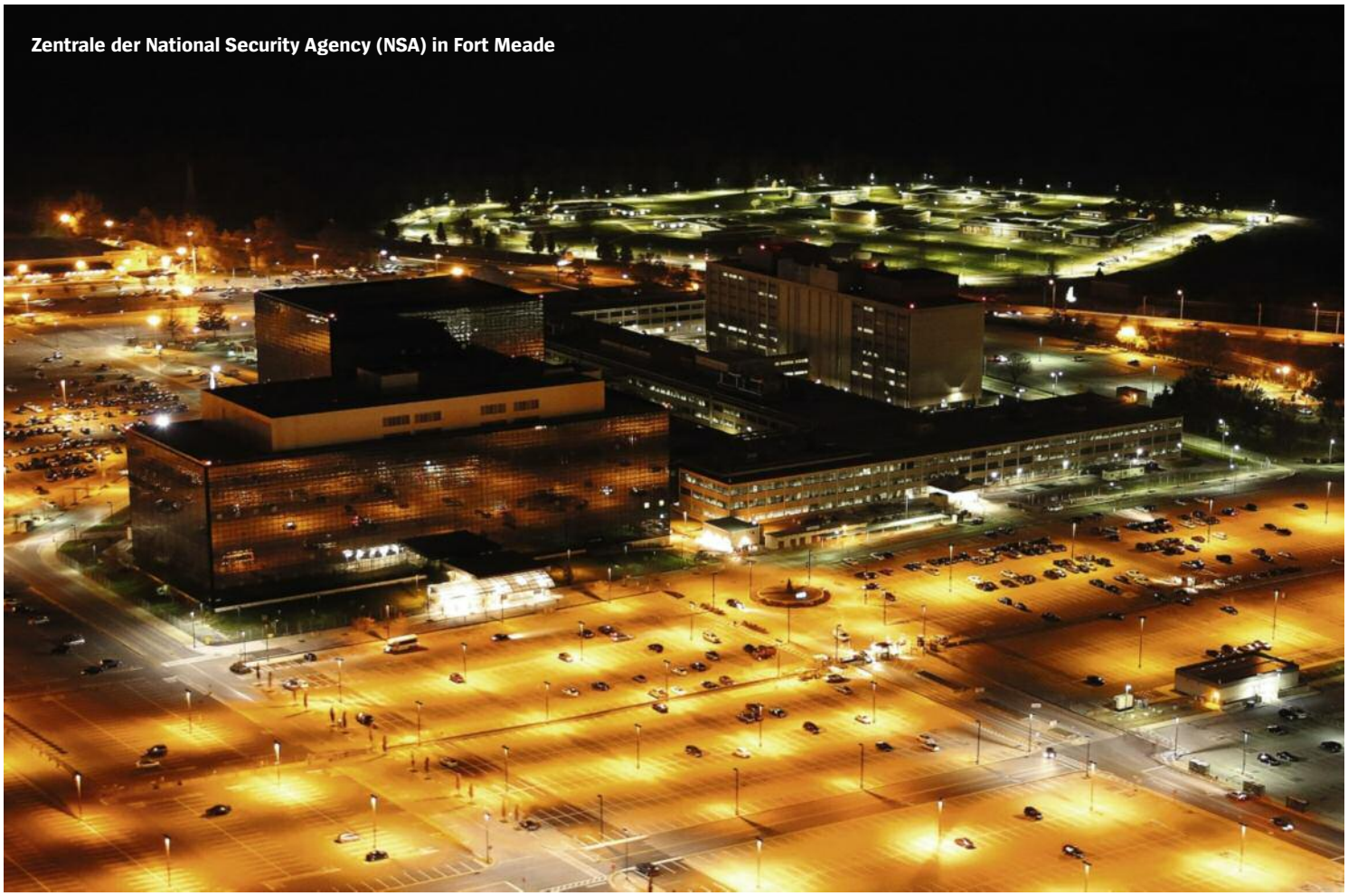


Zentrale der National Security Agency (NSA) in Fort Meade

NSA-Direktor und Chef des US-Cyberkommandos Rogers (M.)

Kontrollierte Eskalation

Überwachung Die Geheimdienste betreiben nicht mehr nur Spionage. Dokumente von Edward Snowden zeigen: Sie wollen die Herrschaft im Internet und bereiten einen digitalen Krieg vor.

Normalerweise müssen Praktikanten imposante Lebensläufe vorlegen, ehrenamtliche Arbeit in Sozialprojekten macht sich immer gut. Bei „Politerain“ verlangt die Ausschreibung andere Neigungen: „Praktikanten gesucht, die Dinge kaputt machen wollen“, heißt es da.

Aber Politerain ist auch nicht das Projekt einer konventionellen Firma, sondern des US-Geheimdienstes National Security Agency (NSA). Oder genauer: das Projekt der NSA-Scharfschützen, der Truppe für maßgeschneiderte Computereinbrüche mit Namen TAO (Tailored Access Operations).

Zum Ausforschen fremder Rechner, so wurden Bewerber weiter aufgeklärt, komme die „Manipulation und Zerstörung gegnerischer Computer“. Mit dem Programm „Passionatepolka“ beispielsweise soll man „Netzwerkkarten schrotten“. Programme wie „Berserkr“ und „Barnfire“ („Scheunenbrand“) sollen Computer mit einer Hintertür versehen oder zentrale Daten löschen. Und TAO-Praktikanten sollten auch fremde Festplatten unbrauchbar machen. Ziel der Ausbildung sei es, „zu lernen, wie ein Angreifer denkt“.

Die Job-Ausschreibung ist schon acht Jahre alt, inzwischen ist die Denkweise eines Angreifers für die Datenjäger der NSA zu einer Art Doktrin geworden. Der Geheimdienst hat es nicht nur auf die totale Überwachung der Kommunikation im Internet abgesehen. Die Digitalspione der sogenannten Fünf-Augen-Allianz aus USA, Großbritannien, Kanada, Australien und Neuseeland wollen mehr.

Sie planen Schlachten im Internet, um Computernetzwerke lahmlegen zu können – und damit potenziell alles, was die steuern: Strom- und Wasserversorgung, Fabriken, Flughäfen oder Zahlungsverkehr. So zeigen es streng geheime Dokumente aus dem Archiv des NSA-Whistleblowers Edward Snowden, die der SPIEGEL exklusiv einsehen konnte und die SPIEGEL ONLINE teilweise veröffentlicht.

Im 20. Jahrhundert entwickelten Wissenschaftler sogenannte ABC-Waffen, atomare, biologische und chemische. Es dauerte Jahrzehnte, bis ihr Einsatz reguliert und teilweise geächtet wurde. Für den Krieg im Netz sind nun digitale Waffen entwickelt worden: Für diese D-Waffen gibt es keine internationalen Konventionen. Es gilt das Recht des Stärkeren.

Der kanadische Medientheoretiker Marshall McLuhan hat es kommen sehen, er schrieb bereits 1970: „Der Dritte Weltkrieg wird ein Guerilla-Informationskrieg sein, ohne Trennung zwischen Militärs und Zivilisten.“ Die Spione bereiten sich genau darauf vor.

Die U. S. Army, die Navy, das Marine Corps und die Air Force haben eigene Cybertruppen aufgebaut; doch die NSA, die eine militärische Behörde ist, spielt längst die Führungsrolle. Nicht umsonst trägt ihr Leiter – seit April 2014 Admiral Michael Rogers – neben dem Titel „DIRNSA“ für „Director of the NSA“ den des Chefs des „Cyber Command“ der US-Streitkräfte. Der ranghöchste Überwacher ist in Personalunion also Chef der Cyberkrieger. Die rund 40 000 NSA-Mitarbeiter sind für Spionage und zerstörerische Netzangriffe gleichzeitig zuständig.

In der militärischen Sicht auf das Netz ist die Überwachung nur die „Phase 0“ in der Cyberkrieg-Strategie – und internen Unterlagen zufolge die Voraussetzung für alles Folgende: Durch sie sollen die Schwachstellen der gegnerischen Systeme ausspioniert werden. Wenn sie mit „verborgenen Implantaten“ infiltriert und mit „permanenten Zugängen“ kontrollierbar sind, ist Phase drei erreicht, die mit „Dominieren“ überschrieben ist: „Durch die in Phase 0 gelegten Zugänge kritische Systeme nach Belieben kontrollieren/zerstören.“ Als kritische Infrastruktur gilt alles, was eine Gesellschaft am Laufen hält: Energie, Kommunikation, Transport. Ziel, so interne Unterlagen, sei schließlich die „kontrollierte Eskalation in Echtzeit“.

In einer NSA-Präsentation heißt es: „Der nächste größere Konflikt wird im Internet beginnen.“ Die US-Regierung treibt die Aufrüstung mit enormem Aufwand voran. Laut dem unveröffentlichten Haushalt für die US-Geheimdienste wurde 2013 für die Stärkung des Angriffspotenzials in Sachen Computer-Netzwerk-Operationen über eine Milliarde Dollar veranschlagt. Allein für „unkonventionelle Lösungen“ wurden zusätzlich 32 Millionen in den Etat gestellt.

Zuletzt tauchten Schadprogramme auf, die Experten aufgrund etlicher Indizien der NSA und der Fünf-Augen-Allianz zugeschrieben haben: „Stuxnet“ beispielsweise zum Angriff auf das Atomprogramm Irans. In Deutschland machte gerade „Regin“ Furore, ein leistungsfähiger Schnüffeltrojaner, der auf dem USB-Stick einer ranghohen Mitarbeiterin der Bundeskanzlerin gefunden worden war. Auch beim Angriff auf die EU-Kommission 2011 und auf die belgische Telekom-Firma Belgacom war Regin im Einsatz (SPIEGEL 1/2015).

Der Gefahr, nichts ahnend Opfer eines Datenangriffs zu werden, ist jeder Internetnutzer ausgesetzt. Denn Spione können routinemäßig fast jede Firewall knacken; auf manchen Rechnern herrscht ein munteres Kommen und Gehen diverser Eindringlinge; auch in Facebook-Chats wird eingebrochen und kopiert mithilfe von Programmen wie „Quantumdirk“; und zum Abtransport brisanter Daten können die Handys Unbeteiligter missbraucht werden.

In diesem Guerilla-Krieg um Informationen wird kaum zwischen zivil und militärisch unterschieden, wie die Snowden-Dokumente zeigen. Jeder Websurfer kann mit seinen Daten und seinem Rechner einen Kollateralschaden erleiden. Und sollte eine D-Waffe wie Barnfire aufgrund eines Programmierfehlers die Steuerzentrale eines Krankenhauses „schrotten“, wären selbst jene betroffen, die nicht einmal ein Mobiltelefon besitzen.

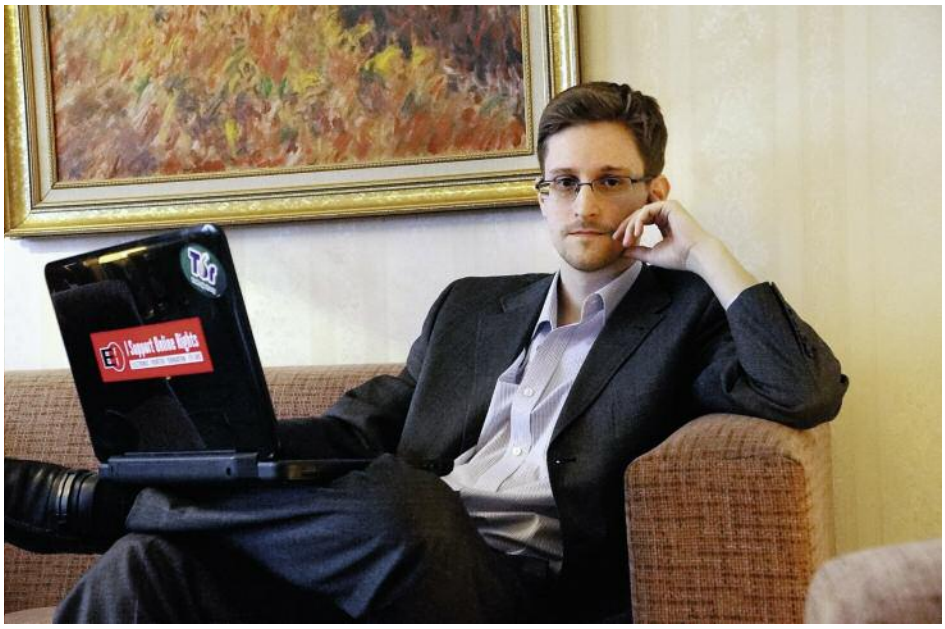
Die Geheimdienste haben für ihre Netzoperationen die Devise der „plausible deniability“ ausgegeben, die Attacken müssen sich glaubwürdig leugnen lassen. Wer für einen Angriff verantwortlich ist, soll nicht nachweisbar sein.

Ein atemberaubender Ansatz, denn die Digitalspione unterlaufen damit vorsätzlich das Fundament aller Rechtsstaaten. Sie machen das Internet zu einem rechtsfreien Raum, in dem die Großmächte und deren Geheimdienste nach Gutdünken operieren, ohne dafür zur Verantwortung gezogen werden zu können.

Zur Kerntruppe der NSA zählen jene Männer und Frauen, die in Fort Meade im Bundesstaat Maryland unter dem Codenamen S321 im Remote Operations Center (ROC) arbeiten, dem Zentrum für ferngesteuerte Einsätze. Der ROC-Trupp sitzt in der dritten Etage eines der NSA-Hauptgebäude. Angefangen hätten sie als „ein Haufen Hacker“, erinnert sich ein NSA-Mann in einem Bericht aus dem Snowden-Archiv. „Spontan improvisiert“ habe man zunächst; inzwischen gestalteten sich die Abläufe „systematischer“. Schon bevor die NSA-Führung die ROC-Mannschaft im Sommer 2005 massiv verstärkte, hieß deren Motto: „Deine Daten sind unsere Daten, deine Geräte sind unsere Geräte.“

Die Agenten mit diesem erstaunlichen Eigentumsbegriff sitzen rund um die Uhr im Schichtbetrieb vor ihren Monito-

FOTOS: VICTOR J. BLUE/BLOOMBERG VIA GETTY IMAGES (U.); TREVOR PAGLEN / DPA (O.)



NSA-Aussteiger Snowden: „Einen neuen internationalen Verhaltenskodex schaffen“

ren. Wie nahe die NSA der angestrebten „globalen Netzvorherrschaft“ schon gekommen ist, zeigt sich vor allem in der Arbeit der Abteilung „Transgression“. Das kann man mit dem deutschen Wort „Überschreitung“ übersetzen; im religiösen Kontext aber auch mit „Sünde“.

Die Aufgabe der Abteilung ist das Aufspüren und Analysieren fremder Cyberattacken – und im besten Fall das Abschöpfen der Erkenntnisse konkurrierender Geheimdienste. Diese Form der „Cyber-Gegenspionage“ gehört zum Delikatesten im Agentenwesen.

Das Archiv von Edward Snowden gewährt nicht nur Einblicke in das digitale Angriffspotenzial der USA selbst, sondern auch in das von anderen Staaten. Die Transgression-Mitarbeiter können dafür auf jahrelange Vorarbeit und Erfahrungen zurückgreifen – und auf Datenbanken, in denen sie die Schadprogramme und Angriffswellen anderer Staaten katalogisieren.

Den Snowden-Unterlagen zufolge haben die NSA und ihre Fünf-Augen-Partner in den vergangenen Jahren eine Vielzahl von Cyberattacken aus anderen Staaten für ihre eigenen Zwecke genutzt. Schon 2009 galt es, fremde Angriffe „zu entdecken, zu verstehen, zu bewerten“. In einem anderen Dokument heißt es: „Stehlt ihre Werkzeuge, ihr Know-how, ihre Opfer und ihre Ergebnisse.“

Im Jahr 2009 bemerkte eine NSA-Einheit einen Dateneinbruch bei Mitarbeitern des US-Verteidigungsministeriums. Die Abteilung spürte daraufhin eine IP-Adresse in Asien auf, die als Kommandozentrale der Angriffe fungierte. Am Ende der detektivischen Arbeit gelang es den Amerikanern nicht nur, China als Ausgangspunkt der Ausspähung zu lokalisieren: Sie griffen auch die Spionageergebnisse aus anderen chinesischen Raubzügen ab – darunter die elektronische Beute bei den Vereinten Nationen. Seither las man in Fort Meade mit, was die Chinesen an Interna aus der Uno abzweigten. „Die NSA kann sich in die chinesische Aufklärung einklinken“, heißt es in einer internen Erfolgsmeldung aus dem Jahr 2011.

Die Praxis, andere Dienste spionieren zu lassen und sich deren Erkenntnisse anzueignen, wird „Fourth Party Collection“ genannt. Alle Länder, die nicht zur Fünf-Augen-Allianz gehören, gelten als potenzielle Ziele für diese „nicht traditionelle“ Methode – also auch Deutschland.

Dank der Fourth Party Collection konnte die NSA, Snowden-Dokumenten zufolge, in den vergangenen zehn Jahren zahlreiche Fälle der Datenspionage aufspüren, viele davon aus China und Russland. So enttarnte die für „maßgeschneiderte Zugangsoperationen“ zuständige Abteilung TAO mit der Hilfe von IP-Adressen zunächst die Steuerungsrechner in China und arbeitete sich von dort aus zu den Drahtziehern in der Volksbefreiungsarmee vor. Ihre Gegner hätten es ihnen dabei durchaus schwer gemacht, berichten die US-Spione: Sie hätten mit wechselnden IP-Adressen gearbeitet, „schwierig zurückzuverfolgen, schwer anzugreifen“. Letztendlich sei es ihnen dennoch gelungen, „zentrale Router auszubeuten“.

Kniffliger war es wohl, den Spieß umzudrehen und die Angreifer selbst zu attackieren. Erst nach langem „Waten durch uninteressante Daten“ drangen die Amerikaner auf einen Rechner eines hochrangigen chinesischen Militärs vor – und ergatterten sogar Angaben zu geplanten Zielen in der US-Regierung, weiteren internationalen Regierungen und den Quellcode chinesischer Schad-Software.

Diesen Operationen stehen allerdings auch chinesische gegenüber. Aus den Snowden-Unterlagen geht die NSA-interne Schadensbilanz von vor ein paar Jahren hervor. Demnach gab es mehr als 30 000 erkannte Zwischenfälle allein im Bereich des US-Verteidigungsministeriums; mehr als 1600 seiner Netzwerkrechner seien gehackt worden. Der Aufwand für die Schadensabschätzung und den „Wiederaufbau“ des Netzwerks wird mit einer erstaunlich hohen Summe angegeben: mehr als hundert Millionen Dollar.

Zu den betroffenen „sensiblen Militärtechnologien“ gehörten Zeitpläne für die Luftbetankung von Flugzeugen, das militärische Logistikplanungssystem, Raketen-Navigations-Systeme der Marine, Informationen zu Atom-U-Booten, Raketenabwehr und weiteren hochgeheimen Rüstungsprojekten.

Von der Gier, alles wissen zu wollen, sind freilich nicht nur Chinesen und Amerikaner, Russen und Briten getrieben: Schon vor Jahren fielen den US-Diensten auch Dateneinbrüche aus Iran auf – sie analysierten sie unter dem Codewort „Voyeur“. Hinter der Angriffswelle „Snowglobe“ dürften Franzosen gesteckt haben.

Mittlerweile läuft die Suche nach fremden Cyberattacken und deren Abwehr bei der NSA und den Fünf-Augen-Partnern weitgehend automatisiert. Das System „Tutelage“ kann Angriffe erkennen und dafür sorgen, dass sie das Opfer gar nicht erreichen.

In den Snowden-Unterlagen werden als Beispiele nicht nur chinesische Angriffe genannt, sondern auch die relativ simple „Low Orbit Ion Cannon“ (LOIC). So heißt eine Schad-Software, mit der etwa die Bewegung „Anonymous“ missliebige Websites unerreichbar macht. In diesem Fall, heißt es in einem Dokument, könne Tutelage die IP-Nummern der Rechner erkennen, von denen die Überlastungsangriffe ausgingen, und diese wiederum blockieren.

Die NSA vermag inzwischen auch die Verteidigung in einen Angriff zu verwandeln: „Umnutzen und nachbauen“ heißt diese Methode. Dabei geht es um sogenannte Botnetze, die mitunter aus Millionen Rechnern von Privatpersonen bestehen, auf denen eine Software eingeschmuggelt wurde. So lassen sie sich als Teil einer „Zombie-Armee“ fernsteuern, um etwa Firmen lahmzulegen und zu erpressen. Statt diese Botnetze zu stoppen und die ahnungslosen Opfer zu warnen, versklaven NSA-Programme wie „Quantumbot“ und „Defiantwarrior“ („Trotziger Krieger“) sie teils für eigene Zwecke.

Diese Zombie-Rechner seien ideal als „nicht zurückverfolgbare Wegwerfknoten für Netzangriffe“. Statt private Internetnutzer zu schützen, missbraucht Quantumbot sie als menschliche Schutzschilde, um eigene Attacken zu tarnen.

Die Spezialisten des Remote Operations Center besitzen eine ganze Palette von digitalen Nachschlüsseln und Brechstangen, um selbst in die bestgeschützten Rechenzentren einzudringen. Sie geben ihren Werkzeugen brachiale Namen, als böte man sie in einem App-Store für Cyber-

FOTO: BARTON GELLMAN / GETTY IMAGES

kriminelle an: „Hammerchant“, erlaubt das Mitschneiden von Internettelefonaten (Voip), „Warriorpride“ bietet eine Art universelles Software-Esperanto, das alle fünf Partnerdienste verwenden, unter anderem für Einbrüche in iPhones. Und mit „Foxacid“ lassen sich kleine Schadprogramme, sobald sie sich auf fremden Rechnern eingenistet haben, aus der Ferne mit immer neuen Funktionen aufrüsten. Als Projektlogo dient ein Fuchs, der schreiend in einem Säurebad aufgelöst wird. Die NSA will sich, wie üblich, zu operativen Details nicht äußern, beteuert aber, dass man sich strikt an die Gesetze halte.

Doch so raffiniert die Waffen des Cyberkriegs auch sein mögen – im Durchleuchten und Knacken fremder Netze lauert ein Paradox: Wer garantiert, dass nicht auch die Geheimdienste selbst Opfer ihrer eigenen Methoden werden können, zum Beispiel durch private Hacker, Kriminelle oder andere Geheimdienste?

Um die Schadprogramme zu steuern, sind die ROC-Spione mit ihnen verbunden – und das geschieht über eigene, abgeschottete Netze, durch welche hochsensible Telefonmitschnitte, Angriffsprogramme und Passwörter schwappen.

Der Anreiz, hier einzubrechen, ist enorm. Wo immer geheimes Herrschaftswissen konzentriert liegt, diese Zugangsinformationen und VPN-Schlüssel sind sein hochpotentes Konzentrat. Wer über sie verfügt, kann Konten plündern, militärische Aufmarschpläne durchkreuzen, Jagdbomber nachbauen, Kraftwerke abschalten. Globale Netzvorherrschaft eben.

Aber die Welt der Geheimdienste ist schizophren: Die NSA soll das Netz verteidigen und gleichzeitig seine Sicherheitslücken ausnutzen; Räuber und Gendarm sein, Bock und Gärtner. Ganz nach dem unter Spionen gängigen Motto: „Enthülle ihre Geheimnisse, schütze deine eigenen.“

Auf einigen gehackten Servern geht es deshalb zu wie in einem Taubenschlag, Geheimdienste geben sich die Klinke in die Hand, es herrscht ein Kommen und Gehen, von dem die rechtmäßigen Besitzer keinen Schimmer haben. Als würde die Polizei ungerührt bei der Plünderung eines Supermarkts zuschauen.

Es ist absurd: Die Spitzel werden bei ihren Raubzügen ständig von anderen Spitzeln beim Spitzeln bespitzelt. Also versuchen sie routinemäßig, ihre Spuren zu beseitigen oder falsche zu legen.

Technisch gesehen läuft das Legen falscher Spuren durch die ROC-Mitarbeiter unter anderem so ab: Nach dem Eindringen in fremde Rechner folgt die Exfiltration, also der Rücktransport der erspitzelten Daten. Dabei wird die Beute nicht direkt an die Internetadresse des ROC geleitet, sondern an einen sogenannten Sündenbock-Empfänger („Scapegoat“). Geklaute Informationen können so auf den Servern von Gegnern landen, womit diese dann am Pranger stehen.

Natürlich hat das NSA-System, bevor die Daten als Ablenkungsmanöver beim Sündenbock landen, die Daten unterwegs abgefangen, kopiert und zum ROC geschickt. Derlei Vertuschungstaktiken bergen das Risiko einer kontrollierten oder unkontrollierten Eskalation zwischen den Diensten.

Freilich müssen es gar nicht unbedingt die Rechner sein, die systematisch geknackt, ausgespäht oder für Botnetze missbraucht werden. Auch Mobiltelefone werden für den Datenklau am Arbeitsplatz benutzt. Das unwissende Opfer, dessen Handy mit einem Spionageprogramm infiziert worden ist, schmuggelt dann die Beute aus dem Büro hinaus, woraufhin sie auf dem Heimweg per Funk abgegriffen wird. Die Digitalspione verhöhnen die Schmuggler wider Willen im Slang von Drogendealern als „ahnungslose Datenmaultiere“.

Sie fühlen sich sicher dabei. Weil sie für die mächtige NSA arbeiten und weil sie praktisch keine Spuren hinterlassen, die gerichtsfest wären. Und wo es keinen Schuldbeweis gibt, kann es auch keine Strafjustiz geben, keine parlamentarische Kontrolle der Geheimdienste, keine internationalen Abkommen. Bislang sind die Risiken und Nebenwirkungen der neuen D-Waffen noch kaum bekannt und gesetzlich kaum reguliert.

Edward Snowden hat enthüllt, wie die Geheimdienste der Welt, allen voran die NSA, sich bemühen, das Internet zu einem rechtsfreien Raum zu degradieren. Der Aussteiger macht sich inzwischen große Sorgen, dass für die NSA die „Verteidigung eine viel geringere Priorität hat als der Angriff“ – so formulierte er es in einem vorige Woche veröffentlichten Interview mit dem US-Sender PBS.

Snowden will das nicht hinnehmen und forderte schon vor Monaten: „Wir müssen einen neuen internationalen Verhaltenskodex schaffen.“

Jacob Appelbaum, Aaron Gibson, Claudio Guarnieri, Andy Müller-Maguhn, Laura Poitras, Marcel Rosenbach, Leif Ryge, Hilmar Schmundt, Michael Sontheimer