammelte, während er noch beim Computerhersteller Dell angestellt war, wo er Kundenwünsche der CIA bearbeitete. Die Angabe des Journalisten Glenn Greenwald, der erste Kontakt durch Snowden sei am 1. Dezember 2012 erfolgt, spricht ebenfalls dafür, dass Snowden schon vor der Zeit beim Sicherheitsdienstleister Booz Allen Hamilton sensible Informationen beschafft hatte.

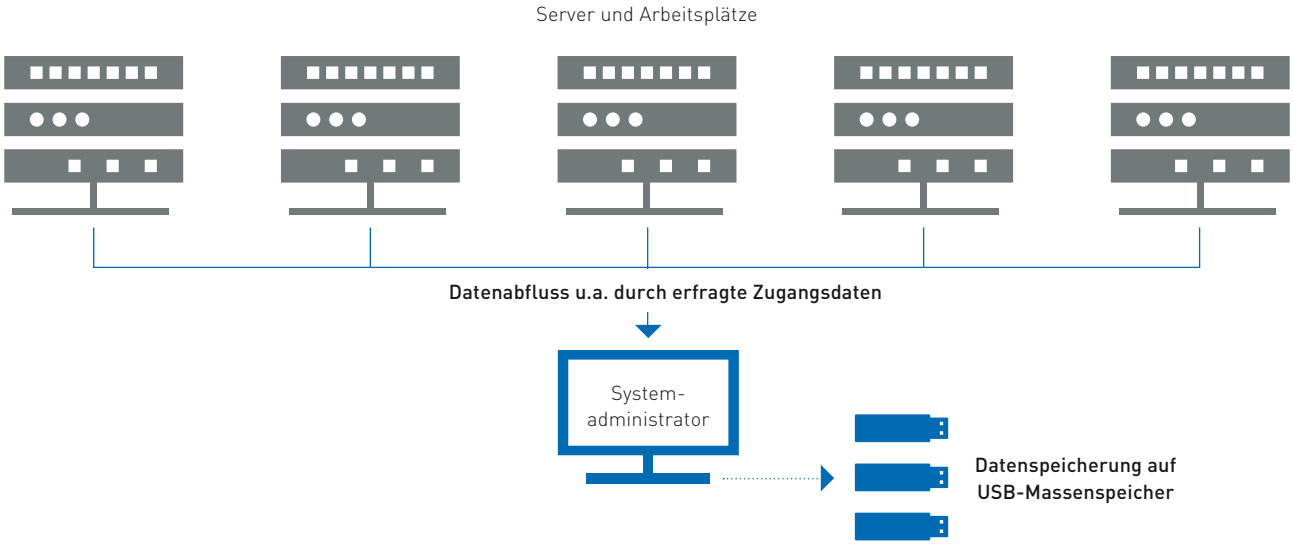
Keith Alexander, damaliger Direktor der NSA, deutete im August 2013 an, wie es zu dem Leck kommen konnte. Die NSA habe Menschen damit beschäftigt, Daten zu transferieren, Netzwerke zu sichern und Dinge zu tun, die Maschinen wahrscheinlich besser können. „Am Ende des Tages geht es um Menschen und Vertrauen" – sagte Alexander.

Unbestritten scheint, dass Edward Snowden die weitreichenden Berechtigungen eines Systemadministrators zugewiesen wurden, welche nur ca. 1.000 der 40.000 Angestellten besaßen. Ferner erhielt er zur Durchführung seiner Aufgaben die Berechtigung, Daten zu transferieren und bei Bedarf auch auf USB-Massenspeicher zu kopieren.

Allerdings musste er immer damit rechnen, dass seine Aktivitäten überwacht wurden und er bei Überprüfungen stets plausible Erklärungen benötigen würde. Mit der Stationierung auf Hawaii war er mehrere Zeitzonen entfernt vom Hauptquartier der NSA in Fort Meade (Maryland) und verrichtete seine Arbeit zumeist, wenn die meisten Angestellten an der US-Ostküste schon Feierabend hatten, womit seine Aktivitäten weniger Kontrollen unterworfen waren.

Seine Zugriffsmöglichkeiten müssen sich zwischen Dell und Booz Allen Hamilton unterschieden haben, da er später als Grund für den Arbeitgeberwechsel den Zugriff auf sensible Informationen nannte. Gegebenenfalls gelang ihm erst durch den Wechsel der weitreichende Zugriff auf Anwendungen des NSA-Intranets. Dem Anschein nach nutzte er erfragte Zugangsdaten von Kollegen, um seine Zugriffsmöglichkeiten zu erweitern bzw. zu verschleiern. Dabei hebelte er mutmaßlich mit selbst erzeugten Schlüsseln und Zertifikaten Restriktionen aus und setzte anschließend Web-Crawler-Techniken ein, um interne Anwendungen (z. B. Wikis) nach interessanten Dokumenten zu durchsuchen und diese zu sammeln. Schlussendlich lud er die gesammelten Informationen kurz vor seiner Flucht auf USB-Massenspeicher herunter.

Risiko Datenabfluss durch Innentäter

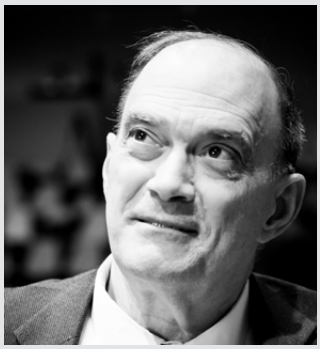


Quelle: Corporate Trust 2017

Zeitstrahl Veröffentlichung

Whistleblower vor Edward Snowden

Whistleblower kreiden Überwachung der amerikanischen Telekommunikation an



- 2002 William Binney mit Kirk Wiebe, Edward Loomis, Diane Roark

- 2005 Russell Tice

- 2005 Thomas Drake

- 2005 Mark Klein

WERDEGANG EDWARD SNOWDENS 1983 - 2009

21.06.1983

geboren in North Carolina; während seiner Kindheit zieht die Familie nach Maryland in die Nähe des NSA-Hauptquartiers bei Fort Meade.

1999 - 2001
2004 - 2005

studiert er zeitweise Informatik; er erlangt die Hochschulreife, aber keinen Hochschulabschluss.

2004

absolviert er als Rekrut der US-amerikanischen Special Forces einen mehrmonatigen Trainingskurs; diesen kann er nach einem Trainingsunfall nicht beenden.

2005

arbeitet er als „security specialist" für eine der NSA nahestehende Einrichtung der University of Maryland.

2006

wechselt er zur Central Intelligence Agency und erhält anschließend „top secret clearance".

2007

wird er als Netzwerk-Sicherheitstechniker unter diplomatischer Tarnung nach Genf gesandt.

2009

nach dem Verdacht der CIA, er versuche unerlaubt Zugriff auf geheime Daten zu erlangen, verlässt er die CIA, um für die Subunternehmer der NSA, Dell und Booz Allen Hamilton, zu arbeiten.

Vermutlich zu dieser Zeit beginnt er Wege zu erarbeiten, um Informationen über verschiedene, für ihn überbordende, NSA-Aktivitäten zu sammeln.

Zeitstrahl Veröffentlichung

Der Weg zur Veröffentlichung

2009

beginnt er als Angestellter von Dell für eine NSA-Einrichtung in Japan zu arbeiten.

2011

geht er zurück nach Maryland, wo er für Dell als Lead Technologist Kundenwünsche der CIA bearbeitet.

2012

arbeitet er in ähnlicher Position im Auftrag von Dell in Hawaii in einer regionalen NSA-Station, zu deren Aufgaben unter anderem das Ausspähen von chinesischen Belangen zählt.

2013

wechselt er von Dell zu Booz Allen Hamilton, um, wie er später angibt, Informationen über die weltweiten NSA-Überwachungsaktivitäten zu sammeln.

Mai 2013

Snowden kopiert (die letzten) Dokumente, die er veröffentlichen will bzw. als Verhandlungsmasse benötigt. Anschließend reicht er wegen einer angeblich diagnostizierten Epilepsie eine krankheitsbedingte Fehlzeit ein.

20. Mai

Snowden fliegt nach Hongkong, um von dort aus die NSA-Überwachungsaktivitäten öffentlich zu machen. Mit im Gepäck ist IT-Equipment, zumindest vier Laptops, welche ihm Zugriff auf die entwendeten sensiblen Informationen ermöglichen. In Hongkong arbeitet er unter anderem mit dem Journalisten Glenn Greenwald zusammen.

5. Juni

Die erste Veröffentlichung aus den Snowden-Dokumenten erfolgt im Guardian und behandelt den Beschluss des Foreign Intelligence Surveillance Court, der Verizon zwingt, tagesaktuelle Telefonverbindungsdaten der amerikanischen Kunden an die NSA weiterzugeben.

ARBEITSSTATIONEN UND FLUCHTZIELE

Quelle: Corporate Trust 2017

ab 6. Juni
Etliche Medien, darunter der Guardian, die Washington Post, die New York Times und der Spiegel, berichten aus dem Material und veröffentlichen es auszugsweise (u. a. PRISM, Boundless Informant), weiterhin ohne Snowden als Quelle offenzulegen.

9. Juni
Snowden gibt sich als Quelle der Dokumente zu erkennen.

14. Juni
Die USA reichen via FBI bei einem Bundesgericht in Virginia Anklage gegen Edward Snowden wegen Spionage und Diebstahl von Regierungseigentum ein.

22. Juni
Ein US-Bundesgericht stellt einen Haftbefehl gegen Edward Snowden aus und Hongkong wird aufgefordert, ihn auszuliefern. Kurz darauf wird auch sein Reisepass für ungültig erklärt.

23. Juni
Snowden flieht mit der Hilfe der Organisation WikiLeaks nach Moskau.

Snowden und die Folgen

Edward Snowden hat mit seinen Enthüllungen ein Umdenken angestoßen, auch in Deutschland. Die Sicherheit von Daten im Land prägt mittlerweile viele Diskussionen – und diese werden inzwischen in aller Öffentlichkeit und nicht nur zwischen Computerfreaks und Sicherheitspolitikern geführt.

Mit den bisherigen Enthüllungen ist ein enormer Vertrauensverlust gegenüber den USA einhergegangen. Dies zeigt sich beispielsweise im massiven Widerstand gegen die geheim verhandelten Freihandelsabkommen TTIP und CETA.

Die freiwillige, teilweise auch unfreiwillige Zusammenarbeit von nationalen Kommunikationsbetreibern und IT-Produzenten mit der NSA war in diesem Ausmaß vorher nur denjenigen bekannt, die spezielle Literatur über die NSA verfolgten.

US-amerikanische Soft- und Hardwareprodukte, die den Markt weltweit dominieren, werden zunehmend kritischer bewertet. Das Silicon Valley fürchtet dauerhaften Schaden durch den entstandenen Vertrauensverlust. Daten werden im großen Stil von US-Clouds weg verlagert.

Selbst die private Kommunikation wird heute teilweise unter einem neuen Aspekt gesehen: Kommunizierte man bisher nach dem Motto „Ich habe ja nichts zu verbergen", spielen heute Verschlüsselung und Sicherheitsapplikationen eine immer wichtigere Rolle, um staatlichen Stellen die Einschränkung der informationellen Selbstbestimmung zu erschweren.

Im Rahmen der Snowden-Veröffentlichungen kam der Begriff „digitale Souveränität" auf, der seither die Diskussionen immer wieder prägt.

In der Politik sind die anfänglichen Spannungen (Kanzlerin Merkel: „Ausspähen unter Freunden, das geht gar nicht!") mittlerweile völlig abgeflaut. Selbst der Parlamentarische Untersuchungsausschuss wird zu einem Ergebnis kommen, das kaum neue Spannungen aufkommen lassen wird. Eine Befragung Snowdens wurde vermieden, um die USA nicht zu verprellen. Diese betrachten ihn als Landesverräter, der die nationale Sicherheit untergraben hat.

Im NATO-Bündnisrahmen wird man aus strategischen Gründen kein dauerhaft abgekühltes Verhältnis zu den USA riskieren wollen. Aufgrund der traditionell engen Zusammenarbeit der „Five-Eyes-Staaten" (USA, Großbritannien, Kanada, Australien und Neuseeland) wird Kontinentaleuropa durch den „Brexit" noch stärker in den Fokus dieser Nachrichtendienste treten.

Die Aufklärungsbemühungen des britischen GCHQ gegen EU-Einrichtungen sind bekannt und werden zukünftig sicherlich intensiviert werden. Während in der öffentlichen und privatwirtschaftlichen Diskussion die Bemühungen um „digitale Souveränität" oft als Streben nach mehr Unabhängigkeit von staatlicher Kontrolle aufgefasst werden, verstehen deutsche Sicherheitspolitiker diesen Begriff etwas anders: Hier wird eher das Ungleichgewicht zwischen den Möglichkeiten der „Five Eyes" und den eigenen Diensten betont. Ziel dieser Diskussion ist eine Stärkung der eigenen Fähigkeiten.

Offensichtlich sind die beiden Ziele gegenläufig und die Suche nach dem Ausgleich gestaltet sich so schwierig wie eh und je. Neu ist lediglich, dass die Diskussion mehr im Licht der Öffentlichkeit und unter Einbeziehung vieler gesellschaftlicher Gruppierungen geführt wird und nicht – wie vor Snowden – nur zwischen Computerfreaks und Sicherheitspolitikern.

Direkte Veränderungen durch Snowden

- Bundesregierung beendet Vertrag mit Provider Verizon
- Bundestag verabschiedet das IT-Sicherheitsgesetz
- Bundesregierung setzt ein BND-Gesetz mit klaren Befugnissen in Kraft
- Aufbau der neuen „Entschlüsselungsbehörde" ZITIS in Deutschland
- In Deutschland wurde für sicherheitsrelevante öffentliche Aufträge eine No-Spy-Klausel eingeführt
- Brasilien kündigt Vertrag über die Lieferung von 36 Kampfjets mit Boeing
- Indien kündigt Zusammenarbeit mit Google zur Wählerregistrierung
- Cisco-Verkaufszahlen in China fallen um 10 %
- China nennt das iPhone eine „Bedrohung der nationalen Sicherheit".
- Russland plant, Intel- und AMD-Prozessoren durch BAIKAL-CPUs sowie Windows durch Linux zu ersetzen.

Abgelehnte bzw. nicht umgesetzte Vorschläge nach Snowden

- „Schengen-Netz": Innereuropäischer Datenverkehr darf nicht über das Ausland geroutet werden.
- No-Backdoor-Klausel: IT-Hersteller dürfen keine geheimen Zugriffsmöglichkeiten in Produkte einbauen.
- „Plattform vertrauenswürdige IT": Deutschland baut eigene sichere IT-Produkte.
- Verbindliche Einführung BSI-zertifizierter Lösungen für die Verwaltung
- Deutschland wird zum Verschlüsselungsstandort Nr. 1.

Das Snowden-Leak

Was können Unternehmen lernen?

Das war der Kern von Snowdes Interesse: aufzuzeigen, wie die NSA organisatorisch und technisch strukturiert ist – das heißt, wie sie arbeitet.

Die NSA sammelt und verwaltet in erheblichem Umfang sensible Daten und unternimmt große Anstrengungen, diese zu schützen. Dies trifft auch auf so manches Unternehmen zu. Es lohnt sich also ein näherer Blick, welche Schlüsse aus dem Datenabzug durch Edward Snowden für die Sicherung sensibler Informationen in Unternehmen gezogen werden können.

Die NSA beschäftigte im Mai 2013 rund 1.000 Systemadministratoren, welche zumeist externe Dienstleister waren. Nach Snowden kam der Gedanke auf, die Anzahl der Systemadministratoren radikal zu reduzieren und viele der administrativen Tätigkeiten zu automatisieren, statt durch Menschen ausführen zu lassen. Ferner sollte das Vier-Augen-Prinzip für bestimmte Tätigkeiten ausgeweitet werden.

Außerdem beschloss die NSA, technische Maßnahmen, wie das Zugriffsmonitoring oder die Überwachung der Zugangsschlüssel, zu verbessern.

Aus unserer Sicht sind dies gute organisatorische und technische Maßnahmen, die jedoch auf Symptom- und nicht auf Ursachenebene ansetzen. Folgende Aspekte aus diesem Vorfall sind zu beachten, um auf Dauer wirksame Maßnahmen abzuleiten:
Nach den Anschlägen vom 11. September 2001 stellte die NSA fest, dass Hinweise übersehen bzw. nicht rechtzeitig ausgewertet worden waren. Eine Konsequenz daraus war, Analysten einfachen und schnellen Zugriff auf die zu analysierenden Daten zu ermöglichen, in der Hoffnung, dass dadurch weniger Hinweise übersehen werden – frei nach dem Motto: Mehr Augen sehen mehr. Diese Vorgabe hatte natürlich auch Auswirkungen auf die gesamte Organisation, beispielsweise darauf, wie mit Daten umgegangen wurde.

Die bereichsübergreifende Zusammenarbeit von Abteilungen wurde gestärkt und störende Einschränkungen teilweise gelockert. Der zunehmende Wissensaustausch über mehrere Abteilungen hatte augenscheinlich auch zur Folge, dass verstärkt bereichsübergreifende Dokumentationen erstellt wurden, um eine effiziente Zusammenarbeit zu ermöglichen.

Es ist festzuhalten, dass Snowden offenbar kaum Datenbanken mit sensiblen abgefangenen Überwachungsdaten mitgenommen hat. Viele der Informationen scheinen vielmehr aus den internen Wissensdatenbanken zu stammen, welche für die Zusammenarbeit größerer Gruppen gedacht sind.

Welchen Trend setzen US-Präsidenten zur Nutzung der NSA-Kapazitäten zur wirtschaftlichen Vorteilsbeschaffung? Eine Einschätzung:

Die Mission wirtschaftlicher Vorteilsbeschaffung durch die NSA im Laufe der Präsidentschaft und im Vergleich zum vorhergehenden US-Präsidenten:

- in Teilen durch eine strategische Schwerpunktverlagerung stärker gewichtet
- im Wesentlichen nicht verändert
- in Teilen durch eine strategische Schwerpunktverlagerung niedriger gewichtet

George Bush
1989 - 1993

Bill Clinton
1993 - 2001

Das war der Kern von Snowdens Interesse: aufzuzeigen wie die NSA organisatorisch und technisch strukturiert ist – das heißt, wie sie arbeitet.

Mit der „Öffnung nach innen" erfolgte jedoch keine ausreichende Stärkung derjenigen Strukturen, an die sich Mitarbeiter mit Bedenken wenden konnten bzw. deren Aufgabe es war, auf Warnhinweise, so genannte Red Flags, angemessen zu reagieren. Zwar existierte eine Hotline für Whistleblower im Department of Defense Inspector General (DoD IG), diese konnte allerdings den zugesagten Schutz der Hinweisgeber (z. B. bei Thomas Drake) am Ende nicht einhalten und war offensichtlich auch nicht in der Lage, Probleme frühzeitig ordentlich zu behandeln.

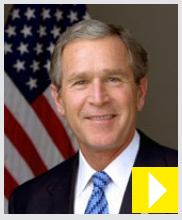
Dabei hätte auffallen können, dass verschiedene Personen faktisch gesehen wegen derselben Bedenken gegen die NSA zu Felde zogen – nämlich die überbordende Überwachung der amerikanischen Gesellschaft. William Binney, Kirk Wiebe, Edward Loomis und Diane Roark wandten sich 2002 gemeinsam an die Aufsichtsbehörde des US-Verteidigungsministeriums (DoD IG), Russ Tice 2005 an den Kongress und die Medien, Thomas Drake und Mark Klein (Telefonanbieter AT&T) ebenfalls 2005 an die Medien. Wären effektive Strukturen zur Erkennung vorhanden gewesen und wären die richtigen Schlussfolgerungen gezogen worden, hätte es die Veröffentlichungen von Edward Snowden mit ziemlicher Sicherheit in dieser Form nicht gegeben.

Die Reaktionen der Whistleblower rühren unter anderem daher, dass der Grundsatz „Du sollst US-Personen nicht ohne FISA-Gerichtsbeschluss ausspionieren" (abgeleitet aus dem 4. Zusatzartikel zur Verfassung der Vereinigten Staaten) den NSA Intelligence Officers immer wieder als eine der wichtigsten Richtlinien eingeschärft wurde. Aus Sicht der Whistleblower wie Snowden hatte die NSA-Führung ihre eigenen Prinzipien wiederholt gebrochen, war also nicht mehr glaubwürdig. Snowden zog seine Konsequenzen und wählte seinen eigenen Weg.

Für Unternehmen, die ebenfalls sensible Informationen schützen müssen, sind folgende einfache aber wichtige Leitgedanken festzuhalten:

- Hinweisen auf einen Verstoß gegen Grundsätze sollte im Unternehmen angemessen nachgegangen werden bzw. es sollte aktiv nach Warnhinweisen gesucht werden.
- Bei stichhaltigen oder mehrmaligen Hinweisen sollten entweder
  - die problematischen Prozesse eingestellt, also den Bedenken Rechnung getragen werden, oder
  - die problematischen Bereiche auf eine kleine Gruppe von Wissensträgern eingeschränkt und diese angemessen überwacht werden.

Die NSA wollte sich wegen konkurrierender Ziele nicht zu diesen Maßnahmen entscheiden, mit bekanntem Ausgang.



George W. Bush
2001 - 2009

Barack Obama
2009 - 2017

Donald Trump
2017 -


NSA

Aufklärungsziel Deutschland

Zusammenfassung der Ziele der NSA

Eine der wichtigsten Erkenntnisse aus den Snowden-Dokumenten für Deutschland ist, dass unsere Wirtschaft erklärtes Spionageziel der NSA ist. Das gilt natürlich nicht für die gesamte Wirtschaft, sondern insbesondere für Bereiche von US-strategischem Interesse.

Die Seiten 22 – 39 betrachten tiefgehend das Aufklärungsziel Deutschland. Zusammenfassend ist dabei festzuhalten: Von Interesse sind nach der „Strategic Mission List" aus dem Jahr 2007 „kritische Technologien, die einen strategischen militärischen, wirtschaftlichen oder politischen Vorteil bieten". Darunter fallen:

- Hoch- und Niedrig-Energielaser
- Fortschritte bei der Datenverarbeitung und Informationstechnologie
- Waffen mit gerichteter Energie
- Tarnungs- und Tarnungsentdeckungstechnik
- Elektronische Kriegsführung
- Raumfahrt- und Fernsensoren
- Elektro-Optik
- Nanotechnologie und energetische Materialien.

Diese Technologien stellen dem Strategiepapier zufolge eine potentielle Bedrohung für die Vormachtstellung der USA dar. Die Länder im Fokus dabei sind Russland, China, Indien, Japan, Deutschland, Frankreich, Korea, Israel, Singapur und Schweden.

Länder im Fokus der NSA bei kritischen Technologien:

Es ist zu erwarten, dass diese Liste von Prioritäten und Technologien sich über die Jahre bereits verändert hat und tendenziell die Zahl der Ziele eher zu- als abnimmt. Das heißt, je innovativer Deutschland in Bereichen ist, die die politische, militärische und wirtschaftliche Dominanz der USA gefährden könnten, desto interessanter werden Deutschlands Unternehmen für die NSA-Überwachung.

Da bisher lediglich rund drei Prozent der von Edward Snowden entwendeten Dokumente veröffentlicht worden sind, ist denkbar, dass sich im Rest noch weitere Informationen über das Aufklärungsziel Deutschland befinden. Doch bisher ist das Strategiepapier aus 2007 der deutlichste Hinweis darauf, dass die deutsche Wirtschaft seit geraumer Zeit im Fadenkreuz der NSA steht.

Worauf sich die Spionage im Einzelnen konzentrieren soll, wird aus einem Spionageauftrag gegen Frankreich deutlich, der in einem Dokument, veröffentlicht auf Wikileaks, enthalten ist.

Die „National SIGINT Requirements List (NSRL): Information Need (IN) - France: Economic Developments 2012" gibt den Auftrag, die politische Meinungsbildung in der französischen Regierung aufzuklären (z. B. Sichtweisen auf G-8/G-20 Themen), aber auch konkrete französische Geschäftsaktivitäten zu durchleuchten:

- Vertragsverhandlungen und Machbarkeitsstudien zu Großprojekten über $ 200 Mio.
- Informationen über die Finanzierung dieser Großprojekte

Die Branchen, die dabei im Fokus stehen, sind zahlreich:

- IT
- Netzwerk- und Kommunikationstechnologie
- Strom- und Energie
- Öl und Gas
- Kernenergie und erneuerbare Energien
- Transport- und Verkehrsinfrastruktur wie Häfen
- Flughäfen und U-Bahnen
- Umwelttechnik
- Gesundheits- und Biotechnologie

Es ist davon auszugehen, dass Spionageaufträge wie die „National SIGINT Requirements List" gegen deutsche Ziele ähnlich aussehen, wenn nicht sogar genauso, wie der Auftrag gegen Frankreich.

Aufklärungsziel Deutschland

Kunden und Aufgaben der NSA

Präsentationsfolie aus den Snowden-Unterlagen zu Kunden und internen Interessensgruppen der NSA.

Die Snowden-Unterlagen zeigen es deutlich, die NSA hat eine klare Vorstellung, wer ihre Kunden sind. Ihr Geschäftsmodell ist es, die eigene Tätigkeit so auszurichten, dass genug wichtige Ziele überwacht werden, um den Entscheidern und Informationsabnehmern ständig wertige Informationen und Dienste liefern zu können.

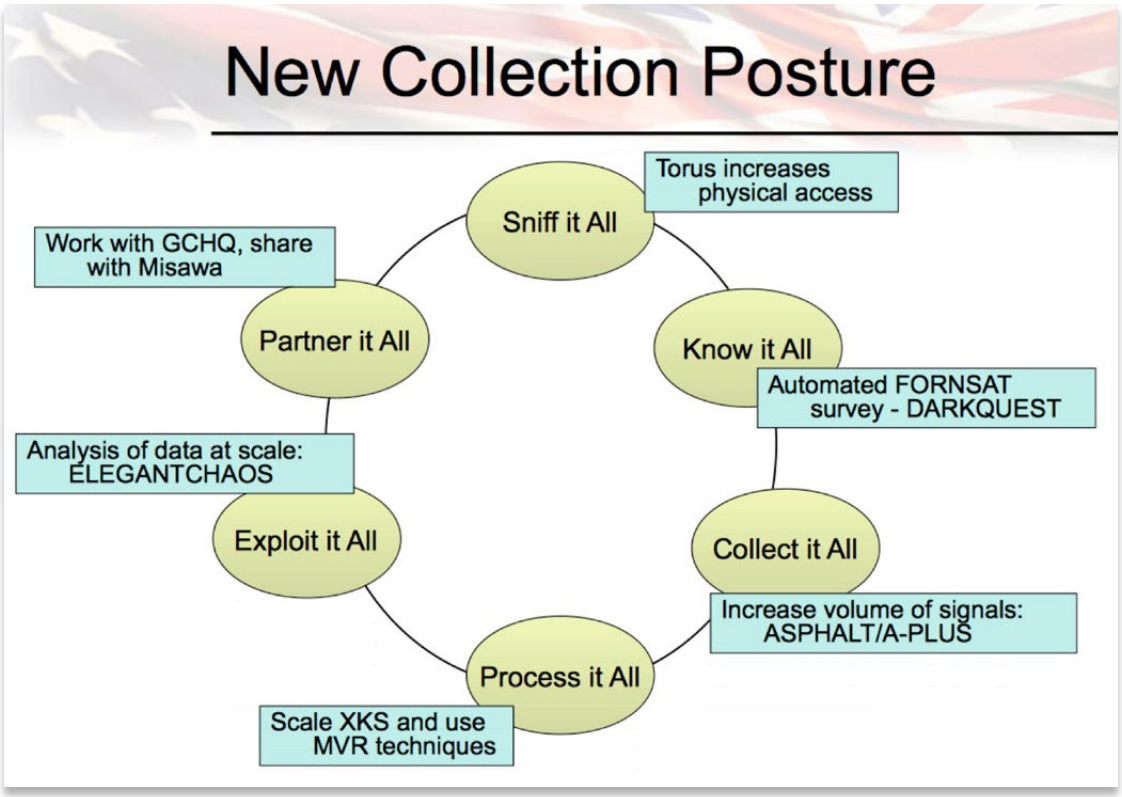
Die oben stehende Präsentationsfolie aus den Snowden-Unterlagen (siehe Abbildung) zeigt sehr übersichtlich aufbereitet, wer alles die möglichen Kunden der NSA sind. Dass diverse Militäreinheiten, Militärallianzen, Geheimdienste und politische Entscheidungsträger mit Informationen versorgt werden, überrascht nicht. Die Nennung der Strafverfolgung, als eine der Säulen, ist allerdings von Interesse.

An Wirtschaftsinformationen dürften vor allem folgende Kunden interessiert sein:

- US Handelsvertretungen
- Landwirtschaftsministerium
- Justizministerium
- Finanzministerium
- Handelsministerium
- Energieministerium

BEWERTUNG
Kunden der NSA haben in Teilen ein natives Interesse an ökonomischen Aspekten.

Präsentationsfolie aus den Snowden-Unterlagen zu Kunden und internen Interessensgruppen der NSA.



In einer weiteren Präsentationsfolie aus den Snowden-Unterlagen (oben stehende Abbildung) stellt die NSA ihr verändertes Aufgabenverständnis aus technischer Sicht dar.

- Alles abgreifen
- Alles wissen
- Alles sammeln
- Alles bearbeiten
- Alles ausnutzen
- Mit allen partnern

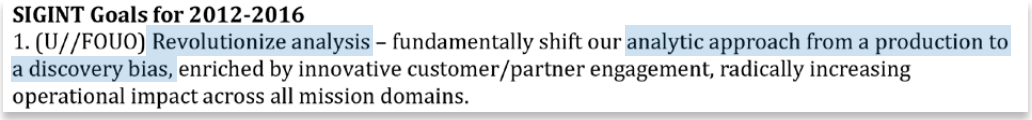
BEWERTUNG

Aus technischer Sicht ist es die Aufgabe der NSA, alle interessanten Informationen zu sammeln, aufzubereiten und zu verteilen.

Aufklärungsziel Deutschland

Strategischer Plan der NSA

Auszug aus „SIGINT Strategy 2012-2016“ aus den Snowden-Unterlagen zu ersten strategischen Ziel in diesem Zeitraum.



SIGINT Goals for 2012-2016

1. (U//FOUO) Revolutionize analysis – fundamentally shift our analytic approach from a production to a discovery bias, enriched by innovative customer/partner engagement, radically increasing operational impact across all mission domains.

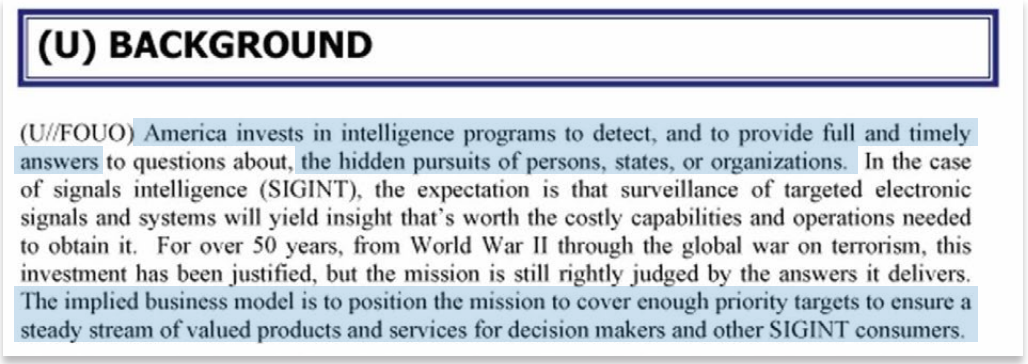
Der strategische Plan „SIGINT Strategy 2012-2016“ aus den Snowden-Unterlagen (oben stehende Abbildung) fasst neben kurzen Vision & Mission Statements auch allgemein zu erreichende Ziele für den Zeitraum 2012-2016 auf fünf Seiten zusammen. Dabei steht die Weiterentwicklung der Analyse- und Erfassungsfähigkeiten aber auch der internen Strukturen im Fokus. Ein interessantes übergeordnetes Ziel ist beispielsweise:

Analyse revolutionieren – Grundlegende Änderung unseres Analyseansatzes weg von einem Produktions- zu einem Entdeckungs-Ansatz, angereichert mit einer innovativen Kunden-/Partner-Einbindung, um drastisch die operative Auswirkung über alle Missionsfelder zu steigern.

BEWERTUNG

Die NSA will gemeinsam mit ihren Kunden die gesammelten Daten nach interessanten Erkenntnissen durchforsten und nicht mehr erst Aufklärungsziele festlegen und darauf aufbauend passende Daten sammeln.

Auszüge aus „SIGINT Mission Strategic Plan FY2008-2013“ aus den Snowden-Unterlagen zu Hintergründen des strategischen Plans.



(U) BACKGROUND

(U//FOUO) America invests in intelligence programs to detect, and to provide full and timely answers to questions about, the hidden pursuits of persons, states, or organizations. In the case of signals intelligence (SIGINT), the expectation is that surveillance of targeted electronic signals and systems will yield insight that's worth the costly capabilities and operations needed to obtain it. For over 50 years, from World War II through the global war on terrorism, this investment has been justified, but the mission is still rightly judged by the answers it delivers. The implied business model is to position the mission to cover enough priority targets to ensure a steady stream of valued products and services for decision makers and other SIGINT consumers.

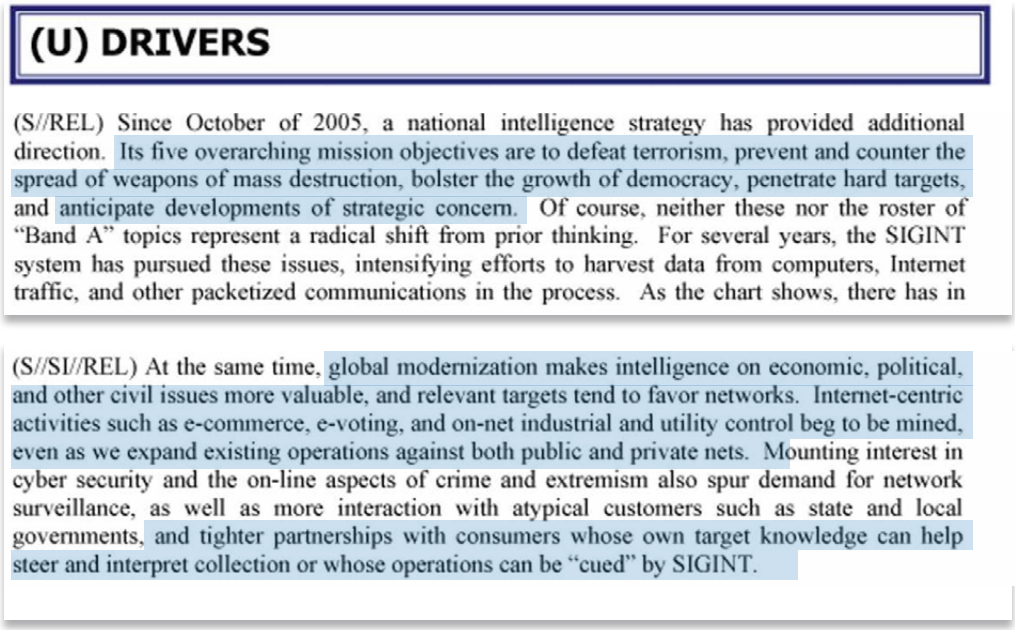
Detaillierter wird der Plan „SIGINT Mission Strategic Plan FY2008-2013“, der auf elf Seiten neben den Hintergründen und Treibern auch Schlüsselziele und Handlungsweisen beschreibt. Im Folgenden werden in Auszügen (Abbildung oben und auf den folgenden Seiten) die wichtigsten Erkenntnisse aus diesem Plan zusammengefasst.

Die NSA definiert sowohl Staaten als auch Organisationen und Einzelpersonen als Ziele der NSA Aufklärung. Dabei gilt es, Entscheidern und Informationsabnehmern ständig wertige Informationen und Dienste zu liefern.

BEWERTUNG

Staaten, Organisationen und Einzelpersonen sind Ziele der NSA Aufklärung.

Auszüge aus „SIGINT Mission Strategic Plan FY2008-2013“ aus den Snowden-Unterlagen zu den Treibern des Plans.



(U) DRIVERS

(S//REL) Since October of 2005, a national intelligence strategy has provided additional direction. Its five overarching mission objectives are to defeat terrorism, prevent and counter the spread of weapons of mass destruction, bolster the growth of democracy, penetrate hard targets, and anticipate developments of strategic concern. Of course, neither these nor the roster of "Band A" topics represent a radical shift from prior thinking. For several years, the SIGINT system has pursued these issues, intensifying efforts to harvest data from computers, Internet traffic, and other packetized communications in the process. As the chart shows, there has in

(S//SI//REL) At the same time, global modernization makes intelligence on economic, political, and other civil issues more valuable, and relevant targets tend to favor networks. Internet-centric activities such as e-commerce, e-voting, and on-net industrial and utility control beg to be mined, even as we expand existing operations against both public and private nets. Mounting interest in cyber security and the on-line aspects of crime and extremism also spur demand for network surveillance, as well as more interaction with atypical customers such as state and local governments, and tighter partnerships with consumers whose own target knowledge can help steer and interpret collection or whose operations can be "cued" by SIGINT.

Von den fünf genannten strategischen Missionszielen sind die letzten zwei auch aus wirtschaftlicher Sicht interessant:

- Vordringen zu schwierigen Zielen
- Entwicklungen von strategischer Wichtigkeit antizipieren

Die Feststellung passt dazu, dass die weltweite Modernisierung geheimdienstliche Aufklärung von wirtschaftlichen, politischen und anderen zivilen Informationen wertvoller macht und relevante Ziele zunehmend die Kommunikation über Computernetzwerke bevorzugen.

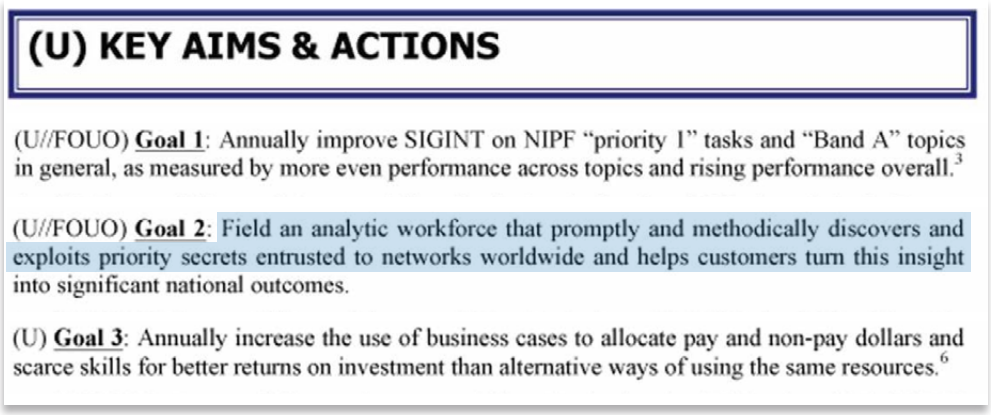
Vor dem Hintergrund der Ausweitung von bestehenden NSA-Operationen gegen öffentliche und private Netzwerke weist die NSA darauf hin, dass folgendes im Hinterkopf behalten werden soll: Internetaktivitäten wie e-Commerce, elektronische Wahlen und die netzwerkbasierte Steuerung von Industrieanlagen und Infrastrukturen.

BEWERTUNG

Wirtschaftliche, politische und andere zivile Informationen werden immer wertvoller. Die NSA denkt unter anderem an e-Commerce, elektronische Wahlen und die netzwerkbasierte Steuerung von Industrieanlagen und Infrastrukturen.

Aufklärungsziel Deutschland

Auszug aus „SIGINT Mission Strategic Plan FY2008-2013“ aus den Snowden-Unterlagen zu den Zielen und Tätigkeiten.



(U) KEY AIMS & ACTIONS

(U//FOUO) **Goal 1**: Annually improve SIGINT on NIPF "priority 1" tasks and "Band A" topics in general, as measured by more even performance across topics and rising performance overall.[3]

(U//FOUO) **Goal 2**: Field an analytic workforce that promptly and methodically discovers and exploits priority secrets entrusted to networks worldwide and helps customers turn this insight into significant national outcomes.

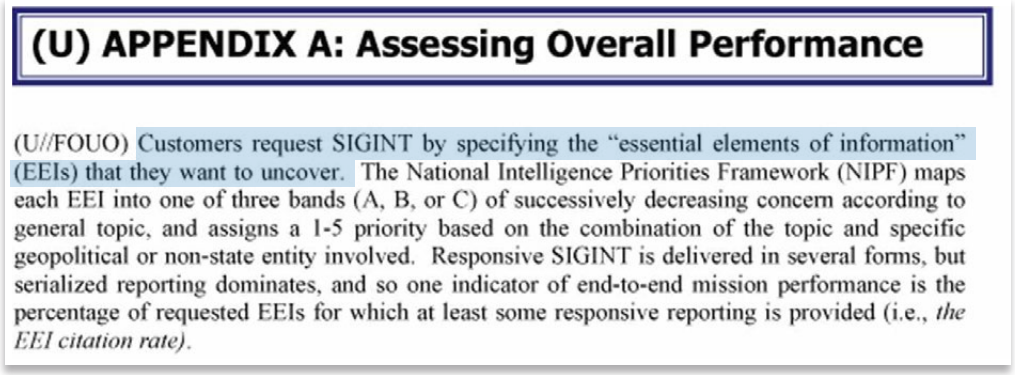
(U) **Goal 3**: Annually increase the use of business cases to allocate pay and non-pay dollars and scarce skills for better returns on investment than alternative ways of using the same resources.[6]

Im Einklang mit dem NSA-Ziel „Analyse revolutionieren“ aus der SIGINT Strategy 2012-2016“ steht das formulierte Ziel 2:

Aufbau einer Analysten-Einheit, die schnell und methodisch hochwertige Geheiminformationen aus Netzwerken rund um die Welt entdecken und extrahieren sowie den Kunden helfen kann, diese Information in signifikante innerstaatliche Ergebnisse umzusetzen.

BEWERTUNG
Die Sammlung und Auswertung soll bei der NSA schnelllebiger werden.

Auszug aus „SIGINT Mission Strategic Plan FY2008-2013“ aus den Snowden-Unterlagen, wie Kunden Spionageaufträge an die NSA stellen können.



(U) APPENDIX A: Assessing Overall Performance

(U//FOUO) Customers request SIGINT by specifying the "essential elements of information" (EEIs) that they want to uncover. The National Intelligence Priorities Framework (NIPF) maps each EEI into one of three bands (A, B, or C) of successively decreasing concern according to general topic, and assigns a 1-5 priority based on the combination of the topic and specific geopolitical or non-state entity involved. Responsive SIGINT is delivered in several forms, but serialized reporting dominates, and so one indicator of end-to-end mission performance is the percentage of requested EEIs for which at least some responsive reporting is provided (i.e., *the EEI citation rate).*

Im Anhang wird darauf verwiesen, dass Kunden der NSA die elektronische Informationsgewinnung beauftragen können, indem Sie die wichtigen Informationselemente (EEIs) beschreiben, die sie aufdecken wollen.

BEWERTUNG
Spionageaufträge werden in der NSA-Fachsprache als „Essential Elements of Information“ (EEI) bezeichnet und diese werden durch NSA-Kunden definiert.

Zusammenfassung NSA Vision & Mission

NSA/CSS Vision

Wir liefern DEN entscheidenden Vorsprung, um das volle Spektrum der nationalen US Sicherheitsinteressen voranzutreiben - das ist unsere Vision. Dabei wollen wir unverzichtbarer Informations- und Dienste-Lieferant für Entscheider und Informationsabnehmer sein. Wir ermitteln Informationen und geben Antworten zu Staaten, Organisationen und Einzelpersonen und deren verborgenen Aktivitäten.

Interpretation von Corporate Trust auf Basis "SIGINT Strategy 2012-2016" & „SIGINT Mission Strategic Plan FY2008-2013"

NSA/CSS Mission

Wir verteidigen unsere Nation mit qualifizierten Arbeitskräften, ausgebildet, ausgestattet und befähigt, auf Geheimnisse unserer Widersacher zuzugreifen und diese zugänglich zu machen.

Unser Anspruch gilt weltweit, DER Geheimdienst mit technischem Fokus zu sein, der globale Dominanz in allen Netzwerken hat.
Hierzu:

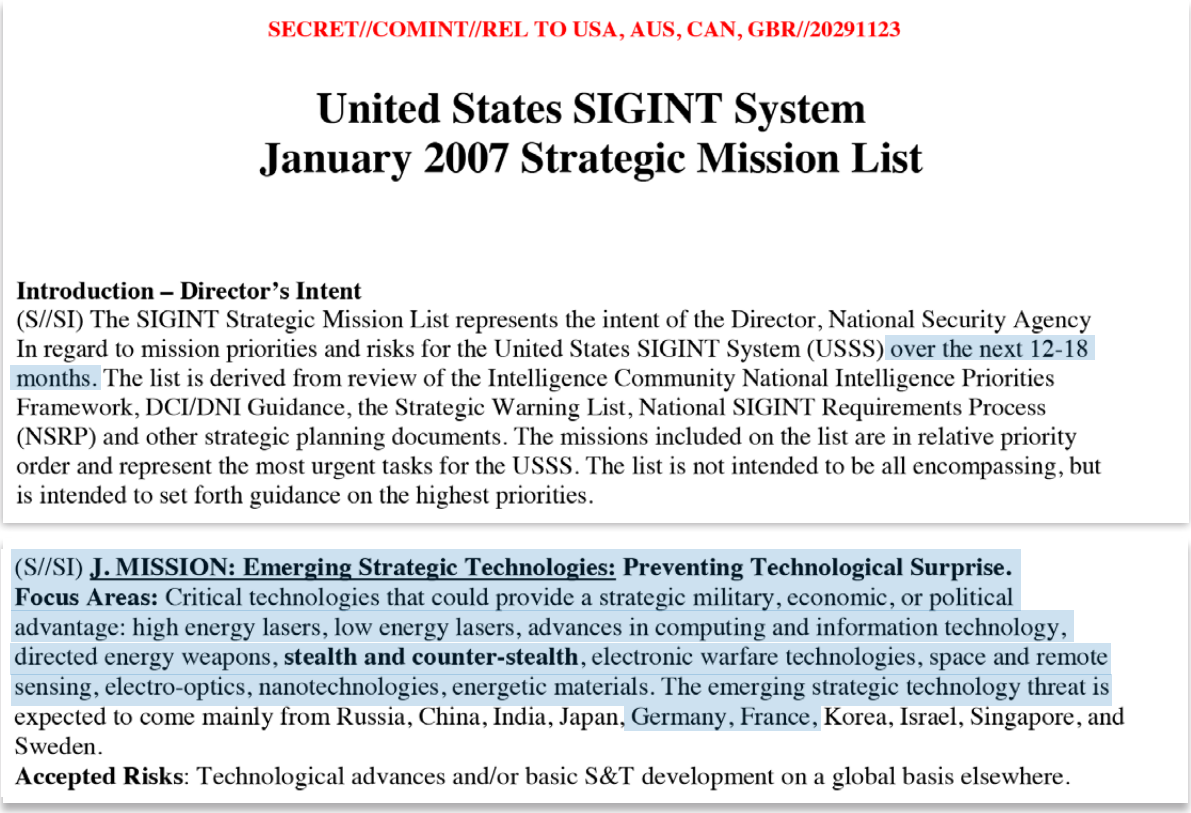
- Greifen wir alles ab
- Wissen wir alles
- Sammeln wir alles
- Bearbeiten wir alles
- Nutzen wir alles aus
- Teilen wir alles mit unseren Partnern

Interpretation von Corporate Trust auf Basis "SIGINT Strategy 2012-2016", „SIGINT Mission Strategic Plan FY2008-2013" und Präsentationsfolie "New Collection Posture"

Aufklärungsziel Deutschland

Spionageaufträge

Auszug aus „United States SIGINT System – January 2007 Strategic Mission List“ aus den Snowden-Unterlagen zum strategischen Sendungsauftrag.



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

United States SIGINT System
January 2007 Strategic Mission List

Introduction – Director's Intent
(S//SI) The SIGINT Strategic Mission List represents the intent of the Director, National Security Agency In regard to mission priorities and risks for the United States SIGINT System (USSS) over the next 12-18 months. The list is derived from review of the Intelligence Community National Intelligence Priorities Framework, DCI/DNI Guidance, the Strategic Warning List, National SIGINT Requirements Process (NSRP) and other strategic planning documents. The missions included on the list are in relative priority order and represent the most urgent tasks for the USSS. The list is not intended to be all encompassing, but is intended to set forth guidance on the highest priorities.

(S//SI) **J. MISSION: Emerging Strategic Technologies: Preventing Technological Surprise.**
Focus Areas: Critical technologies that could provide a strategic military, economic, or political advantage: high energy lasers, low energy lasers, advances in computing and information technology, directed energy weapons, **stealth and counter-stealth**, electronic warfare technologies, space and remote sensing, electro-optics, nanotechnologies, energetic materials. The emerging strategic technology threat is expected to come mainly from Russia, China, India, Japan, Germany, France, Korea, Israel, Singapore, and Sweden.
Accepted Risks: Technological advances and/or basic S&T development on a global basis elsewhere.

Verdeutlicht wird der in Teilen wirtschaftliche Fokus der NSA bei der Betrachtung konkreter Aufklärungsaufträge oder darauf zielender Unterlagen.

Die „United States SIGINT System – January 2007 Strategic Mission List“, ein bislang viel zu wenig beachtetes Dokument aus den Snowden-Unterlagen, benennt auf zehn Seiten konkrete Missionsziele auch gegen Deutschland. Es handelt sich dabei um eine Liste des Jahres 2007 für die strategischen Missionen für die nächsten 1 - 1,5 Jahre. Im Folgenden werden in Auszügen (Abbildung oben und folgende Seite) die wichtigsten ökonomischen Zielsetzungen aus dieser Liste zusammengefasst.

Von besonderem Interesse für europäische Unternehmen ist „Mission J“, da dort erstaunlich klar umrissen Technologien und Länder genannt werden, die für die NSA von Interesse sind:

Mission J: neue strategische Technologien: Technische Überraschungen vermeiden.

Fokus: Kritische Technologien, die einen strategischen militärischen, wirtschaftlichen oder politischen Vorteil bieten könnten: Hoch-Energielaser, Niedrig-Energielaser, Fortschritte bei der Datenverarbeitung und Informationstechnologie, Waffen mit gerichteter Energie, Tarnungs- und Tarnungsentdeckungstechnik, elektronische Kriegsführung, Raumfahrt- und Fernsensoren, Elektro-Optik, Nanotechnologie und energetische Materialien. Die Bedrohung durch neue strategische Technologien wird aus Sicht der NSA hauptsächlich aus Russland, China, Indien, Japan, Deutschland, Frankreich, Korea, Israel, Singapur und Schweden kommen.

BEWERTUNG
Es gibt einen klaren Aufklärungsauftrag zu benannten strategischen Technologien. Bei diesen strategischen Technologien gibt es auch kein Pardon bei nahestehenden Ländern wie Deutschland, Frankreich oder Israel.

Auszug aus „United States SIGINT System – January 2007 Strategic Mission List“ aus den Snowden-Unterlagen zu strategischen Missionsaufträgen.

(S//SI) **M. MISSION: Foreign Intelligence, Counterintelligence; Denial & Deception Activities: Countering Foreign Intelligence Threats.**
Focus Areas: Espionage/intelligence collection operations and manipulation/influence operations conducted by foreign intelligence services directed against U.S. government, military, science & technology and Intelligence Community from: China, Russia, Cuba, Israel, Iran, Pakistan, North Korea, France, Venezuela, and South Korea
Accepted Risks: Espionage/intelligence collection operations against U.S. government, military, science & technology and Intelligence Community from: Taiwan and Saudi Arabia

Mission M gibt Hinweise, wen die NSA als besonders aktiv bei der (Wirtschafts-)Spionage einstuft. Dabei sticht aus europäischer Sicht Frankreich heraus.

Mission M: Auslandsgeheimdienste, Spionageabwehr; Tarnungs- und Täuschungsaktivitäten; Abwehr von ausländischen Geheimdienst-Bedrohungen

Fokus: Spionage-/Informationssammlungs-Operationen [...] gegen [...] US Forschung & Technologie von China, Russland, Kuba, Israel, Iran, Pakistan, Nordkorea, Frankreich, Venezuela, Südkorea.

BEWERTUNG
Als einziges europäisches Land wird Frankreich als nennenswerte Spionage-Bedrohung empfunden.

Auszug aus „United States SIGINT System – January 2007 Strategic Mission List“ aus den Snowden-Unterlagen zu strategischen Missionsaufträgen.

(S//SI) **O. MISSION: Economic Stability/Influence: Ensuring U.S. Economic Advantage and Policy Strategies.**
Focus Areas: Economic stability, financial vulnerability, and economic influence of states of strategic interest to the US: China, Japan, Iraq, and Brazil.
Accepted Risks: Economic stability, financial vulnerability, and economic influence of states of strategic interest to the US: Turkey and India.

Mission O ist aus volkswirtschaftlicher Sicht als bedenklich einzustufen. Es geht hervor, dass die USA in einigen Ländern die NSA benutzt, um den wirtschaftlichen Vorteil der USA und politische Strategien sicherzustellen. Als Unterpunkte hierzu sind unter anderem Instabilitäten in der Wirtschaft und im Finanzsystem von Interesse.

Mission O: Wirtschaftliche Stabilität/Einwirkungsmöglichkeit: Sicherstellen des wirtschaftlichen Vorteils der USA und der politischen Strategien.

Fokus: Wirtschaftliche Stabilität, finanzielle Angreifbarkeit und wirtschaftlichen Einfluss von Staaten von strategischem Interesse für die USA.

BEWERTUNG
Die USA nutzt die NSA, um in einigen Ländern ihren wirtschaftlichen Vorteil und politische Strategien sicherzustellen.

Aufklärungsziel Deutschland

Auszug aus „National SIGINT Requirements List: Information Need (IN) - France: Economic Developments“ aus einer Wikileaks-Veröffentlichung von Juni 2015.

```
IN Standard Report: S-C-2002-204

Title : (S//REL TO USA, AUS, CAN, GBR, NZL) France: Economic
Developments

Originator Classification : SECRET//REL TO USA, AUS, CAN, GBR, NZL

Table of Contents

   EEI A : (U//FOUO) Economic Relations with the United States
   EEI B : (S//REL TO USA, AUS, CAN, GBR, NZL) French Business
Practices
   EEI C : (S//REL TO USA, AUS, CAN, GBR, NZL) French
Financial/Macroeconomic Policy Development
   EEI D : (U//FOUO) Views On G-8, G-20 Developments/Issues
   EEI E : (U//FOUO) Budgetary Constraints/Contributions To NATO
   EEI F : (S//REL TO USA, AUS, CAN, GBR, NZL) French Views
   EEI G : (U//FOUO) Relations With Least Developed Countries (LDCs)
And Transitional States
   EEI H : (U//FOUO) Foreign Contracts/Feasibility
Studies/Negotiations
   EEI I : (U//FOUO) Relations With International Financial
Institutions
   EEI J : (S//REL TO USA, AUS, CAN, GBR, NZL) French Trade Policies

   EEI K : (U//FOUO) Questionable Trade Activities

(U//FOUO) Supported Element(s):

   CIA              DIA/DI           FEDERAL RESERVE BOARD    US TRADE REP
   COMMERCE         DIA/OSR-2        STATE/INR                DOE/IN
   DHS              DIA/USEUCOM      TREASURY
```

Durch die Wikileaks-Plattform wurden ferner US-Aufklärungsaufträge gegen Frankreich veröffentlicht, die die internen Prozesse der NSA weiter erhellen.

In der oben stehenden Abbildung werden elf Spionageaufträge zu neuen Entwicklungen in der französischen Wirtschaft angefordert (Punkte A-K).

Schon diese recht umfassenden, übergeordneten Aufklärungsziele enthalten interessante Erkenntnisse:

A. Ökonomische Beziehungen mit den Vereinigten Staaten
B. Französische Geschäftspraktiken
C. Entwicklungen der französischen Finanzpolitik/makroökonomischen Politik
D. Sichtweisen auf G-8/G-20 Themen
E. Haushaltsbeschränkungen/Beiträge zur NATO
F. Französische Sichtweisen
G. Beziehungen mit am wenigsten entwickelten Ländern und Transformationsländern
H. Verträge mit dem Ausland/Machbarkeitsstudien/Verhandlungen
I. Beziehungen zu internationalen Finanzinstituten
J. Französische Handelspolitik
K. Fragwürdige Handelsaktivitäten

In Verbindung mit den genannten Kunden, insbesondere Handelsministerium, Finanzministerium und US Handelsvertretungen bekommt man einen Eindruck, für welchen Zweck die Informationen unter anderem gesammelt werden sollen.

BEWERTUNG

Die Anforderung zur Informationssammlung gegen Frankreich betrifft auf breiter Front wichtige ökonomische und wirtschaftspolitische Aspekte. Interesse zeigen u.a. Handelsministerium, Finanzministerium und US Handelsvertretungen.

Auszug aus „ National SIGINT Requirements List: Information Need (IN) - France: Economic Developments: EEI: H - Foreign Contracts/Feasibility Studies/Negotiations“ aus einer Wikileaksveröffentlichung von Juni 2015.

EEI : H

EEI Classification : SECRET//NOFORN

Originator EEI Classification : SECRET//REL TO USA, AUS, CAN, GBR, NZL

EEI Title : (U//FOUO) Foreign Contracts/Feasibility Studies/Negotiations

Question(s) :

1. (S//REL TO USA, AUS, CAN, GBR, NZL) Report impending French contract proposals or feasibility studies and negotiations for international sales or investments in major projects or systems of significant interest to the foreign host country or $200 million or more in sales and/or services, including financing information or projects of high interest including:

A. Information and telecommunications facilities networks and technology?

B. Electric power, natural gas, and oil facilities and infrastructure to include nuclear power and renewable energy generation?

C. Transportation infrastructure and technology to include ports, airports, high-speed rail, and subways?

D. Environmental technologies used domestically and for export?

E. Health care infrastructure, services, and technologies, including biotechnology developments?

Zu Punkt H der Anforderung zur Informationssammlung gegen Frankreich findet sich auf Wikileaks ferner eine aufschlussreiche Detaillierung.

Zu berichten ist über konkrete französische Geschäftsaktivitäten. Dazu zählen Angebote und Machbarkeitsstudien für internationale Aufträge bzw. Investitionen, die 200 Mio. USD betragen oder übersteigen, inklusive Informationen finanzieller Natur. Interessant sind Technologien der Bereiche IT, Netzwerk- und Kommunikationstechnologie, Strom- und Energie, Öl und Gas, Kernenergie und erneuerbare Energien, Transport- und Verkehrsinfrastruktur wie Häfen, Flughäfen und U-Bahnen, Umwelttechnik, Gesundheits- und Biotechnologie.

WEITERE INFORMATIONEN

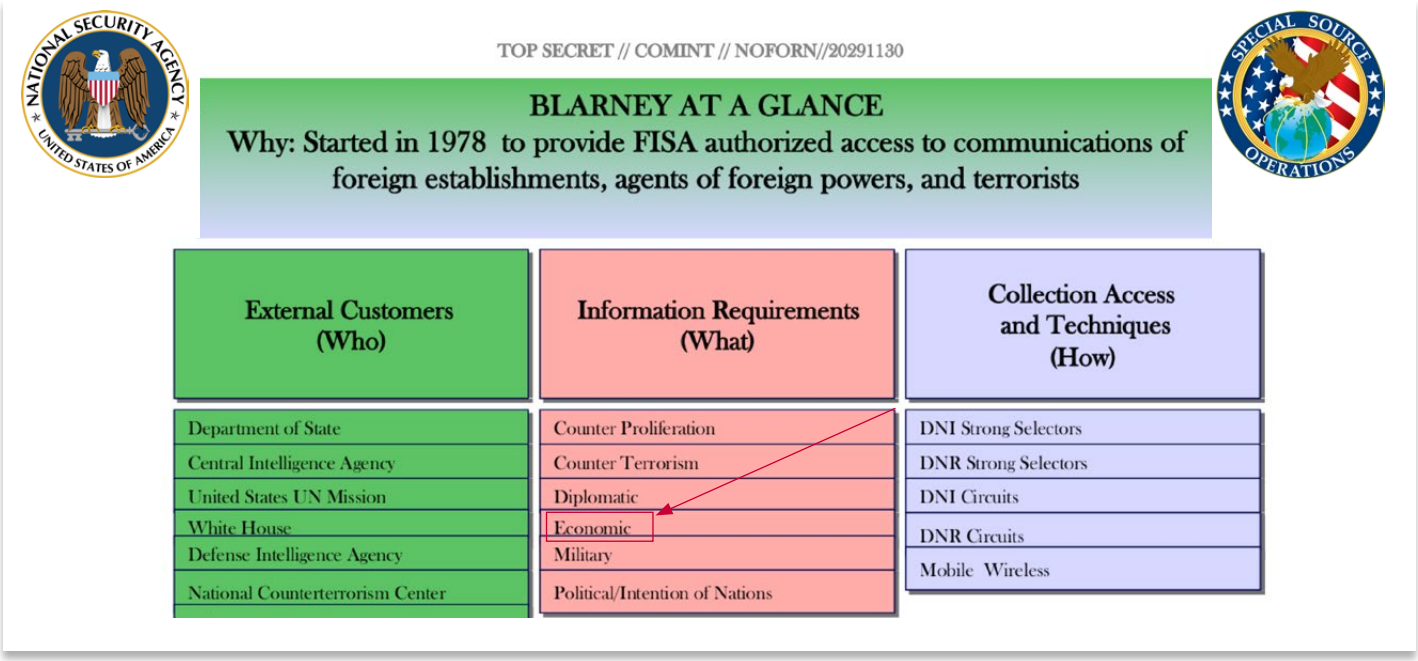
In einer sogenannten „National SIGINT Requirements List“ (NSRL) legt die NSA fest, in welchen Ländern was abgehört werden soll. Dabei handelt es sich um eine Art Spionage-Wunschkatalog. NSA-Kunden melden darin ihren Informationsbedarf an. Diese „Information Needs (IN)“ werden wiederum in Form von Essential Elements of Information (EEI) spezifiziert.

BEWERTUNG

Der Spionageauftrag gegen Frankreich zeigt ein breites Interesse an wirtschaftlichen Vorgängen, wie bevorstehende Auftragsvergaben, Machbarkeitsstudien oder Großprojekte generell.

Aufklärungsziel Deutschland

Präsentationsfolie aus den Snowden-Unterlagen zum Programm „BLARNEY“ und dessen auch wirtschaftlicher Ausrichtung.



In den Snowden-Unterlagen findet sich zu guter Letzt eine Präsentationsfolie, die aufzeigt, dass das Programm „BLARNEY“, welches zur Kommunikationsüberwachung dient, auch für wirtschaftliches Interesse genutzt wird.

BEWERTUNG

Auch Daten aus Programmen zur Kommunikationsüberwachung werden für wirtschaftliche Zwecke ausgewertet.

Aufklärungsziel Deutschland

Nuancen der Wirtschaftspionage

Amerikanische Behördenmitarbeiter sagen, dass es zwei unterschiedliche Dinge sind, ob man in Unternehmen nach Erkenntnissen über Wirtschaftsstrategie gräbt, oder tatsächlich Unternehmensgeheimnisse stiehlt.
Tageszeitung The Guardian, 2013

Stiehlt die NSA bei ihrer Spionage nur übergeordnete Informationen aus den Unternehmen, wie z. B. zu Strategie, Vertragsverhandlungen, Finanzierung, Großprojekten? Oder dringt sie weiter in die Tiefe vor bis zu dem, was die Amerikaner „trade secrets" nennen, den Firmengeheimnissen? Die Mittel dazu hätte sie.

Zur Beleuchtung dieser Nuancen fasste James Clapper, Direktor der nationalen Nachrichtendienste, nach den Veröffentlichungen bezüglich der Ausspähung von Brasiliens größtem Öl-Unternehmen Petrobras die Herangehensweise so zusammen:

James Clapper
Nationaler Geheimdienstdirektor der Vereinigten Staaten

„It is not a secret that the intelligence community collects information about economic and financial matters, and terrorist financing." „What we do not do, as we have said many times, is use our foreign intelligence capabilities to steal the trade secrets of foreign companies on behalf of – or give intelligence we collect to – US companies to enhance their international competitiveness or increase their bottom line." (September 2013)

Es ist davon auszugehen, dass diese Stellungnahme zwar glaubwürdig ist, aber auch wortwörtlich interpretiert werden muss. Schon der Begriff „trade secrets" lässt viel Spielraum: Informationen gelten nur dann als „trade secrets", wenn angemessene Anstrengungen unternommen wurden, um diese geheim zu halten. Clapper zufolge ist das Ausspähen von wirtschaftlichen Daten also in Ordnung, wenn es sich nicht um „trade secrets" handelt.

Ferner ist – laut dieser Aussage – auch das Stehlen von „trade secrets" erlaubt, wenn diese nicht bei Unternehmen selber, sondern beispielsweise von staatlichen Stellen, die im Besitz von Firmeninformationen sind, ausgespäht werden; oder wenn der Diebstahl nicht im Auftrag von US-Unternehmen geschah, um deren internationale Wettbewerbsfähigkeit oder ihren Profit zu steigern.

Die vorrangigen Kriterien bei jeder Form von Spionage der US-Dienste, auch bei der Wirtschaftsspionage, sind nationale strategische oder Sicherheitsinteressen der USA – ein weites Feld, das Spielraum für breit angelegte Spionageprogramme lässt.

Man erinnere sich nur an die ökonomischen Zielsetzungen aus der Strategic Mission List 2007: „Critical technologies that could provide strategic military, economic, or political advantage" – es folgt eine Aufzählung von im Jahr 2007 aktuellen Technologien und die Nennung von Ländern wie Deutschland und Frankreich. Ebenso sind die formulierten Informationsbedürfnisse in Bezug auf Frankreich aufschlussreich.

Das Interesse an „trade secrets" in Bezug auf bestimmte strategische Technologien ist also gut dokumentiert. Es ist aber nicht ausgeschlossen, dass weitere „trade secrets" bei den Datenausspähungen der NSA und anderer Dienste mit in den Sog geraten. Schon allein weil es technisch schwierig sein dürfte und Aufwand bedeuten würde, die „trade secrets" bei den groß angelegten Datenabzügen der NSA im Vorhinein herauszufiltern oder zu umgehen.

Insgesamt zeigt die Informationslage, dass die US-Geheimdienste derzeit breit angelegte Spionage mit wirtschaftlichem Interesse betreiben. Einschränkungen gibt es bei „trade secrets", ansonsten werden ökonomische Daten weitreichend gesammelt, ausgewertet und verwertet.

Das Internet [...] ermöglicht natürlich auch Feinden und Gegnern unserer demokratischen Grundordnung, mit völlig neuen Möglichkeiten und völlig neuen Herangehensweisen unsere Art zu leben in Gefahr zu bringen.

Angela Merkel,
Bundeskanzlerin, Juni 2013

Aufklärungsziel Deutschland

Lob und Dank von „Kunden“ der NSA

United States Department of State
Washington, D.C. 20320

May 7, 2009

TOP SECFRET//COMINT
DECL: 20340506

Dear General Alexander,

(TS//SI) On behalf of the Department of State, I would like to express my gratitude and congratulations for the outstanding signals intelligence support we received from the National Security Agency in the lead-up and aftermade of the Fifth Summit of the Americas (April 17-19). The Summit was a critical point of departure for U.S. Foreign Policy in our hemisphere: our new Administration was determined to build a productive, positive relationship with our neighbours, while our rivals in the region were equally determined to emberrass and discredit us. We succeeded and our rivals failed, and our success owes in good measure to the abundant, timely, and detailed reporting that you provided. The more than 100 reports we received from the NSA gave us deep insight into the plans and intentions of the Summit participants, and ensured that our diplomats were well prepared to advise President Obama and Secretary Clinton on how to deal with contentious issues, such as Cuba, and interact with difficult counterparts, such as Venezuelan President Chavez.

(TS//SI) Our work is far from done the Organization of American States General Assembly meeting next month will probably feature renewed discussion of Cuba, and such countries as Venezuela and Bolivia remain intent on challenging our interests in the short term - h.r. I am confident that NSA reporting will continue to give us the edge that our diplomacy needs.

Sincerely,

Thomas A. Shannon, Jr.
Assistant Secretary
Bureau of Western Hemisphere Affairs

TOP SECRET//COMINT
Classified by: John Dinger, INR A/S, Acting.
REASON FOR CLASSIFICATION: E.O. 12958 1.4 (c) and (d)
DECL ON: 20340506

Erstveröffentlichung: Epoca Aug 2, 2013.

Thomas A. Shannon, Jr.
Assistant Secretary (2009)
Bureau of Western Hemisphere Affairs

„Die mehr als hundert Berichte, die wir von der NSA bekamen, haben uns einen tiefen Einblick in die Pläne und Zusammenhänge anderer Gipfelteilnehmer verschafft.

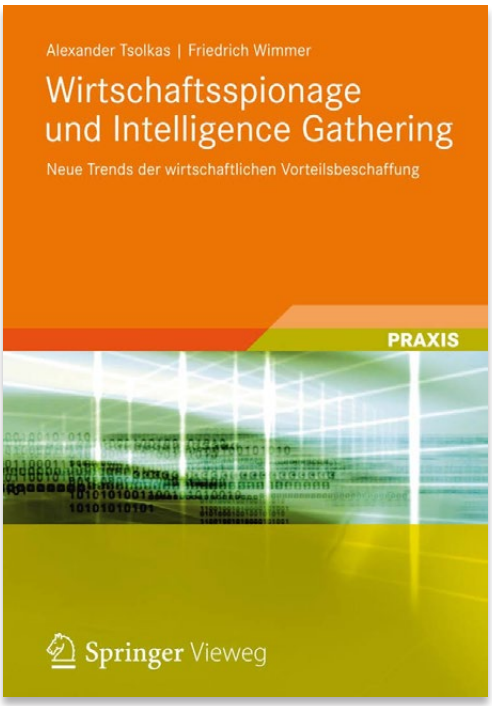
Dies hat sichergestellt, dass unsere Diplomaten gut vorbereitet waren, um Präsident Obama und Ministerin Clinton bei umstrittenen Themen, wie z. B. Kuba, und im Umgang mit schwierigen Gesprächspartnern, wie z. B. dem venezolanischen Präsidenten Chavez, richtig zu beraten."

Der Assistant Secretary for Western Hemisphere Affairs ist ein Amt im Außenministerium der Vereinigten Staaten. Innerhalb der Organisation des Außenministeriums untersteht dieser dem Unterstaatssekretär des Außenministeriums für politische Angelegenheiten (Under Secretary of State for Political Affairs).

Aufklärungsziel Deutschland

Schatten der Globalisierung

Informationsbeschaffung durch Auswertung von Massendaten (Big Data) ist der aktuelle Trend bei der Wirtschaftsspionage im 21. Jahrhundert.



Titel: Wirtschaftsspionage und Intelligence Gathering – Neue Trends der wirtschaftlichen Vorteilsbeschaffung
Autoren: Friedrich Wimmer, Alexander Tsolkas
Verlag: Vieweg+Teubner Verlag; Auflage: 2013 (1. Juli 2012)
Sprache: Deutsch
ISBN-10: 383481539X
ISBN-13: 978-3834815392

Zwei Einkäufer eines Unternehmens erhalten den Auftrag, innerhalb einer Stunde 2.000 Liter Benzin so günstig wie möglich zu beziehen. Einer darf hierzu ein Anbieter-Vergleichsportal mit aktuellen Benzinpreisen im Internet als Recherchequelle nutzen, der andere nur ein Branchenbuch. Auf wessen Erfolg würden Sie wetten?

Informationsvorsprung zählt und führt mit der Zeit zu einem enormen Wettbewerbsvorteil. Mag sein, dass der Einkäufer mit dem Branchenbuch beim ersten Mal Glück hat und genauso günstig einkaufen kann wie sein Konkurrent. Auf die Dauer gesehen wird er aber zwangsläufig ins Hintertreffen geraten. Ist er sich dieser Informationslücke nicht bewusst, wird er auch nicht feststellen können, wieso der andere Einkäufer erfolgreicher ist.

Intelligence Gathering mittels Big Data – das Kind der Wirtschaftsspionage im 21. Jahrhundert.

Zugegeben: Fälle, bei denen es um das Ausspionieren von technischem Know-how oder das Abhören von Beteiligten bei der Auftragsvergabe geht, sind spannend und die Auswirkungen meist offensichtlich. Es macht Spaß, darüber zu reden und nachzudenken. Gefordert wird der Zuhörer, wenn beispielsweise vom Abfluss von Informationen über Wettbewerbsstrategien, Preisgestaltung und Konditionen eines Unternehmens berichtet wird. Was sind die Auswirkungen, wie äußern sie sich? Für betriebs- oder volkswirtschaftlich Begeisterte erschließt sich der Zusammenhang sofort, für viele der anderen Zuhörer vielleicht nie. Die Gründe sind darin zu suchen, dass einerseits ein tiefgehendes Verständnis wirtschaftlicher Zusammenhänge benötigt wird und andererseits offensichtliche, kurzfristige Auswirkungen nur selten nachzuweisen sind. Man hat Kunden an einen Konkurrenten verloren – das muss nichts damit zu tun haben.

Technisch und wirtschaftlich hoch entwickelte Staaten sind genau an solchen Informationen interessiert und schätzen den Umstand der verdeckten Auswirkungen. Es besteht keine Gefahr, den Vorwurf der Wirtschaftsspionage auf sich zu ziehen, und gleichzeitig hat man alle Möglichkeiten der Wirtschaftssteuerung und -unterstützung.

Die Geheimdienste sammeln weitreichende Informationen, aus denen insbesondere mittels Big Data detaillierte Erkenntnisse zur wirtschaftlichen Tätigkeit von Unternehmen extrahiert werden können – wie etwa SWIFT-Bankdaten, Flugpassagier- und Verbindungsdaten, um nur einige zu nennen.

Erinnern wir uns noch einmal an die Benzin-Einkäufer. Mit korrekten Kennzahlen oder auch nur nützlichen Hinweisen können Entscheider konkrete wirtschaftliche Vorteile erlangen. Wie so etwas funktionieren kann, zeigt das im Jahr 2012 erschienene Buch „Wirtschaftsspionage und Intelligence Gathering – Neue Trends der wirtschaftlichen Vorteilsbeschaffung".

Nun wurden viele, der im Buch beschriebenen, Szenarien durch die Snowden-Veröffentlichungen mit Praxisbeispielen hinterlegt, obwohl diese nur einen kleinen Teil der U.S. Intelligence Community (Verbund der wichtigsten US-Nachrichtendienste) abdecken.

Ein NSA-Zweig namens „Follow the Money" ist für das Ausspähen von Finanzdaten zuständig, berichtete der Spiegel im September 2013. Die dort gewonnenen Informationen fließen in die NSA-eigene Finanzdatenbank „Tracfin".

Die Auswertung der Flug- und Verbindungsdaten wurden mit mehreren Programmen durchgeführt, allen voran „XKEYSCORE". Aber auch Programme wie „BLARNEY" arbeiten mit Verbindungsdaten.

Allerdings wird durch die Veröffentlichungen auch deutlich, dass GCHQ und NSA wirtschaftliche Interessen verfolgen. Viele der gesammelten Rohdaten werden in verschiedenen technischen Systemen zur Auswertung aufbereitet. Bei einigen dahinterliegenden Programmen finden sich Dokumente, die auch ökonomische Zielsetzungen beschreiben. Dies deckt sich mit NSA-Papieren auf strategischer Ebene der SIGINT-Abteilung, welche in unterschiedlicher Tiefe die ökonomischen Ziele beleuchten.

Dabei sind solche Informationen nicht nur auf betriebswirtschaftlicher, sondern auch auf volkswirtschaftlicher Ebene von Interesse.

Unbestritten ist etwa, dass mit einem Informationsvorsprung am Finanzmarkt systematisch Überrenditen erzielt werden können, weshalb beispielsweise der Insiderhandel in vielen Ländern eine Straftat darstellt. Hätten bestimmte Akteure am Markt dauerhaft einen Informationsvorsprung, würde dies langfristig eine wirtschaftliche Dominanz dieser Akteure bedeuten.

Wichtig zu verstehen ist, dass im Wirtschaftskreislauf immer mehr Daten über die wirtschaftliche Tätigkeit von Unternehmen anfallen oder gesammelt werden, mit denen sich bei entsprechender Analyse wirtschaftlich aufschlussreiche Erkenntnisse für interessierte Kreise extrahieren lassen. Dabei kommt es den Akteuren zugute, dass automatisiert über sehr viele Vorgänge der wirtschaftlichen Tätigkeit gewacht werden kann, ohne dass Unternehmen Einfluss auf die Generierung oder Verwendung dieser Daten ausüben können. Diese neue Thematik wird im Buch als „unbeherrschbare externe Datenhalden" oder „ungovernable external data heaps" (UEDH) definiert. Die Bezeichnung „Datenhalden" bzw. „data heaps" soll deutlich machen, dass es sich bei den thematisierten Daten nicht nur um Datenbanken im klassischen Sinne handeln kann, sondern um jegliche Ansammlung von Daten.

Dabei stehen die im Buch beschriebenen Datenbanken und die dazugehörigen Szenarien nur für eine neue, sich in Zukunft beschleunigende Thematik insgesamt. Aus diesen Gründen sollten vor allem besonders gefährdete Unternehmen einen anderen Blickwinkel bei der Spionageabwehr einnehmen. Um sich vor Spionage zu schützen, gilt es, sich nicht mehr nur mit klassischen Feldern zu befassen, sondern sich auch mit der Problematik der Gefährdung durch unbeherrschbare externe Datenhalden zu beschäftigen.

Würden Sie als Sicherheitsverantwortlicher Ihres Unternehmens freiwillig den gesamten Kundenstamm, die Termine aller Mitarbeiter bei Kunden und Lieferanten in Echtzeit oder die Vorlieben und Gewohnheiten Ihrer Führungspersonen freiwillig an die Konkurrenz weitergeben? Wahrscheinlich nicht. Aber genau solche (und mehr) Informationen lassen sich aus Daten generieren, die bei der tagtäglichen wirtschaftlichen Tätigkeit anfallen und auf die Unternehmen keinen oder nur geringen Einfluss haben. Genau deshalb können diese so aussagekräftig sein.

Intelligence Gathering – das Kind der Wirtschaftsspionage im 21. Jahrhundert: Es ist noch nicht erwachsen, aber es hat laufen gelernt.


PASSWORD
CRACKER
SPYWARE
CYBER
CODE
ENCRYPTION
TROJAN
SECURITY
IDENTITY
HACKER
THEFT
PHISHING
PRIVACY
VIRUS
INTRUSION
DETECTION

Derzeit ist ein Anwachsen von Mini-NSAs in aller Welt zu beobachten.

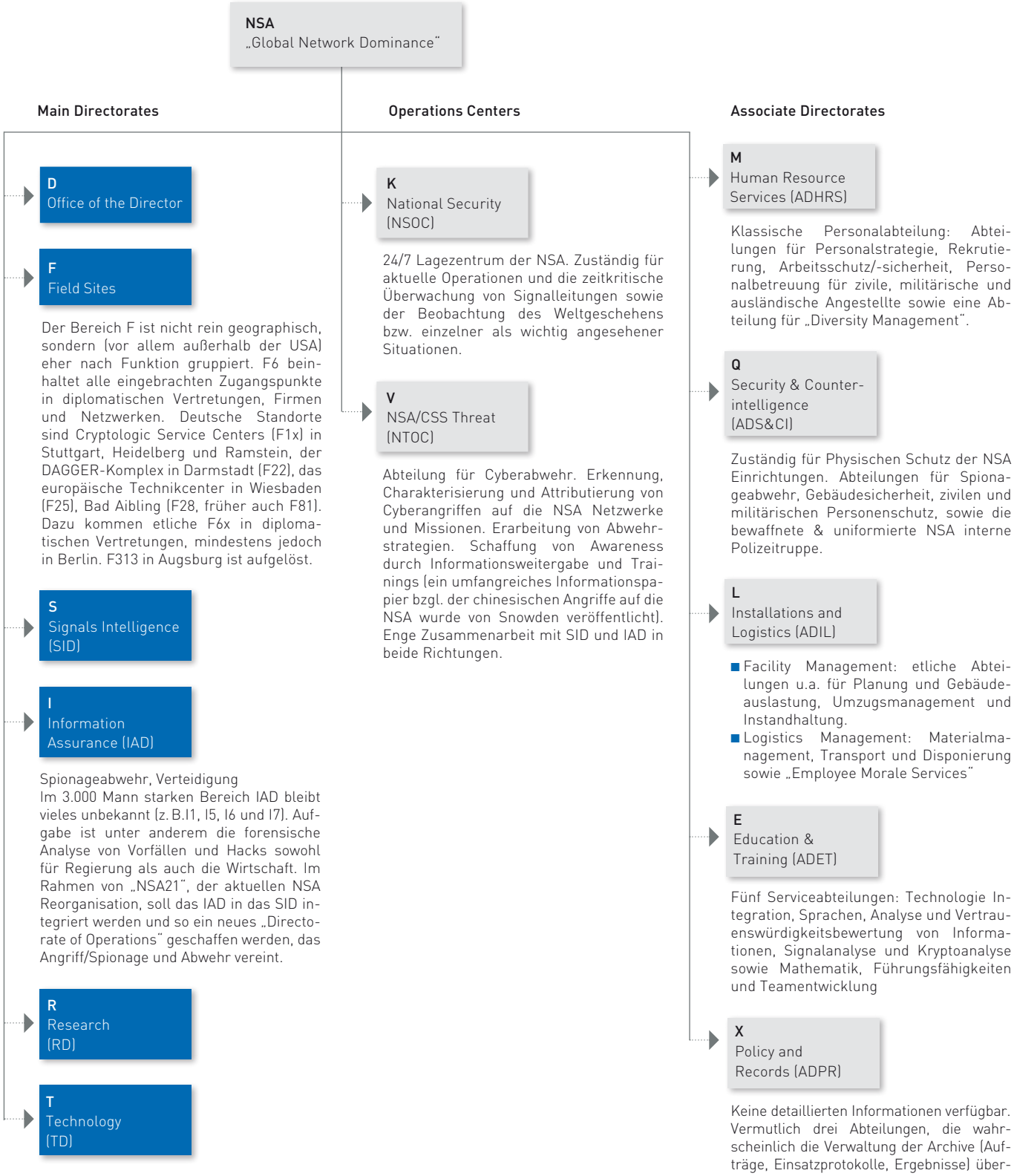
Dr. Ben Wagner, Direktor der Forschungsstelle Internet und Menschenrechte
an der Europauniversität Viadrina in Frankfurt an der Oder
17.12.2015

Es darf für Geheimdienste keine rechtsfreien Räume geben. Rechtsstaat und Grundrechte enden nicht an Deutschlands Grenzen.

Heiko Maas, Bundesminister der Justiz und für Verbraucherschutz
16. Juni 2015

Die NSA

Fähigkeiten und Aufbau der NSA



*einzelne Erläuterungen finden Sie auf den nachfolgenden Seiten

Die NSA ist mit etwa 40.000 Mitarbeitern in 31 Ländern offiziell aktiv. Sie ist zudem einer der größten Arbeitgeber im US-Bundesstaat Maryland, wo ihre Zentrale liegt.

Wer den Aufbau einer Organisation im Detail kennt, kann sich über ihre Fähigkeiten ein Bild machen. Durch die zahlreichen Veröffentlichungen von Edward Snowden und anderen Whistleblowern, aber auch durch Reden und Artikel von NSA-Mitarbeitern sowie Stellenausschreibungen auf dem NSA-Jobportal, ist dieses Bild über die Zeit immer präziser geworden. So werden Zusammenhänge sichtbar, die auch die Strukturen anderer Geheimdienste prägen – und auch nichtstaatliche Cybereinheiten werden an vielen Stellen denselben Prinzipien gehorchen. Ein intensiver Blick lohnt sich also.

In der NSA gibt es sechs Hauptabteilungen („main directorates"). Das „Office of the Director" ist die Leitungsorganisation der NSA Führung. Die Hauptabteilung „Field Sites" organisiert die dezentrale Arbeit. Die Struktur der Forschungsabteilung „Research Directorate" erlaubt einen Blick in die Zukunft, die Strukturen von IT-Betrieb („Technology Directorate") und Informationsschutz („Information Assurance Directorate") sind wenig überraschend.

Der interessanteste Bereich ist sicherlich die Spionageabteilung „Signal Intelligence Directorate", die sich in drei Unterabteilungen gliedert. Abteilung S3 ist für die Datensammlung und –akquise zuständig. S2 analysiert die gewonnenen Daten und generiert Auswertungen, die die NSA als ihre eigentlichen „Produkte" bezeichnet. S1 ist dann für den Vertrieb und die Kundenkommunikation verantwortlich.

Dementsprechend ist S2 nach Produktlinien organisiert: Eine Unterabteilung kümmert sich um Südasien-Auswertungen, eine andere um die Verbreitung von Massenvernichtungswaffen, eine dritte um Gegenspionage (also das Erkennen und Ausspähen anderer Geheimdienste). Abteilung S1 ist quasi als „Vertrieb" zuständig für die Weitergabe der Produkte. Hier finden sich Abteilungen für die Weitergabe an Partnerdienste, die Betreuung von Sonderereignissen (wie z. B. einen G7-Gipfel) oder das Account Management für die inländischen Anforderer (z. B. die CIA, das Weiße Haus, ein Ministerium, ein US-Botschafter oder eine Militäreinheit).

Technisch gesehen ist Abteilung S3 die interessanteste. Sie beschäftigt sich mit dem Knacken von Verschlüsselungen (S31), dem gezielten Eindringen in Netzwerke und Systeme (S32), der systematischen Erfassung von Kommunikations- und Verbindungsdaten an Kabeln, Internetknotenpunkten und per Satellit (S33), der Überwachung von Zielpersonen (S34) und dem umfassenden Zugriff auf die Daten in großen Rechenzentren (S35).

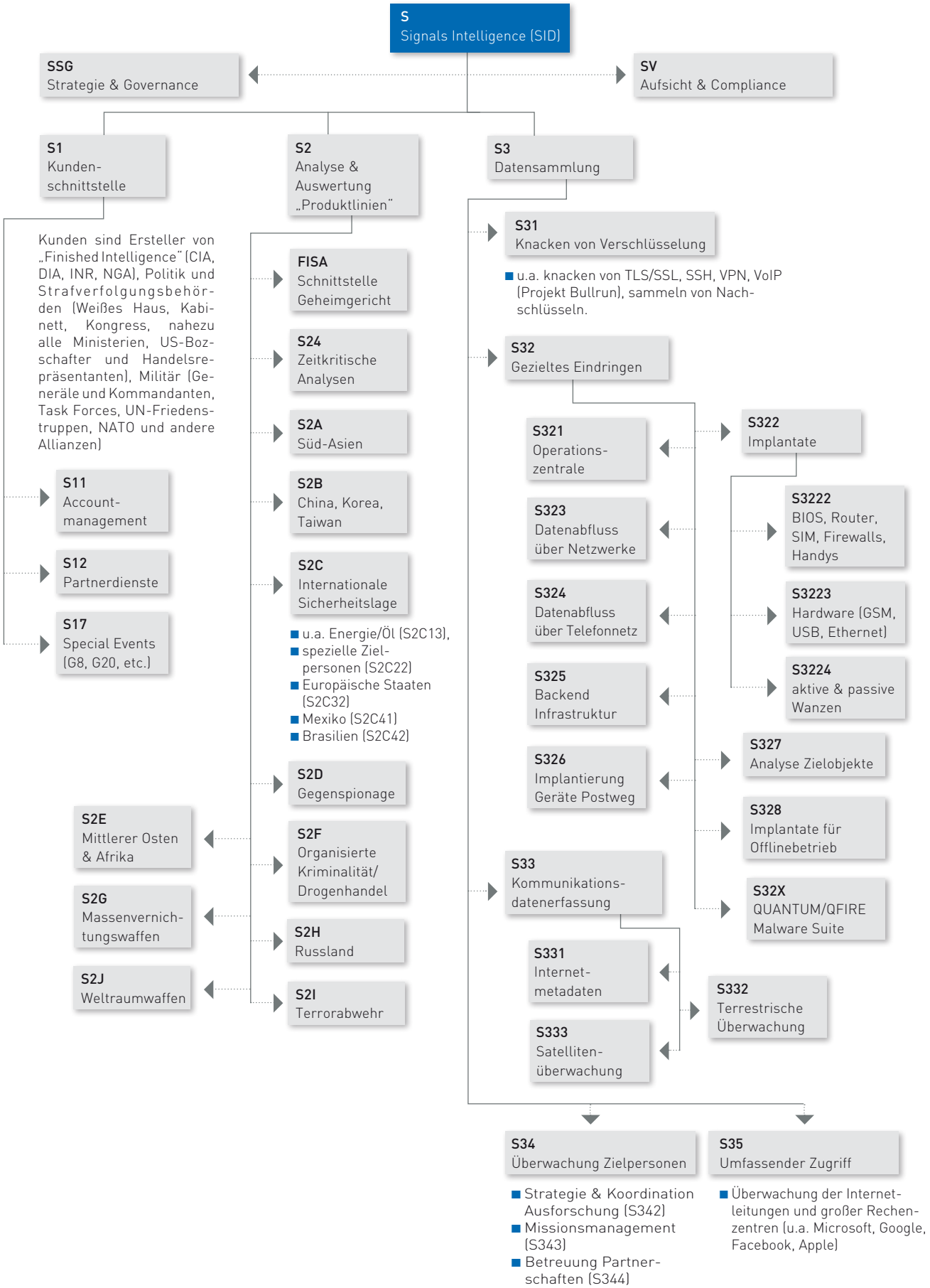
Aus Sicht der Technik ist die NSA beim Eindringen in Systeme („Tailored Access Operations", S32) sehr weit fortgeschritten. Etwa 150 Mitarbeiter arbeiten allein an der technischen Betreuung der laufenden Operationen (S321) und etwa 90 an der Analyse von Zielobjekten und der Angriffsplanung (S327).

Abteilung S322 stellt in diversen Unterabteilungen Hard- und Software her, die in Räume, Geräte und Netzwerke implantiert werden kann und diese ausspioniert. Server, PCs, Firewalls, Netzwerkrouter, SIM-Karten und Handys – S322 hält für alles passende Softwareimplantate bereit. Und falls das nicht funktioniert, gibt es ein umfangreiches Sortiment an Audio- und Datenwanzen, die eingebaut werden können. Danach kommen die Abteilungen S323 und S324 ins Spiel, die den Abfluss der generierten Daten über Netzwerk bzw. Telefonnetz organisieren, und S325 kümmert sich um die Infrastruktur, welche die Daten annimmt.

S326 fängt Geräte gegebenenfalls auf dem Postweg ab und implantiert die Hardware im Transport. S328 stellt Implantate für Hardware und Firmware her (z.B. Bios, Festplatten, etc.), um netzwerktechnisch isolierte Rechner auszuspionieren. S32X entwickelt eine Softwaresuite in der Art klassischer Trojaner, um PCs auf Betriebssystemebene zu infizieren.

Die NSA

Hauptabteilung S



HAUPTABTEILUNGEN I, R UND T

I
Information Assurance (IAD)

- **I2** Lösungsbau
  - u.a. Absicherung Nuklearsenal, verteidigbare Cyber Architekturen, automatische Cyberverteidigung
- **I3** Prüfungen
  - u.a. 24/7 Monitoring, Audits, Evaluations, Pentests
- **I4** Analyse & Abwehr
- **I8** Sicherheitshardware
  - u.a. Smartcards & Tokens, Anti-Tampering Chips
- **IV** Aufsicht & Compliance

R
Research (RD)

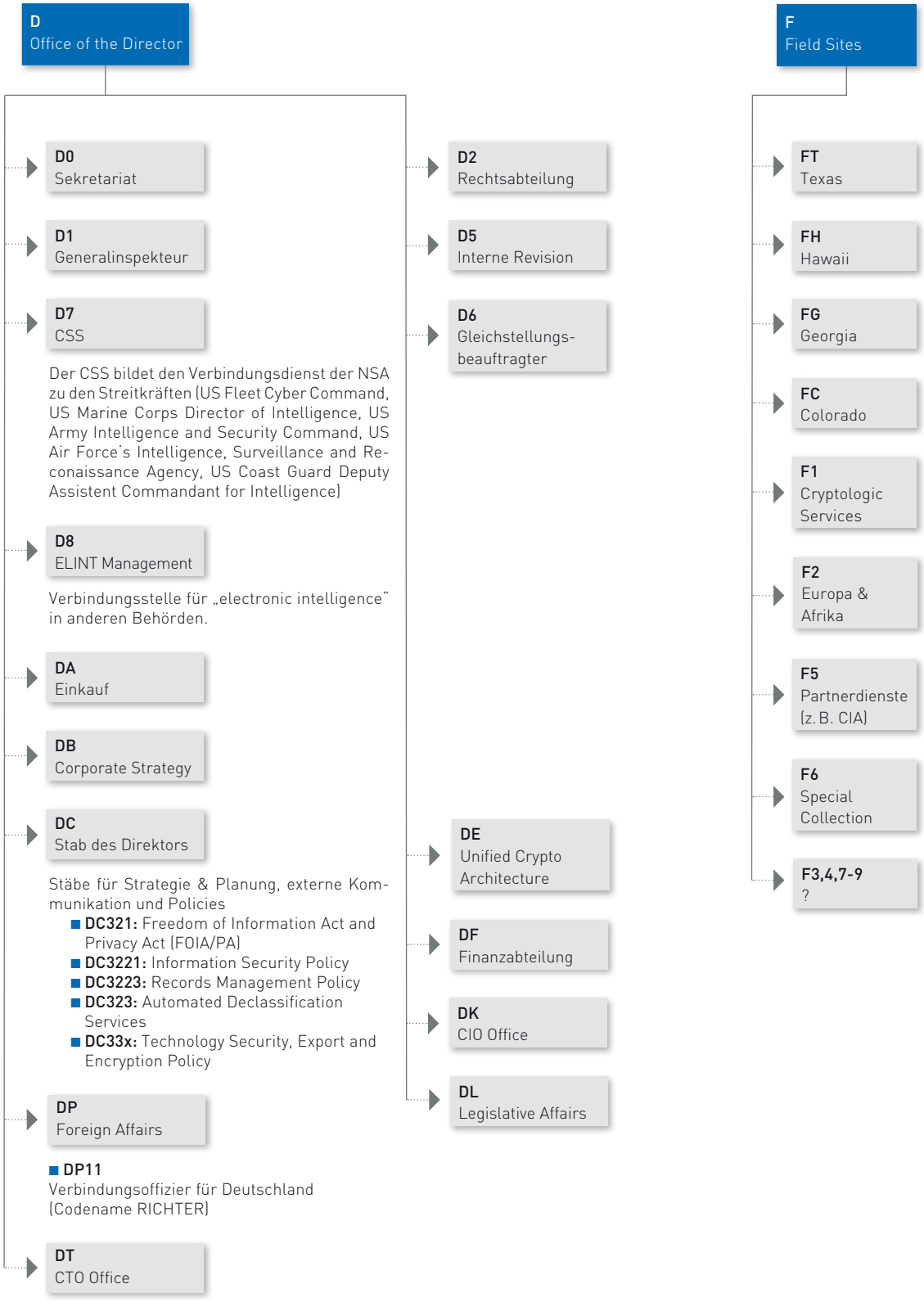
- **R1** Mathematik
- **R2** Absicherung von Systemen
  - u.a. beweisbar sichere Systeme, Anti-Tamper Technologien
- **R3** Physik-Labor
- **R4** Telekom-Labor
- **R5** Sprachforschung
- **R6** Informatik
  - u.a. Spracherkennung, Beherrschung der Informationsflut, disruptive Zukunftstechnologien
- **RX** Absicherung und Zugangsbeschränkung von Forschungsergebnissen
- **RV** Aufsicht & Compliance

T
Technology (TD)

- **T1** Technische Missionsunterstützung
- **T2** Zusammenarbeit mit der Wirtschaft („Commercial Solutions Center")
  - „Wir brauchen die Hilfe der Wirtschaft um die aktuellen und künftigen technologischen Herausforderungen zu lösen".
- **T3** Rechenzentren und Operationszentralen
- **T5** Supercomputer Technologien
- **T6** Elektronische Aufklärung und Bodenstationen
- **TE** Systems Engineering und Architektur
- **TS** IT-Systeme & Sicherheit (PKI, Großprojektleitungen)
- **TT** Test und Evaluierung
- **TV** Compliance

Die NSA

Hauptabteilungen D und F



REORGANISATION DER NSA

Während die NSA außerordentliche Leistungen im Bereich der Spionageangriffe vollbringt, ist die Verteidigung sicher noch ausbaufähig. Die für 2016 und 2017 vorgesehene Reorganisation „NSA21" soll dies vorantreiben.

Neben den Spionagetätigkeiten des Bereichs SID ist der Informationsschutz (vor allem in den Regierungsnetzen) eine der zentralen Aufgaben der NSA. Diese Verantwortung übernahm bisher der etwa 3.000 Mann starke Bereich IAD. Der Bereich arbeitete an vielen Stellen eng mit der Wirtschaft zusammen, um Lücken aufzudecken und zu schließen, gab Härtungsanleitungen und Sicherheitshinweise heraus und versuchte aktiv die Sicherheit von Computernetzwerken zusammen mit der Soft- und Hardwareindustrie zu verbessern.

Allerdings wurde das IAD in der Vergangenheit im Vergleich zum „spannenderen" Bereich der Spionage NSA-intern wohl eher stiefmütterlich behandelt. Dementsprechend konnte der Bereich nie die vergleichsweise außergewöhnlichen Leistungen des SID erbringen.

Nach den Snowden-Veröffentlichungen kam ein weiteres Problem hinzu: Die Zusammenarbeit mit der NSA wurde für die Wirtschaft zu einer Belastung. Obwohl SID und IAD organisatorisch in verschiedenen Silos getrennt waren, verlor das IAD stark an Glaubwürdigkeit und viele seiner Industriekontakte.

Die Bedeutung des Informationsschutzes und der Verteidigung im Cyberraum gewinnt aber Jahr für Jahr an Bedeutung. Eine von Präsident Obama nach Snowden eingesetzte Kommission schlug eine Abtrennung des IAD von der NSA vor, um (analog dem deutschen BSI) eine eigene Organisation für Cybersicherheit zu gründen.

Dies entspricht nicht der Strategie der NSA, wie sie sich von ihren Anfängen bis 1996 zurückverfolgen lässt. Um die Verteidigung zu stärken, sollte eine bessere Zusammenarbeit mit den Angriffseinheiten etabliert werden. Gleichzeitig wollte man die Trennung der Einheiten damals aufrechterhalten und gründete das NSA Threat Operations Center (NTOC), welches das Know-how der beiden Einheiten IAD und SID quasi „auf neutralem Boden" zusammenbrachte.

Im bereits genehmigten und aktuell in der Umsetzung befindlichen Restrukturierungsprogramm „NSA21" wird diese Strategie (gegen den Rat der Experten) fortgesetzt. IAD und SID werden bis 2017 in einem neuen „Directorate of Operations" zusammengefasst. Präsident Obama beschrieb die Strategie so: „Cybersecurity is more like basketball than football. There's no clear line between offense and defense."

Diese kontroverse Strategie, die eine aktive, auf Gegenangriff ausgerichtete Cybersicherheit befürwortet, wird uns in der Zukunft noch viele Probleme bereiten. Aktuell heißt das, dass der Beitrag des IAD zur Absicherung von Geräten, Betriebssystemen und Anwendungen wegfällt. Lücken, welche die IAD-Mitarbeiter früher an die Hersteller gemeldet haben, werden nun wohl intern verwendet. In einer Welt, in der Cybersicherheitsexperten Mangelware sind, ist der Wegfall von 3.000 Mann auf der Verteidigerseite schwer zu verkraften.

Die NSA

Vernetzung der Nachrichtendienste

Naturgemäß bildet die NSA das Zentrum der Zusammenarbeit der westlichen Geheimdienste. Jeder Partnerdienst muss Informationen oder Zugänge liefern. Je mehr geliefert wird, desto besser das Ranking und desto mehr Informationen bekommt der Partner.

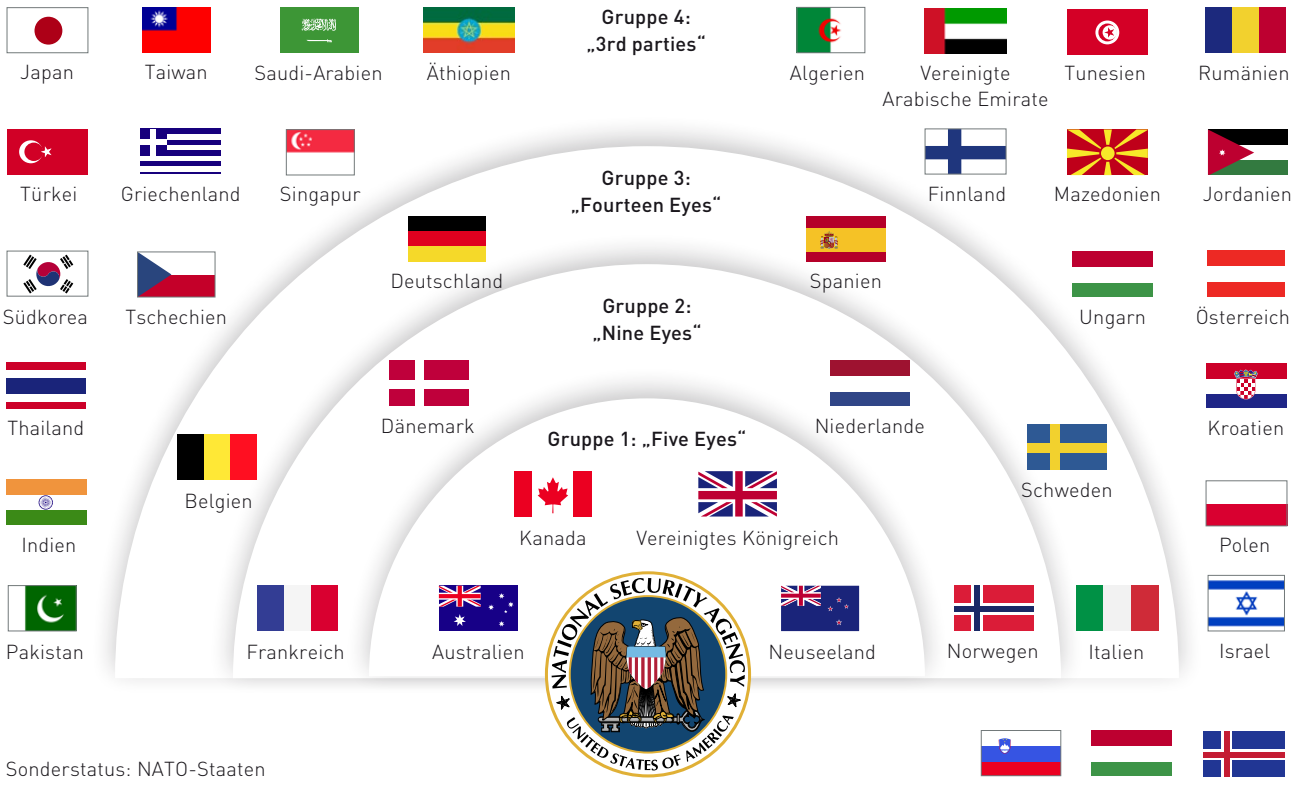
Die NSA teilt ihre Zusammenarbeit in vier Stufen ein:

- Stufe 1: Kanada, Neuseeland, Vereinigtes Königreich, Australien („Five Eyes")
- Stufe 2: zusätzlich Dänemark, Norwegen, Frankreich, Niederlande („Nine Eyes")
- Stufe 3: zusätzlich Belgien, Deutschland, Italien, Schweden, Spanien („Fourteen Eyes")
- Stufe 4: zusätzlich Äthiopien, Algerien, Finnland, Griechenland, Indien, Israel, Japan, Jordanien, Kroatien, Mazedonien, Österreich, Pakistan, Rumänien, Saudi-Arabien, Singapur, Südkorea, Schweiz, Taiwan, Thailand, Tschechien, Türkei, Tunesien, Ungarn, Vereinigte Arabische Emirate

Eine orthogonal dazu liegende Zusammenarbeit existiert mit den NATO-Staaten.

Die „Five Eyes" arbeiten langjährig auf Augenhöhe zusammen und teilen sich die Aufgaben untereinander auf. Alle weiteren Ebenen sind auf gegenseitigen Informations- und Technologieaustausch angelegt. Eine eigene Abteilung der NSA (S12) kümmert sich um die Verwaltung dieser Partnerschaften.

Auf europäischer Ebene wird immer wieder versucht, eine ähnliche Zusammenarbeit der Geheimdienste zu etablieren. Da hier ein „führender" Dienst fehlt, der die Regeln diktieren könnte, ist eine enge Kooperation der europäischen Geheimdienste analog zu den „Five Eyes" bisher nicht zu erkennen.



Sonderstatus: NATO-Staaten

Quelle: Corporate Trust 2017

Lass niemals eine ernsthafte Krise unbeachtet. Was ich damit meine:
Es ist eine Gelegenheit, Dinge zu tun, die du zuvor für undenkbar hieltest.

Rahm Emanuel,
ehemaliger Stabschef von Barack Obama

We can milk this thing all the way to 2015.

Samuel Visner,
NSA-Manager über 9/11

Die NSA

US-Präsidenten über die NSA

Konzentration auf die Unterstützung von Militäroperationen und dazu notwendige Spionage.

"NSA and the service cryptologic elements gave us the critical intelligence we had to have to operate effectively on every front. The information all of you provided enabled me and my key advisers to have a sound understanding of Saddam Hussein's capabilities and solid information about the situation on the ground."

Präsident George Bush

Budgetkürzungen, sinkende Mitarbeiterzahlen und veraltende Infrastruktur bis hin zu einem dreitägigen Totalausfall des Systems im Jahr 2000.

"The computer crash was the perfect metaphor for an agency desperately in need of change. Antiquated computers were a problem. But the reality was actually worse. NSA was in desperate need of reinvention."

Michael Hayden, NSA Director unter Clinton

Einige Monate nach dem 11. September wurden die Befugnisse (und das Budget) der NSA massiv erweitert. Früher notwendige Gerichtsbeschlüsse waren nun in vielen Fällen nicht mehr erforderlich.

„Everything changed at the NSA after the attacks on 9/11. The prior approach focused on complying with the Foreign Intelligence Surveillance Act („FISA"). The post-September 11 approach was that NSA could circumvent federal statutes and the Constitution as long as there was some visceral connection to looking for terrorists.

Ex-NSA Analyst J. Kirk Wiebe

Nach den Snowden Veröffentlichungen wurde eine kleinere NSA Reform angekündigt, die aber hauptsächlich die inländischen Aktivitäten der NSA in den USA betraf.

"[...] the men and women of [...] the NSA, consistently follow protocols designed to protect the privacy of ordinary people. They're not abusing authorities in order to listen to your private phone calls or read your emails. [...] What sustains those who work at NSA and our other intelligence agencies through all these pressures is the knowledge that their professionalism and dedication play a central role in the defense of our nation."

Präsident Barack Obama

Donald Trump befürwortet die Wiedereinführung des Patriot Act und die Telefonüberwachung im Inland (unter Auflagen). Experten erwarten einen Ausbau der NSA unter Trump.

"I support legislation which allows the NSA to hold the bulk metadata. For oversight, I propose that a court, which is available any time on any day, is created to issue individual rulings on when this metadata can be accessed."

Präsident Donald Trump

Deutsche Dienste und die NSA

Nationale Cyberfähigkeiten

Im grenzenlosen Cyberraum existieren keine Logistik-, Nachschub- oder Versorgungsprobleme wie in traditionellen Armeen. Cyberattacken skalieren gut, Teamarbeit macht sowohl Angriff als auch Verteidigung effizienter.

In den klassischen Armeedisziplinen (Land, Meer, Luft) spielen Transport, Logistik, Nachschub und Versorgung eine große Rolle; die Komplexität dieser Aufgaben steigt überproportional zur Personalstärke. Da solche Themen im Cyberraum keine Bedeutung haben, gilt hier die Formel „Der Größere gewinnt" umso mehr.

Hinzu kommt, dass die Fähigkeiten einzelner Topleute im Cyberraum gut von anderen, weniger qualifizierten Cyber-Soldaten dupliziert werden können. Dieses Muster wird in den aktuellen Angriffen ebenso deutlich wie in der organisierten Kriminalität. Ein Tophacker entwickelt ein Vorgehen, zeigt dies dann einer Gruppe von Leuten, die wiederum diese Methodik – situationsbedingt manchmal leicht abgeändert – breit gefächert auf hunderte Ziele anwenden. Ähnliches gilt auch für die Verteidigung. Wurde ein Angriff einmal entdeckt und analysiert, ist er meist leicht zu kontern – sofern die Verteidigung schnell genug in die Fläche gebracht werden kann.

Dementsprechend ist im Cyberraum eine Zusammenarbeit in Allianzen besonders effektiv. Dies setzt natürlich großes gegenseitiges Vertrauen voraus, weil dadurch die eigenen Angriffs- und Verteidigungsmethoden verraten werden.

Die Zusammenarbeit der westlichen Geheimdienste wird zwangsläufig von der NSA organisiert. Das Prinzip ist „Quid pro quo". Will ein kleinerer Dienst von den Daten und Auswertungen der NSA profitieren, muss er dafür Daten aus seinen Lokationen sowie seine Fähigkeiten und Zugänge für die NSA und deren Technologien öffnen. So erklärt sich auch der Einsatz von NSA-Technologien bei BND und BfV und die im neuen Anti-Terror-Paket legalisierte Zusammenarbeit mit ausländischen Geheimdiensten.

Die Größe der Cybereinheiten hat aber auch noch einen zweiten, nachgelagerten Effekt. Egal ob direkt bei den Mitarbeitern eines Dienstes oder bei den Mitarbeitern von Technologiepartnern, am Ende wird mit den Geldmitteln immer das Know-how von Menschen gefördert – und diese arbeiten über kurz oder lang auch in der freien Wirtschaft. Investitionen in Geheimdienste sind also automatisch auch ein Konjunkturprogramm für IT-Sicherheitsexperten in der Industrie. Eine Volkswirtschaft, die hier ins Hintertreffen gerät, wird auch bezüglich der eigenen Absicherung nicht mehr aufholen können. Innerhalb von privatwirtschaftlichen Strukturen lässt sich ein derart konzentrierter Know-how-Aufbau, wie ihn z. B. die NSA betreibt, nicht organisieren.

Deutsche Dienste und die NSA

Dienstherren im Vergleich

Ohne zu wissen, wie man angreift, kann man nicht wissen, wie man sich verteidigen soll.

Für einen Vergleich der nationalen Fähigkeiten im Cyberraum ist es notwendig, die Aufgaben der Dienste und Cyber-Einheiten zu analysieren.

Drei Abgrenzungen vorweg: Es gibt in vielen Behörden IT-Abteilungen. Jede dieser Abteilungen hat IT-Sicherheitsmitarbeiter die für die operative Absicherung der eigenen Netze verantwortlich sind. Oft werden in den offiziellen Statistiken diese Mitarbeiter als „Cybereinheiten" gezählt – was natürlich eine gewisse Berechtigung hat. Für diesen Vergleich wurde versucht, diese Mitarbeiter herauszurechnen. Zum anderen erfordern viele klassische nachrichtendienstliche Aufgaben zunehmend IT-Kenntnisse, so dass „Cyberfähigkeiten" oft in vielen Bereichen eines Dienstes zu finden sind. Für diesen Vergleich werden nur Mitarbeiter gezählt, deren Aufgabengebiet ausschließlich der Cyberraum ist. Zuletzt gibt es natürlich neben den Themen Cyberwar und Spionage auch das kritische und wachsende Thema „Cybercrime", das der vorliegende Report außen vor lässt.

Ein Indiz für den Aufgabenbereich einer Organisation, ist die Frage nach dem Dienstherren. Dienste, die dem Innenministerium berichten, sind tendenziell eher mit der Verteidigung betraut. Behörden, die an den Regierungschef oder das Außenministerium berichten, sind eher auf das Ausland fokussiert. Berichtet hingegen eine Cybereinheit an den Verteidiungsminister, ist dies meist ein eher offensiv ausgerichteter Bereich.

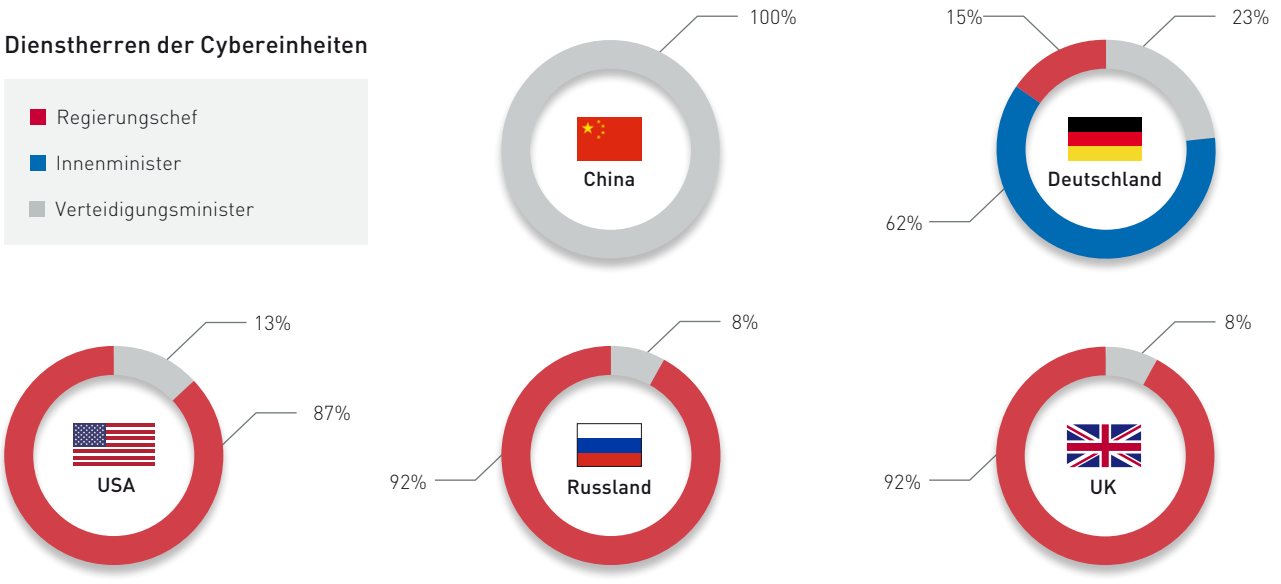
In den meisten Nationen berichtet der Großteil der Cybereinheiten an den Regierungschef (bzw. im Vereinigten Königreich an den Außenminister mit einer engen Bindung an den Regierungschef).

Ein Sonderfall ist China, wo alle Cyberkräfte in der Armee zusammengezogen sind. Begründung: „Ohne zu wissen wie man angreift, kann man nicht wissen, wie man sich verteidigen soll."

Die USA gehen hier einen Mittelweg. Das der Armee zugeordnete U.S. Cyber Command (Angriff) und die an das Weiße Haus berichtende NSA (Spionage und Verteidigung) haben per Dekret denselben Chef und arbeiten somit eng zusammen.

Der BND berichtet zwar auch in Deutschland an den Regierungschef, dennoch sind die meisten Cyberkräfte dem Innenminister zugeordnet (BSI, BfV), Auch die geplante Behörde ZITIS, die neben dem BKA und den LKAs (Fokus Cybercrime) auch das BfV und die LfVs unterstützen soll, berichtet an den Innenminister. Teilweise unterhalten die Bundesländer starke eigene Cybereinheiten, allen voran Bayern, das mit dem Cyber Allianz Zentrum (CAZ) beim Landesamt für Verfassungsschutz und mit dem geplanten Landesamt für IT-Sicherheit, signifikante eigene Kräfte unterhält. Dienstherr ist der jeweilige Landesinnenminister.

Dienstherren der Cybereinheiten



Quelle: Corporate Trust 2017

Deutsche Dienste und die NSA

Mitarbeiterzahlen im Vergleich

Zählt man die Personen, die sich alleine und hauptamtlich mit dem Thema Cyber beschäftigen, steht Deutschland mit seiner Personalausstattung bei den Cyber-Fähigkeiten vergleichsweise schlecht da.

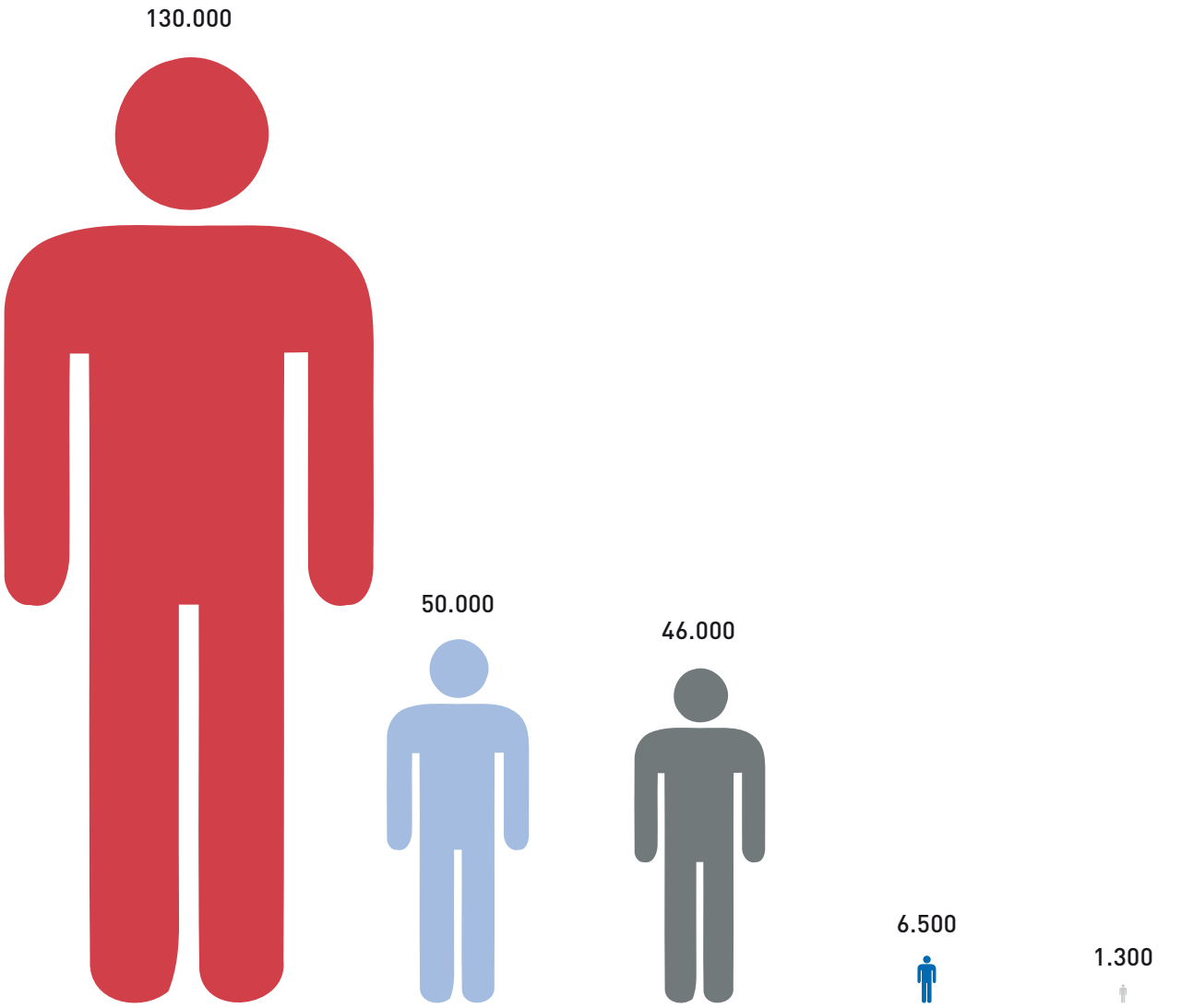
Etwa 800 Mitarbeiter bei Verfassungsschutz und BSI schützen die Bundesrepublik, dazu kommen etwa 500 Stellen beim BND und dem Kommando „digitale Kräfte". Demgegenüber stehen geschätzt rund 46.000 Mitarbeiter beim U.S. Cyber Command und der NSA, mindestens 50.000 bei den russischen Nachrichtendiensten und schlimmstenfalls 130.000 beim chinesischen Ministerium für Staatssicherheit. Vergleicht man Deutschland mit dem Vereinigten Königreich, so sind dort allein 6.000 Mitarbeiter beim GCHQ beschäftigt plus etwa 500 Cyber-Spezialisten bei der Royal Army.

Auch wenn genaue Zahlen kaum verfügbar sind, lassen sich Rückschlüsse aus gesicherten Erkenntnissen, z. B. in Pressemitteilungen genannten Stellenzahlen (auch wenn diese noch gar nicht besetzt sind) und Gerüchten aus den letzten vier Jahren, ziehen.

Vor allem die Zahlen zu Russland und China sind Schätzungen, da diese auf einzelnen Quellen beruhen. Das russische FAPSI hatte vor seiner Eingliederung in FSO (als Abteilung SSSI) und FSB vor 13 Jahren etwa 50.000 Mann. Während der Eingliederung verließen viele Experten den Dienst und Russland setzte zunehmend auf private, staatsnahe Hacker. Während des Cyberangriffs auf Estland stellte sich jedoch heraus, dass diese schlecht zu führen sind. Russland baute daher die eigenen Cyberfähigkeiten wieder stärker aus.

Da uns aber die russische organisierte Kriminalität fast täglich vor Augen führt, dass Cyber-Security-Know-how in ausreichendem Maße im Land vorhanden ist, scheint die Größenordnung für Russland realistisch. Russland betreibt zwei Hackerschulen in Woronesch und Moskau, deren Absolventen fast alle in den Staatsdienst übernommen werden. Bezüglich China ist die Lage schwieriger. Die Abteilung 3 beschäftigt viele Sprachexperten, was die Zahlen natürlich in die Höhe treibt. Auch die nach innen gerichtete Überwachung des Internet, Stichwort „great Firewall", könnte hier angesiedelt sein. Andererseits werden offenbar immer wieder externe Hackergruppen rekrutiert und die Abteilung 4 übernimmt zunehmend Aufgaben im Bereich des Cyberangriffs. Beides wurde in den Zahlen nicht berücksichtigt und könnte diese noch weiter erhöhen.

Mitarbeiterzahlen in den Cybereinheiten



Quelle: Corporate Trust 2017

Deutsche Dienste und die NSA

Aufgabenbereiche im Vergleich

Reaktive Verteidigung heißt „aus Schaden klug werden". Für eine vorrausschauende Verteidigung sind Informationen über die Angreifer notwendig.

Vorweg: Gemäß Verlautbarungen dient jede Cybereinheit auf der Welt allein der Verteidigung der eigenen Grenzen, Werte oder Wirtschaft. Die Frage, ab wann eine aggressiv-offensive „Verteidigungsstrategie" als Angriff interpretiert werden darf, wird dieser Report nicht endgültig klären. Die Grenzen zwischen Angriff und Verteidigung sind im Cyberraum jedoch fließend.

Grundsätzlich werden im Bereich der Computer Network Operations (CNO) drei Fähigkeiten unterschieden. Die klassische Spionage (Computer Network Exploitation – CNE) ist die Grunddisziplin. Sie umfasst das Eindringen in Computer und Netzwerke, die Gewinnung von Rohinformationen, deren Transport in eigene Systeme (Exfiltration) sowie die Bewertung und Aufbereitung der Informationen bzw. die Kombination der Informationen aus verschiedenen Quellen.

Eine gute Informationssammlung ist die Basis für Angriff und Verteidigung gleichermaßen. Je besser man die Cyberfähigkeiten des Gegners kennt (Strategien & Pläne, Ziele, Modus operandi, typische „Cyberwaffen", IP-Adressen, etc.), umso besser kann man die Verteidigung organisieren. CNE-Operationen sind also notwendig, um die Verteidigung im Cyberraum sicherzustellen. Die NSA trägt dieser Erkenntnis organisationsintern Rechnung und reißt mit der Reorganisation NSA21 die Grenzen zwischen Verteidigung und Spionage nieder.

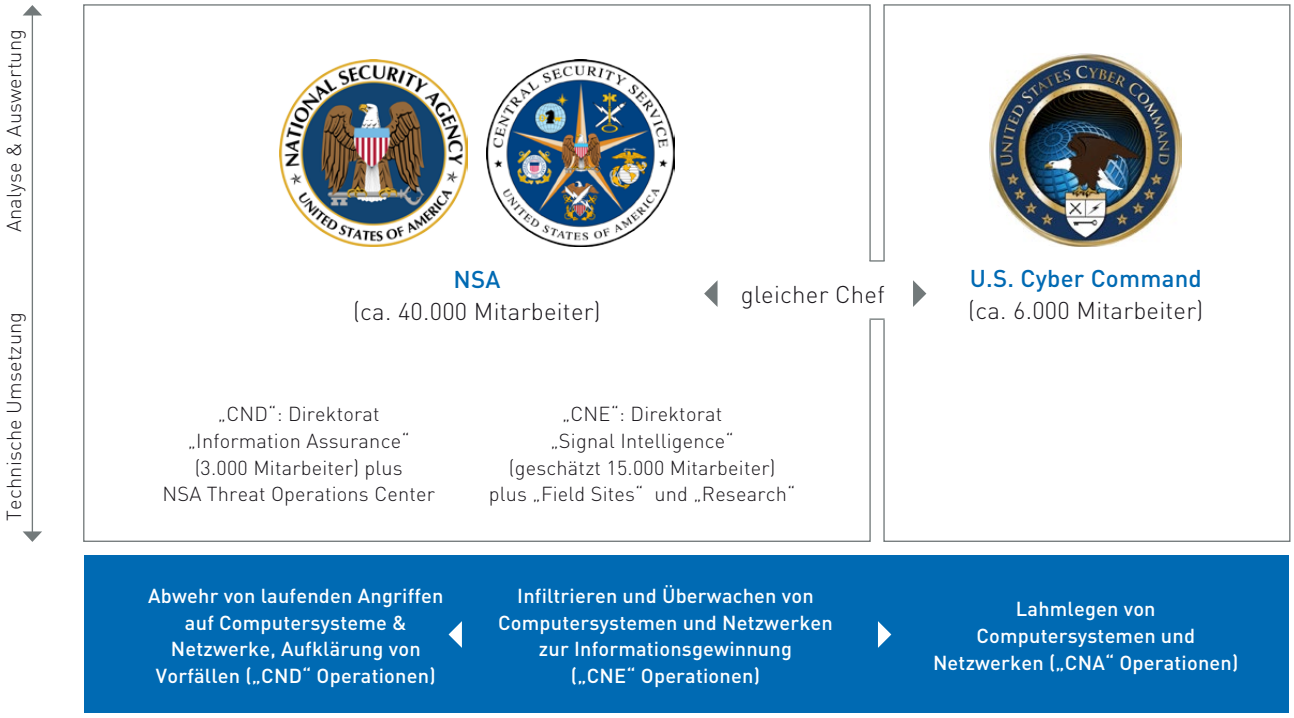
Ausgehend von der „Spionageabwehr" ergibt sich die Notwendigkeit für Fähigkeiten im Bereich Computer Network Defense (CND). Dazu gehören die Beobachtung von Angriffen der Gegner, die Erstellung eines Lagebilds und die folgende strategische Planung von Abwehrmaßnahmen. Auch der Bereich der Computer Network Forensics (CNF), also der Aufklärung von Fällen bzw. der Abwehr von laufenden Angriffen, wird zu dieser Fähigkeit gezählt. Die rein operative IT-Sicherheit, d. h. der Aufbau und Betrieb von Sicherheitsfunktionen in Netzwerken (die klassische „IT-Sicherheitsabteilung"), ist darin nicht enthalten.

Die dritte und historisch gesehen jüngste Fähigkeit ist der Cyberangriff (CNA). Mit zunehmender Abhängigkeit der Gesellschaft von IT-Technologien wächst die militärische Bedeutung der Fähigkeit, durch einen Angriff auf feindliche Computersysteme bestimmte Infrastrukturen auszuschalten und so die gegnerischen Fähigkeiten zu reduzieren. Obwohl als Disziplin noch sehr jung, wurden solche Fähigkeiten bereits 2007 in Estland (Stilllegen eines Staates) und 2008, während des Krieges zwischen Russland und Georgien, demonstriert.

In jeder der drei Disziplinen gibt es einen fließenden Übergang zwischen analytischen Fähigkeiten (Auswertung der vorhandenen Informationen) und konkreten technischen Umsetzungen.

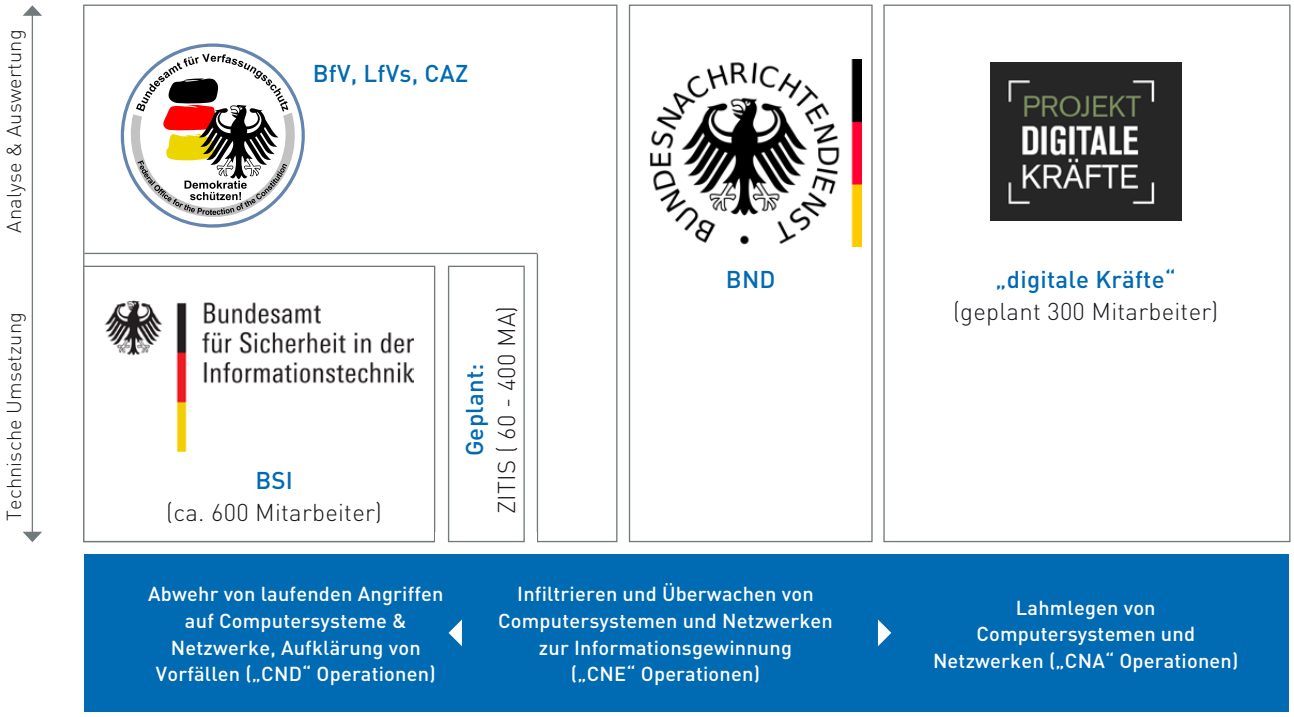
Auch hier ist bezüglich der Organisation der Behörden ein deutlicher Unterschied zwischen Deutschland und den USA erkennbar. Die Amerikaner bemühen sich, alle Cyberfähigkeiten möglichst in eine Hand zu geben und die NSA als Dienstleister für alle weiteren Behörden (CIA, Ministerien, etc.) zu etablieren. In Deutschland werden viele Behörden mit einem eher engen Fokus betraut. Diese Klarheit der eigenen Mission erlaubt eine hohe Fokussierung, andererseits sind Ressourcen mit gleichem Know-how über verschiedene Einheiten zersplittert, die nur mühsam miteinander zusammenarbeiten können.

Aufgabenbereiche der Dienste in den USA



Quelle: Corporate Trust 2017

Aufgabenbereiche der Dienste in Deutschland



Quelle: Corporate Trust 2017

Wenn Privatsphäre ungesetzlich wird, haben nur noch Gesetzlose Privatsphäre.

Phil Zimmermann,
Experte für Kryptografie

Deutsche Dienste und die NSA

BUDGETS IM VERGLEICH

Mit der derzeitigen finanziellen Ausstattung werden das BSI und die Nachrichtendienste die wirtschaftlichen Interessen Deutschlands nicht angemessen vor Spionage schützen können.

Ungeschönte Einblicke in die Finanzierung von fremden Geheimdiensten erhält man nur sehr selten. In den Snowden-Archiven finden sich allerdings Dokumente, die für die 16 Nachrichtendienste der Vereinigten Staaten (US Intelligence Community) ein Budget[1] von 52,6 Milliarden (US: Billion) US-Dollar für das Jahr 2013 ausweisen. Dem stehen zusammengenommen[2] gerade mal 1,1 Milliarden Euro bei den deutschen Nachrichtendiensten (BND/BfV/MAD/LfVs) inklusive dem Budget des Bundesamts für Sicherheit in der Informationstechnik (BSI) gegenüber. Aktuell (Jahr 2016) beträgt das deutsche Budget etwas über 1,3 Milliarden Euro.

Aufgrund der unterschiedlichen wirtschaftlichen Stärke der beiden Länder liegt es auf der Hand, dass das Budgetvolumen der US-Geheimdienste wesentlich höher ist, als das der deutschen Nachrichtendienste.

Setzt man die Ausgaben allerdings ins Verhältnis zum jeweiligen Bruttoinlandsprodukt (BIP), schneidet Deutschland noch schlechter ab als im absoluten Vergleich. Das heißt Deutschland investiert gemessen an der Größe seiner Wirtschaft wesentlich weniger als die USA in Cyber-Fähigkeiten.

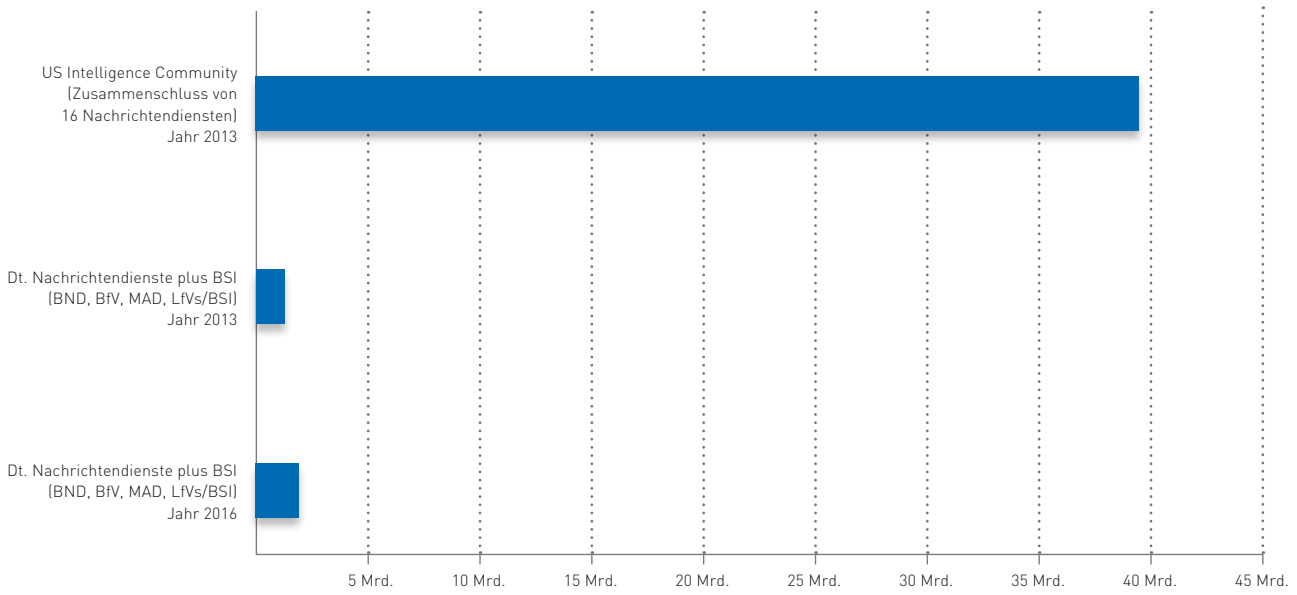
Im Jahr 2013 lag die US-Quote über 0,31 % des BIP, die deutsche Quote bei unter 0,04 %. Im Jahr 2016 erhöht sich die deutsche Quote auf annähernd 0,05 %. Potenziell dürften dabei aber die Mittel für die „Strategische Initiative Technik" und Kosten für den Umzug ihren wesentlichen Anteil an der Erhöhung haben.

Auch unter Berücksichtigung, dass der Vergleich der US Intelligence Community mit den deutschen Nachrichtendiensten plus BSI hinkt, wird ersichtlich, welches Gefälle zwischen den beiden Ländern besteht. Dieses Bild bleibt im Wesentlichen auch dann unverändert, wenn man US-Dienste mit dem Fokus auf wirtschaftliche Vorgänge und deutsche Nachrichtendienste mit Wirtschaftsschutz-Aufgaben plus BSI vergleicht.

Unternehmen sollten sich nicht darauf verlassen, dass deutsche Nachrichtendienste und Behörden ihre wirtschaftlichen Interessen energisch schützen können, weil hierzu schlichweg die Mittel fehlen, um auf Augenhöhe agieren zu können.

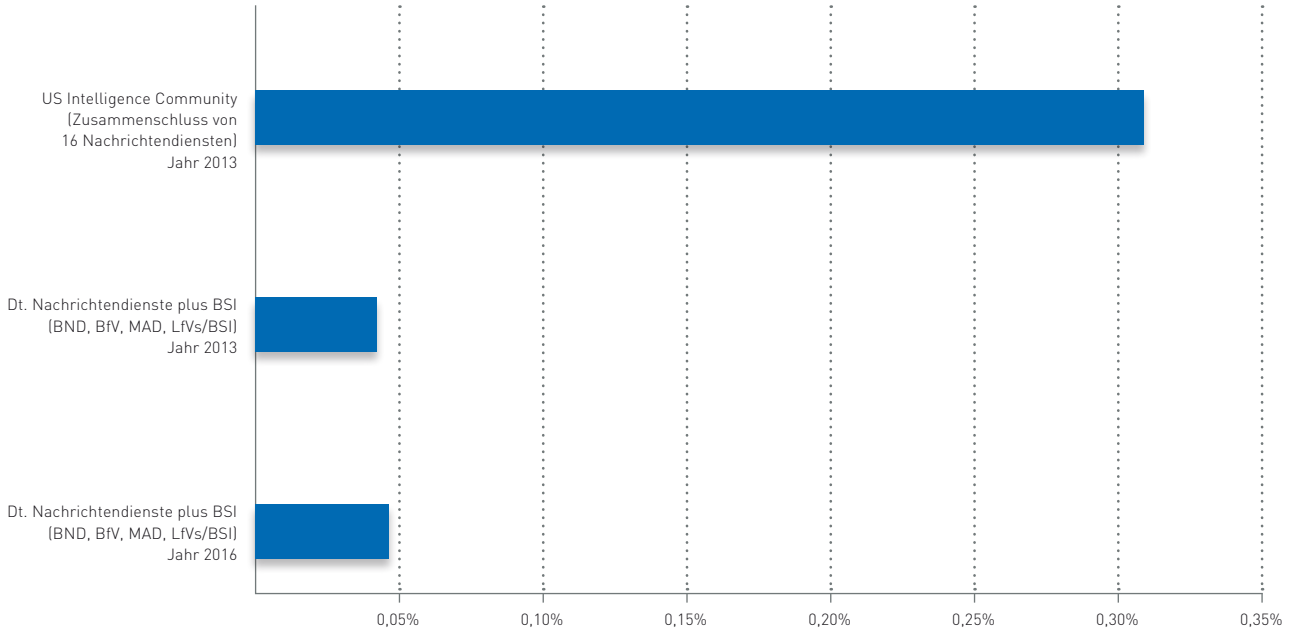
1) Verborgene Teile, wie in militärischen Etats versteckte weitere Pfründe, könnten das US- und deutsche Geheimdienstbudget weiter erhöhen.
2) Der Etat für BND, BSI, BfV und MAD wurde aus den Einzelplänen des Bundeshaushalts oder aus Verfassungsschutzberichten entnommen. Der Etat der Landesbehörden für Verfassungsschutz (LfV) wird von vielen Behörden selbst ausgewiesen, findet sich in den Landeshaushalten oder musste anhand der verfügbaren Informationen errechnet werden. Somit handelt es sich hierbei nur um einen Näherungswert.
Zur Umrechung von US-Dollar auf Euro wurden die Umsatzsteuer-Umrechnungskurse des Bundesministeriums für Finanzen des Jahres 2013 gemittelt.
Das den Berechnungen zugrundeliegende Bruttoinlandsprodukt der USA und Deutschlands stammt aus den Daten des Internationalen Währungsfonds (Stand: April 2016).

Budgetvergleich in Euro
US-Intelligence Community & Deutsche Nachrichtendienste plus BSI



Quelle: Corporate Trust 2017

Budgetvergleich im Verhältnis zum Bruttoinlandsprodukt in Prozent
US-Intelligence Community & Deutsche Nachrichtendienste plus BSI

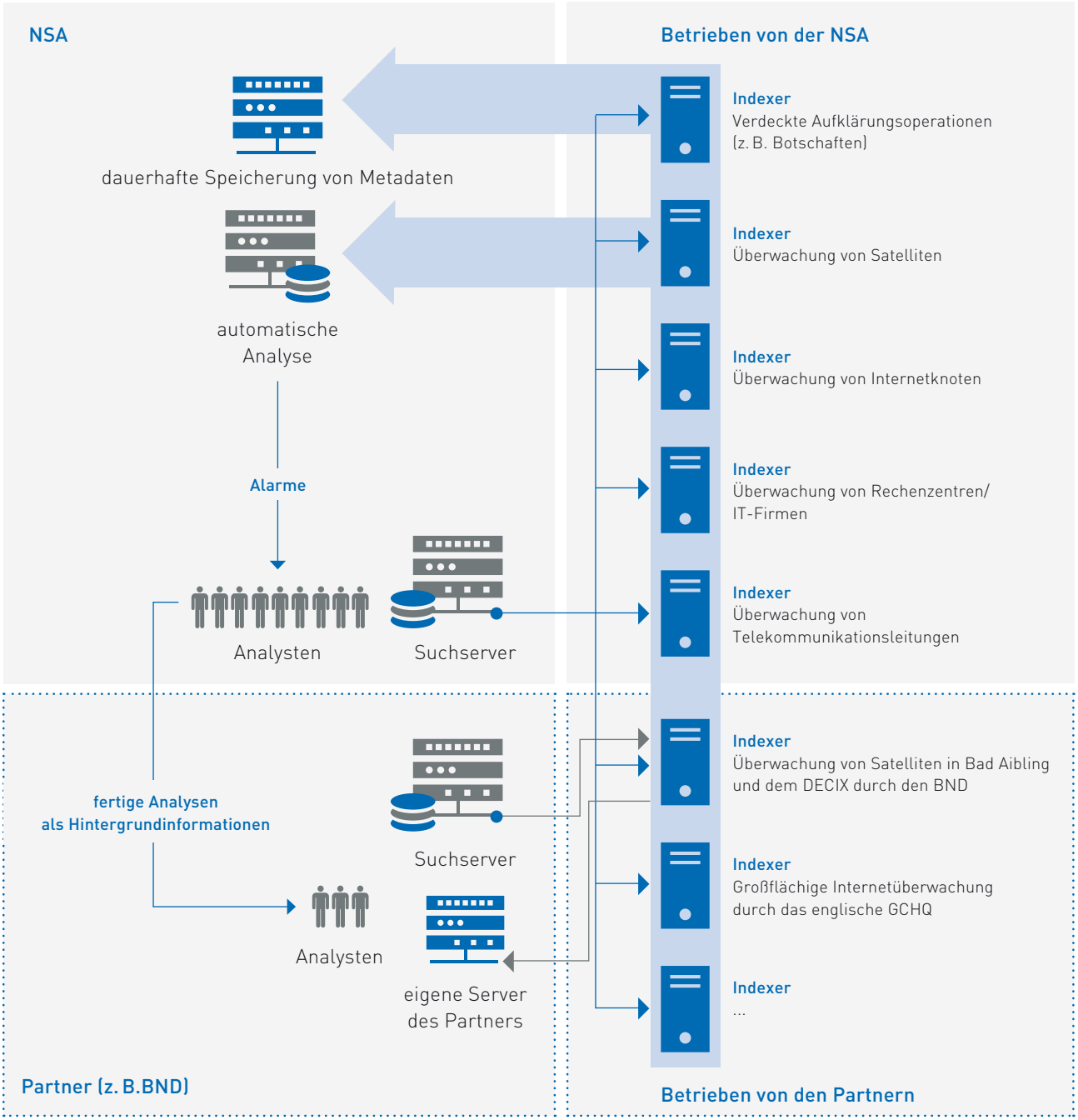


Quelle: Corporate Trust 2017

Deutsche Dienste und die NSA

Zusammenarbeit

Zusammenarbeitsmodell von XKeyscore



Quelle: Corporate Trust 2017

Die NSA koordiniert nicht nur die Zusammenarbeit der westlichen Geheimdienste - sie liefert ihnen auch die technologische Basis zur Sammlung und Auswertung von Massendaten.

Der ehemalige NSA-Direktor Michael Hayden hat nach den Enthüllungen von Edward Snowden vorhergesagt, dass die Veröffentlichungen eine Neuausrichtung bei gegnerischen Nachrichtendiensten zur Folge haben werden. Die beeindruckenden Fähigkeiten der NSA wecken Begehrlichkeiten bei allen Nachrichtendiensten, die nun rund um die Welt versuchen, ähnliche Kapazitäten auf- bzw. auszubauen.

Viele kleinere Dienste besitzen nicht die Kapazität, um die operationellen Taktiken und notwendigen Technologien mittels eigenem bzw. nationalem industriellen Entwicklungspotenzial zu realisieren und zu finanzieren. Um auf bestimmten Aufklärungsfeldern einigermaßen in Augenhöhe zusammenarbeiten zu können, ist eine Zusammenarbeit notwendig.

Im westlichen Geheimdienstverbund liefert die NSA nicht nur Technologie sondern dadurch automatisch auch eine gewisse Standardisierung von Prozessen und Vorgehensweisen. Damit werden sowohl der Austausch einfacher als auch die Zusammenarbeit effizienter. Herunter gebrochen auf die nationalen Nachrichtendienste Deutschlands (BND, BfV) gilt dieser Ansatz ebenso.

Der BND muss Bundesregierung, Ministerien und die Bundeswehr zur richtigen Zeit bedarfsgerecht mit belastbaren Informationen versorgen. Die aktuellen Themen sind ABC-Waffen, Cyber-Sicherheit, illegale Migration, internationaler Rauschgifthandel, islamistisch motivierter internationaler Terrorismus, Konfliktregionen weltweit, Proliferation (Verbreitung von Massenvernichtungswaffen), Wehrtechnik und der Schutz der Bundeswehr im Auslandseinsatz.

Im Rahmen seines gesetzlichen Auftrags hat der BND die Befugnis zur Erfassung internationaler Datenverkehre. Dadurch ergeben sich vielfache Interessensüberschneidungen mit der NSA und anderen verbündeten Diensten. Auch historisch gesehen hat der BND als Nachkriegszieh-kind amerikanischer Dienste (Organisation Gehlen) eine enge Verbindung zu US-Organisationen und dem „großen Bruder" NSA.

(S//SI//REL TO USA, FVEY) **Introduction**: NSA established a relationship with its SIGINT counterpart in Germany, the BND-TA, in 1962, which includes extensive analytical, operational, and technical exchanges. In the past year, Germany displayed both eagerness and self-sufficiency in transforming its SIGINT activities and assumed greater risk in support of U.S. intelligence needs and efforts to improve information sharing within the German government, with coalition partners, and NSA. The BND supports NSA's emerging counterterrorism (CT) intelligence relationship with the German domestic services, taking steps to strengthen its SIGINT Development (SIGDEV) capabilities to perform a key technical advisory and support role within Germany.

[...]

(S//NF) The Information Assurance Directorate (IAD) has a long-standing relationship with the Bundesamt für Sicherheit in der Informationstechnik (BSI) – the Federal Office of Information Security. After the German Government announced their Cybersecurity Strategy and identified BSI as the lead Agency for cyber defense, BSI expressed great interest in expanding the information assurance (IA) partnership to include computer network defense (CND) collaboration on cyber threats.

Ausschnitt NSA-Informationspapier vom 17.01.2013

Zusammenarbeit NSA und deutsche Dienste

In Bad Aibling arbeiten die beiden Nachrichtendienste bei der Überwachung des Internetverkehrs aus Ländern des „islamischen Krisenbogens" zusammen, wozu die Staaten Afghanistan, Syrien, der Irak und Libyen gehören. Nachdem aus den Reihen der NSA (und des BND) immer wieder Kritik an den deutschen Einschränkungen bzgl. technischer Maßnahmen laut wurde, wurde in 2016 das BND-Gesetz neu gefasst. Dabei wurde es letztlich erheblich erweitert und die bisherige Praxis im Wesentlichen legalisiert.

(U) Success stories:

[...]

- (S//REL TO USA, FVEY) The German government modified its interpretation of the G-10 Privacy Law, protecting the communications of German citizens, to afford the BND more flexibility in sharing protected information with foreign partners.

[...]

- (TS//SI//NF) Problems/Challenges with the partner: Since 2008 NSA has started to foster other areas of cooperation with the BND to satisfy U.S. intelligence requirements at an appropriate level of investment. The BND's inability to successfully address German privacy law (G-10) issues has limited some operations, but NSA welcomed German willingness to take risks and to pursue new opportunities for cooperation with the U.S, particularly in the CT realm. NSA is open to holding a dialogue on topics to address mutual intelligence gaps, including [redacted] and CP-related activities.

Ausschnitt NSA-Informationspapier vom 17.01.2013

Kooperation NSA & Deutschland: Erfolge und Probleme

Der BND darf nun auch in inländischen Telekommunikationsnetzen abhören, die Daten bis zu 6 Monate aufbewahren und mit ausländischen Partnerdiensten teilen. Nicht erlaubt ist dem BND das Abhören deutscher Staatsbürger, das gezielte Ausspähen befreundeter Staats- und Regierungschefs sowie Wirtschaftsspionage.

Die Fähigkeiten der NSA für gezielte Cyber-Kommandoaktionen und Infiltrationen sind groß. Es ist davon auszugehen, dass die NSA in diesem Bereich weder ihre Vorgehensweise noch ihre Geheimnisse preisgibt. Im Bereich der Erfassung und Auswertung von Massendaten sind jedoch umfangreiche Zugänge auf der ganzen Welt notwendig. Dazu hat die NSA das Programm XKeyscore entwickelt.

Deutsche Dienste und die NSA

ZUSAMMENARBEIT

Die IT-Architektur von XKeyscore scheint dabei weitgehend modernen Log-Auswertesystenen zu ähneln. Direkt an den jeweiligen Datenquellen steht ein Indexer. Dieser Indexer rekonstruiert Kommunikationssitzungen aus den Paketen und archiviert diese zusammen mit extrahierten Schlüsseldaten wie z. B. IP- oder E-Mail Adressen sowie Lokationsdaten (sogenannte Metadaten). An manchen Indexern kommt so viel Datenverkehr vorbei, dass eine komplette Archivierung des Datenverkehrs nicht möglich ist. Dann wird der Datenverkehr durch spezielle Suchbegriffe (die vielzitierten „Selektoren") indiziert.

Solche Indexer stehen in den großen Satelliten Abhörstationen (wie z. B. in Bad Aibling), bei großen Internetfirmen, Telekommunikationsunternehmen, Internetknoten (z. B. dem DE-CIX) bzw. den Providern für Unterseekabel. Auch die Abhöreinrichtungen in den US-Botschaften und die verdeckten Operationen zum Abhören von Diplomaten und internationalen Organisationen (z. B. der IAEO in Wien) schicken die Daten an solche Indexer.

Während die meisten Indexer von der NSA betrieben werden, werden einige auch von Partnern betreut, wie z. B. dem BND. Die NSA stellt dann die Software zur Verfügung, hilft bei der Installation und schult das Personal.

Die Indexer sind aber nur ein Teil des Gesamtsystems. Ein wichtiger Teil sind die Analystenarbeitsplätze, mit denen Suchanfragen formuliert werden können. Jeder Suchserver kann mehrere Indexer befragen.

Es gibt bei der NSA Suchserver, die alle Indexer der Welt befragen können. Suchserver, die bei Partnern wie dem BND stehen, sind normalerweise auf die Indexer des jeweiligen Partners limitiert. Der übliche Deal ist also, dass die NSA die Technologie kostenlos zur Verfügung stellt und dafür Zugriff auf die gesammelten Daten erhält. Im Rahmen gemeinsamer Programme (wie z. B. dem Anti-Terrorprogramm) stellt die NSA zusätzlich sinnvolle Suchbegriffe und andere Hilfestellungen für die lokalen Analysten in Form von aufbereiteten Hintergrundinformationen zur Verfügung. Die Frage, ob den NSA Partnern technischer Zugang zu eigenen Indexern gewährt wird und wenn ja, in welcher Form, bleibt unklar.

Die meisten Indexer können die vollen Daten nur für wenige Tage, manche nur für Stunden speichern. Für aktuelle Aktionen von Analysten, wie z. B. die Überwachung bestimmter Gruppen, Zielpersonen oder Firmen, ist dies ausreichend. Gleichzeitig werden bestimmte Metadaten (wer kommuniziert mit wem? wer sucht nach was?) an NSA-Zentralsysteme (Projekt MARINA) ausgeleitet, wo diese dann dauerhaft gespeichert und weiterverarbeitet werden (Projekte Pinwhale und Trafficchief). Auch das Einrichten von „Alarmen" (sonderbares Verhalten, Suche nach verdächtigen Begriffen oder Orten, etc.) ist möglich.

Neben dem Bundesnachrichtendienst arbeiten sowohl das Bundesamt für Verfassungsschutz, als auch das Bundesamt für Sicherheit in der Informationstechnik mit der NSA zusammen.

Die NSA ist in Deutschland sehr präsent und unterhält etliche Standorte, unter anderem in Augsburg, Bad Aibling, Baumholder, Berlin, Bremerhaven, Herzogenaurauch, Frankfurt, Stuttgart und Rothwesten bei Kassel.

Bereits seit 1962 gibt es eine intensive Zusammenarbeit zwischen BND und NSA, die sich mittlerweilte auf alle Ebenen erstreckt. Es werden Analysen und Technologien ausgetauscht sowie beim Betrieb von Systemen und bei Einzelaktionen zusammengearbeitet. Laut einem NSA-internen Memo von 2013 steht dabei der deutsche Datenschutz der Zusammenarbeit immer wieder im Weg, Es wird aber dem BND auch bescheinigt, dass er hart daran arbeitet, dennoch Wege zur Zusammenarbeit zu finden.

Im selben Memo wird die modifizierte Auslegung der Bundesregierung bzgl. des Datenschutzes im Rahmen von Überwachungsmaßnahmen als positiver Schritt herausgehoben.

Die gute Zusammenarbeit mit dem BND in der großen Koalition zur Überwachung von Afghanistan wird von der NSA gelobt. Auch die moderne Infrastruktur, mit einmaligen Fähigkeiten für das Abhören von Mobilfunkverbindungen und Internettelefonie, ist für die NSA wertvoll.

Bereits seit längerem existiert eine aus Sicht der NSA vertrauensvolle und intensive Zusammenarbeit zwischen der eigenen Cyber-Verteidigungseinheit (IAD) und dem BSI.

Formal seit Mitte 2013 existiert auch eine intensive Zusammenarbeit zwischen dem Bundesamt für Verfassungsschutz (BfV) und der NSA in Sachen Anti-Terror-Kampf. Der BfV soll XKeyscore nutzen um die Ergebnisse von Überwachungs- und Abhörmaßnahmen zu sammeln und auszuwerten.

Der BfV erhält damit eine professionelle Software, die NSA erhofft sich durch die Informationen Fortschritte im Anti-Terror-Kampf. Motiviert ist diese Zusammenarbeit durch die Erkenntnis, dass eine der Terrorzellen, die 9/11 plante, aus Hamburg stammte. Dementsprechend wurde auch ein Verbindungsmann der NSA für den BfV abgestellt.

Zusammenarbeit mit der NSA

Quelle: Corporate Trust 2017

Made in Germany

Die deutsche Sicherheitsarchitektur

Die deutsche Cybersicherheitsarchitektur ist nicht nur organisatorisch zu kompliziert aufgestellt, sondern auch zahlenmäßig unterbesetzt. Dadurch gerät die deutsche Wirtschaft direkt in Gefahr und droht auch mittelfristig durch den Mangel an Sicherheits-Know-how den Anschluss zu verlieren.

Egal ob Terrorismus, Landesverteidigung, Wirtschaftskriminalität, Industriespionage oder klassische Straftaten – Strafverfolgung und Gefahrenabwehr sind ohne IT-technische Kompetenzen heute nicht mehr denkbar. Die forensische Untersuchung von Computern und Handys, das Knacken von Verschlüsselungen, die Überwachung von Netzwerken zur Aufdeckung der Organisationsstrukturen von Kriminellen, das Durchforsten versteckter Stellen im Cyberraum und die Überwachung von technischen Geräten von Verdächtigen sind nur die wichtigsten Themen. Faktisch die gleichen technischen Kompetenzen werden auch für die Spionageabwehr und die Verteidigung der Computernetze von staatlichen Institutionen, Politik, Firmen und Unternehmen sowie letztendlich auch den Bürgern benötigt. Selbst das Militär ist für die Spionageabwehr und die Verteidigung der eigenen Netzwerke auf diese Kompetenzen angewiesen.

So unterschiedlich die Beweggründe und Ziele für die vorher genannten Themen auch sein mögen, das notwendige Know-how für eine erfolgreiche Arbeit überschneidet sich stark. Deutschland bleibt jedoch weiterhin seinem Trennungsgebot treu: Cyber-Security-Kompetenzen werden, mehr oder weniger intensiv, bei BND, BfV, 16 LfVs, BKA, 16 LKAs, BSI, in der Bundeswehr und bei etlichen Bundes- und Landesministerien aufgebaut. Dabei hat jede Einheit eine leicht unterschiedliche Aufgabenstellung und operiert auf Basis unterschiedlicher gesetzlicher und rechtlicher Rahmenbedingungen. Dass die Unternehmen ihre Netze selbst schützen müssen und dazu eigene Spezialisten benötigen, versteht sich von selbst.

Nun sind IT-Experten generell ein knappes Gut, um das alle Arbeitgeber konkurrieren, und für Cyber-Security-Experten gilt dies erst recht. Richtig gut werden Teams aber erst, wenn mehrere Topspezialisten zusammenarbeiten. Die USA haben dies schon vor Jahren erkannt und die NSA als „Superdienstleister" für alle oben genannten Aufgaben installiert. Auch China und Russland haben ihre technischen Kompetenzen gebündelt. Und während es in Deutschland erste zaghafte Pläne zur Zusammenführung technischer Kompetenzen gibt (wie z. B. die Stärkung des BSI durch das Sicherheitsgesetz oder die Planungen rund um die „Zentrale Stelle für Informationstechnik im Sicherheitsbereich" – ZITIS), werden an anderen Stellen die Kompetenzen wieder bewusst verteilt (z. B. die Quick Reaction Forces, die in drei Teile geteilt bei BSI, BfV und BKA installiert werden sollen).

ZITIS soll ab 2017 mit 60 Mitarbeiterm starten und bis 2022 auf 400 Mitarbeiter anwachsen. Mit ihr sollen die Bundespolizei, das Bundeskriminalamt und der Verfassungsschutz in die Lage versetzt werden, verschlüsselte Nachrichten zu dechiffrieren. Der BND wird sich daran ausdrücklich nicht beteiligen. Er will damit vermeiden, in gerichtlichen Strafverfahren offenlegen zu müssen, mit welchen Methoden er verschlüsselte Nachrichten dechiffriert. Sollte sich diese Behörde einmal etabliert haben und arbeitsfähig sein, fände man auch hier das Potenzial einer „internationalen bilateralen" Zusammenarbeit.

Die gesamte Betrachtung fokussiert sich bisher rein auf den defensiven Bereich der Cybersicherheit. Dabei ist die Welt um uns herum längst dabei, offensive Kapazitäten aufzubauen. Die Frage, inwieweit Deutschland eigene Cyberspionage-Kapazitäten für Politik, militärische Aktionen und evtl. sogar für die Wirtschaft braucht, wird nicht bzw. nur hinter vorgehaltener Hand diskutiert. Und auch die Kapazitäten für Cyberangriffe zur Begleitung militärischer Aktionen bzw. die Mittel zur Meinungsbeeinflussung in anderen Ländern über die sozialen Medien sind in Deutschland nicht offen diskutierbar.

Dabei benötigt die Welt hier eine moderate Stimme. Das Potenzial der Cyberwaffen wächst mit jeder neuen IT-Revolution und wird im Zeitalter von Industrie 4.0, selbstfahrenden Autos, computergesteuerten Stromnetzen und dem „Internet of Things" die Zerstörungskraft von Atomwaffen erreichen.

BENÖTIGTES CYBER SECURITY KNOW-HOW

Cyber-Security-Fähigkeiten:

- IT-Forensik: Aufdecken von maliziösen Veränderungen und forensische Untersuchungen an Clients, Handys und sonstigen Geräten und in Netzwerken
- E-Discovery: Auswerten von Massendaten, Verbindungsdaten, Logs und E-Mails
- Monitoring: Überwachung von Netzwerken und Computern, Entdeckung von IT-Angriffen
- Präventive Gefahrenabwehr: Überwachung von Foren, Chats und Webseiten, um Angriffsvorbereitungen frühzeitig erkennen zu können
- Spionage/Informationsdiebstahl: Sammlung von Daten und Informationen aus fremden Netzen und Computern
- Präventive IT-Sicherheit: Aufbau von Sicherheitsmaßnahmen, um Spionage in und Angriffe auf eigene IT-Netze und Computer zu erschweren
- Aktive Verteidigung: Abwehr von laufenden Angriffen, IT-Krisen- und Notfallmanagement
- Cyber-Angriffe: Lahmlegen von IT-Systemen und Netzwerken, Ausschalten von IT-Abteilungen
- Cyber-Propaganda: Schaffung bestimmter Meinungsbilder, Durchführen von Desinformationskampagnen in sozialen Medien und Bewertungssystemen
- Informationsaufklärung: Erkennung und Abwehr von elektronischen Desinformationskampagnen und (versteckter) Propaganda in sozialen Medien, Kommentarfunktionen und Shops

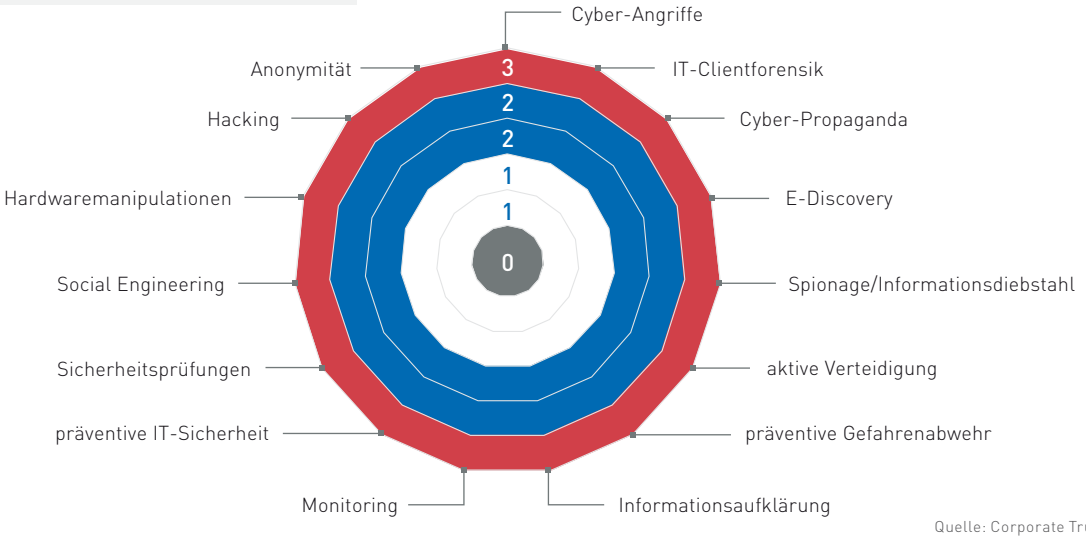
Basis-Fähigkeiten als Grundlage:

- Social Engineering: Aufbau von Legenden im Cyberraum, Vorspiegeln falscher Identitäten, ggf. Diebstahl von Authentifizierungsinformationen
- Hardwaremanipulationen: Entwurf und Implantierung von Hardware (Wanzen für Räume und IT-Hardware, Keylogger, USB-Logger, etc.)
- Sicherheitsprüfungen: Finden von Lücken in IT-Systemen und Software
- Hacking: Knacken von Verschlüsselungen, Passwörtern und Sicherheitsmaßnahmen
- Anonymität: Aufbau und Betrieb von anonymen Internetzonen und versteckten Rechnerkapazitäten (z. B. Botnetze), verdeckte Kommunikation (Steganographie)

Quelle: Corporate Trust 2017

Legende für den Know-how Vergleich auf den folgenden Seiten

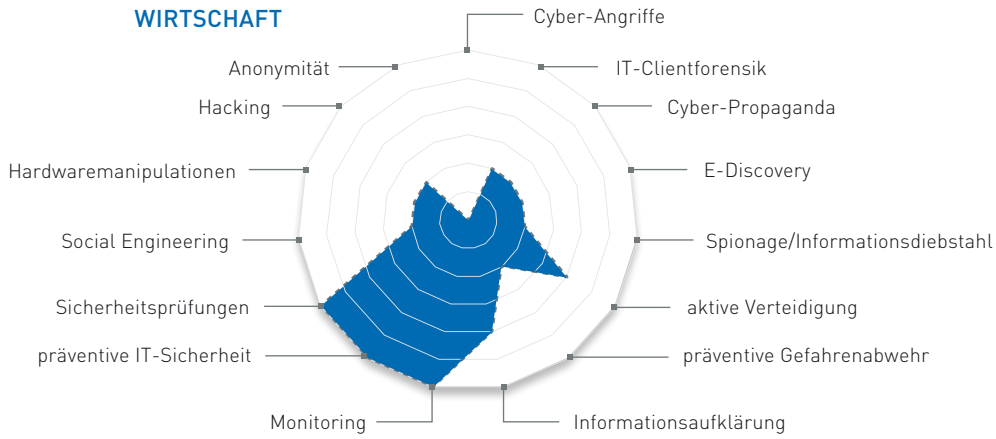
0 Know-how wird nicht gebraucht
1 Know-how ist selten notwendig
2 Know-how muss ständig verfügbar sein
3 Know-how ist Kernkompetenz

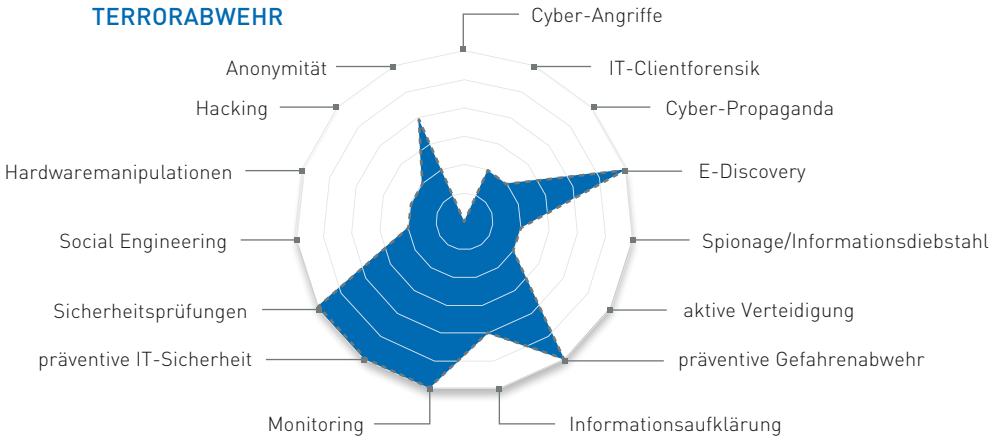


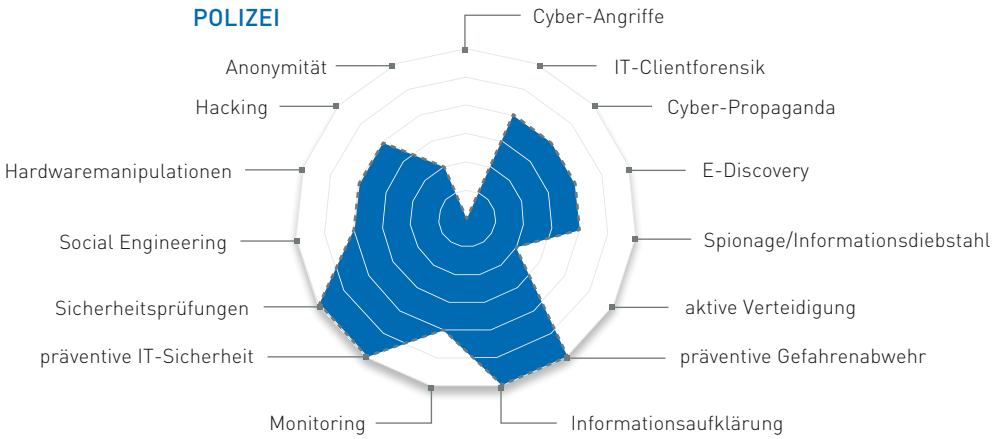
Quelle: Corporate Trust 2017

Made in Germany

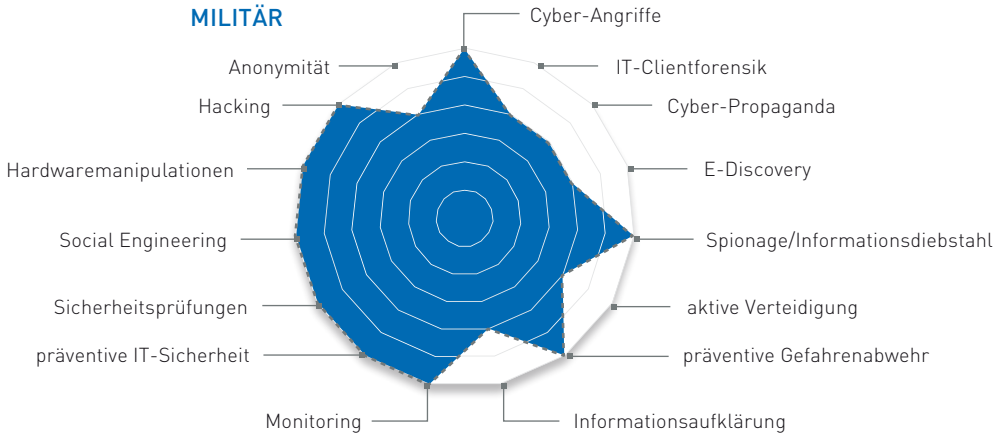
Benötigtes Cyber Security Know-How



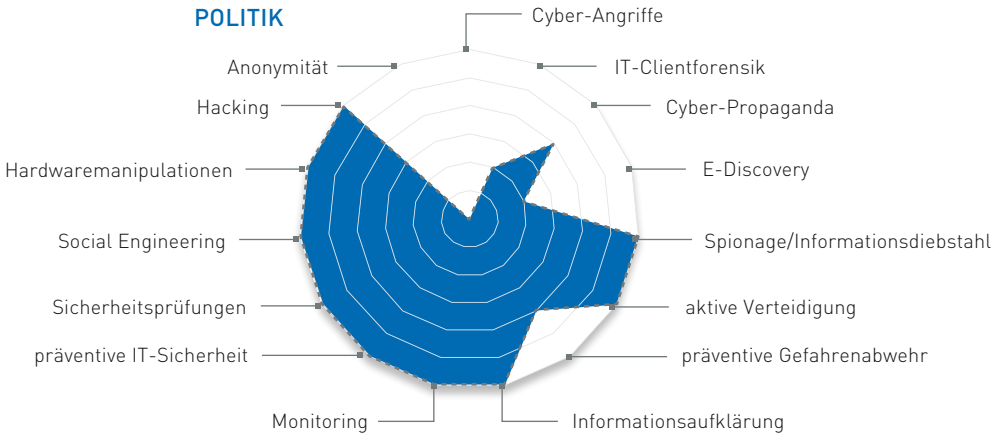




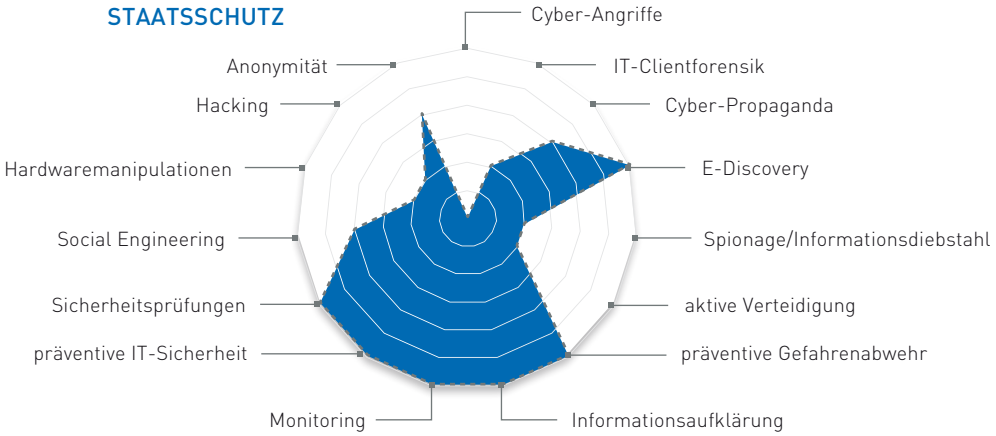
MILITÄR



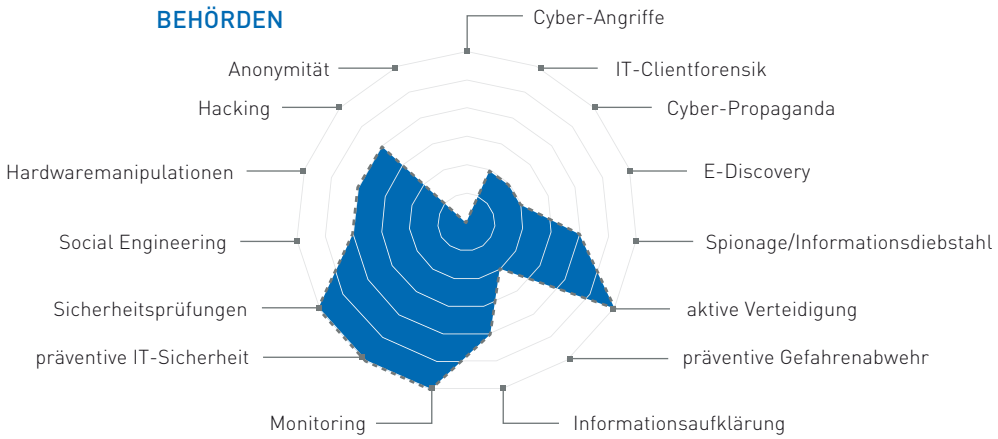
POLITIK



STAATSSCHUTZ



BEHÖRDEN



Quelle: Corporate Trust 2017

Wer sagt, Privatsphäre sei ihm egal, weil er nichts zu verbergen habe, könnte genauso behaupten, die Meinungsfreiheit sei ihm egal, weil er nichts zu sagen habe.

Edward Snowden,
Informatiker & NSA-Whistleblower

Made in Germany

Deutschland wird bei Cyber abgehängt

Fünfstellige Mitarbeiterzahlen bei den eigenen Geheimdiensten und Armeen für das Thema Cyber, Kaderschulen für Cyber Security Experten, Millionenausgaben für staatliche Cyber-Einheiten. Dies alles generiert einen riesigen Bedarf an Cyber Security Experten. Ausbildung wird dementsprechend groß geschrieben. Und wenn die gut ausgebildeten Kräfte später in die freie Wirtschaft wechseln, bringen Sie nicht nur ein hohes Wissen sondern auch wertvolle Kontakte mit.

So läuft das in China, Russland und – vor allem – natürlich in Amerika. Jeder IT-Sicherheitsexperte auf der Welt könnte in der NSA etwas lernen. Dementsprechend hat die NSA auch kaum Probleme, guten Nachwuchs zu finden und auszubilden. Die staatlichen Investitionen in Geheimdienste und Cyber-Einheiten erweisen sich so zusätzlich als Subventionsprogramm für die eigene IT-Sicherheitswirtschaft, die entsprechende Software entwickeln und Mitarbeiter aufbauen kann.

In Deutschland hingegen teilt sich die Cyber-Sicherheitslandschaft in zwei Teile. Neben den staatlichen Anstrengungen zur Cybersicherheit gibt es eine lebendige Szene hochqualifizierter Hacker. Historisch bedingt besteht in Deutschland ein großes Misstrauen gegenüber jeder Form von staatlicher Überwachung. Die deutschsprachige Hackerszene macht hier keine Ausnahme – eine gewisse anarchistische Grundhaltung mit einem Hang zur Paranoia und einer gewissen Sympathie für Verschwörungstheorien gehören zum guten Ton in deutschsprachigen Hackerkreisen.

Von staatlicher Seite werden zunehmend mehr Investitionen in Cyber-Einheiten getätigt. Allerdings zeigt sich hier der Föderalismus in Deutschland von seiner schwierigsten Seite. Anstatt alles in einer Behörde zu bündeln, werden Cyberfähigkeiten an verschiedensten Stellen aufgebaut: BSI, BfV, LfVs in den Bundesländern, BKA, LKAs in den Bundesländern, BND, Bundeswehr, LSI, CAZ, etc.

Die Angreifer sind aber längst einen Schritt weiter. Eine hierarchisch strukturierte Führung erarbeitet Strategien und vergibt klar formulierte Angriffsziele an die Einheiten. Gut organisierte Hacker-Einheiten bauen um ihre Top-Hacker eine Schar von Leuten herum, die noch in der Ausbildung sind und die Ideen der Profis schnell und großflächig umsetzen können. So laufen dann auch die derzeit beobachteten Angriffe. Ein wirklich guter Hacker findet ein Vorgehen, wie eine bestimmte Lücke in der Verteidigung eines Unternehmens ausgenutzt werden kann. Binnen Stunden wird diese Vorgehensweise dann von den „Hacker-Azubis" dupliziert und im gesamten Unternehmensnetzwerk auf alle angreifbaren Stellen angewandt. Wenn die Verteidiger die Lücke dann schließen, dauert es ein paar Tage bis der Top-Hacker wieder Zeit für dieses Projekt findet. Dann entwickelt dieser binnen Stunden einen neuen Angriff und übergibt ihn wieder in die Breite. Die typischen Ziele sind Zukunftstechnologien, wie z. B. Elektromobilität, erneuerbare Energien und mehr.

Gegen solche Strategien ist auch der beste Verteidiger machtlos, wenn er als „einsamer Wolf" einzeln unterwegs ist. Sowohl die deutschen Behörden als auch die IT-Verantwortlichen in den Unternehmen sind solchen Angriffen nicht bzw. nur mühsam gewachsen.

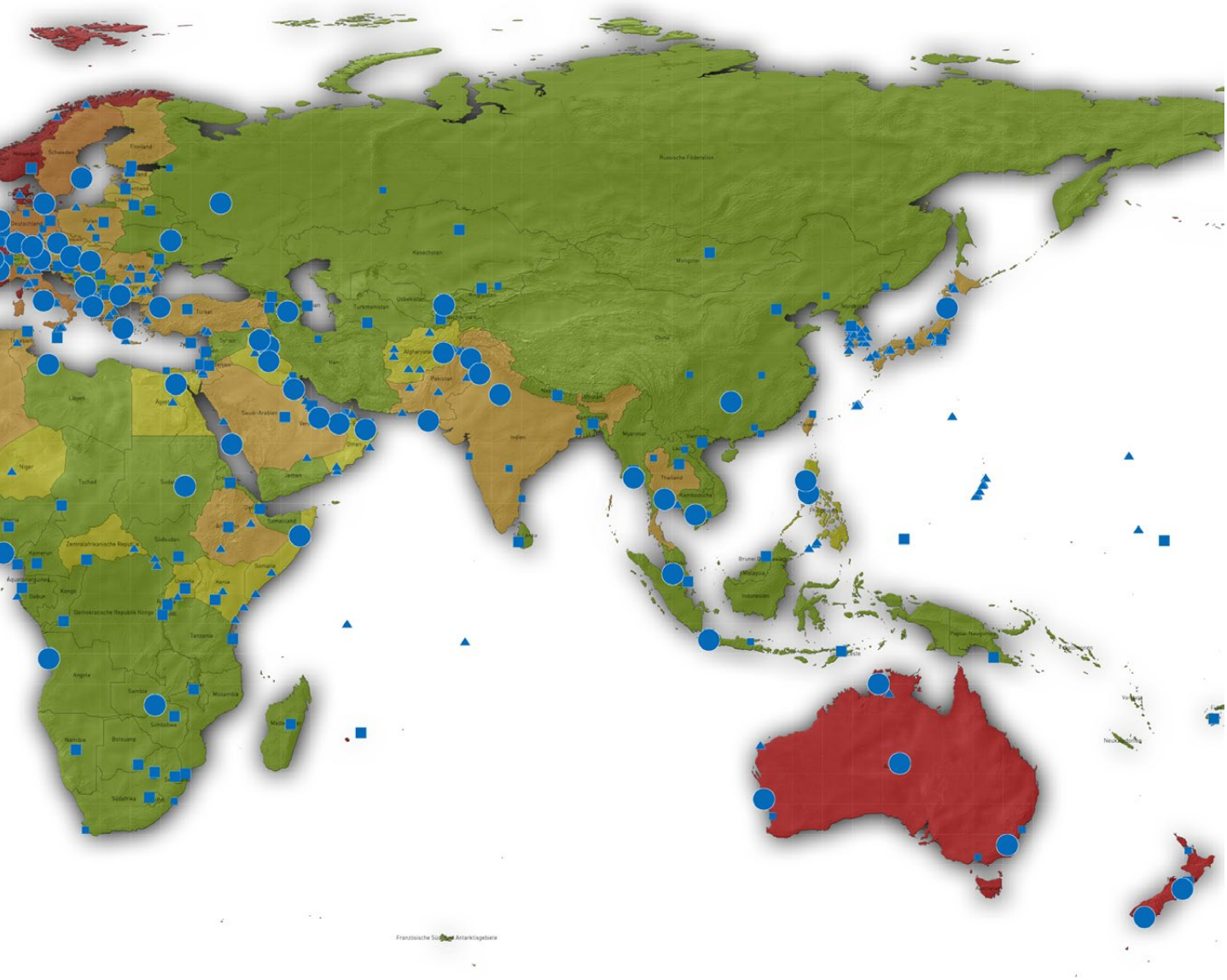
Deutschland hat im Bereich IT an vielen Stellen Nachholbedarf und der Fachkräftemangel ist hoch. Durch die mangelnden Investitionen in Cybersicherheit fällt es in diesem Bereich, im Vergleich zu den anderen Nationen, sogar deutlich weiter zurück.

Weltkarte der NSA-Cyberspionage

Überwachungspunkte der NSA

Das Hauptinstrument der NSA zur elektronischen Massenüberwachung ist XKeyscore, eine spezielle Software zum Auswerten von Metadaten. Installationen von XKeyscore werden von der NSA und von Partnern betrieben. Die technische Architektur von XKeyscore wird auf Seite 62 in diesem Report erläutert. Die Snowden-Papiere berichten von 700 Installationen in 150 Lokationen. 83 Lokationen konnten anhand der Dokumente eindeutig zugeordnet werden und sind in der Karte mit einem Kreis markiert.

Wir wissen außerdem, dass die NSA in Botschaften Spionageequipment installiert. Alle US-Botschaften sind mit einem größeren Quadrat markiert, alle Generalkonsulate mit einem kleineren Quadrat. Die NSA koordiniert und steuert außerdem die Geheimdiensteinheiten der US Streitkräfte. Alle extraterritorialen Kasernen und Lager der US-Streitkräfte sind mit einem Dreieck markiert.



Quelle: Corporate Trust 2017

Legende:

Partnerstatus mit der NSA

- Five Eyes
- Nine Eyes
- Fourteen Eyes
- 3rd Partner
- NATO
- Militärabkommen
- keine Verbindung

Formen

- XKeyscore Installation
- US-Botschaft
- US-Generalkonsulat
- US-Armeestützpunkt

Weltkarte der NSA-Cyberspionage

Abhörstandorte & Internet-Knotenpunkte

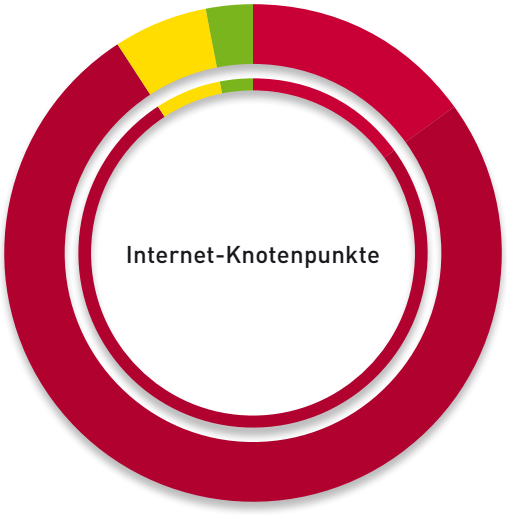
Die NSA überwacht rund 92% der gesamten Strecke weltweiter Unterseekabel und 91% der weltweiten Kapazität aller Internet-Knoten.

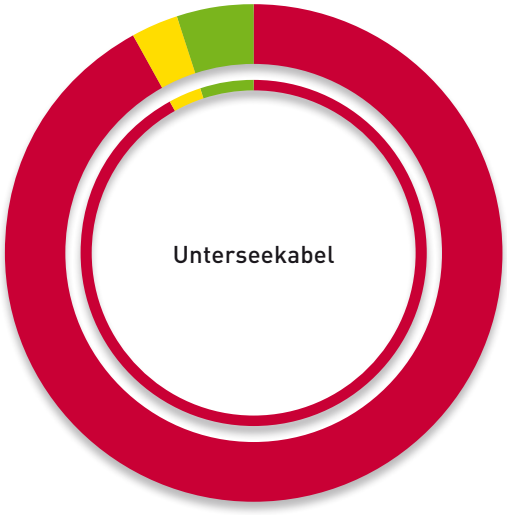
Die NSA betreibt Niederlassungen rund um die Welt. In der Karte sind 70 bekannte Standorte von XKeyscore Abhörsystemen eingezeichnet. Insgesamt gibt es mindestens 150 Standorte. Dazu kommen etwa 250 größere Botschaften und dutzende Armeestützpunkte, in denen potentiell NSA- oder CIA-Mitarbeiter sitzen.

Internationaler Informationstransfer funktioniert heute entweder per Satellit, über Seekabel oder über ein weitverzweigtes Netz an landgestützten Glasfaserkabeln, die an bestimmten Internet-Knotenpunkten zusammenlaufen. Die Überwachung der Satellitenkommunikation ist einfach. Einige spezialisierte Stationen (z. B. Bad Aibling) können viele Satelliten überwachen. Dementsprechend geht man von einer flächendeckenden Überwachung der Datenübertragungen per Satellit aus. Internet-Knotenpunkte und Seekabel müssen für eine Überwachung vor Ort angezapft werden.

Derzeit sind etwa 360 Unterseekabel und 90 größere Internetknoten in Betrieb. Aufgrund der NSA-Standorte gehen wir davon aus, dass an einem Großteil davon Spionageeinrichtungen installiert sind. Etwa 92% der gesamten Strecke der verlegten Unterseekabel und mindestens 91% der weltweiten Kapazität aller Internet-Knoten werden somit von der NSA überwacht.

Zugriffsmöglichkeiten der NSA





Internet-Knotenpunkte in 157 Städten mit gesamt 34.169 Gbit/s

- XKeyscore-Installation am selben Ort
- XKeyscore-Installation im Land vorhanden
- Land ist Partner der NSA
- NSA-Zugriff unwahrscheinlich

360 Unterseekabel mit insgesamt 1.888.162 km

- NSA-Zugriff fast sicher
- NSA-Zugriff wahrscheinlich
- NSA-Zugriff unwahrscheinlich

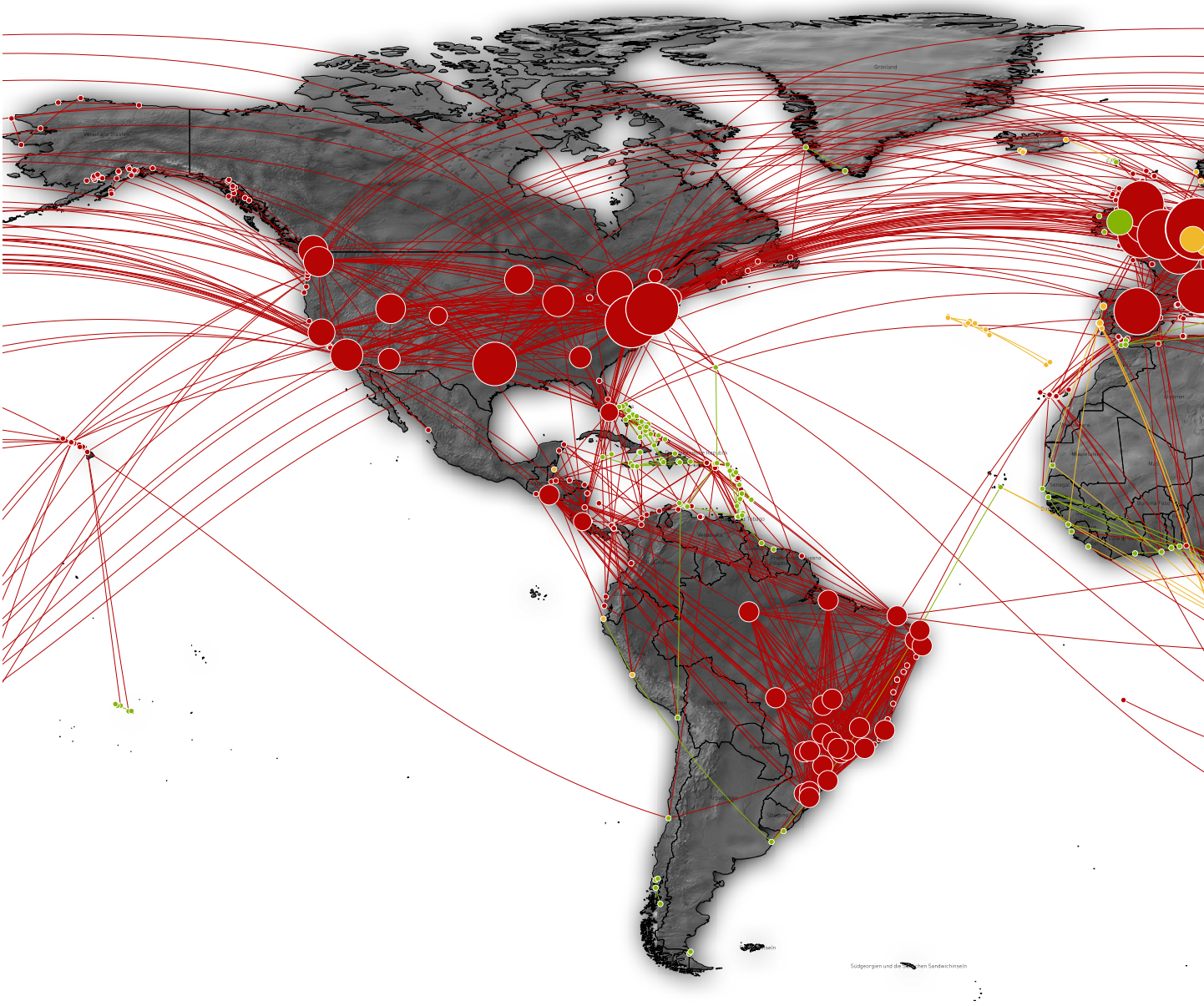
Quelle: Corporate Trust 2017

Wenn jeder Kriminelle etwas zu verbergen hat, heißt das nicht, dass jeder, der etwas zu verbergen hat, ein Krimineller ist. Es geht einfach darum, dass jeder ein Recht auf Geheimnisse hat, auf persönliche Dinge, die keinen anderen Menschen etwas angehen.

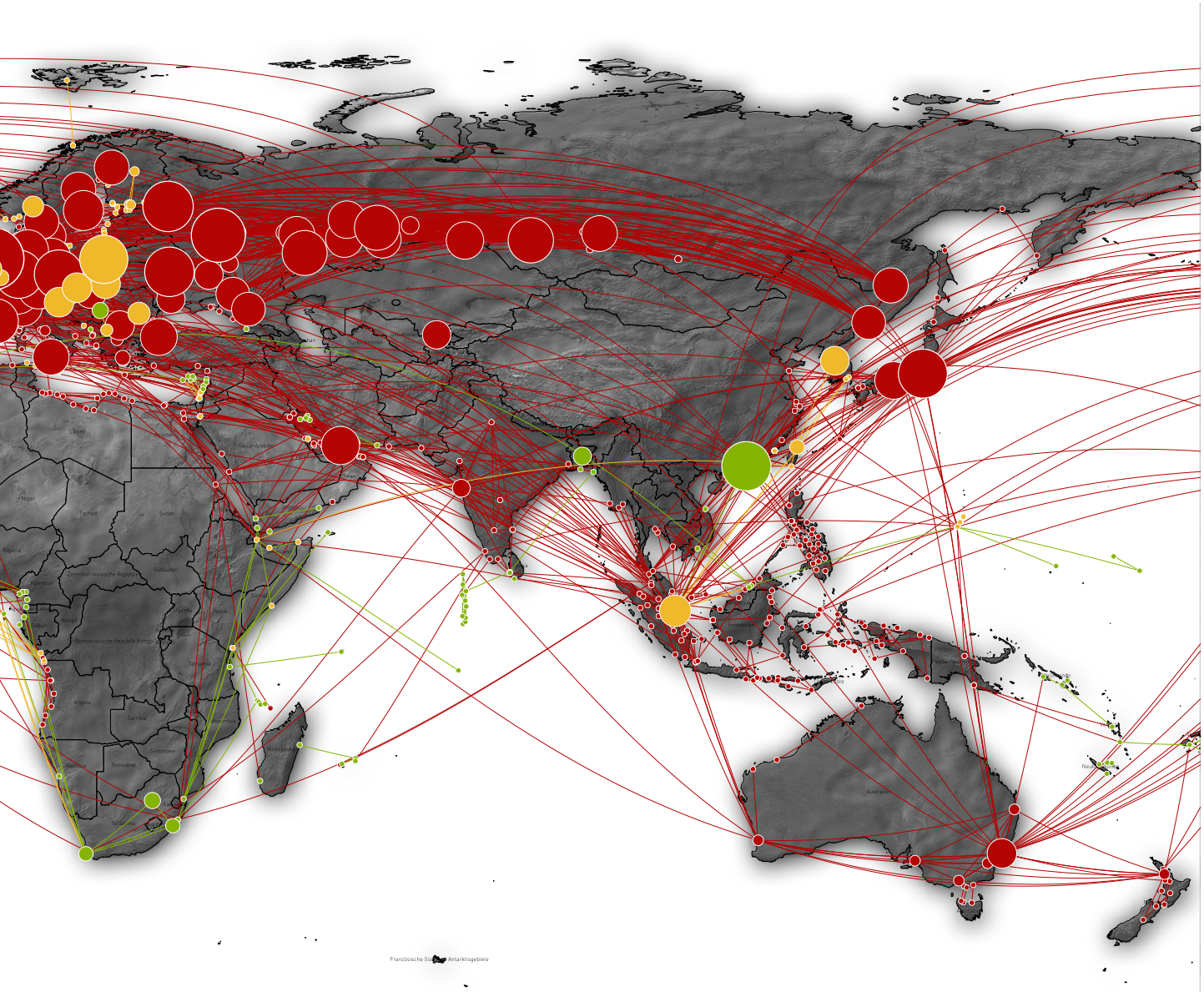
Sabine Leutheusser-Schnarrenberger,
ehemalige Bundesjustizministerin, 11.04.2016

Weltkarte der NSA-Cyberspionage

Internet-Knotenpunkte & Unterseekabel



Die NSA besitzt ausreichend Fähigkeiten, um nahezu jedes kommerziell betriebene System zu infiltrieren. Die Frage ist, ob ausreichend Infrastruktur für eine großflächige Extraktion von Daten vorhanden ist. Dementsprechend sind alle Knotenpunkt rot markiert, in deren Land es Hinweise auf entsprechende Infrastrukturen gibt. Gelb sind weiterhin die Infrastrukturen aller Länder markiert, die in der Vergangenheit bereits mit der NSA zusammengearbeitet haben, da hier ein Zugriff nicht auszuschließen ist. Grün bedeutet, dass keine Hinweise auf einen Zugriff der NSA bestehen. Die eingezeichnet Netzwerkverbindungen sind Unterseekabel und bekannte Verbindungen zwischen Internetknoten. Ist einer der Endpunkte rot, wird die Leitung rot markiert. Wenn beide Endpunkte maximal gelb oder grün sind wird die Leitung entsprechend gelb oder grün eingefärbt. Je größer der Kreis, desto größer ist der über diesen Knotenpunkt abgewickelte Internetverkehr. In der Grafik fehlen die – durchaus relevanten – Netze der großen Telekommunikationsprovider. Es ist davon auszugehen, dass die Situation bzgl. eines Zugriffs der NSA in diesen Netzen ähnlich ist.



Quelle: Corporate Trust 2017

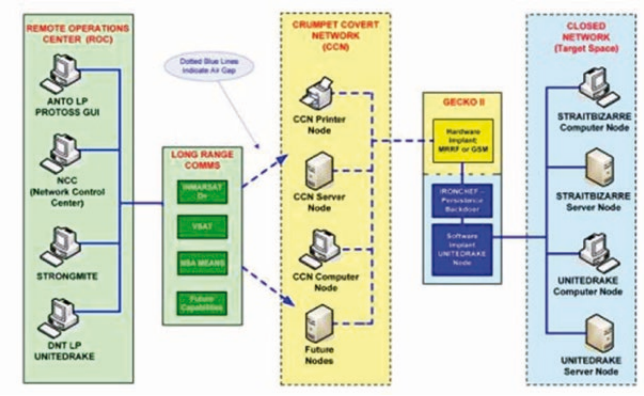
Legende:

- Internetknotenpunkt oder Kopfstelle eines Unterseekabels
- je größer, desto mehr Volumen („Traffic")
- es existiert eine bekannte Direktverbindung zwischen den beiden Punkten
- NSA-Zugriff fast sicher
- NSA-Zugriff wahrscheinlich
- NSA-Zugriff unwahrscheinlich

AUSBLICK

FÄHIGKEITEN DER NSA GESTERN UND MORGEN

NSA-Technologie 2009



Quelle: IRONCHEF Extendend Concept of Operations

Forecast: Fähigkeiten 2019

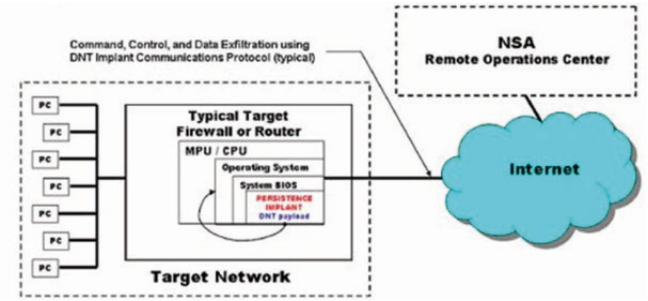
NSA kann das BIOS bestimmter Computer unterwandern

Jeder Prozessor besitzt mehrere Ebenen, auf denen er Programme ausführen kann. Dabei kann jeweils die übergeordnete Ebene auf die unteren Ebenen zugreifen. Dies wird benutzt, um den Betriebssystemkern, die Treiber und normale Software voneinander zu trennen. Moderne Prozessoren kennen jedoch unter der Betriebssystemebene noch den System-Management-Modus, mit dem bestimmte Hardwarefunktionen gesteuert werden können. Die NSA hat für Dell-Server (Projekt „Deitybounce") seit 2006 und für HP-Server (Projekt „Ironchef") seit 2007 Möglichkeiten, durch Manipulation des BIOS dauerhaft und unbemerkt vom Betriebssystem eigene Programme auszuführen. Für die Installation ist ein physischer Zugang zum Server notwendig.

Manipulation des BIOS aller Computer

Seit 2005 wird eine neue Alternative mit dem Namen UEFI (Unified Extensible Firmware Interface) für das in die Jahre gekommene BIOS entwickelt. Diese Software ist der erste Code, der nach dem Einschalten des Rechners ausgeführt wird, und ist für die richtige Initialisierung der Hardware zuständig. Neuerungen im UEFI sind die Zugriffsmöglichkeiten auf das Netzwerk und die Möglichkeit, während der gesamten Nutzung Codeteile auch parallel zum Betriebssystem auszuführen. Hinzu kommt, dass nahezu alle UEFI-Versionen auf eine gemeinsame Codebasis (Intel TianoCore) zurückgreifen. Es ist davon auszugehen, dass Geheimdienste auf dieser Basis über Softwareimplantate für faktisch jede Plattform (Server oder Clients) verfügen. Nach einmaligem physischem Zugang ist damit eine komplette, ggf. ferngesteuerte Kontrolle möglich.

NSA-Technologie 2009

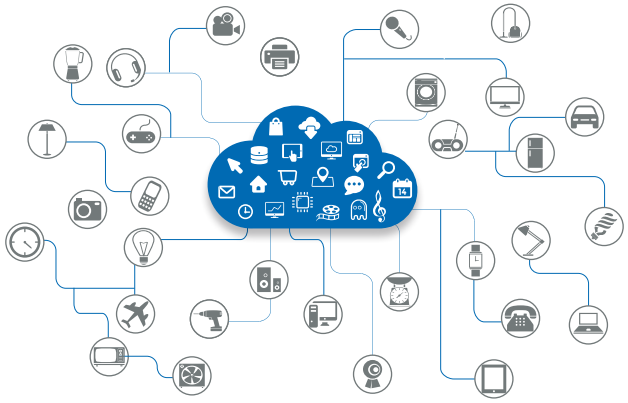


Quelle: SOUFFLETHROUGH Persistence Implant Concept of Operations

Umgehung von Firewalls

Für viele Firewalls bietet die NSA Technikabteilungen BIOS-Updates an, die von der NSA definierte Hintertüren in das eigentlich geschützte Netz öffnen. Verfügbar sind unter anderem Lösungen für Juniper-Netscreen-Firewalls und -Router (Projekte „Feedtrough", „Gourmettrough", „Souffletrough", „Schoolmontana", „Sierramontana", „Stuccomontana"), Huawei-Firewalls und -Router (Projekte „Halluxwater", „Headwater") sowie Cisco-ASA- und PIX-Firewalls (Projekt „Jetplow") (Stand 2007). Die Lösungen sind im inaktiven Zustand praktisch nicht detektierbar, voll konfigurierbar, fernsteuerbar und überleben BIOS- bzw. Softwareupdates. Zur Installation ist einmalig Zugang zum Gerät notwendig. Weitere Angriffe, unter anderem gegen Fortinet und Cisco Geräte, wurden mittlerweile bekannt (Projekte „Epicbanana", „Extrabacon").

Forecast: Fähigkeiten 2019



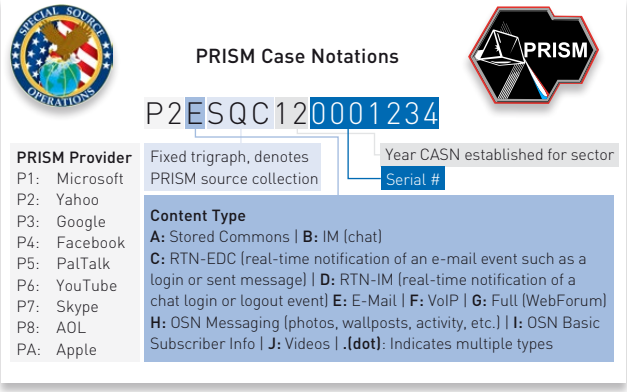
Kühlschrank bis Kläranlage: NSA manipuliert das Internet der Dinge

In den letzten zehn Jahren haben immer mehr Geräte Zugang zum Netz erhalten. Getränkeautomaten, Kantinenkassen, Schließsysteme, Telefon- und Durchsageanlagen, Alarmanlagen und Kameras funktionieren auf IP-Basis, ganz zu schweigen von den unzähligen Maschinensteuerungen der Industrie 4.0. Aber auch Smart-TVs werden z. B. für Mitarbeiterinformationen in Firmen und Behörden eingesetzt. Die Geräte basieren nahezu alle auf der gleichen, von Smartphones und Tablets bekannten, Architektur. Wie früher für Netzwerkgeräte ist davon auszugehen, dass Geheimdienste über Möglichkeiten verfügen, die häufigsten Plattformen der „Internet-of-Things-Welt" mit eigener Software zu infizieren und die Geräte fernzusteuern.

AUSBLICK

FÄHIGKEITEN DER NSA GESTERN UND MORGEN

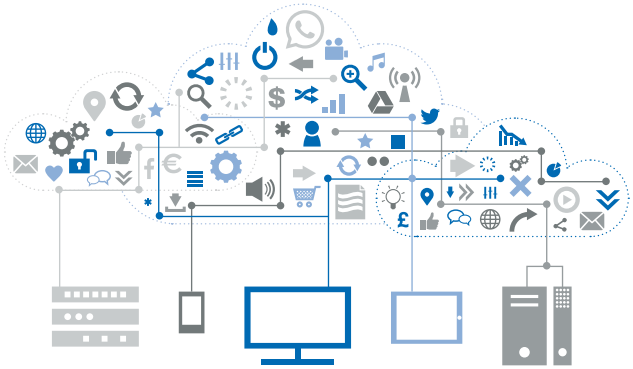
NSA-Technologie 2009



Speicherung der Nutzerdaten aller populären Internetdienste

Die NSA hat Zugriff auf die Produkte aller großen amerikanischen Internetdienste (Microsoft, Google, Facebook, YouTube, Skype, AOL und Apple) und sammelt deren Daten im Projekt „PRISM". Katalogisiert werden Suchanfragen, Chats, E-Mails, Telefonie (Voice-over-IP), Videos und sonstige Daten. Zusätzlich wurde 1999 bekannt, dass eine Hintertür („NSAKEY") in Microsoft Windows eingebaut ist.

Forecast: Fähigkeiten 2019

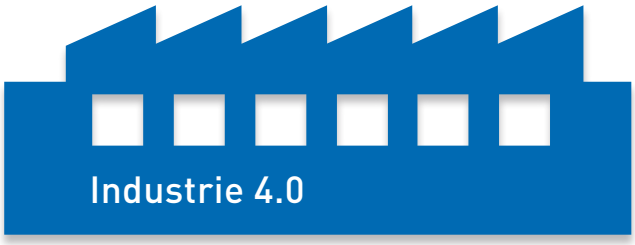


Clouds in aller Welt werden zum Ziel

Durch die zunehmenden Cloudstrategien konzentriert sich die Rechenleistung auf immer weniger Rechenzentren. Gleichzeitig steigt der Grad der Standardisierung in den Cloudrechenzentren. Es ist davon auszugehen, dass die NSA mittlerweile jedes größere Cloudrechenzentrum mit geeignetem Equipment implantiert hat, um eine Komplettüberwachung sicherstellen zu können. Dies dürfte sich kaum auf die USA und ihre Partnerländer beschränken. Angesichts der technischen Fähigkeiten der NSA ist mit einer zumindest unfreiwilligen und mittelbaren Implantierung (z. B. durch manipulierte Router) bei jedem Cloudprovider auf der Welt zu rechnen.

Gezielte Ausspähung von Monitoren, WLANS und DECT-Telefonen

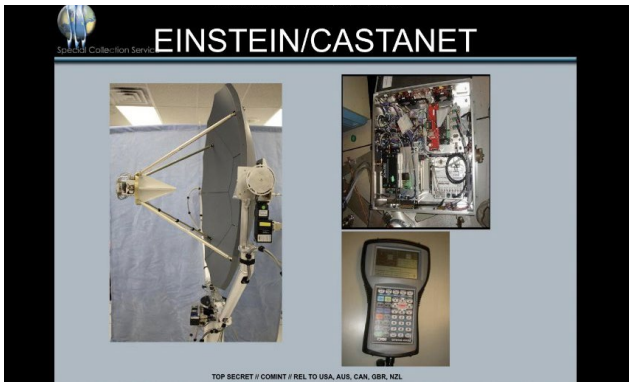
Mit einem komplexen System aus Wanzen, Verstärkern und Abhörequipment (Projekte „Nightstand", „Nightwatch", „Vagrant", „Dropmire", „Photoangelo") kann die NSA Monitorbilder, WLANs oder DECT-Signale aus einer Entfernung von bis zu 12,5 Kilometern mitlesen. Bei hochauflösenden Monitoren hilft ein manipuliertes Kabel (Projekt Ragemaster). Außerdem ist es möglich, Pakete in WLAN-Netzwerke einzuschleusen.



Ausspähen der Industrie direkt an der Maschine

Während die Angriffsszenarien früher auf Besprechungsräume und Vorstandsetagen beschränkt waren, eröffnet sich mit der zunehmenden Computerisierung der Industrie- und Steuerungsanlagen ein völlig neues Betätigungsfeld für diese Technologie. Es ist davon auszugehen, dass eine Liste strategisch interessanter Ziele existiert, die der Reihe nach mit den Nachfolgetechnologien versorgt werden.

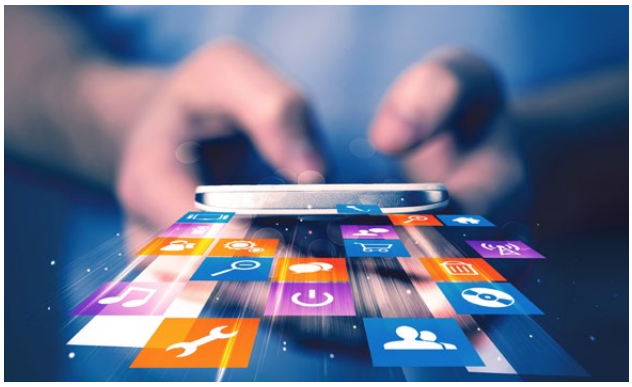
NSA-Technologie 2009



Abhören durch Antennen auf US-Gebäuden

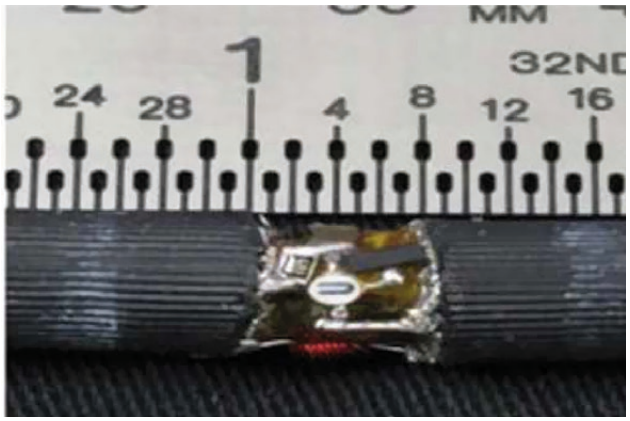
In allen größeren US-Botschaften sowie in diversen zugekauften Liegenschaften und Büros (z. B. im Gebäude der Internationalen Atomenergie-Organisation IAEO) befinden sich Antennenanlagen zum Abhören verschiedener Funknetze. „Wer im Berliner Regierungsviertel mit dem Handy telefoniere, gehe ein ganz großes Risiko ein, abgehört zu werden", so Burkhard Even, Leiter der Spionageabwehr beim Bundesamt für Verfassungsschutz. Das NSA-Arsenal umfasst Basisstationen für GSM, UMTS und LTE (Proj. „Nebula", „Cyclon Hx9", „EBSR", „Typhon HX"), Handyortungsgeräte (Proj. „Waterwitch"), Angriffsmöglichkeiten auf Handymasten (Proj. „Candygram") und SIM-Karten (Proj. „Gopherset" und „Monkeycalendar").

Forecast: Fähigkeiten 2019



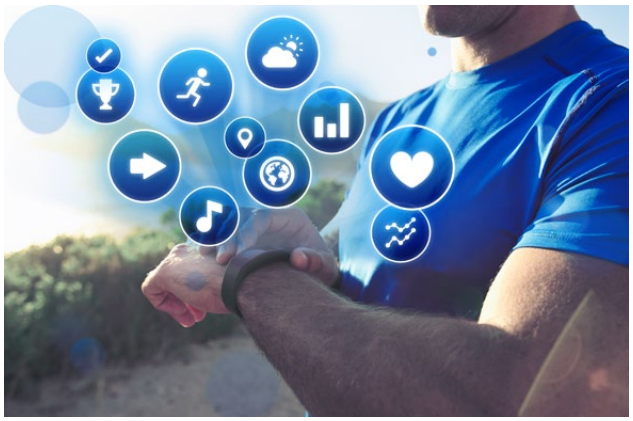
Apps, die alles über den User verraten

Die mobile App-Revolution begann 2008 mit der Eröffnung des App Store. Seitdem werden über mobile Datenverbindungen nicht mehr nur Anrufe und SMS übertragen, sondern auch viel mehr Informationen über ihre Nutzer als früher: Gesundheitsdaten der Fitnessarmbänder, der zukünftige Standort und die dorthin gewählte Route aus dem Navigationsprogramm, Standorte von Freunden und Bekannten, Kalendereinträge und E-Mails. Das Abhören von Telefonnetzen lohnt sich also wesentlich mehr. Es ist davon auszugehen, dass portables Equipment zum Abhören moderner Smartphones existiert.



Weit vorangeschrittene Miniaturisierung

Im Bereich Spionageequipment ist das Hardwarearsenal der NSA riesig: undetektierbare passive Sender, die von einem Abhörgerät aus der Entfernung angepeilt und stimuliert werden müssen, um zu senden (z. B. der zwölf Millimeter große Funk-Keyboardsniffer aus dem Projekt „Surlyspawn"), acht Millimeter große Minisender zur Datenextraktion mit 15 Metern Reichweite, die mehr als sechs Monate mit einer Knopfbatterie laufen, oder in Kabel integrierte Abstrahlverstärker (Projekt „Ragemaster", siehe Bild oben).



Cyber in Alltagsgegenständen

Der ständige Trend zur Miniaturisierung, der derzeit in intelligenter Kleidung und Stromerzeugung durch Körperbewegung und -wärme mittels Nanotechnologie gipfelt, ist sicherlich an der NSA-Technologie nicht spurlos vorübergegangen. Halbe Größe, doppelte Reichweite und unendliche Stromversorgung durch Nanotechnologie sind höchstwahrscheinlich im Bereich des Möglichen.

FÄHIGKEITEN DER NSA GESTERN UND MORGEN

NSA-Technologie 2009

Response to improving security

- For the past decade, NSA has lead an aggressive, multi-pronged effort to break widely used Internet encryption technologies
- Cryptanalytic capabilities are now coming on line
- Vast amounts of encrypted Internet data which have up till now been discarded are now exploitable
- Major new processing systems, SIGDEV efforts and tasking must be put in place to capitalize on this opportunity

Standard-Verschlüsselungen geknackt

Die Abteilung S31 der NSA (Cryptanalysis and Exploitation Services – CES) ist der Dienstleister für das Knacken von Verschlüsselungen. Ihre Fähigkeiten kommen für eine Vielzahl von Protokollen und landesspezifischen Methoden und Implementierungen zum Einsatz, u. a. für TLS, SSH und VPN (Projekt „Bullrun"). Neben Brute Force Cracking werden Hintertüren in kryptografische Methoden während des Designs oder Nachschlüssel in der Implementierung eingebaut.

Manipulierbare Festplatten

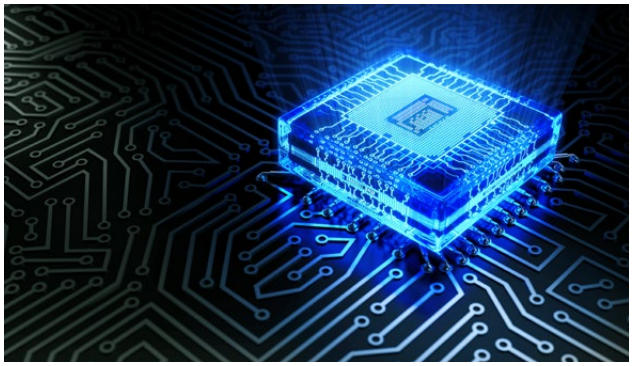
Die NSA verfügt über Technologie, um eigenen Code in der Firmware von Festplatten und SSDs (Projekt „IrateMonk") der Marken Western Digital, Samsung, Maxtor, Hitachi, Fujitsu und Seagate zu verankern. Die zum Zeitpunkt der Veröffentlichung wichtigsten Dateisysteme werden unterstützt: Neben den für Windows relevanten FAT und NTFS sind auch EXT3 (Linux) und UFS (BSD Unix) vorgesehen.

Bild: Eric Gaba, Wikimedia Commons user Sting

Forecast: Fähigkeiten 2019

Quantencomputer knacken Verschlüsselung ohne Zeitverzug

Peter Shor hat bereits 1994 einen Algorithmus vorgestellt, der die Ganzzahlfaktorisierung, eine der wichtigsten mathematischen Grundlagen vieler Verschlüsselungsalgorithmen, auf einem Quantencomputer blitzschnell lösen kann. Viele der heute eingesetzten Verschlüsselungen wären damit wertlos. Forscher der Universität in Maryland (30 Kilometer von der NSA-Zentrale entfernt) präsentierten im April einen Durchbruch bei der Konstruktion von Quantencomputern. Es ist davon auszugehen, dass der NSA eher früher als später die Fähigkeiten eines Quantencomputers zur Verfügung stehen.



Manipulation auf Chipebene

Während früher häufig spezialisierte Chips (sogenannte ASIC) in Geräte eingebaut wurden, dominieren heute frei programmierbare Mikro- und Signalprozessoren in allen Geräteklassen. Diese benötigen eine Firmware, um ihre Aufgabe zu erfüllen. Gleichzeitig ist der Markt für solche Prozessoren überschaubar, sodass einige Dutzend Prozessortypen den Gesamtmarkt ausmachen. Es ist davon auszugehen, dass der NSA neben Grafik- und Netzwerkkarten auch Implantierungstechniken für Spielekonsolen, Fernseher, Smartwatches, Fitnessarmbänder, Navigationsgeräte, Autosteuergeräte sowie andere Bluetooth- und USB-Geräte zur Verfügung stehen.

Das Geheimnis der Freiheit ist der Mut.

Perikles

AUSBLICK

CYBER-PROLIFERATION

Unter dem Begriff „Proliferation" versteht man die Weiterverbreitung von Massenvernichtungswaffen bzw. der zu ihrer Herstellung verwendeten Produkte, einschließlich des dafür erforderlichen Know-hows, sowie von entsprechenden Waffenträgersystemen. Die Verbreitung atomarer, biologischer oder chemischer Massenvernichtungswaffen stellt global derzeit eines der größten Sicherheitsrisiken dar. Die Verbreitung derartiger Waffen bedroht auf unkalkulierbare Art und Weise den Weltfrieden und birgt letztlich die Gefahr eines nicht mehr kontrollierbaren Flächenbrandes. (Quelle: Bundesamt für Verfassungsschutz).

Die verschiedenen Dienste und Militäreinheiten der Welt produzieren aktuell „Waffen" für ihre Operationen im Cyberraum. Mit diesen „Exploit" genannten Softwarestücken kann man in geschützte IT-Systeme eindringen, Informationen stehlen oder Computer lahmlegen. Die Idee hinter einem solchen Exploit ist oft genial und einzigartig. Da die „Waffen" im Einsatz aber von verschiedensten Personen benutzt werden sollen sind sie in der Bedienung möglichst einfach und entsprechend gut dokumentiert. Die Wertigkeit einer Cybereinheit bemisst sich anhand der Anzahl und Qualität der Exploits, die sie in ihrem Arsenal hat.

Das Potenzial dieser Cyberwaffen wächst mit jeder neuen IT-Revolution und wird im Zeitalter von Industrie 4.0, selbstfahrenden Autos, computergesteuerten Stromnetzen und dem „Internet of Things" die Zerstörungskraft von Atomwaffen erreichen.

Cyberwaffen haben aber eine ganze Reihe weiterer besonderer Eigenschaften. Manche dieser Waffen hinterlassen Spuren, durch deren Analyse man die Idee hinter der Waffe herausfinden kann. Ein Experte kann diese Waffe dann nachbauen oder eine Verteidigung dagegen entwickeln. Es besteht also die Gefahr, dass durch den Einsatz einer solchen Waffe, diese in falsche Hände gerät oder nutzlos wird. Außerdem ist eine Cyberwaffe am Ende einfach nur ein Stück Software. Dadurch kann eine solche Waffe einfach kopiert werden. Bricht also ein Hacker in das Netzwerk einer Cybereinheit ein, kann er das ganze Arsenal der Cyberwaffen stehlen. Dies passiert bereits heute. Eine Gruppe namens Shadowbrokers verkauft die Cyberwaffen einer NSA Einheit an den Meistbietenden.

Das Thema Proliferation muss also im Cyberraum komplett neu gedacht werden. Dies ist für die Wirtschaft essentiell. Solange staatliche Cybereinheiten überall auf der Welt aufrüsten und gleichzeitig Hackergruppen deren Arsenale stehlen können, wird sich die Wirtschaft ständig hochentwickelten Cyberwaffen gegenüber sehen. Damit wird die Verteidigung teuer.

Der derzeit einzige Schutz: je länger eine Cyberwaffe lagert, desto größer ist die Chance, dass sie nur noch eingeschränkt oder gar nicht mehr nutzbar ist.

!!! Attention government sponsors of cyber warfare and those who profit from it !!!!

How much you pay for enemies cyber weapons? Not malware you find in networks. Both sides, RAT + LP, full state sponsor tool set? We find cyber weapons made by creators of stuxnet, duqu, flame. Kaspersky calls Equation Group. We follow Equation Group traffic. We find Equation Group source range. We hack Equation Group. We find many many Equation Group cyber weapons. You see pictures. We give you some Equation Group files free, you see. This is good proof no? You enjoy!!! You break many things. You find many intrusions. You write many words. But not all, we are auction the best files.

Einladung zur Auktion der Cyber-Waffen der NSA-Elitegruppe "Equation Group" durch eine Gruppe namens „Shadow Brokers.

Befreundete Nachrichtendienste

Auswirkungen neuer Strategien

Die Re-Industrialisierungsstrategien und die politischen Veränderungen bei unseren westlichen Partnern sind mit Aufmerksamkeit zu begleiten.

Britain First - America first - Les Français d'abord. In weiten Teilen der westlichen Welt sind politische Re-Industrialisierungs-Tendenzen mit dem Ziel zu erkennen, Industrieproduktion verstärkt wieder im eigenen Land zu etablieren. Einher geht dies zumeist mit der Betonung auf nationale Interessen. Diese politischen Veränderungen bei unseren westlichen Partnern sind mit Aufmerksamkeit zu begleiten, da steigende geheimdienstliche Aktivitäten zur Stärkung der nationalen Wirtschaftskraft durchaus denkbar erscheinen. „Im Interesse des wirtschaftlichen Wohlergehens des Vereinigten Königreichs" spioniert beispielsweise der britische GCHQ und beschreibt dies öffentlich als eine seiner drei Hauptaufgaben. Auch Frankreich ist in diesem Bereich seit jeher aktiv, was der NSA die Aufgabe einbrachte, Spionagetätigkeiten der französischen Geheimdienste mit wirtschaftlichem Fokus abzuwehren.

Re-Industrialisierung ist nicht nur der Hoffnungsträger der Regierungen in London, Washington und Paris, sondern beispielsweise auch von Madrid sowie der Brüsseler EU-Kommission. Diese hatte im Herbst 2012 das Ziel formuliert, den Industrieanteil in Europa von 16% bis 2020 wieder auf 20% zu steigern. So einfach das klingt, so schwierig ist das Unterfangen. In der Europäischen Union sackte im Jahr 2013 der Anteil der produzierenden Unternehmen an der gesamten Wertschöpfung auf nur noch ca. 15 Prozent ab und seit 2007 gingen EU-weit 3,8 Millionen Arbeitsplätze in der Industrie verloren.

Der Wunsch nach einer Renaissance der Industrie resultiert einerseits aus der Feststellung, dass Deutschland dank einer breit aufgestellten und stabilen industriellen Basis ohne Massenentlassungen und soziale Verwerfungen durch die Krise gekommen ist. Andererseits setzt sich die Erkenntnis durch, dass der Anteil des verarbeitenden Gewerbes an den gesamten privaten Forschungs- und Entwicklungsausgaben in vielen Ländern häufig über der 60%-Marke liegt. Durch wichtige Trends wie Industrie 4.0, selbstfahrende Autos oder intelligente Stromnetze, kurz durch die Verschmelzung von Informationstechnologie und langlebigen Produkten, wird die Industrie zunehmend mit forschungsintensiven Tätigkeiten und moderner, umweltverträglicher Produktion in Verbindung gebracht. Eine funktionierende Industrie hilft also, international wettbewerbsfähig zu bleiben.

Die Wiederansiedlung von verarbeitender Industrie in einer globalisierten Welt, dies zeigen erste Erfahrungen, ist jedoch eine schwierige Aufgabe. Dabei können wirtschaftliche Informationen über Industrien anderer Länder durchaus hilfreich sein. Einige Snowden-Unterlagen offenbaren interessanter Weise, dass eine Analyse der Daten aus dem Projekt Tempora, ein Programm zur Überwachung des weltweiten Telekommunikations- und Internet-Datenverkehrs des britischen GCHQ, bis ca. Mai 2010 nur durchgeführt werden durfte bei

- Verdacht auf Terrorismus,
- Handel mit Waffen,
- in großen Betrugs- und Drogenfällen,
- bei Fragen zur militärischen Ausrichtung fremder Regierungen und
- deren politischen Absichten.

Nach diesem Zeitpunkt erstellte Unterlagen verweisen hingegen auf Großbritanniens „economic well-being", also dem wirtschaftlichen Wohlergehen des Landes, als Grundlage für eine Tempora-Analyse. Ein Freibrief zur Wirtschaftsspionage, der verklausuliert nun auch auf der Webseite des GCHQ nachzulesen ist. Es bleibt also nur noch die Frage zu beantworten, wie weitreichend und gegen wen diese Befugnisse eingesetzt werden.

Zentrale des britischen Geheimdienstes GCHQ

Mit dem Brexit-Votum macht sich Großbritannien weitgehend unabhängig von der EU, steht aber auch vor enormen Herausforderungen. Dabei ist es ein erklärtes Ziel, verstärkt Industrie anzusiedeln und sich nicht mehr nur auf den Dienst- bzw. Finanzdienstleistungssektor zu konzentrieren. Unterstützt wird das Unterfangen mit einem Geheimdienst, der sogar die NSA mit seinen weitreichenden und teilweise überlegenen Fähigkeiten beeindruckt hat, wie Snowden-Unterlagen zeigen.

Natürlich gilt das Augenmerk bei Schutz vor Spionage hauptsächlich den Akteuren wie Russland oder China. Mit dem Wissen, dass beim Trend Re-Industrialisierung auch Daten über die wirtschaftliche Tätigkeit, wie aktuelles Know-how zu Prozessen und Prozesstechniken, sowie Forschungs- und Entwicklungstätigkeiten im Fokus stehen, sollten die politischen Veränderungen bei unseren westlichen Partnern mit Aufmerksamkeit begleitet werden.

PRÄVENTION

SCHUTZ DER DEUTSCHEN WIRTSCHAFT

Oft wird behauptet, gegen die NSA könne man sich nicht schützen. Das ist nicht korrekt. Korrekt ist, um sich gegen die NSA zu schützen, muss man mit mehreren derzeit üblichen Paradigmen brechen.

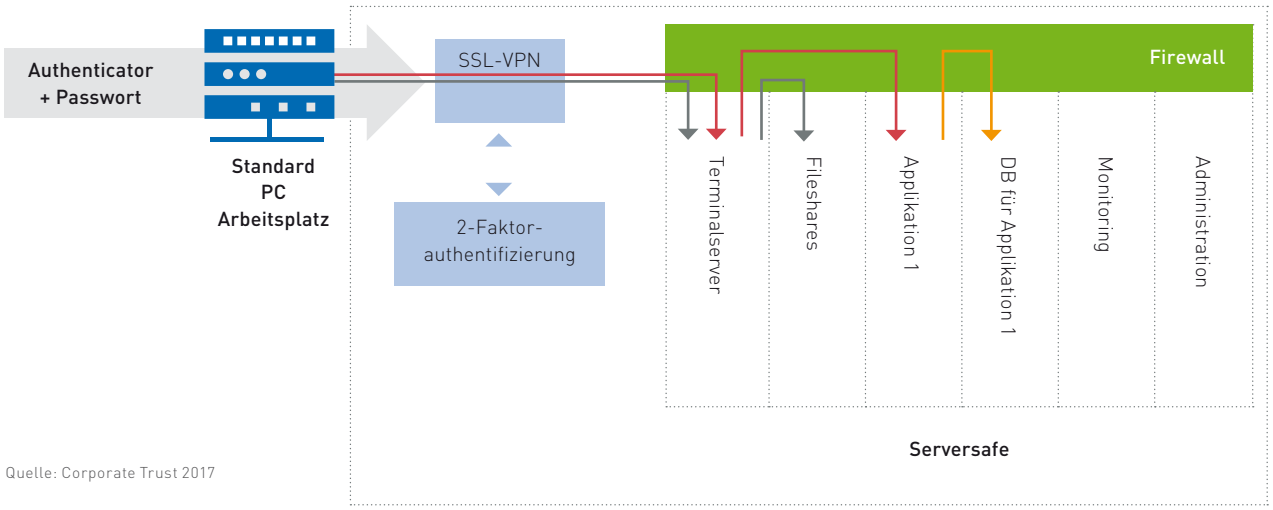
Ein Schutz gegen Angreifer vom Level einer NSA ist nicht für alle Daten und Applikationen möglich. Realistisch gesehen kann ein Unternehmen höchstens 1-2% der Informationen auf dieser Ebene absichern. Wir sprechen also vom „Kronjuwelenschutz". Diese müssen dementsprechend zuerst identifiziert werden. Die IT eines Unternehmens muss Kompromisse eingehen: Kosten, Verfügbarkeitsanforderungen und Benutzerfreundlichkeit müssen gegen den Schutz der Vertraulichkeit abgewogen und ein Kompromiss gefunden werden. Für 98% der Daten gilt dies weiterhin. Für die Kronjuwelen gelten drei Regeln. Erstens: Vertraulichkeit geht vor Verfügbarkeit. Zweitens: Die Benutzerfreundlichkeit muss mindestens so gut sein wie in der „normalen" IT. Drittens: Die Kosten für Konzeption, Anschaffung und den laufenden Betrieb müssen akzeptabel sein, dürfen aber, relativ zur Größe der Umgebung, höher sein als für die normale IT.

Dazu kommen einige operative Veränderungen für die Benutzer. Alle Aktivitäten jedes Users rund um die Kronjuwelen werden komplett aufgezeichnet, sind komplett rückverfolgbar und die Protokolldateien werden auf unbestimmte Zeit archiviert. Es findet keine Anonymisierung statt. Dies wird jedem User klar mitgeteilt und jeder Benutzer muss dem explizit zustimmen. Jeder Benutzer muss außerdem eine gesonderte Vertraulichkeitserklärung unterzeichnen und ein polizeiliches Führungszeugnis vorlegen. Alle Berechtigungen werden auf maximal 6 Monate vergeben und erlöschen zum Ende dieses Zeitraums automatisch. Alle ausgehenden bzw. verarbeiteten Daten werden protokolliert und verifiziert (Full Data Loss Prevention).

Auch die Administration wird verändert. Administratoren dürfen nicht auf die Daten zugreifen, sondern nur die Systeme administrieren und die Rechte vergeben. Konzeptionsarbeiten und tiefgehende Administrationseingriffe dürfen nur direkt am Gerät und im Vier-Augen Prinzip durchgeführt werden können. Alle Systeme für die Kronjuwelen müssen sehr robust, stabil, selbstheilend und autark arbeiten. Die Anzahl der notwendigen administrativen Aktionen ist durch konsequente Simplifizierung/Automatisierung auf ein Minimum zu reduzieren. Alle IT-Systeme für die Kronjuwelen befinden sich in einer physikalisch hoch gesicherten Umgebung (Stichwort „Serversafe") und sind videoüberwacht. Der Videoserver befindet sich wiederum im Serversafe. In diesen Serversafe führen zwei Kabel: 1x Strom und 1x Netzwerk.

Es existiert eine Monitoringmannschaft, die sämtliche Vorgänge im Safe überwacht. Diese Mannschaft wird sinnvoll mit Tools und Alarmsystemen unterstützt – am Ende zählt aber die menschliche Intelligenz. Die Monitoringmannschaft sieht nur die Logs, nicht die Daten. Kein Administrator ist in der Monitoringmannschaft (und vice versa).
Nur wirklich einfache Systeme können abgesichert werden. Die Systeme, auf denen Kronjuwelen lagern, sind auf die absolut essentiellen Komponenten reduziert, maximal gehärtet, maximal vereinfacht und in Ihrer Funktionsvielfalt maximal reduziert. Zugriffe auf die Kronjuwelensysteme sind immer verschlüsselt und mit einer 2-Faktor-Authentifizierung geschützt. Die Umgebung ist voll segmentiert, mit einem streng definierten Firewallregelwerk. Jedes Segment hat dedizierte Server und dedizierte Hardware, es gibt keine segmentübergreifende Virtualisierung oder segmentübergreifende Serverblades.

NSA-sichere IT-Systeme



Quelle: Corporate Trust 2017

[...] Während des kalten Krieges gab es eine rege öffentliche Debatte über Nuklearwaffen und ihren Einsatz. Für den Cyber-Bereich gibt es sowas aktuell nicht.

Frage von Thom Shanker, The New York Times,
an ein Expertenpanel November 2014

Richtig, weil Cyber bezüglich der offensiven Einsatzmöglichkeiten immer noch in den Kinderschuhen steckt. Ich denke, das kommt schon noch. [...] Aber von unserer Perspektive aus gesehen: Es ist unsere Absicht, das volle Spektrum des Cyber-Potenzials auszuschöpfen, um unsere Politiker und Befehlshaber mit einer möglichst großen Bandbreite an Optionen zu versorgen, falls sie diese nutzen wollen.

Admiral Michael Rogers,
Chef der NSA und des U.S. Cyber Command

Prävention

Cyber-Versicherungen nach Mass

Michael Dutz
Prokurist
Leiter IT- und Cyberversicherungen

Dr. Hörtkorn München GmbH
Lochhamer Schlag 5
82166 Gräfelfing
michael.dutz@hoertkorn-muenchen.de
www.hoertkorn-muenchen.de

DR. HÖRTKORN
VERSICHERUNGSMAKLER

Seit Einführung der ersten Cyberpolicen in Deutschland sind inzwischen mehrere Jahre vergangen. Gleichwohl ist das Thema, nicht zuletzt aufgrund täglicher Berichterstattung, aktueller denn je.

Bislang war herrschende Meinung gerade im Mittelstand, dass in erster Linie die Großindustrie akut bedroht ist und ein Cyberangriff auf mittelständische Unternehmen eher die Ausnahme darstellt.

Diese Einschätzung war und ist falsch. Gerade im Mittelstand lassen sich seit Beginn des Jahres 2016 verstärkt ungezielte Angriffe mittels Ransomware bzw. durch Krypto-trojaner beobachten, die einzig und allein das Ziel verfolgen, kurzfristig Erpressungelder zu generieren. e-Crime ist für organisierte Kriminelle zwischenzeitlich lukrativer als Drogenhandel.

Bereits 2014 war laut der Studie „Industriespionage 2014" von Corporate Trust beinahe jedes zweite deutsche Unternehmen im Mittelstand von e-Crime oder einem Verdachtsfall betroffen, Tendenz steigend. Diesen Trend zeigen auch Berichte zur aktuellen Bedrohungslage. Hier belegt Cyber durch die stetige Zunahme an Vorfällen bereits einen Platz unter den TOP 3 der Unternehmensrisiken.

Im Zusammenhang mit Cyberkriminialität wird oft eine Tätergruppe übersehen, der eigene Mitarbeiter oder Unternehmen im direkten Umfeld. Rund 50 Prozent aller Informationssicherheitsverletzungen, sei es durch reine Fahrlässigkeit oder vorsätzliches Handeln, sind auf diesen Personenkreis zurückzuführen.

Nahezu jedes Unternehmen ist so stark abhängig von seiner EDV, dass eine Informations- oder Netzwerksicherheitsverletzung meist eine Betriebsunterbrechung mit hohem finanziellem Schaden zur Folge hat. Neben dem reinen Ertragsausfall sind gesetzliche und/oder vertragliche Haftpflichtansprüche, zum Beispiel aufgrund Verletzung von Geheimhaltungs- oder Vertraulichkeitsvereinbarungen, Meldepflichten bei Behörden, Benachrichtigung von Dateninhabern, Kosten für forensische Dienstleistungen, Erpressung und Lösegeldforderungen Szenarien, die Unternehmen in Ihrer Existenz gefährden können.

Grundsätzlich ist diesem Risiko nur mit einem ganzheitlichen IT-Sicherheitsmanagement zu begegnen. Dieses besteht aus notwendigen technischen, organisatorischen und personellen Maßnahmen, sowie dem Risikotransfer des Restrisikos. Allerdings, selbst bei bestmöglicher Umsetzung der vorgenannten Maßnahmen, kann kein hundertprozentiger Schutz gewährleistet werden!

Dennoch ist die Marktdurchdringung von Cyberpolicen zur Absicherung dieses Restrisikos (Risikotransfer) noch erschreckend gering. Ein Grund hierfür ist sicher die in der Vergangenheit fehlende Transparenz der angebotenen Produkte.

Nach unserer Einschätzung besteht diese noch immer. Nur langsam setzen sich gewisse Standards durch. So bieten die meisten Anbieter modulare Produkte, die sich grob in die Bausteine Assistance-Dienstleistungen, einen Haftpflicht- und einen Eigenschadenbaustein unterteilen. Innerhalb dieser Dreiteilung sind die Unterschiede allerdings nach wie vor gravierend. Es ist für einen Laien fast unmöglich, die Versicherungslösungen miteinander zu vergleichen.

Die Hörtkorn München GmbH hat als einer der ersten Versicherungsmakler ein eigenes Bedingungswerk auf den Markt gebracht. Neben innovativen und marktführenden Deckungserweiterungen in allen Bausteinen wurde auf klare und einheitliche Definitionen in einer verständlichen Struktur Wert gelegt.

Wir sind davon überzeugt, dass in Kürze eine Cyberpolice, ähnlich wie eine Feuer- oder Betriebs-Haftpflicht-Versicherung, zum Standardportfolio eines jeden Unternehmens zählen wird.

Ihr

Michael Dutz

DR. HÖRTKORN MÜNCHEN GMBH

Spezialisten für Cyber- und IT-Versicherungen

Die Dr. Hörtkorn München GmbH beschäftigt sich schwerpunktmäßig mit der Absicherung von e-Crime-Risiken für alle mittelständischen und großgewerblichen Kunden, national wie international.

Darüber hinaus agiert die Dr. Hörtkorn München GmbH als spezialisierter Versicherungsmakler der IT-/ ITK-Branche. Zu den Kunden zählen insbesondere Softwarehäuser, IT-Dienstleister, Systemhäuser sowie Telekommunikationsunternehmen.

Versicherungsschutz für Unternehmen:
CYBER PROTECTION PLUS BY HÖRTKORN

Versicherungsschutz für die IT-/ITK-Branche:
IT MULTILINE COVER BY HÖRTKORN

siehe auch:
https://www.dr-hoertkorn.de/dienstleistungen/cyber-und-it-management.html

Glossar

Organisationsnamen

- **NSA – National Security Agency**
  Technisch orientierter militärischer Geheimdienst der USA. Die NSA ist vor allem mit der Fernmeldeaufklärung und dem Knacken von Verschlüsselungen betraut, aber auch mit der Sicherung eigener Systeme. Sie untersteht dem US-Verteidigungsministerium und arbeitet als Teil der Intelligence Community (IC) mit den 16 anderen Geheimdiensten der USA sowie mit Behörden befreundeter Staaten zusammen, insbesondere im Verbund UKUSA. Obwohl schon 1952 gegründet, wurde die Existenz der NSA lange geheim gehalten, sodass die Abkürzung scherzhaft auch als „No such agency" oder „Never say anything" übersetzt wurde.
- **CAO – Close Access (Technical) Operation**
  Technische Überwachungsmaßnahmen, die von Agenten der UKUSA-Geheimdienste direkt vor Ort in der unmittelbaren Umgebung der Zielperson/des Zielsystems (Targets) durchgeführt werden, beispielsweise durch NSA-F6 (Special Collection Service).
- **CNA – Computer Network Attack**
  Aufgabenbereich von z. B. NSA-TAO, U.S. Cyber Command, GCHQ-JTRIG.
- **CNCI – National Cyber Security Initiative**
  Unterstützt finanziell die Programme „Blarney", „Fairview", „Stormbrew" und „Oakstar".
- **CND – Computer Network Defense**
  Begriff der UKUSA-Geheimdienste für alle Maßnahmen, die der Absicherung und dem Schutz ziviler, geheimdienstlicher und militärischer Netzwerke dienen.
- **CNE – Computer Network Exploitation**
  Begriff der UKUSA-Geheimdienste für Operationen zur Infiltration und Überwachung von Computern und Computernetzwerken.
- **CNIO – Computer Network Information Operations**
  Begriff der UKUSA-Geheimdienste für Operationen zur Verbreitung von Informationen zwecks Manipulation/Beeinflussung, Desinformation, Propagandaverbreitung und Diskreditierung.
- **CNO – Computer Network Operation**
  Überbegriff für CNA, CND und CNE.
- **CSEC – Communications Security Establishment Canada**
- **CSOC (GCHQ) – Cyber Security Operations Centre**
  Abteilung im GCHQ-Hauptquartier, die mit der Absicherung britischer IT-Systeme und -netzwerke, aber auch mit der Entwicklung offensiver Angriffsplattformen für elektronische Kriegsführung und Sabotage, befasst ist. Ihre Mitglieder rekrutieren sich neben dem GCHQ aus anderen britischen Geheimdiensten und Polizeibehörden. Ähnlicher Aufgabenbereich wie das NTOC der NSA.
- **CSS – Central Security Service**
  Militärischer Teil der NSA, der für den Austausch und die Koordination mit dem Militär im Zusammenhang mit SIGINT zuständig ist. Direktor ist derzeit Admiral Michael S. Rogers, er ist gleichzeitig auch Chef der NSA.
- **ECC – European Cryptologic Center (NSA-F22)**
  2011 als Nachfolgeorganisation des European Security Operations Center (ESOC) im Dagger Complex bei Griesheim/Darmstadt eröffnet. Es soll zukünftig nach Wiesbaden in das neue Consolidated Intelligence Center verlagert werden.
- **ESC – European Security Center**
  Identisch mit ESOC Darmstadt.

- **ESOC – European Security Operations Center**
  Seit 2011 als Nachfolgeorganisation ECC im Dagger-Complex bei Griesheim.
- **ETC – European Technical Center (NSA-F25)**
  Europäische Kommunikationszentrale der NSA (2011 modernisiert).
- **F6**
  Zentrale des Special Collection Service (SCS), die ein gemeinsames Aktivitätsfeld von NSA und CIA darstellt.
- **IAD – Information Assurance Directorate**
- **IC – Intelligence Community**
  Oberbegriff, unter dem die Geheimdienste der USA zusammengefasst werden, die eng zusammenarbeiten. Zur IC gehören militärische Nachrichtendienste wie die NSA und der Marinegeheimdienst, aber auch zivile Behörden wie die Bundespolizei FBI und das Heimatschutzministerium DHS.
- **INSCOM – Intelligence and Security Command (NSA-Abteilung)**
- **IOCC – Interagency Operations Coordination Center**
- **IOD – Interactive Operations Division**
- **MOC – Meade Operations Center (NSA-F74)**
- **MSOC – Misawa Security Operations Center (Japan – NSA-F79F)**
- **NAC (NSA) – Network Analysis Center (NSA-SSG22)**
- **NAC (GCHQ) – Network Analysis Center**
  Analyse- und Überwachungszentrum des GCHQ, das u. a. fremde Netzwerktopologien analysiert und QUANTUM-INSERT-Angriffe gegen Zielpersonen durchführt, die eine Rolle in diesen Netzwerken innehaben.
- **NAC (CSEC) – Network Analysis Centre**
  Analyse- und Überwachungszentrum des CSEC, das ähnliche Operationen durchführt wie das NAC des GCHQ oder das NTOC der NSA.
- **NACSI – NATO Advisory Committee on Special Intelligence**
- **NIOC (= NAVIOCOM) – Navy Information Operations Command (Maryland)**
- **NTOC – NSA Threat Operations Center**
  Abteilung für Cyberabwehr der NSA. Aufgabe: Erkennung, Charakterisierung und Attributierung von Cyberangriffen auf die NSA Netzwerke, Erarbeitung von Abwehrstrategien und Schaffung von Awareness durch Informationsweitergabe und Trainings.
- **SFC (NSA) – SIGINT Forensics Center**
- **TAO – Tailored Access Operations (NSA-S32)**
  Spezialeinheit der NSA, die sich vorwiegend mit der maßgeschneiderten Überwachung einzelner Zielpersonen beschäftigt. TAO wurde 1997 gegründet und vor allem nach den Anschlägen vom 11. September 2001 deutlich ausgebaut. Die Truppe soll deutlich jünger als der Rest der NSA-Einheiten sein und systematisch Hacker rekrutieren. Zu ihren Werkzeugen gehört das Programm QUANTUMTHEORY, das gezielt Rechner manipulieren kann.
- **TCC – Texas Cryptologic Center**
  Das TCC ist auf dem Gelände (Satelliten-Campus) des Medina Annex der Lackland Air Force Base, San Antonio, disloziert und wird von der NSA betrieben. Dieses Gelände war früher unter dem Namen Medina Regional SIGINT Operations Center (RSOC) bekannt, welches das Regional Technical Control and Analysis Element (TCAE) mit einschloss. Das TCC hat circa 4.000 Mitarbeiter. TAO ist ein Teilbereich des TCC.

Glossar

Geheimdienstprojekte

- **5-ALIVE**
  GCHQ-Metadaten-Datenbank mit Datensätzen zum Traffic zwischen Routern und NOCs, um bereits abgefangene Router-Konfigurationsdaten zu ergänzen und alle Router, Server und Computer eines Netzwerks, die von Admins zum Netzwerkmanagement verwendet werden, zu identifizieren. CARBON ROD und HYPERION sind zwei weitere Datenbanken für den gleichen Zweck.

- **AIRWOLF (GCHQ)**
  Datenbank, aus der Metadaten per SQUEAKY DOLPHIN zum Kontext bereits abgefangener Daten abgerufen werden können, um sie für SQUEAKY-DOLPHIN-Analysen „anzureichern".

- **ANGRY BIRD (GCHQ)**
  App zum Angriff von Smartphones.

- **APEX – Active/Passive Exfiltration**
  Aktives oder passives Ausleiten von Daten aus Netzwerken.

- **ATLAS (CSEC)**
  Datenbank mit Geolokalisierungs- und Netzwerk-Metadaten, u. a. zur Zuordnung von IP-Adresse und Netzwerk-ID zwecks Contact-Chaining-Analysen, „Netzwerk-Tracking" für mobile WLAN-Geräte, Lokalisierungs- und Bewegungsüberwachung.

- **BACKGROUND-Programm**
  Department of Homeland Security (DHS) und ICN benötigen Aufklärung zu Drogenhandel, Menschenschmuggel und Grenzsicherheitsthemen.

- **BLACKHOLE (GCHQ)**
  Datenbank, in der per MTI TEMPORA erfasste Geolokalisierungs-, Selektor- und Verkehrs-Metadaten gespeichert werden; Teil des Programms ROUGH DIAMOND.

- **CARNIVORE**
  NSA-Projekt, um bestimmte Schlüsselbegriffe und Stimmprofile überprüfen zu können.

- **Co-Traveler**
  Begriff der UKUSA-Geheimdienste für Analysesysteme zur Identifizierung, Lokalisierung und Bewegungsverfolgung von Personen, die eine Gruppe bilden (könnten), über die Auswertung und den Vergleich der Meta-, Geräte- und Geolokalisierungsdaten (Wegpunktdaten bzw. Bewegungs-routen und -radius) mehrerer Mobilfunkgeräte (u. a. aus FASCIA, GM-PLACE, OCTAVE), bezogen auf bestimmte Zeiträume und geografische Gebiete.

- **FIFTYEXCLAIM**
  NSA-Codename für die Vertragsbeziehung mit dem Unternehmen Computer Sciences Corporation (CSC), das für die SUSLAG/JSA als Vertragspartner tätig war.

- **FIRE ANT (GCHQ)**
  Anwendung zur geografischen Visualisierung von Hauptthemen, die öffentliche Debatten bestimmen – siehe auch SQUEAKY DOLPHIN.

- **Glimmerglass**
  Das wenig bekannte Unternehmen fungiert als Zulieferer für Lauschaktionen an Glasfasern. In einer nicht öffentlichen Präsentation warb Glimmerglass 2011 damit, dass seine Schnittstellen erfolgreich von US-Geheimdiensten eingesetzt werden: „CyberSweep" könne aus IP- und ATM-Datenströmen beispielsweise Gmail-Mails, Facebook-Daten oder Twitter-Tweets in Echtzeit extrahieren und speichern.

- **GLOTAIC**
  BND/CIA-Kooperation (2003–2006) mit Hilfe der deutschen Tochter des US-Providers MCI (ab 2006 Verizon), die den Datenabgriff (Auslandsstrecken mit Telefon und Fax) vom nordrhein-westfälischen Hilden an eine zwischengeschaltete Tarnfima weiterleitete. Von dort wurden die abgegriffenen Strecken zur Weiterverarbeitung verschlüsselt an die BND-Außenstelle Rheinhausen weitergeschaltet. Die zu überwachenden Leitungen wurden anhand von Metadaten ausgewählt und nach bestimmten Anschlüssen durchsucht. Zudem wurden Filter eingesetzt, die Inhalte deutscher und US-amerikanischer Staatsbürger aussortiert haben sollen. Angeblich war die Ausbeute sehr spärlich.

- **ICREACH**
  Suchmaschine der NSA, mit der 23 US-Behörden (darunter FBI und DEA) auf Metadaten in den NSA-Datenbanken zugreifen können.

- **INSPECTOR (GCHQ)**
  Werkzeug des JTRIG, um Domäneninformationen und die Verfügbarkeit von Webseiten zu überwachen.

- **INTELINK**
  Das Intranet INTELINK, an dem NSA, CIA, NRO und andere Mitglieder der Intelligence Community beteiligt sind, expandierte 2001 auf andere englischsprachige Staaten.

- **INTERQUAKE (IQ)**
  SCS-Signaldatenbank zur Analyse von Mikrowellensendern, auf die alle SCS-Erfassungsstellen Zugriff haben (https://interquake-in.f6.f.nsa/iq). Sie enthält alle wichtigen technischen Parameter zu den erfassbaren Emittern: Frequenzen, Modulationsverfahren, Nutzbandbreite, Datenrate, Signalpegel, Antennenparameter, Payloadstandards, Kurzzeitaufzeichnungen, Meldungen, Berichte und die Kenner der eigenen Reception-Sites.

- **INTSUM – Intelligence Summary**

- **JTRIG – Joint Threat Research and Intelligence Group (GCHQ)**
  GCHQ-Einheit für Online-HUMINT, SOCMINT, CNA/CNE und verdeckte Onlinekampagnen zur Diskreditierung identifizierter Meinungsführer, die als Bedrohung eingestuft werden. Durchführung von CNIO zur Desinformation und Beeinflussung der öffentlichen Meinung über manipulative, virale Kampagnen oder das Streuen von Falschinformationen in sozialen Netzwerken, Medien und Presse. Führt auch ähnliche Operationen wie NSA-TAO durch.

Glossar

Geheimdienstprojekte

- **JPEL – Joint Priority Effects List**
  Im Rahmen dieses Projekts setzt die NSA Drohnentechnik ein, um Ortungs- und Abhörtechnik an Ihre Zielobjekte heran zu bringen und so die Funksignale, z. B. Lokationsdaten und Gespräche von Mobiltelefonen, abzufangen.

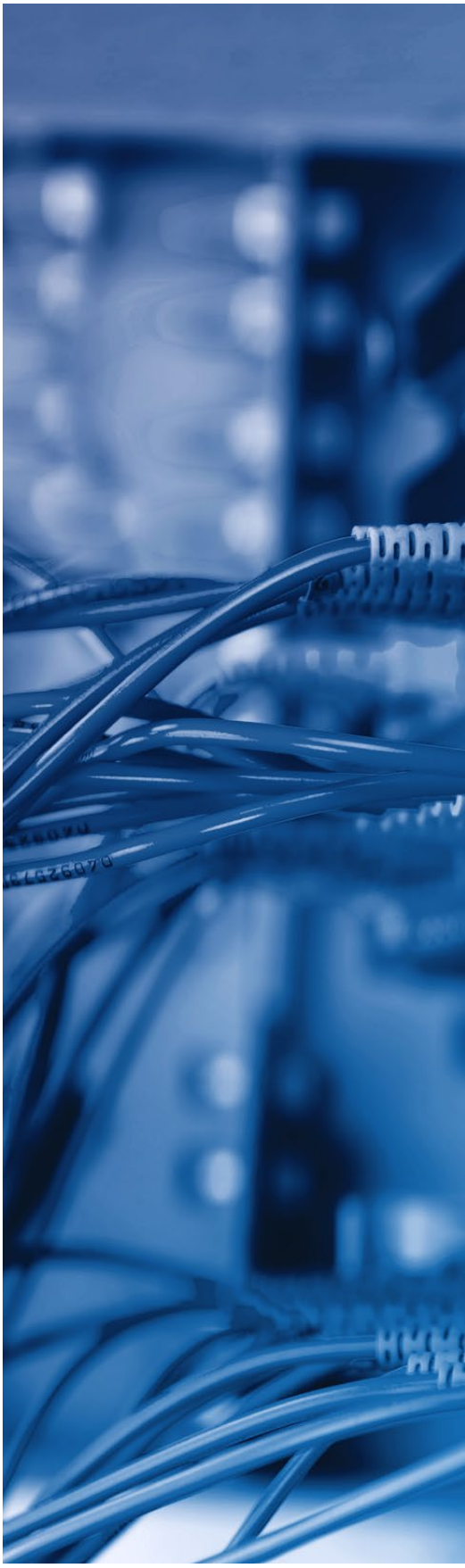
- **LANDMARK**
  Das LANDMARK-Programm wird vom CSEC zur Expansion verdeckter Infrastruktur betrieben. Diese besteht aus sogenannten Operational Relay Boxes (ORBs), die verwendet werden, um den tatsächlichen Aufenthaltsort eines Angreifers zu verschleiern, wenn die Five Eyes Exploits gegen Ziele einsetzen oder Daten stehlen.

- **MAINWAY**
  Überwachungsprogramm, um Telefonverbindungsdaten zu sammeln. Hauptquelle der MAINWAY-Datenbank sind die Daten des Telefonunternehmens Verizon. Mit der Veröffentlichung des entsprechenden Gerichtsbeschlusses, der Verizon zur Zusammenarbeit mit der NSA zwang, startete der Guardian die Enthüllungsserie von Edward Snowden am 6. Juni 2013. Zusammen mit MARINA, NUCLEON und PINWALE ist MAINWAY eine der vier Datenbanken der NSA, wie aus den Dokumenten von Snowden hervorgeht.

- **MORECOWBELL (MCB)**
  Verdecktes HTTP/DNS-Monitoring-System (Operation Support). NSA-NTOC-V43. Setzt auf die Infrastruktur und den Abdeckungsmechanismus von PACKAGEGOODS auf. Überwachung von tausenden Internetwebsites in annähernd Echtzeit (ausländische Regierungswebsites, Webforen etc.). Angemietete und verdeckt arbeitende Bot-Server in Malaysia, Deutschland und Dänemark. Mittels ständiger DNS und HTTP Anfragen werden Änderungen an den Servern mitverfolgt.

- **Narus**
  Ehemaliges israelisches Unternehmen, das auf den Bau von Supercomputern spezialisiert ist, die für Geheimdienste sogar an 100-GBit-Glasfaserleitungen den Datenverkehr mitschneiden und nahezu in Echtzeit filtern können. Das neueste Produkt „Narus nSystem" bietet nach Angaben des Unternehmens eine Komplettlösung, inklusive Data-Warehouse, Big-Data-Reduzierung und Forensikportal. Schon im Jahr 2004 war klar, dass Narus zum Zulieferer des US-amerikanischen Geheimdienstes avancierte – der ehemalige NSA-Direktor William Crowell wurde als Vorstand installiert. Seit 2010 gehört Narus zur Rüstungssparte des Boeing-Konzerns. Ein ehemaliger Techniker des US-Telekommunikationsriesen AT&T hatte nachgewiesen, dass das Unternehmen der NSA gestattete, sämtliche Telefongespräche und IP-Daten direkt an den Backbones auszuleiten. Dazu hatte die NSA nach Angaben des Technikers in einem geheimen Raum im AT&T-Datacenter San Francisco eine Abhörschnittstelle des Typs Narus STA 6400 installiert.

- **OPC-1 – Overseas Processing Centre 1**
  Netzwerk aus den drei GCHQ-MTI-TEMPORA-Überwachungsstationen TIMPANI, CLARINET und GUITAR im Oman, in denen die abgefangenen Daten der angezapften Unterseekabel im Nahen Osten eingehen und weiterverarbeitet werden.



- **PINWALE**
  Codename für eine Datenbank der NSA, die ausländische und inländische E-Mails erfasst. Die Existenz dieses Abhörprogramms ist seit 2009 bekannt, die Datenbank existiert demnach mindestens seit 2005. Im Zusammenhang mit dem PRISM-Programm dient sie auch als Datenbank für Videodokumente. Zusammen mit MARINA, MAINWAY und NUCLEON ist PINWALE eine der vier Datenbanken der NSA, wie aus den Dokumenten von Snowden hervorgeht.

- **QUOVA (CSEC)**
  Datenbank mit Datensätzen über „Anonymizers" (Webproxys) und Geolokalisierungsdaten zu ITK-Zugangsanbietern, die mit der ATLAS-Datenbank verknüpft werden. Lieferant der Daten ist das US-amerikanische Unternehmen Neustar (ehemals Quova).

- **RENOIR**
  Erstellung von Beziehungsgeflechten (US-Eigenentwicklung)

- **SENTRY-Program**
  SENTRYHAWK: Kooperation mit US-amerikanischen und ausländischen Konzernen für Angriffe auf Computernetzwerke (CNE). SENTRYOWL: unbekannte Kooperation mit ausländischen Unternehmen, um Geräte bzw. Produkte für die Überwachung nutzbar zu machen. SENTRYRAVEN: Kooperation mit bestimmten US-Konzernen, um Kryptografiesysteme aus den USA für die Überwachung nutzbar zu machen.

- **STELLARWIND**
  Codename für ein Bündel von Überwachungsprogrammen der NSA, die unter der Regierung von US-Präsident George W. Bush gestartet und später aufgegeben worden sein sollen. Laut Washington Post kann STELLARWIND als Vorläufer für vier Datensammlungen betrachtet werden, die weiterhin bestehen und auch mit dem PRISM-Programm verbunden sind. Dazu gehören MARINA, MAINWAY, NUCLEON und PINWALE.

Glossar

Geheimdienstprojekte

- **TAREX – Target Exploitation Program**
  National Initiative NSA/CSS Core Secrets – Protection Program (ECI): (SECRET// SI// NOFORN vom 06.02.2012). Weltweit agierende TAREX-Einheiten (Hawaii, Texas, Georgia, Südkorea, China) versuchen Zugriff („Eingriff in Lieferketten") auf die Hardware von Herstellern von Netzwerktechnik zu erlangen. Die NSA hat offenbar auch in Deutschland Agenten stationiert, die beispielsweise Postsendungen abfangen und die darin enthaltene Netzwerktechnik manipulieren, bevor sie an ihr eigentliches Ziel weitergeleitet werden.

- **TEMPORA (GCHQ)**
  Mit diesem Überwachungsprogramm wird der globale Internetverkehr angezapft und zwischengespeichert (Internet Buffer Business Capability). Das 2011 in Betrieb genommene Programm speichert einem Bericht des Guardian zufolge die Inhaltsdaten drei Tage (full take) und die sogenannten Metadaten für 30 Tage. Die Daten würden mit dem US-amerikanischen Geheimdienst NSA geteilt. Mehrere Hundert Mitarbeiter des GCHQ und der NSA werten die Daten aus.

- **TRACFIN**
  In der NSA-eigenen Finanzdatenbank werden Informationen zu weltweiten Finanztransaktionen gespeichert. Die dafür zuständige Abteilung (Branch) „Follow the Money" soll bis 2011 dort 180 Millionen Datensätze gesammelt haben; davon sollen 84 Prozent von dem Kreditkartenunternehmen VISA stammen. Weitere Datensätze hat die NSA von der europäischen SWIFT geholt, über die Banken ihren Zahlungsverkehr abwickeln. Ziel der NSA waren Kunden in Europa, dem Mittleren Osten und Asien.

- **TREASUREMAP**
  Eine interaktive Landkarte des globalen Internets in nahezu Echtzeit, die das öffentliche Internet zeigt – überall und wie es sich aktuell darstellt. Hinweis auf eine Version, die am 10. Januar 2011 verteilt wurde. Alle 90 Tage werden neue Eigenschaften ausgeliefert. Täglich werden mehr als 30 GB an zusätzlichen Daten hinzugefügt bzw. ersetzt. Von der Technology Development Division (NSA-V45) im NSA NTOC entwickelte Anwendung zur Erkundung und Analyse der globalen, logischen Struktur des Internets und aller damit verbundenen Geräte, die in interaktive, permanent aktualisierte Karten visualisiert werden. TREASUREMAP ist für alle Five-Eyes- und US-Geheimdienste verfügbar. Internet-, Verkehrs- und Gerätedaten für TREASUREMAP stammen aus Abfragen bei OSINT-Quellen, hinzugekauften Datensätzen kommerzieller Anbieter und Datensätzen universitärer Forschungsprojekte zur Analyse und Kartografierung des globalen Internet-Datenverkehrs. Zusätzlich werden Daten ausgewertet, die in Datenbanken der Five-Eyes-Geheimdienste gespeichert oder mit SIGINT-Analysetools und Abhörsystemen der Five-Eyes-Geheimdienste erhoben und erfasst werden. Die Zuordnung gesammelter Attribute/Fingerprints zu allen netzwerkfähigen Geräten, ihre geografische Verortung sowie die Aufbereitung der Beziehungen und Routingdaten zwischen Netzwerkgeräten dienen der Darstellung bereits angegriffener und überwachter Router, Server, Proxys, WLAN-Access-Points und VPN-Endpunkte, möglicher Überwachungsschnittstellen und -systeme in deren Bereich, zur Erlangung ihrer Daten und zur Planung von CNA/CNE-Operationen gegen Netzwerkgeräte in den Netzen von Netzwerkbetreibern und -anbietern bis hin zu angeschlossenen Geräten ihrer Kunden.

- **TURBINE**
  Ermöglicht ein zentralisiertes und automatisiertes Command and Control in einem großen Netzwerk aktiver TAO-Implantate. Um den entsprechenden Code auf PCs einschleusen zu können, verwendet TURBINE eine Reihe von Täuschungsmanövern, um Nutzer auf manipulierte Webseiten umzuleiten. Dazu bediente sich der US-Geheimdienst gefälschter Facebook-Seiten, Spam-E-Mails mit bösartigen Links, Man-in-the-middle-Angriffen, die das Zielsystem mit unsinnigen Daten bombardieren, sobald TURBINE entdeckt, dass die anvisierte Person gerade eine Webseite aufruft, die vom Geheimdienst ausgenutzt werden kann, um den Rechner zu kapern. Sobald die digitalen Implantate auf dem Zielrechner installiert sind, erhält die Software Zugriff auf Daten, noch bevor diese verschlüsselt werden. Als Beispiel für verschiedene Arten dieser aggressiv eingeschleusten Trojaner werden CAPTIVE-AUDIENCE, GUMFISH, FOGGY-BOTTOM und SALVAGE-RABBIT genannt. Die Programme wurden dazu entwickelt, Gespräche direkt vom Mikrofon eines Computers mitzuschneiden, unbemerkt Bilder über die Webcam zu schießen, die Browserhistorie zu kopieren, Logindaten abzugreifen, Keyboardeingaben aufzuzeichnen und den Inhalt angeschlossener Flash-Laufwerke zu kopieren.

- **TURMOIL**
  Passives Hochgeschwindigkeits-Erfassungssystem gegen weltweite Satellitensysteme, Richtfunk- und Kabel-Kommunikationssysteme (Glasfasernetzwerke). Wird der Datenverkehr eines Zielsystems detektiert, liefert TURMOIL einen Hinweis (Tipping) an das TURBINE-System. Damit geht auch eine 15-jährige Vorratsdatenspeicherung einher, die außer Verbindungsdaten und Standortinformationen auch Kommunikationsinhalte umfasst. Die Vorgehensweise wurde vom zuständigen US-Geheimgericht FISC im Rahmen einer Generalvollmacht abgesegnet.

- **UPSHOT**
  Portscans in ganzen Ländern und Identifizierung anfälliger Server, die für weitere Angriffe übernommen werden können.

- **UPSTREAM**
  Überwachungsprogramm der NSA, um die Kommunikation über transatlantische Glasfaserleitungen abzuhören. Zu UPSTREAM gehört auch die Überwachung einer nicht näher bezeichneten Infrastruktur mit den Komponenten FAIRVIEW, STORMBREW, BLARNEY und OAKSTAR. Die NSA-Agenten sind einem von der Washington Post veröffentlichten Dokument zufolge angehalten, für Suchanfragen sowohl UPSTREAM als auch PRISM zu benutzen.

Quellenverzeichnis

- **Die bisher veröffentlichten Snowden Papiere bis 7. Juni 2016**
  https://cryptome.org/2013/11/snowden-tally.htm
  im Speziellen: https://www.eff.org/files/2014/01/06/20131230-appelbaum-nsa_ant_catalog.pdf
- **Diverse Veröffentlichungen des „Project 2049 Institute" über das „Department 3" der chinesischen Armee bzw. die chinesischen Cyber-Operationen:**
  http://project2049.net/publications.html
- **Mandiant Report APT1 – Exposing One of China's Cyper Espionage Units**
  http://intelreport.mandiant.com/
- **Publikationen des "Studies and Research Center" Agentura.ru**
  http://studies.agentura.ru/centres/csrc/
- **Die Daten und Analysen von Electrospaces.net**
  https://electrospaces.blogspot.cz/
- **Stellenausschreibungen der NSA**
  https://www.intelligencecareers.gov/NSA/index.html
- **Liste der Geheimdienste der Welt**
  https://fas.org/irp/world/index.html
- **Offizielle NSA und DoD Webseiten, unter anderem:**
  https://www.nsa.gov/about/cryptologic-heritage/historical-figures-publications/nsa-60th/assets/files/NSA-60th-Anniversary.pdf

  http://www.defense.gov/News

  https://www.nsa.gov/business/

  https://www.iad.gov/iad/library/ia-guidance/secure-architecture/trusted-engineering-solutions.cfm
- **Diverse Artikel aus der deutschen und englischen Wikipedia**
  https://www.wikipedia.org/
- **Diverse Artikel und Bücher von Matthew M. Aid**
  http://www.matthewaid.com/
- **Buch „Bits und Bomben: Cyberwar: Konzepte, Strategien und reale digitale Kontroversen"**
  30. August 2012, von Manfred Kloiber, Jan Rähm und Peter Welchering
- **300 Millionen Programm des BND auf netzpolitik.org**
  https://netzpolitik.org/2015/strategische-initiative-technik-wir-enthuellen-wie-der-bnd-fuer-300-millionen-euro-seine-technik-aufruesten-will/
- **Report on the Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation:**
  http://nsarchive.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-030.pdf
- **Veröffentlichungen des deutschen Verteidigungsministeriums:**
  http://www.bmvg.de/resource/resource/MzEzNTM4MmUzMzMyMmUzMTM1MzMyZTM2MzIzMDMwMzAzMDMwMzAzMDY5NmU2ODY1NzE3NTYxNmMyMDIwMjAyMDIw/Folien%20CIR%20Online.pdf
- **Artikel „NSA Plans Controversial Restructure" von Robert Hackett in der "Fortune"**
  http://fortune.com/2016/02/03/nsa-reorg-combine-offense-defense/
- **Reagan National Defense Forum: Building Peace Through Strength for American Security - Panel Session 6: „Cyberwar: The Role of Cyber in the 21st Century Warfare"**
  https://www.nsa.gov/news-features/speeches-testimonies/speeches/reagan.shtml
- **China's Cyber Warfare Capabilities von Desmond Ball:**
  http://indianstrategicknowledgeonline.com/web/china%20cyber.pdf
- **Diverse Artikel von Reuters, Zeit, etc. – zum Beispiel:**
  http://www.reuters.com/article/us-usa-cyber-nsa-idUSKCN0VH21H

  http://www.reuters.com/article/us-usa-security-snowden-dell-idUSBRE97E17P20130815

  http://pdf.zeit.de/digital/datenschutz/2016-02/ueberwachung-nsa-umbau-geheimdienst.pdf

  http://www.theguardian.com/world/2013/jun/23/edward-snowden-nsa-files-timeline

  http://www.nbcnews.com/news/other/how-snowden-did-it-f8C11003160

  https://www.venafi.com/blog/post/deciphering-how-edward-snowden-breached-the-nsa/

  http://www.reuters.com/article/us-usa-security-nsa-leaks-idUSBRE97801020130809
- **Artikel über die Biografie Snowdens:**
  http://www.britannica.com/biography/Edward-Snowden

  http://www.biography.com/people/edward-snowden-21262897#synopsis

https://www.wired.com/2014/08/edward-snowden/

https://www.theguardian.com/world/2014/feb/01/edward-snowden-intelligence-leak-nsa-contractor-extract

http://www.zeit.de/politik/ausland/2013-06/prism-usa-snowden-anklage

http://msnbcmedia.msn.com/i/MSNBC/Sections/NEWS/A_U.S.%20news/US-news-PDFs/Snowden-Complaint.pdf

- **Artikel über den Vorwurf der (Wirtschafts-)Spionage:**
  http://www.sueddeutsche.de/politik/edward-snowden-im-ard-interview-snowden-beschuldigt-usa-deutsche-firmen-auszuspionieren-1.1872619

  https://www.theguardian.com/uk-news/2013/dec/20/gchq-targeted-aid-agencies-german-government-eu-commissioner

  http://www.spiegel.de/politik/ausland/gchq-briten-ueberwachten-ministerien-telefonnetz-in-berlin-a-940364.html

  http://www.welt.de/politik/deutschland/article140364838/Worin-die-wahre-Sprengkraft-der-BND-Affaere-liegt.html

  http://www.welt.de/politik/ausland/article124281154/USA-betreiben-ohne-Zweifel-Wirtschaftsspionage.html

  http://epoca.globo.com/tempo/noticia/2013/08/carta-em-que-o-atual-bembaixadorb-americano-no-brasil-bagradece-o-apoio-da-nsab.html

  https://www.theguardian.com/world/2013/sep/09/nsa-spying-brazil-oil-petrobras

  http://www.nytimes.com/2014/05/21/business/us-snooping-on-companies-cited-by-china.html

- **Informationen über das Budget der Geheimdienste und des BSI**

  https://www.washingtonpost.com/world/national-security/black-budget-summary-details-us-spy-networks-successes-failures-and-objectives/2013/08/29/7e57bb78-10ab-11e3-8cdd-bcdc09410972_story.html

  https://www.verfassungsschutz.de/embed/vsbericht-2013.pdf

  https://www.verfassungsschutz.de/embed/vsbericht-2014.pdf

  https://www.bundeshaushalt-info.de

- **Artikel zum Thema XKeyscore**
  https://en.wikipedia.org/wiki/XKeyscore

  https://daserste.ndr.de/panorama/aktuell/NSA-targets-the-privacy-conscious,nsa230.html

  https://www.law.upenn.edu/live/files/1718-ambinder10-things

  http://blog.erratasec.com/2014/07/reading-xkeyscore-rules-source.html

- **Artikel über die Internetinfrastruktur**
  https://en.wikipedia.org/wiki/List_of_Internet_exchange_points_by_size

  http://www.submarinecablemap.com/#/

- **Ergebnisse der transatlantischen Ad-hoc-Arbeitsgruppe zum Datenschutz/NSA-Spionage**
  https://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/jha/139745.pdf

  http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2016987%202013%20INIT

- **Informationen über das GCHQ**
  https://www.gchq.gov.uk/features/gchq-oversight
  https://www.tagesschau.de/ausland/gchq-hintergrund100.html

- **Informationen zur Re-Industrialisierung**
  https://www.deutsche-bank.de/fk/de/docs/Re-Industrialisierung_Europas__Anspruch_und_Wirklichkeit.pdf

  https://www.welt.de/wirtschaft/article124555561/Duestere-Aussichten-fuer-Re-Industrialisierung-der-EU.html

Bildnachweis

William Binney (S. 12)
Rama, Wikimedia Commons, Cc-by-sa-2.0-fr
https://commons.wikimedia.org/wiki/File:William_Binney-IMG_9040.jpg
https://creativecommons.org/licenses/by-sa/2.0/legalcode/

Russ Tice (S. 12)
Work for hire
https://commons.wikimedia.org/wiki/File:Russ_Tice_2009.jpg
https://creativecommons.org/licenses/by-sa/3.0/legalcode

Mark Klein (S.12)
EFF
https://commons.wikimedia.org/wiki/File:Mark_Klein_AT&T.jpg
https://creativecommons.org/licenses/by/2.0/legalcode

Edward Snowden (S. 13, 14)
Laura Poitras / Praxis Films
https://commons.wikimedia.org/wiki/File:Edward_Snowden-2.jpg
https://creativecommons.org/licenses/by/3.0/legalcode

Donald Trump (S. 19, 51)
© Gage Skidmore - CC BY-SA 3.0

© Carsten Reisinger – shutterstock.com (S. 20)

© Stefan90 – istockphoto.com (S. 33)

© Nagy-Bagoly Arpad – shutterstock.com (S. 40)

© fotogestoeber – shutterstock.com (S. 48)

© hywards – shutterstock.com (S. 58)

© ra2 studio – fotolia.com (S. 81)

© Monkey Business Images – shutterstock.com (S. 81)

© jijomathaidesigners – shutterstock.com (S. 82)

© Eric Gaba, Wikimedia Commons user Sting (S. 82)

© GraphicCompressor – fotolia.com (S. 82)

© BrianAJackson – istockphoto.com (S. 84)

GCHQ aerial view
licensed under the Open Government Licence v1.0. (S. 87)

© Henrik5000 – istockphoto.com (S. 92/93)

© Rob Hyrons – shutterstock.com (S. 94/95)

© asharkyu – shutterstock.com (S. 96/97)

© cookiecutter – fotolia.com (S. 98/99)

Wir können den Wind nicht ändern, aber wir können die Segel richtig setzen.

Aristoteles

Schlussfolgerung

Alfred Czech, BSc
Geschäftsführer Österreich
Corporate Trust

Unternehmen müssen sich klar darüber sein, dass die Reaktion auf Spionageangriffe vorwiegend in den eigenen Wirkungsbereich und die eigene Verantwortung fällt.

Aufgrund der weltpolitischen Neuausrichtung nach dem Wegfall der klassischen Ost/West-Blöcke, der durch die Sowjetunion massiv repräsentierten kommunistischen Ideologie gegen Ende der 1980er und der sich exponentiell entwickelnden Globalisierung seit den 1990er Jahren, wurde der wirtschaftliche Erfolg von Staaten, Gesellschaften, Konzernen und Unternehmen wesentlich mehr nach kapitalistischen Erfolgskriterien bewertet, als zu Zeiten des ideologischen Kräftevergleichs.

Daher waren neu entstandene Staaten und Systeme gezwungen, ihre Wirtschaft in Schwung und auf dem Weltmarkt in Stellung zu bringen. Weltbank, Börsen und Ratingagenturen bestimmen über Prosperität oder wirtschaftlichen Untergang ganzer Staaten. Unter diesem Druck sind politische Systeme gezwungen, auf Basis der wirtschaftlichen Entwicklung den Wohlstand der jeweiligen Bevölkerung voranzutreiben.

Wissens- und Know-how-Transfer bedeutet letztendlich Wohlstandstransfer. Und in diesem Zusammenhang ist das Engagement von Geheimdiensten zu sehen, die im staatlichen Auftrag durch Wirtschaftsspionage an der Verwirklichung des jeweiligen nationalen wirtschaftspolitischen Ziels mitwirken.

Vor knapp zwei Jahren wurde unter Beteiligung von zwei Ministern und einem Staatssekretär die österreichische Resilienz-Strategie vorgestellt. Im Wesentlichen wurde dabei vermittelt, dass sich die politisch Verantwortlichen bewusst sind, dass die österreichische Wirtschaft das Rückgrat für einen sozialen Wohlfahrtsstaat darstellt und alle Verantwortlichen aufgefordert sind, auf dieses besondere Asset Acht zu geben.

Seither ist in Österreich auf diesem Gebiet aber nicht viel geschehen. Es zeigt sich zwar, dass das Risiko der Wirtschafts- und Industriespionage in der öffentlichen Wahrnehmung angekommen ist, die Achtsamkeit der Entscheidungsträger hinkt jedoch weit hinterher. Die Bereitschaft, die „Kronjuwelen" und den nachhaltigen Bestand von Unternehmen zu sichern, ist noch nicht so stark ausgeprägt, wie es aufgrund der aktuellen Gefährdungslage sein sollte.

Der vorliegende Report soll dazu beitragen, politischen und wirtschaftlichen Entscheidungsträgern die Möglichkeiten von modernen Geheimdiensten vor Augen zu halten und unter Berücksichtigung dieser Möglichkeiten an die Sicherung eigener Entwicklungs- und Wirtschaftsinformationen zu denken. Das heißt aber, sich mit der Vielschichtigkeit der Thematik auseinanderzusetzen. Denn neben

der Gefahr, von Geheimdiensten (oder der Konkurrenz) ausgespäht zu werden, muss auch mit intensiveren und vermehrten Angriffen seitens der internationalen organisierten Kriminalität gerechnet werden, die sich ähnlicher Methoden wie Geheimdienste – mit leichter zeitlicher Verzögerung – bedient.

Ein Kardinalfehler vieler Organisationen, der aktuell zu beobachten ist, ist das Herangehen an das geschilderte Problem durch alleinige Fokussierung auf die Informationstechnologie. Medien berichten über „Cyberattacken" auf Unternehmen, die sich letztendlich als klassische Betrugshandlungen unter Verwendung von zeitgemäßer Technik entpuppen. Auf solche Angriffe ausschließlich mit IT-Maßnahmen zu reagieren, wäre vollkommen falsch. Bessere gesamtorganisatiorische Maßnahmen sind in solchen Fällen angebracht.

Es kommt darauf an, den Gesamtzusammenhang zu erkennen, um Unternehmen nachhaltig zu schützen und den wirtschaftlichen Erfolg zu sichern. Ganzheitliche Betrachtungsweisen unter Zuhilfenahme von professionellen Analysen, auch Intelligence genannt, im besten Fall im Rahmen eines (Security-) Risk Managements, sind vielen Unternehmen noch immer fremd. Risikomanagementsysteme werden hierzulande vor allem im Finanzsektor, aufgrund internationaler Vorgaben, angewendet. Gesamtheitliche organisationsweite Maßnahmen zur Spionageabwehr sind weitgehend nicht vorhanden.

In der Bundesrepublik Deutschland wurden Unternehmen durch das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich – kurz KonTraG – gesetzlich dazu verpflichtet, Risikomanagementsysteme zur Härtung der eigenen Unternehmensstrukturen einzuführen. Bei Unterlassung tragen die verantwortlichen Entscheidungsträger die Haftungsrisiken selbst. Auch in Österreich lassen sich diese Verpflichtungen aus den einschlägigen unternehmensrechtlichen Normen ableiten, darauf wird aber nur sehr halbherzig eingegangen. Vor allem im mittelständischen Bereich ist dieser Mangel an Bereitschaft, die rasanten Entwicklungen der Angriffsmöglichkeiten und die Tatsache, dass es permanent zu Spionageangriffen kommt, zur Kenntnis zu nehmen, vehement zu bemerken. International agierende Konzerne haben dagegen bereits entsprechend aufgerüstet. Da aber der Großteil der österreichischen Wirtschaftsbetriebe Mittelständler sind, ist es höchst an der Zeit, im Sinne der österreichischen Resilienz-Strategie an die Umsetzung von Schutzmaßnahmen gegen Spionage zu denken.

Damit meine ich aber, wie bereits erwähnt, nicht die alleinige Konzentration auf die Härtung von IT- Systemen, sondern den systematischen Zugang unter Berücksichtigung der Sicherheitspolitik eines Unternehmens, der Unternehmenskultur, der Schulung, des Trainings – vor allem im Hinblick auf den Incident Response einschließlich der Vorbereitung darauf – und die unternehmensweite Entwicklung von Achtsamkeit (Awareness), um Angriffe überhaupt erkennen zu können.

Österreichische Unternehmen müssen sich klar sein, dass die Reaktion auf Spionageangriffe vorwiegend in den eigenen Wirkungsbereich und die eigene Verantwortung fällt. Diese Erkenntnis wiegt für Entscheidungsträger besonders schwer, wenn es um Haftungsfragen nach schädigenden Attacken geht. Wurde die Implementierung von Sicherheitsmaßnahmen nach dem Stand der Technik unterlassen, und hier hat sich bei der Entwicklung von internationalen und österreichischen Normen doch einiges getan, sind schwerwiegende Konsequenzen zu befürchten. Staatliche Einrichtungen, wie das Bundesamt für Verfassungsschutz und Terrorismusbekämpfung (BVT) oder spezialisierte militärische Einrichtungen, können aufgrund der herrschenden Rechtslage und der auf dieser basierenden Zuständigkeiten im besten Fall unterstützend eingreifen. Die Sicherung der „Kronjuwelen" erfolgreicher Unternehmen fällt – und man kann es nicht oft genug betonen - in die Eigenverantwortung der Unternehmen selbst.

Der vorliegende Report zeigt die Möglichkeiten moderner Geheimdienste auf, die aufgrund der exponentiellen technischen Entwicklungen beeindruckend sind. Doch wesentliche Elemente dieser Entwicklungen stehen allen zur Verfügung und können bei gezielter Anwendung auch effizient zur Spionageabwehr eingesetzt werden. Voraussetzung für den effizienten Einsatz von Spionageabwehr ist aber eine fundierte und funktionierende Sicherheitsorganisation als Basis.

Spionageabwehr ist Managementaufgabe. Die Implementierung von entsprechenden Managementsystemen ist höchst an der Zeit. Agieren österreichische Unternehmen im Sinne der gesamtstaatlichen Resilienz und werden durch effiziente Kooperationen mit spezialisierten Unternehmen und staatlichen Organisationen unterstützt, erhöht sich die Wirkung der Abwehr von Wirtschafts- und Industriespionage schlagartig und stärkt die österreichische Wirtschaft auf lange Sicht.

Ihr

Alfred Czech

Schlussfolgerung

Florian Oelmaier
Prokurist, Leiter Cyber-Sicherheit & Computerkriminalität

Wir müssen unsere Behörden mit IT-Know-how ausstatten, damit diese Ihre Aufgaben auch im 21. Jahrhundert erfüllen können. Gleichzeitig müssen wir uns für ganz neue Bedrohungen aus dem Cyberraum wappnen. Hier ist es die Aufgabe der Sicherheitskräfte, dafür zu sorgen, dass die Kontrolle über alle IT-Systeme der Welt (auch die eigenen) klar und transparent geregelt ist und von Dritten nicht ausgehebelt werden kann.

Ich bin Informatiker, unterstütze den Chaos Computer Club, die Electronic Frontier Foundation und Digitalcourage e.V. Um es kurz zu machen, ich habe Angst vor Datensammlungen und deren Mißbrauchspotential. Ich würde mir eine Welt ohne Geheimdienste und ohne Überwachungsinstrumente wünschen. Das müssten dann natürlich aber alle Staaten der Welt so halten, weil sich Grenzen im Cyberraum nunmal schlecht ziehen lassen. Und natürlich dürfte es auch keine Kriminellen geben, die neue technische Mittel ausnutzen, um ihre schlechten Absichten noch raffinierter, noch bösartiger und noch schädlicher umzusetzen.

Ich habe mich also damit abgefunden, dass es die Welt, die ich mir eigentlich wünschen würde, nicht geben wird. Im Gegenteil, die Welt wird immer unübersichtlicher. Neue politische Entwicklungen vom Brexit, über die Türkei bis hin zu einer zunehmenden Radikalisierung der westlichen Gesellschaften sind nicht gerade die Vorboten einer friedlichen Welt. Dazu kommen die künftigen technischen Entwicklungen vom Internet of Things bis zum selbstfahrenden Auto. Auch diese Entwicklungen werden das Thema Cyber-Sicherheit nicht gerade vereinfachen.

Ich bin fest davon überzeugt, dass wir in Deutschland unsere Cyber-Sicherheitsfähigkeiten ausbauen müssen. Es wird dabei auch nicht ausreichen, dies allein dem privaten Sektor zu überlassen. Gleichzeitig wird der Fachkräftemangel in der IT – und im Speziellen in der Cyber-Sicherheit – nicht abnehmen. Es gilt also die vorhandenen Ressourcen möglichst sinnvoll einzusetzen.

Im Groben haben wir zwei Aufgaben. Einerseits erfordert die klassische Arbeit der Sicherheitsbehörden zunehmend IT-Kompetenz für die Erfüllung des eigenen Auftrags. Andererseits kommen aus dem Cyberraum ganz neue Bedrohungen, die mit den klassischen Sicherheitsthemen nichts mehr zu tun haben. Hätten wir keinen Fachkräftemangel, wäre die erstgenannte Aufgabe vergleichsweise einfach. Jede Behörde identifiziert das notwendige Know-how und stellt die entsprechenden Kollegen ein bzw. bildet sie aus. So aber müssen wir nun nach Möglichkeiten suchen, wie die vorhandenen Ressourcen möglichst effizient genutzt werden können. Das BSI und die neue Behörde ZITIS sind hier der richtige Weg. Hier gilt es nun im Wesentlichen, Kurs zu halten und aufzupassen, dass dieses wichtige Thema nicht im föderalistischen Klein-Klein untergeht. Gleichzeitig muss auf europäischer Ebene die Zusammenarbeit organisiert und vorangetrieben werden.

Die Wahl der Mittel wird dabei heiß umstritten bleiben. Wie viel Vorratsdatenspeicherung und Massenüberwachung brauchen wir? Wie viel Geheimdienst brauchen wir? Wie viel Freiheit und Anonymität müssen wir auf dem Altar der Sicherheit opfern? Das sind schwierige Fragen, die sich nicht schnell lösen lassen werden. Ich bin aber überzeugt, dass wir als Gesellschaft die richtigen Antworten finden werden, solange wir uns an drei Regeln halten:

1. Wir benötigen ausreichend Cyber-Sicherheits-Fachkompetenz in allen Behörden und auf allen Ebenen (inklusive der Entscheidungsebenen). Nur mit ausreichender Kompetenz können sinnvolle Kompromisse entstehen.

2. Wir bemühen uns um volle Transparenz. Vorgehen und Fähigkeiten aller Cyber-Sicherheitsmaßnahmen wird der Bevölkerung verständlich gemacht.

3. Alle Seiten bemühen sich um einen gesamtgesellschaftlichen Diskurs zu diesen Themen. Verständliche Sprache ist ein Muss. Wir verzichten auf Polemik und Pseudoargumente, die in der Sicherheitsdiskussion leider auf allen Seiten gang und gäbe sind.

Mir ist klar, dass vor allem der zweite Punkt auf viel Ressentiments stößt. Lassen Sie mich kurz erklären, warum dies unabdingbar ist. Durch die rasante Entwicklung in der IT verlieren wir die Gesellschaft ohnehin in zunehmendem Maße. Menschen fühlen sich durch die neuen Technologien überfordert. Ich frage auf meinen Vorträgen regelmäßig: „Halten Sie die IT im aktuellen Zustand für beherrschbar?" Egal ob ich vor Managern, IT-Verantwortlichen oder Technikern spreche, so richtig guten Gewissens meldet sich auf diese Frage selten jemand mit „Ja".

Klar ist sicherlich, keiner hält die IT für unbeherrschbar – es ist halt so ein Zustand mittendrin. In Wirklichkeit ist uns das auch egal, das Leben geht weiter – auch wenn der Computer oder das Smartphone ausfallen. Noch! Unsere Abhängigkeit von der IT wird ständig größer. Wir müssen daher dringend die IT so umbauen, dass die Menschen sagen: „Ja, die IT in Deutschland ist beherrschbar". Und da spielt die emotionale Komponente des Themas Cyber-Sicherheit eine große Rolle. Ich will nicht, dass ein Bundestag in 20 Jahren entscheidet: „Aus der Hoch-Risikotechnologie IT steigen wir aus.". Volle Transparenz, auch wenn sie schwierig ist, ist damit absolut notwendig.

Es wird weiterhin Themen geben, bei denen die Transparenz eingeschränkt werden muss, weil bestimmte Informationen beim Gegner die eigenen Fähigkeiten schwächen würden. Realistisch gesehen ist dies aber nur bei einem Bruchteil der Themen der Fall und auch diese Fähigkeiten können dann auf einer höheren Abstraktionsebene durchaus transparent gemacht werden. Die Frage, was geheim bleiben muss, muss möglichst sparsam beantwortet werden. Für solche geheimen Themen brauchen wir eine hochkompetente und mächtige Kontrollinstanz. Auch die Frage, ob die Kontrolle durch die Regierung und das Parlament hier bereits optimal organisiert ist, muss in Zukunft diskutiert werden.

Der Philosoph und Autor Karl Popper (u. a. „Die offene Gesellschaft und Ihre Feinde") hat sich gefragt, wie wir unsere politischen Einrichtungen so aufbauen können, dass auch unfähige und unredliche Machthaber keinen großen Schaden anrichten können. Wir legen in diesen Tagen die Grundlagen für die neue Cyber-Sicherheitsarchitektur in Deutschland, Europa und der westlichen Welt. Dabei müssen wir diese Fragestellung auch auf die IT-Infrastrukturen ausdehnen. Unser Ziel muss sein: IT dient den Menschen, nicht umgekehrt.

Wir müssen also vermeiden, dass die Menschen den neuen Cyber-Sicherheitsapparat als unbeherrschbar wahrnehmen. Aufgabe der Sicherheitskräfte ist es im Gegenteil, dass die Kontrolle über alle IT-Systeme der Welt (auch die eigenen) klar und transparent geregelt ist und von Dritten nicht ausgehebelt werden kann. Dies setzt hohe Standards im Bereich IT-Sicherheit und Datenschutz voraus.

Ihr

Florian Oelmaier

Schlussfolgerung

Friedrich Wimmer
Leiter IT-Forensik &
Cyber Security Research
Corporate Trust

Geheimdienste müssen sich rechnen, offenbar auch wirtschaftlich. Hier macht der US-Geheimdienst NSA keine Ausnahme. Dabei stehen wir mit der Vernetzung der meisten Prozesse des täglichen Lebens mittels Informationstechnologie vor einer disruptiven Entwicklung.

Geheimdienste müssen sich rechnen, zumindest aus Sicht der Entscheider. Dies kann militärische, wirtschaftliche oder (sicherheits-) politische Vorteile bedeuten.

Es ist US-Stragegie, ihre Geheimdienste auch zu nutzen, um wirtschaftliche Vorteile durch die Sammlung und Auswertung von „wirtschaftlichen Einsichten" zu erreichen. Gleichzeitig ist das direkte Weitergeben von Betriebsgeheimnissen zur reinen Stärkung der heimischen Wirtschaft untersagt.

Aufgabe der politisch Verantwortlichen ist es, ein Gleichgewicht aus europäischer Sicht zu erreichen, da sonst diese Art der wirtschaftlichen Vorteilsbeschaffung höhere Schäden verursacht, als das Stehlen von technologischem Know-how. Die Aufgabe der Sicherheitsabteilungen in den Unternehmen muss es sein, neben dem Schutz des technologischen Know-hows verstärkt darauf zu achten, sensible wirtschaftliche Prozesse und Zusammenhänge abzuschirmen.

Ähnlich verhält es sich mit auffallend hohen Strafzahlungen europäischer Unternehmen an die USA in den letzten Jahren. Allein im Bankenbereich summieren sich die Zahlungen auf hohe zweistellige Milliardenbeträge. Aber auch Unternehmen, u. a. aus dem Automobil-, Luftfahrt- und Energiesektor, blieben nicht verschont.

Wie von US-Seite generell bestätigt wurde, gibt die NSA gewonnene Daten unter Einhaltung von Vorschriften auch an andere Behörden außerhalb des Geheimdienstkreises weiter, wenn Anhaltspunkte für strafbares Verhalten gefunden werden. Ein Zusammenhang bei einigen Strafzahlungsfällen der letzten Zeit ist naheliegend und die Betrachtung der Snowden-Veröffentlichungen mit Fokus Wirtschaft stärkt diese These.

Dass Unternehmen eingehend auf korrektes Verhalten kontrolliert werden, ist eigentlich positiv. Allerdings stört es mich, dass fast alle Forderungen von europäischer Seite, ähnliche Befugnisse (z. B. Zugriff auf US-Bankdaten) zu erhalten, von US-Seite lässig abgeblockt wurden. Ein weiterer Grund, hier ein Gleichgewicht zum Wohle Aller zu fordern.

Betrachtet man die generelle Entwicklung der Geheimdienste, sollte überdies im Hinterkopf behalten werden, dass wir erst am Anfang einer Revolution stehen, die unser Leben und Arbeiten massiv verändert, nämlich die Vernetzung der meisten Prozesse des täglichen Lebens mittels Informationstechnologie.

Man denke nur an die Einführung des ersten iPhones im Jahr 2007 und wie sich das Kommunikationsverhalten der meisten Menschen seither verändert hat. WhatsApp ist für manche Oma wichtiger, als das gute alte Telefon. Intelligente Stromnetze, Industrie 4.0 oder selbstfahrende Autos/LKWs, um nur wenige Trends zu nennen, werden die Abhängigkeit großer Teile der Bevölkerung von Informationstechnologien massiv verstärken. Diese Vernetzung ist gut und muss auch gefördert werden, da bei richtiger Umsetzung das Wohl jedes einzelnen Menschen verbessert werden kann.

Allerdings sind die Fähigkeiten der Geheimdienste und anderer Gruppen, mittels IT das tägliche Leben von Millionen von Menschen zu überwachen bzw. die Informationstechnologie massiv zu stören, besorgniserregend.

Warum? Einerseits lehrt uns die Geschichte, dass bisher noch nie auf Dauer etwas Gutes entstand, wenn Anstrengungen unternommen wurden, große Teile der Bevölkerung anlasslos zu überwachen. Andererseits wird eine gewollte großflächige Störung von wichtigen Prozessen, die mittels Informationstechnologie vernetzt sind, schon in wenigen Jahren die Gefahr bergen, dass nach einer kurzen Störungszeit schon viele Verletzte oder gar Tote zu beklagen sind.

Unternehmen müssen ihre Bestrebungen stark intensivieren, schon in der Konzeptionsphase verschiedene Sicherheits-Aspekte zu berücksichtigen. Das beginnt mit dem Bereich Safety, führt über Security for Safety („Hacker-Resistenz") bis zu Prozessen, um Sicherheitsprobleme schnell erkennen und beseitigen zu können.

Generell muss die Menschheit den richtigen Umgang mit Informationstechnologien noch erlernen. Klingt übertrieben, aber hier stehen wir tatsächlich erst am Anfang. Es müssen überstaatliche Rahmenwerke definiert und festgelegt werden, was erlaubt bzw. nicht erlaubt sein soll. Aber das war schon immer so - siehe Atomkraft.

Ihr

Friedrich Wimmer

Ansprechpartner

Florian Oelmaier

Prokurist, Leiter Cyber-Sicherheit &
Computerkriminalität

Corporate Trust Business Risk
& Crisis Management GmbH

www.corporate-trust.de
oelmaier@corporate-trust.de

Friedrich Wimmer

Leiter IT-Forensik &
Cyber Security Research

Corporate Trust Business Risk
& Crisis Management GmbH

www.corporate-trust.de
wimmer@corporate-trust.de

Dieser NSA Report wurde durch die Corporate Trust Business Risk & Crisis Management GmbH, in Partnerschaft mit der Dr. Hörtkorn München GmbH, erstellt. Selbstverständlich stehen Ihnen alle Ansprechpartner jederzeit für Fragen zur Verfügung. Wir würden uns über Anregungen oder eine Nachricht bezüglich Ihrer Erfahrungen mit Industriespionage freuen.

Michael Dutz

Prokurist,
Leiter IT- und Cyberversicherungen

Dr. Hörtkorn München GmbH
Lochhamer Schlag 5
82166 Gräfelfing

michael.dutz@hoertkorn-muenchen.de
www.hoertkorn-muenchen.de

CORPORATE TRUST
Business Risk & Crisis Management GmbH

Graf-zu-Castell-Straße 1
D-81829 München

Tel.: +49 89 599 88 75 80
Fax: +49 89 599 88 75 820

infocorporate-trust.de
www.corporate-trust.de

Regelmäßig aktuelle Informationen
von Sicherheitsexperten

Follow us: twitter
www.twitter.com/corporatetrust