ADLAS

Magazin für Außen- und Sicherheitspolitik

AUSGABE 1/2013

7. Jahrgang

ISSN 1869-1684

FOKUS

Cyber-Security

PERSÖNLICHE SICHERHEIT

Vom Spielzeug zum Codebrecher

ORGANISIERTE KRIMINALITÄT

Krieg den Narcobloggern

www.adlas-magazin.de

Publikation für den BSH

Nicht nur der Bundesgerichtshof sieht im reibungslosen Internetzugang mittlerweile eine Lebensgrundlage: Die USA investierten 2012 über 100 Millionen Dollar, um mit »Internet aus dem Koffer« in Ländern mit autoritären Regimes Netzzugang für Oppositionelle zu sichern – das Internet lässt sich durch die Machthaber damit nicht mehr einfach abschalten, Regimegegner können sich weiterhin über soziale Netzwerke koordinieren und die Weltöffentlichkeit informieren. Statt Waffen, so ein US-Offizieller, schmuggele die CIA nunmehr Internetzugänge. Die Cyber-Dimension, das illustriert diese Episode, ist für Sicherheits- und Außenpolitik mittlerweile nicht mehr wegzudenken – ein wichtiger Grund für *ADLAS*, seine Reihe zu diesem Thema mit einem Schwerpunktheft abzuschließen.

Die Autoren dieser Ausgabe betrachten dabei die ganze Bandbreite des Themas. Aus der technischen Sicht betrachtet Thomas Reinhold Angriffsvektoren und Trends im Cyberkrieg – und zeigt, dass großangelegte Attacken wie durch »Stuxnet« und »Duqu« hochorganisierten und gut ausgerüsteten Angreifer vorbehalten bleiben (**Seite 7**). Cyberkrieg scheint zumindest auf dieser Ebene noch Sache der Staaten zu sein. Angesichts dieses Befunds ist die Frage, ob das »erfolgreichste Bündnis der Geschichte«, die Nato, der Cyberbedrohung gewachsen ist, umso wichtiger. Ob die Allianz hier voll oder nur bedingt abwehrbereit ist, erörtern Andrea Pretis (**Seite 30**) und Julian Schibberges (**Seite 34**) in ihren Beiträgen.

Unter dem Stichwort »Internet Governance« erläutert Isabel Skierka die Diskussionen um die Regelung der Kommunikationsnetze (**Seite 12**). Bei diesem Machtkampf zwischen Aktivisten, Staaten und Unternehmen geht es nicht nur um den freien Zugang zu Netz, sondern auch um viel Geld. Und um Bedrohungsängste, wie Sören Ludwig findet: Ob und wie solche Ängste geschürt werden, zeigt seine Analyse des »Securitisation«-Prozesses (**Seite 17**).

Diese Ausgabe markiert aber nicht nur den Höhepunkt der Reihe zu Cybersicherheit, sondern auch einen personellen Wechsel im *ADLAS*: Nach sechs Jahren als Herausgeber endet für mich diese spannende und interessante Aufgabe mit Erscheinen dieses Hefts. Auch nach sechs Jahren bleibt aber »keine Zeit für Selbstbeweihräucherung« (**Seite 66**) – die Redaktion des *ADLAS* und sein neuer Herausgeber, Stefan Dölling, haben auch in Zukunft alle Hände voll zu tun.

Mir bleibt noch, mich herzlich bei all jenen zu bedanken, die am Gelingen des Projekts »ADLAS« mitgewirkt haben, bei den guten Mitstreitern im BSH, bei der unermüdlichen Redaktion, und bei Ihnen, liebe Leserinnen und Leser, für Ihr Interesse. ◂◂◂◂

HERAUSGEBER

Die Cyber-Dimension ist für Sicherheits- und Außenpolitik nicht mehr wegzudenken.

INHALT

FOKUS: CYBER-SECURITY

DIE WELT UND DEUTSCHLAND

INHALT

BEDIENUNGSANLEITUNG: Liebe Leserinnen und Leser,

wussten Sie schon, dass Sie sich durch den *ADLAS* nicht nur blättern, sondern dass Sie sich auch **durch unser eJournal *klicken*** können? Neben den Internetverknüpfungen, denen Sie über unsere Infoboxen »Quellen und Links« in das World Wide Web folgen können, ist jede Ausgabe unseres Magazins intern verlinkt.
Über das Inhaltsverzeichnis können Sie durch das Heft navigieren: Klicken Sie hier einfach auf einen Eintrag, oder das Bild dazu, und schon springen Sie in unserem PDF-Dokument auf die gewünschte Seite.
Am Ende eines jeden Beitrags finden Sie die Text-Endzeichen ◂◂◂◂ oder einen Autorennamen. Klicken Sie einmal darauf und schon kommen Sie wieder auf die Seite im Inhaltsverzeichnis, von der aus Sie in den Beitrag gesprungen sind. Welchen Weg Sie auch bevorzugen – wir wünschen Ihnen eine interessante Lektüre!

Schöne neue digitale Welt?

Illustration: Jamie Zawinski

Die Lage ist ernst.
Die Unsicherheit, die im virtuellen Raum entsteht und in ihm floriert, beeinflusst alle Ebenen unseres realen Lebens. Neue Player und Akteure treten auf, Staaten und Gesellschaften hinken mit der Abwehr deutlich hinterher.

ADLAS widmet sich seit sieben Ausgaben einem nur vermeintlichen Modethema, das zu viele Fragen aufwirft und zu wenige Antworten gibt. Aber eines ist klar: Dieser Abschluss der Reihe »Cyber-Security« ist noch kein Ende der Debatte.

Malware als Waffe

von Thomas Reinhold

Seit Staaten im Cyberspace militärisch agieren stellt sich die Frage, welche Folgen das hat: Droht ein unkontrollierter Rüstungswettlauf oder sind internationale Abkommen möglich?

Analysiert man die Natur der neuen Wirkmittel, ergeben sich einige Hinweise.

Kadetten der US-Armee bei einer Cyber-Übung der NSA.

Foto: Westpoint Public Affairs

>> Im Mai 2012 wurden in der *New York Times* hochrangige US-Militärs damit zitiert, dass sie Cyberwaffen mit offensiven Kapazitäten entwickeln und einsetzen. Auch die deutsche Bundeswehr bestätigte unlängst die » Anfangsbefähigung für das Wirken in fremde Netzen« und es ist sicher, dass noch weitere Nationen an ähnlichen Möglichkeiten arbeiten. Dabei verunsichert das unklare destruktive Potential von gezielt als Kriegswaffe entwickelter Schadsoftware (Malware) die internationale Politik.

Noch ist nicht absehbar, ob diese neue Technologie einen weiteren Rüstungswettlauf auslösen wird und wie man dem mit bestehenden internationalen Abkommen zu Krieg und Rüstung begegnen kann. Für die Entwicklung und Anwendung von Rechtsnormen und Konventionen der internationalen Zusammenarbeit ist eine klare Unterscheidung von zwischenstaatlichen Konflikten durch Cyberattacken auf der einen und Formen von Cyberkriminalität auf der anderen Seite notwendig.

Während es für den Kampf gegen Cyberkriminalität bereits internationale Vereinbarungen gibt, fehlen für Cyberattacken verbindliche Definitionen oder international einheitliche Gefährdungseinschätzungen. Einige Staaten >>

behalten sich deshalb in einseitigen Erklärungen das Recht auf konventionelle militärische Reaktionen vor, ohne näher einzugrenzen, ab wann Angriffe gegen ihre IT-Systeme als Cyberattacke angesehen und wie die sehr unterschiedlichen Techniken von Angriffen bewertet werden.

Eine Möglichkeit, Cyberkrieg von Phänomenen der Cyberkriminalität zu differenzieren, ist die Analyse der technologischen Qualität der bisher entdeckten staatlichen Malware und deren Einsatz. Die Untersuchung zeigt, dass eine Unterscheidung auf dieser Ebene weniger in den einzelnen Infektions-, Verbreitungs- und Verschleierungstechniken besteht, als vielmehr in der Qualität, der Integration der unterschiedlichsten Methoden und dem Entwicklungsaufwand, um eine Malware auf Ziel und Zweck auszurichten. Hinzu kommt die mögliche Unterstützung durch Nachrichtendienste.

Die erste Malware, die vor diesem Hintergrund für Aufsehen sorgte, war das im Juni 2009 entdeckte »Stuxnet«, dessen Hauptzweck in der verborgenen Manipulation und Sabotage von Industriesteuerungsanlagen iranischer Urananreicherungszentrifugen bestand. Derartige kritische Computer- und Industrieanlagen werden aus Sicherheitsgründen in aller Regel vom Internet entkoppelt um einen unbefugten Zugriff zu unterbinden. Dieser sogenannte »Air-Gap« wurde bei Stuxnet vermutlich mit Hilfe eines infizierten USB-Sticks überwunden. Bei diesem, auch aus dem Bereich der klassischen Cyberkriminalität bekannten Angriffsmuster, wird ein USB-Stick gezielt platziert, um beispielsweise einen Mitarbeiter zur unabsichtlichen Infektionen durch den als »verloren aufgefundenen« Stick zu bewegen. Andere Wege bestehen in der Infektion bei physischen Zugriffsmöglichkeiten wie Flughafenkontrollen oder klassischen Geheimdienstoperationen, bei denen beispielsweise Mitarbeiter der Anlagen für die Infiltration eingesetzt werden.

Die eigentliche Infektion des Computers mit Stuxnet erfolgte durch Einstecken des USB-Sticks, wobei zwei Zero-Day-Exploits der Microsoft Windows Betriebssysteme genutzt wurden, um den Schadcode automatisch und verdeckt auszuführen. Infizierte Rechner wurden dann automatisch derart präpariert, dass sie jeden weiteren USB-Stick infizierten, gesammelte Daten auf USB-Sticks versteckten, sowie die Malware über lokale Netzwerkordner und Netzwerkdrucker weiter verbreiteten.

Um die Sabotage über Monate hinweg zu verbergen, war ein immenser Aufwand notwendig.

Um diese tief greifenden Änderungen am Betriebssystem vorzunehmen, wurden weitere, teilweise unbekannte, Sicherheitslücken sowie sogenannte digitale Zertifikate verwendet, um Stuxnet als legitime Software zu tarnen. Diese digitalen Zertifikate waren im Vorfeld zwei asiatischen Firmen gestohlen worden, was seinerseits einen komplexen physischen oder Cyber-Einbruch erfordert haben dürfte, da derartige Zertifikate in aller Regel besonders gesichert und digital verschlüsselt aufbewahrt werden.

Die Schadfunktion von Stuxnet war für eine spezifische Modellreihe von SCADA-Industriesteuerungseinheiten der Firma Siemens programmiert. Diese Geräte werden für die Überwachung und Regelung von Pumpen, Ventilen und ähnlichem eingesetzt. Mittels einer Modifikation der zentralen Steuerungssoftware wurde die angeschlossene Regelungselektronik umprogrammiert. Dieses Vorgehen bedingte spezielles Expertenwissen über technische Interna der Sie- >>

DIGITALE ZERTIFIKATE

sind mit einem Ausweis vergleichbar, der von dazu berechtigten Instanzen ausgestellt und mittels geeigneter Technik, in diesen Fall kryptografische Verfahren, gegen Fälschungen gesichert wird. Digitale Zertifikate werden zum Beispiel von Betriebssystem-Herstellern an externe Software-Anbieter verteilt, die ihre Programme damit signieren. Auf Seiten des Anwenders wird anhand dieser Signaturen bei Betriebssystem-kritischen Installationen die Authentizität und Integrität des zu installierenden Programms geprüft um Manipulationen durch heimlich eingeschleusten Schadcode zu erkennen und auszuschließen. Digitale Zertifikate werden aber auch bei Zugriffen auf kritische Systeme wie Online-Bankkonten verwendet, um die Authentizität des Servers zu garantieren.

mens-SCADA-Geräte – welches mit hoher Wahrscheinlichkeit nur durch die Firma selbst bereitgestellt werden konnte – sowie exakte Vorkenntnisse über den technischen Aufbau und die im einzelnen verwendeten Geräte der Anlage.

Für die Manipulation der Steuerungssoftware und um die über mehrere Monate hinweg durchgeführte Sabotage vor dem Personal zu verbergen, war ein immenser Aufwand notwendig. Dafür wurde vermutlich auch extra ein Teil der iranischen Anlage nachgebaut, um den Ablauf von der Infektion bis zur Manipulation zu testen und zu optimieren. Analysen des Quellcodes von Stuxnet zeigen, dass mit dessen Entwicklung spätestens 2007 begonnen wurde. Stuxnet wurde auf Basis einer eigens entwickelten Programmier-Plattform namens »Tilded« realisiert, einem »Programmcode-Baukasten«, mit dessen Hilfe noch weitere Malware erstellt wurde.

Einer dieser Ableger ist die 2011 entdeckte Malware »Duqu«, die ähnliche Programmcode-Bestandteile und Angriffsmethoden einsetzt und dafür einige der von Stuxnet benutzten Zero-Day-Exploits und digitalen Zertifikate verwendet. Duqu wurde ausschließlich bei fünf Technologie- und Forschungsorganisationen mit Sitz in Frankreich, Niederlande, Schweiz, Ukraine, Indien, Iran, Sudan und Vietnam entdeckt und vermutlich als Spionage-Werkzeug eingesetzt um diese Organisationen gezielt auszuspähen und deren technische Infrastruktur zu analysieren.

Dafür wurde Duqu mittels eines manipulierten Microsoft Word-Dokuments gezielt per Email in Systeme eingeschleust und dort lokal verbreitet. Erweiterte Streumechanismen auf entfernte Netzwerke und damit eine breitere Infektionsdichte waren nicht vorgesehen. Duqu konnte außerdem per »Killswitch« gezielt und zentral gesteuert auf den infizierten Geräten abgeschaltet und entfernt werden. Dieser Eindruck eines Werkzeugs zur Informationsgewinnung und Vorbereitung weiterer Operationen wird durch den eigentlichen Payload weiter bestärkt. Duqu kopierte Bildschirminhalte und Tastatureingaben, durchsuchte Dateien nach Stichworten und sammelte Informationen über die lokale Technik-Topologie. Alle Informationen, die Duqu an die Command & Control-Server sandte, wurden dabei eindeutig dem infizierten Computer zugeordnet, sodass der Angreifer sich ein sehr klares Bild der infiltrierten Umgebung verschaffen konnte.

Auf eine noch schmalere Infektion ausgelegt ist die Malware »Gauss«, die im Juni 2012 im Libanon, Israel und den palästinensischen Gebieten ent- >>

Im April 2008 besucht der iranische Präsident Mahmoud Ahmadinejad das Prestigeprojekt der Urananreicherungsanlage in Natanz. Später legte die Malware »Stuxnet« die Anlage zeitweise lahm.

Foto: President.ir

deckt wurde. Gauss verfügt im Gegensatz zu Duqu über keine Replikationsmechanismen und ist im direkten Vergleich ein modernisiertes und sehr gezielt eingesetztes Aufklärungswerkzeug, welches vor allem auf das Ausforschen einzelner Personen abzielt. Gauss sammelt zu diesem Zweck insbesondere Informationen über Social-Media, Email- und Online-Zugangsdaten, die Historie der besuchten Webseiten sowie Cookies, und sendet diese Informationen verschlüsselt an die Command & Control-Server zurück.

Neben Stuxnet hat in den letzten Jahren zudem vor allem das im März 2012 entdeckte »Flame« für Aufsehen gesorgt, das auf Computersystemen im Iran, Israel/Palästina, Libanon und Saudi-Arabien entdeckt wurde und in Teilen möglicherweise bereits seit 2007 aktiv war. Flame wurde wie Stuxnet auf Basis einer eigens entwickelten Programmierplattform realisiert, auf der vermutlich auch weitere Projekte entstanden, und zweifelsohne für Spionage und zum Sammeln von Informationen eingesetzt.

Im Gegensatz zu den bisherigen Typen ist Flame aber sehr viel umfangreicher und größer, da es auf eine breite Streuung und eine tiefe und detaillierte Infiltration ausgelegt ist. Flame verfügt über Programmbestandteile die es erlauben, Daten intensiv zu analysieren, komprimierte Dateien sowie lokale Datenbanken zu durchsuchen und die Verschlüsselung von Daten anzugreifen.

Darüber hinaus war Flame in der Lage, neben dem Aufzeichnen von Bildschirminhalten, Tastatureingaben und Audioübertragungen, weitere Programmbestandteile von den Command & Control-Servern nachzuladen. Mit Hilfe dieser nachträglichen Erweiterbarkeit wäre auch ein breite Schadwirkung durch das simultane Löschen von Computerdaten oder der erzwungene Ausfall von Computern durch bewusstes Zerstören der Betriebssysteme realisierbar gewesen.

Von den Command & Control-Servern, die bei Flame zum Einsatz kamen, sind einige aktuell noch online und in der Lage, mit vier verschiedenen Schadprogrammen zu kommunizieren und Daten auszutauschen. Mit Flame selbst und einer unlängst entdeckten, reduzierten Version von Flame, »SPE« oder auch »Mini-Flame« getauft, sind bisher nur zwei dieser vier Programme bekannt. Es ist daher zu vermuten, dass die Flame-Plattform weiterhin verwendet wird.

COMMAND & CONTROL SERVER

Um infizierte Computer aus der Ferne zu kontrollieren, Daten zu entnehmen oder gewünschte Schadfunktionen gezielt auszuführen, verwenden Angreifer oft sogenannte Command & Control-Server (C&C) die als Zwischenschritt zwischen Angreifer und Ziel stehen. Diese Server sind öffentlich im Internet verfügbare Computer, deren Internet-Adressen in die Malware eingebaut werden, die dann ihre Daten an diese Server senden oder in regelmäßigen Abständen anfragen, ob neue, vom Angreifer hinterlegte Befehle vorliegen, um diese auf dem infizierten System auszuführen. Ein Angreifer kann mit einem C&C-Server unzählige infiltrierte Systeme kontrollieren und indirekt steuern.

Lohnt sich das alles? Im Fall von Stuxnet vermutlich eher nicht.

Zwischen den vier bisher entdeckten Schadprogrammen bestehen auffällige Ähnlichkeiten. Zum einen entstammen Duqu und Stuxnet beide der Plattform Tilded. Zum anderen legen Analysen der Quellcode-Bestandteile, der Programmierstruktur sowie identische Programmcode-Passagen den Schluss nahe, dass die Flame-Plattform und Tilded zwar von zwei getrennten Entwicklerteams realisiert wurden, dass diese aber einen gemeinsamen Ressourcenpool verwendeten und eine enge Kooperation bestand. Dieser Schluss wird zum einen dadurch bestärkt, dass Flame und Duqu jeweils einige der Zero-Day-Exploits verwenden die bereits bei Stuxnet eingesetzt wurden. Zum anderen wurde die Infektionsmethodik des infiziertem USB-Sticks bei Flame, Stuxnet und Gauss nahezu identisch implementiert und für das Eindringen in die Zielsysteme angewendet.

Die Verwendung und Kombination vieler unterschiedlicher Technologien und der enorme Entwicklungsaufwand stellen, neben der dafür notwendigen Informationsbeschaffung auf Basis geheimdienstlicher Tätigkeiten, die Beson- >>

derheit staatlich-militärischer Malware dar. Während bei typischer Cyberkriminalität zumeist populäre Betriebssysteme und Programme angegriffen werden um eine möglichst lang andauernde und breite Infektion von Computersystemen zu erreichen, stehen bei staatlichen oder militärischen Zwecken in aller Regel klare Ziele in Form bestimmter Computersysteme im Vordergrund.

Die Informationsbeschaffung zu den Details dieser oft sehr speziellen Technologien – ihrer Soft- und Hardware sowie dem Versions- und Konfigurationsstand – benötigen auf Seiten des Angreifers viel Zeit und Knowhow. Unter Umständen sind vor der eigentlichen Schadoperation weitere Zugriffe auf das Zielsystem oder klassische Operationen der geheimdienstlichen Informationsbeschaffung notwendig. Währenddessen muss der Angreifer seine Aktivitäten permanent geheim halten, denn eine vorzeitige Entdeckung kann alle Erfolgsaussichten mit einem Schlag ruinieren. Staatliche und militärische Angreifer agieren dabei außerdem in aller Regel innerhalb hierarchischer Institutionen, die politische Ziele verfolgen, und benötigen klare Missionsvorgaben mit entsprechenden Do's and Dont's. Diese Aspekte sorgen dafür, dass entsprechende Operationen einen erheblichen Personal- und Finanzaufwand für das Management, die Entwicklung, den Test und die eigentliche Durchführung der Operation benötigen.

Die Mittel eines echten Cyberwar bleiben wohl den reichen Staaten vorbehalten.

Lohnt sich das alles? Im Fall von Stuxnet vermutlich eher nicht. Trotz des erheblichen Aufwandes war der Nutzen gering. Die internationale Atomenergiebehörde IAEO geht in Berichten davon aus, dass durch Stuxnet von mehreren zehntausend im Betrieb befindlichen Anlangen, maximal eintausend zerstört wurden. Das Programm dürfte so nur um wenige Monate verzögert worden sein.

In den vergangenen Jahren hat die Bandbreite an Schadsoftware, deren Einsatzgebiet und Ressourcenaufwand staatliche Aktivität vermuten lassen, deutlich zugenommen. Die bereits entdeckten Malware-Arten reichen dabei von der einfachen, breit gefächerten Spionage bis hin zu gezielt für Schadwirkung entworfenen Typen. Diese Bandbreite, verbunden mit Äußerungen von militärischen Führungspersonal die den Cyberspace als weitere Domäne betrachten, deuten darauf hin, dass Malware gezielt entwickelt wird, um in zukünftigen Konflikten sowohl für die Vorfeldaufklärung als auch begleitend bei invasiven Operationen eingesetzt zu werden.

Betrachtet man aber den notwendigen Aufwand hinter solchen Entwicklungen, dann ist zu vermuten, dass derartige Kriegsmittel vor allem Staaten vorbehalten bleiben werden, die über hohe Budgets für militärische Aufgaben verfügen. Diese asymmetrische Entwicklung, verbunden mit der weiter zunehmenden Abhängigkeit aller Nationen von vernetzen Computersystemen kann zu einer Verunsicherung der technologisch unterlegenen Staaten führen und Aufrüstungswettkämpfe begünstigen. Es bleibt abzuwarten ob die Akteure den Willen und die Fähigkeiten aufbieten, dem Einhalt zu gebieten, vertrauensbildende Maßnahmen zu etablieren und ein internationales Regime zu entwickeln, welches die Entwicklung und den Einsatz derartiger Mittel reglementiert und überwacht. ◂◂◂◂

Thomas Reinhold *forscht als Informatiker und langjähriger IT-Fachmann am Institut für Friedensforschung und Sicherheitspolitik an der Universität Hamburg.*

Quellen und Links:

Rede des Rechtsberater Harald Koh am 18. September 2012: »International Law in Cyberspace«, veröffentlicht vom US Department of State

Herbert Lin: »Escalation Dynamics and Conflict Termination in Cyberspace«, im *Strategic Studies Quarterly*, Ausgabe 3/2012

Scott J Shackelford: »From Nuclear War to Net War: Analogizing Cyber Attacks«, im *Berkeley Journal of International Law*, Ausgabe 3/2009

Kampf um die Netzherrschaft

von Isabel Skierka

Die Neuverhandlung eines Vertrags zur Regelung der Kommunikationsnetze auf einer UN-Konferenz sorgte schon vor Beginn im Dezember für Aufsehen. Westliche Regierungen, Internetkonzerne und Aktivisten sahen die Freiheit des Internets bedroht.
Letztendlich ist die Konferenz am Boykott des Endvertrags von einer Koalition aus Industrienationen gescheitert. Doch der globale Machtkampf ums Netz ist noch lange nicht vorüber: Neben der Freiheit des Internet geht es vor allem auch um viel Geld.

Die »International Telecommunication Union« traf sich im Dezember 2012 in Dubai. Foto: ITU

>> Noch nie sei das freie Internet »so gefährdet [gewesen] wie heute«, warnte Vinton Cerf, einer der »Väter des Internets« und mittlerweile als Vize-Präsident von Google tätig, im Vorfeld der »Weltkonferenz zur internationalen Telekommunikation«, WCIT-12, vom 3. bis 14. Dezember 2012 in Dubai. Elf Tage lang war das arabische Emirat Schauplatz eines internationalen Machtkampfes von Regierungsvertretern aus 193 Ländern sowie Beobachtern aus Privatwirtschaft und Zivilgesellschaft um die Zukunft der Freiheit im Internet.

Wie der Google-Manager Cerf beschuldigten auch die Sprecher anderer Internetkonzerne, Vertreter von Industriestaaten, Wissenschaftler und Internetaktivisten den Organisator der Konferenz – die »International Telecommunication Union« (ITU), eine Unterorganisation der Vereinten Nationen – in Wahrheit die Kontrolle über den weltweiten elektronischen Datenfluss anzustreben und sie der Willkür nationaler Interessen repressiver Regierungen ausliefern zu wollen. Die Sorgen waren nicht unbegründet: Im Vorfeld der Konferenz veröffentlichten anonyme Quellen auf der Webseite *WCITleaks* Vorschläge von Staaten aus Afrika, der arabischen Welt, China und Russland, >>

in den zuletzt 1988 angepassten, noch aus der Zeit vor der weltweiten Internetrevolution stammenden »International Telecommunication Regulations« (ITRs) rechtlich verbindliche Regeln für staatliche Regulierungs- und Zugriffsmöglichkeiten auf das Internet festzuschreiben. Die von China und Russland angeführte Koalition ist damit jedoch vorerst gescheitert.

Die in Dubai neuverhandelten ITRs weiten das Mandat der ITU nicht auf das Internet aus. Allerdings enthalten sie allgemeine Erklärungen zur »Zusammenarbeit der Regierungen zu Spam« und »Netzwerksicherheit« sowie eine rechtlich nicht verbindliche Zusatzerklärung zur Arbeit der ITU im Bereich Internet-Regulierung. Deshalb haben die USA, Europa, Japan, Australien und Kanada die Unterzeichnung des Vertrags boykottiert. Sie beharren auf dem Status quo einer »Internet Governance« durch ein loses Netzwerk nichtstaatlicher Organisationen.

Doch auch wenn die WCIT-12 damit gescheitert ist – der Konflikt zwischen Befürwortern und Gegnern einer Internetregierung ist kaum besiegelt, sondern steht eher erst an seinem Anfang. Laut Jeanette Hofmann, Internetforscherin am von Google finanzierten Institut für Internet und Gesellschaft, war die ITU-Konferenz erst ein Startschuss für eine globale Debatte um die Frage: Wer soll das Internet regieren? Schon im Februar 2013 beginnt am Sitz der UNESCO in Paris der bis voraussichtlich 2015 dauernde Prozess der »Überprüfung des UN-

INTERNET GOVERNANCE

Der Begriff »Governance« bezeichnet im Allgemeinen eine Form des Regierens durch gewählte Vertreter und nicht gewählte Interessenvertreter, im Falle der »Internet Governance« spielen daher Nichtregierungsorganisationen, die zum Beispiel die technischen Standards des Netzes verwalten, ebenso eine Rolle wie Staaten: Innerhalb der momentanen »Internetordnung« ist beispielsweise die Internet Engineering Task Force (IETF) für die Setzung und Implementierung von technischen Standards verantwortlich.

Eine der wichtigsten Institutionen ist die 1998 von der US-Regierung gegründete »Internet Corporation for Assigned Names and Numbers« (ICANN). Wie auch die IETF und andere Internetorganisationen hat ICANN ihren Sitz in Kalifornien in den USA, dem Ursprungsort des Internets. ICANN ist eine private Institution, die den wahrscheinlich einzigen zentralen Punkt des Internets verwaltet: das Domain Name System (DNS). Es legt fest, wie Internet-Adressen, zum Beispiel www.google.de, in IP-Adressen übersetzt werden, im Falle der deutsche Google-Website also 173.194.78.99. Das DNS besteht aus den 13 weltweiten, überwiegend in den USA stehenden Root Name Servern, die die zentrale Anlaufstelle für den Austausch von IP-Adressen bilden.

Wer soll das Internet regieren?

Weltgipfels zur Informationsgesellschaft« (WSIS 10+), und im Mai 2013 findet in Genf das von der ITU veranstaltete »World Telecommunication Policy Forum« (WTPF) statt. Die im Kontext der WCIT-12 aufgetretenen Konflikte werden die internationale Politik daher noch länger beschäftigen.

Im Kern handelt es sich in der Internetpolitik jedoch nicht nur um einen Kampf um die künftige Kontrolle des freien Meinungs- und Informationsaustausches, sondern auch um ein Ringen um die Verteilung der enormen wirtschaftlichen Ressourcen, Gewinnanteile und Perspektiven.

Dabei war das Internet nicht immer so umkämpft. Von der Anfangsphase in den 1970er bis zum Durchbruch in den frühen 1990er Jahren erregte es kaum das Interesse von Staaten oder Telekommunikationskonzernen. Nur durch das Ausbleiben von staatlichen oder privatwirtschaftlichen Initiativen das Internet zu kontrollieren, konnte sich ungehindert aus dem einst kleinen Netzwerk das globale Netz der Netze bilden. Heute ist es mit über zwei Milli- >>

arden Nutzern und einem jährlichen Online-Handelsvolumen von fast einer Billion US-Dollar längst zu einer strategischen Ressource auf nationaler und internationaler Ebene geworden. Mit der zunehmenden Vernetzung von kritischen Infrastrukturen, Finanzmärkten und fast jedem Aspekt des öffentlichen Lebens sind die Weltgemeinschaft und Regierungen jeglicher Couleur heute zunehmend vom Internet abhängig.

Durch seine offene Struktur hat das Internet beispiellose Möglichkeiten für Innovation, wirtschaftliches Wachstum, Kommunikation und politische Freiheit geschaffen. Gleichzeitig birgt aber ebendiese Offenheit des Netzes auch Schattenseiten. Seine zunehmende Nutzung, beispielsweise für Cyberkriminalität oder terroristische Aktivitäten, stellen die internationale Politik in sich überschlagender Geschwindigkeit vor neue Herausforderungen. Die staatliche Absicherung der nationalen Netze gegen Online-Gefahren und die gleichzeitige Wahrung der freien Struktur des Netzes ist oftmals eine riskante Gratwanderung. Die Gefahr, dass Regierungen unter dem Vorwand der Cybersicherheit das Internet, zumindest das nationale Netz, unter ihre Kontrolle bringen, ist allgegenwärtig. Diese heikle Balance zwischen Freiheit und Sicherheit ist es auch, die »Internet Governance« höchst politisch macht.

In Wahrheit geht es in diesem Kampf um das Netz vor allem ums Geld.

Bislang koordiniert ein loses Netzwerk nichtstaatlicher Organisationen – insbesondere die IETF und ICANN – das Netz. Mit der Kontrolle über Root-Server, Domainnamen und IP-Adressen besitzt ICANN die Herrschaft über die wesentlichen technischen Funktionen des Internets. Diese Regeln haben eine wichtige politische Dimension. Die Kontrolle über das weltweite »Domain Name System« (DNS) ermöglicht es dessen Verwalter im Prinzip, den Server zu finden, auf dem eine Website liegt oder die Benutzer einer Webseite zurückzuverfolgen. Auch hat der Betreiber damit die Kontrolle über die Registrierungen von Webseiten und deren Inhalte. Würde das DNS von Regierungen gesteuert, könnte es als Instrument zur politischen Machtausübung missbraucht werden. Beispiele dafür gibt es leider schon: So kontrolliert China bereits heute sein eigenes nationales DNS und kann den Zugriff auf Webseiten der Opposition erschweren, wenn nicht ganz verhindern.

Um ein freies globales Internet zu bewahren, ist also eine Verwaltung der technischen Funktionen durch neutrale Institutionen von essentieller Bedeutung. Die momentan existierende »Internet Governance«-Ordnung wird von vielen, besonders von den USA, als solch ein neutrales Arrangement gesehen. Doch eine Koalition von Staaten aus Afrika, der arabischen Welt, China und Russland plädieren – auch über die WCIT-12 hinaus – für die Übertragung von Kernkompetenzen der Internetregulierung auf die ITU beziehungsweise nationale Entscheidungsorgane. Insbesondere wollen sie damit amerikanische Institutionen wie ICANN schwächen.

Doch auch in diesem Konflikt gibt es keine eindeutigen »good« und »bad guys«. Denn so, wie autoritäre Staaten und die ITU ihre eigenen Interessen verfolgen, tun dies auch ihre Kritiker. Wie die verschiedenen Vorschläge von Russland, China und anderen Staaten zeigten, hätten diese Länder gern die Gelegenheit genutzt, das gegenwärtige Modell der dezentralen Regulierungen durch ein ITU-gesteuertes Modell zu ersetzen. Doch da die ITRs in der Praxis nur durch eine einstimmige Entscheidung aller Mitglieder in Kraft treten können, konnten die USA, Europa und andere Verbündete ihre Verabschiedung blockieren. Obwohl die Argumente einer Bedrohung der Freiheit des Internets auch für zukünftige Verhandlungen bestehen bleibt, schien die Gefahr vor einer Übernahme des Internets durch die ITU auf der diesjährigen WCIT doch etwas übertrieben.

Aus Angst vor einer Regelung dieser Art regte sich schon vor der Konferenz viel Protest. Eine Anti-ITU-Online-Petition von Accesnow.org sammelte vor dem 3. Dezember mehr als 36.000 Unterschriften. Der US-Kongress >>

forderte in einer Resolution, das existierende »Internet Governance«-Modell zu erhalten und stellte sich gegen eine Kompetenzausweitung der ITU auf das Internet. Google veröffentlichte im November ein Kampagnenvideo gegen die ITU. Auch das Europäische Parlament forderte den EU-Ministerrat und die EU-Kommission auf, sich bei der Konferenz in Dubai für den Erhalt eines öffentlichen und freien Internets einzusetzen. Ebenso lehnte die deutsche Bundesregierung Ende November offiziell Vorstöße für eine größere Kontrolle des Internets durch die ITU ab und bestätigte diese Position auch am Ende der WCIT-12.

Im Übrigen haben Regierungen schon heute die Möglichkeit, ohne Unterstützung von außen den Internetzugang ihrer Bürgerinnen und Bürger für bestimmte Inhalte zu sperren. Die »Great Firewall« der chinesischen Regierung, oder die Blockade von Webseiten wie Google im »Halal Netz« des Iran sind nicht nur Beweis für die Möglichkeit, das Netz national zu kontrollieren, sondern auch ein Hinweis auf eine drohende Fragmentierung des weltweiten Internets in einzelne nationale Intranets. Die ITU spielt dabei nur am Rande eine Rolle.

Obwohl die Proteste gegen die ITU die Angst vor der Kontrolle des Internets durch autoritäre Regime in den Vordergrund stellten, war dies nicht die Hauptsorge der Gegner der WCIT-12. In Wahrheit geht es in diesem Kampf um das Internet vor allem um Geld und damit in Verbindung stehende politische Interessen – und zwar auf Seiten aller Beteiligter.

Bei der Neuverhandlung der ITRs sowie im allgemeinen Konflikt um das Internet dreht es sich vor allem auch darum, wer für das Netz und seine Infrastruktur bezahlt und wer davon profitiert. Auf der einen Seite kämpfen Internetfirmen wie Google und Facebook, die immer größere Datenmengen durch das Netz schicken und dabei Gewinnmargen von bis zu 30 Prozent erzielen. Auf der anderen Seite stehen die Betreiber der Netzinfrastruktur. Das sind in der Regel Telekommunikationskonzerne, die von diesen Gewinnen nur Bruchteile weitergeleitet bekommen. Sie verlangen nun von Google und Co. eine angemessenere Beteiligung als Kompensation für die von ihnen bereitgestellte Infrastruktur. Über die »European Telecommunications Network Operators' Association« (ETNO) hatten 41 europäische Telekommunikationskonzerne entsprechende Änderungsvorschläge für den ITU-Vertrag unterbreitet.

Außerdem wollten die ETNO-Mitglieder ein »Business Class«-Internet einführen. Ein heikles Vorhaben: Bisher gilt das Prinzip der »Netzneutralität«, in dem alle Datenpakete – ob Text, Audio, oder Video – gleich behandelt werden. Der Vorstoß der Konzerne würde dieses Prinzip brechen. Die schnelle Übertragung von großen Datenmengen würde nur noch gegen eine erhöhte Gebühr gewährleistet. Die Kosten würden nicht nur für Google, sondern auch für kleine Unternehmen und Start-ups steigen, sodass solche Regelungen auch Innovation erschweren, wenn nicht gar verhindern. Da nur Staaten, also Regierungen, über die Vorschläge abstimmten, war die Konferenz also auch ein Kampf der Lobbyisten.

Traditionelle Diplomatie reicht für Internet Governance nicht aus.

Es ist daher nachvollziehbar, dass Vertreter von großen Konzernen wie Vint Cerf von Google gegen die ITU mobil machen. Doch in ihrer Kritik sagen auch sie nur die halbe Wahrheit. Tatsächlich wäre es schädlich, ja sogar ein Rückschritt für die globale Vernetzung und den Demokratiegedanken im Netz, wenn das offene Internet von einer internationalen Organisation kontrolliert würde. Auch die Netzneutralität muss in einem freien Netz gewahrt werden. Aber zugleich ist offenkundig, dass es bei den Gewinnmargen ein Ungleichgewicht gibt, welches gerade im Interesse der so nachdrücklich beschworenen Prinzipien der Netzneutralität gemeinsam ausgeglichen werden sollte.

Die US-Regierung hat daran jedoch kein Interesse, sondern möchte den Status quo der »Internet Governance« erhalten. Denn praktisch alle wichti- >>

gen Organisationen des aktuellen Systems stehen den Interessen Washingtons nahe. Die IETF, ICANN und andere wichtige Institutionen haben ihren Sitz in Kalifornien und unterliegen damit amerikanischer Rechtsprechung. ICANN bezieht seine Unabhängigkeit aus einem Vertrag mit dem US-Handelsministerium. Obwohl Top-Level-Domains wie ».com«, ».net« und ».org« – die von ICANN vergeben werden – generisch sind, werden sie von amerikanischen Firmen, wie VeriSign, betrieben. Laut US-Gesetzen wie dem letztendlich nicht verabschiedeten »Stop Online Piracy Act« (SOPA), sollte daher für die Webseiten, die diese Top-Level-Domains nutzen, amerikanisches Recht gelten. Damit versuchen die USA, die Geltung amerikanischen Rechts auch global auf das Internet auszuweiten und somit ihre eigenen Souveränitätsprinzipien im Internet durchzusetzen.

Das Verhalten der USA zeigt, dass nicht nur autoritäre Staaten das Internet zu kontrollieren versuchen, sondern auch demokratische Länder Maßnahmen ergreifen, um ihren politischen Einfluss zu manifestieren und auszuweiten.

Gerade wegen der zunehmenden Konflikte um die Kontrolle über das Internet sollte das jetzige Regelungssystem in einem inklusiven Prozess reformiert werden, in dem die Interessen von Regierungen, Privatwirtschaft und vor allem auch Zivilgesellschaft vertreten sind. Formen der traditionellen Diplomatie, wie sie die ITU anwendet, reichen für Internet Governance nicht mehr aus.

Wolfgang Kleinwächter, Professor an der Universität Aarhus und Mitglied der deutschen Delegation in Dubai, fordert daher eine neue »Internetdiplomatie«. Eine Initiative in dieser Richtung besteht seit 2006 in Form des Internet Governance Forum (IGF), das aus der »Working Group of Internet Governance« der UN hervorging. Das IGF hält jährlich internationale Sitzungen ab, an der Vertreter aus Regierungen, Privatwirtschaft, Zivilgesellschaft und Wissenschaft teilnehmen. Dieses Modell folgt dem Prinzip der »Multi-Stakeholder Governance«, bei dem jede Interessengruppe, jeder Stakeholder, ein gleiches Rederecht hat. Neben Konflikten um die technische Regulierung des Internets diskutiert das IGF auch andere Fragen im internationalen öffentlichen Interesse, zum Beispiel die Bekämpfung von Spam und Cyberkriminalität oder auch einer Neuregelung des Systems der Internet-Verbindungsentgelte.

Die Schwäche des IGF ist allerdings offensichtlich: Es hat lediglich beratende, aber keine bindenden Befugnisse. Die wichtigen Entscheidungen werden daher immer noch von großen Konzernen, Lobbyorganisationen oder Regierungen getroffen. Diese verspotten das IGF nicht selten als »talking shop«.

Obgleich momentan nicht sehr erfolgreich, ist das IGF ein erster Schritt in Richtung einer umfassenden Abstimmung über Internetstandards. Aus den Diskussionen des IGF können sich neue Ideen der »Internet Governance« für die Zukunft ergeben und von dort aus in die Entscheidungsorgane getragen werden.

Der britische Journalist John Kampfner, unter anderem Berater von Google, bemerkte auf einer Konferenz in Berlin im November zu diesem Thema in Abwandlung des berühmten Churchill-Zitats zur Demokratie, das Multi-Stakeholder Modell des IGF sei die ineffizienteste aller Formen der »Internet Governance« – abgesehen von all den anderen Formen, die bisher ausprobiert wurden. ◂◂◂◂

Isabel Skierka *studierte am War Studies Department des King's College London und verfasste kürzlich ihre Masterarbeit zum Thema »Cyber Power«.*

Quellen und Links:

Webpräsenz der International Telecommunication Union

Themenportal zum WCIT auf *heise.de*

Website des Whistleblower-Projekts *WCIT-Leaks*

Kommentar von Vinton Cerf in der *New York Times* vom 24. Mai 2012

Mächtige Worte

von Sören Ludwig

Bedrohungen entstehen, indem sie als solche bezeichnet werden. Dann kann die Politik »aktiv« werden, Gesetze erlassen und exekutive Maßnahmen ergreifen. Mehr und mehr scheint das Internet Teil eines solchen Prozesses der »Versicherheitlichung« zu werden.

Dieser ist in Deutschland und in den Vereinigten Staaten unterschiedlich weit vorangeschritten.

Bundesinnenminister Hans-Peter Friedrich auf der CeBIT 2012. Foto: BMI

>> »Die Welt ist weltweit vernetzt – im positiven Sinne. Sie ist dadurch aber auch weltweit verwundbar geworden.« Mit diesen Worten wandte sich der deutsche Innenminister Hans-Peter Friedrich Ende Oktober 2011 auf der Konferenz »Sicherheitspolitik und Verteidigungsindustrie« an sein Publikum und die Öffentlichkeit. Friedrich sprach von »internetbasierten Angriffen« und forderte ein »sicheres und funktionierendes Internet«. Mit dieser Analyse steht der Minister in Deutschland und der Welt nicht allein. Neuartige und komplexe Phänomene können, gerade wenn sie sich so rasch entwickeln wie das Internet, schnell als potentielle Bedrohung wahrgenommen werden. Und wenn der Mensch sich bedroht sieht, versucht er, Kontrolle über die Gefahrenquelle zu erlangen.

Der Begriff »Internet« bezeichnet ein sehr weitreichendes und diffuses Konzept, das selbst von Experten in seiner ganzen Komplexität nur schwer zu verstehen ist. In seiner ursprünglichen Form bestand das Internet lediglich aus einem Netzwerk von Computern, welches vom amerikanischen Militär zum Austausch von Daten genutzt wurde. Dieses Netz öffnete sich in den letzten beiden Dekaden des 20. Jahrhunderts dem zivilen Nutzen und hat >>

sich seitdem rasant über die ganze Welt ausgebreitet. Und auch wenn sich die inhaltliche Komponente dieses Netzwerks, der sogenannte Cyberspace, von seiner technischen Seite, dem Internet, unterscheidet: Häufig vermischen auch Politiker beide Ebenen.

Politische Reaktionen auf Gefahrenpotentiale im Internet zeugen von einer Entwicklung, die in der Politikwissenschaft als »Securitization«, als »Versicherheitlichung«, bekannt ist. Dieser Begriff wurde in den 1990er Jahren von einer Forschungsgruppe um Barry Buzan und Ole Wæver an der Universität Kopenhagen geprägt. Die so genannte Kopenhagener Schule stellte fest, dass es eigentlich keine objektiven Sicherheitsbedrohungen gebe. Vielmehr nehme eine Gesellschaft verschiedene Entwicklungen erst unter gewissen Voraussetzungen überhaupt als eine Gefahr wahr, der ein Staat durch sicherheitspolitische Maßnahmen begegnen kann und soll. So erklärte beispielsweise die Bush-Administration das Arsenal von Massenvernichtungswaffen Saddam Husseins sowie dessen Kooperation mit terroristischen Gruppierungen zu einer Bedrohung und zog diese als Rechtfertigung für eine Invasion des Iraks im Jahr 2003 heran.

Für eine solche soziale Bedrohungskonstruktion spielen Personen, die wie Staats- oder Regierungschefs und Innen- oder Verteidigungsminister über herausragende öffentliche Autorität verfügen, eine zentrale Rolle. Ihre Statements stellen nach Buzan und Wæver nicht nur bloße Kommunikation, sondern bereits politisches Handeln dar. Das lässt sich an den Aussagen des damaligen US-Außenministers, Colin Powell, in einer Rede vor den UN im Februar 2003 verdeutlichen: Er prangerte öffentlich vermeintliche irakische »Massenvernichtungswaffen und die Beteiligung des Irak an terroristischen Aktivitäten« an, sagte, dass »der Irak noch immer eine Bedrohung« darstelle und schloss seine Ausführungen mit der Androhung von »ernsthaften Konsequenzen«. Powell wollte aufzeigen, dass er die Gefahr ernst nimmt und gewillt ist, Maßnahmen zum Schutz davor in die Wege zu leiten.

Deutsche und amerikanische Spitzenpolitiker haben in den vergangenen Jahren vermehrt das Internet als Gefahr benannt und damit auch die Sicherheitspolitik beider Staaten mitgeprägt. Daher stellt sich die Frage, ob beiderseits des Atlantiks eine Versicherheitlichung des Internets stattfindet. Deutscherseits spricht dafür, dass zahlreiche Politiker in den vergangenen Jahren vornehmlich den Missbrauch des Webs für kriminelle Machenschaften und zu terroristischen Zwecken hervorhoben. So sprach der damalige Bundesinnenminister Wolfgang Schäuble zur Eröffnung der CeBIT 2008 beispielsweise von »virtuellen Terrorcamps«.

Objektive Sicherheitsbedrohungen gibt es nicht.

Diese Wahrnehmung einer Bedrohung spiegelt sich auch in den legislativen und institutionellen Neuerungen der Bundesrepublik wider. Für die Internetsicherheit in Deutschland ist vornehmlich das Bundesamt für Sicherheit in der Informationstechnik zuständig. Das 2009 in Kraft getretene »Gesetz zur Stärkung der Sicherheit in der Informationstechnik des Bundes« erweiterte dessen Kompetenzen erheblich: So war das Bundesamt beispielsweise von nun an in der Lage, Protokolldaten von ein- und ausgehender Kommunikation des Bundes zu erheben und für einen Zeitraum von bis zu drei Monaten zu speichern. Lediglich aufgrund heftigen Protests durch den Bundesbeauftragten für Datenschutz und die Informationssicherheit wurde eine Pseudonymisierungspflicht dieser Daten ins Gesetz aufgenommen.

Ferner veröffentlichte das Bundesministerium des Innern im Jahr 2011 eine neue Cyber-Sicherheitsstrategie für Deutschland, die unter anderem die Errichtung eines Nationalen Cyber-Abwehrzentrums vorsieht, das Kompetenzen verschiedener nachrichtendienstlicher und polizeilicher Behörden im Bereich der Internetsicherheit unter einem Dach vereinigt.

Auch die Bundewehr entwickelt Fähigkeiten, um feindliche Computersysteme zu infiltrieren, wie im Juni 2012 von der Financial Times Deutschland >>

berichtet wurde. Seit Ende 2011 bestünde – im Kommando Strategische Aufklärung eingegliedert – eine neue Einheit für »Computernetzwerkoperationen«. Parallel zu dieser Meldung berichteten deutsche Medien von der Entdeckung des neuesten Computerwurms »Flame«.

Unter dem Strich lassen sich so einige Tendenzen ausmachen, die auf Schritte zu einer Versicherheitlichung hindeuten. Dieser Eindruck wird dadurch bekräftigt, dass, so sehr dieser Prozess durch Kommunikation zwar öffentlich geschieht, gerade keine umfassende gesellschaftliche Debatte darüber stattgefunden hat. Eine solche Debatte müsste Statements, die das Internet als potentielle Bedrohung charakterisieren, diskursiv herausfordern. Bislang wird das Internet von der breiten Bevölkerung jedoch nicht als Sicherheitsbedrohung wahrgenommen. Es sind zumeist ökonomische und soziale Themen, die auf der Liste der gefühlten Bedrohungen in Umfragen auf den vorderen Plätzen rangieren.

Gefahr benannt, Gefahr gebannt?

Wesentlich deutlicher zeigen sich Tendenzen zur Versicherheitlichung des Internets in den USA. Auch US-Politiker sehen insbesondere nach der Verwundbarkeitserfahrung des 11. Septembers terroristische Gefahren im Netz. Sie gebrauchen auch häufiger den Begriff des »Cyber-Krieges«. So brachte beispielsweise der Staatssekretär im Pentagon, William J. Lynn, bereits 2010 zum Ausdruck, dass jeder größere Konflikt der Zukunft erhebliche Elemente der Cyber-Kriegführung beinhalten werde.

Ähnlich gefahrvoll betrachtete US-Präsident Barack Obama die Entwicklung des Internets. Bereits im Präsidentschaftswahlkampf 2008 versprach er den Bereich Cyber-Security mit größter Priorität zu behandeln. Es folgten institutionelle Veränderungen, wie zum Beispiel die Ernennung eines Cyber-Security-Beauftragten, der dem Präsidenten direkt unterstellt ist. Während die deutschen Bemühungen im Bereich Internetsicherheit hauptsächlich auf die Initiative des Bundesinnenministers zurückzuführen sind, ist in den Vereinigten Staaten vornehmlich das Pentagon einer der führenden Akteure. Durch das vor zwei Jahren eröffnete »Cyber Command« erklärte das amerikanische Verteidigungsministerium den Bereich des Cyber-Space neben den klassischen Bereichen Luft, Land, See und Weltraum dabei zu einer eigenständigen Militärdomäne. Teile des Internets werden so als ein Schlachtfeld dargestellt, welches den Regeln und Gesetzen des normalen Politikgeschehens enthoben erscheint.

Der Prozess der Versicherheitlichung des Internets scheint somit in beiden Ländern unterschiedlich weit fortgeschritten zu sein. Die USA begreifen sich nach wie vor als militärische Weltmacht, unterstreichen daher auch das militärische Potential, durch welches das Internet zur Bedrohung wird, und gehen offener mit Erweiterungen militärischer Kompetenzen und Aufgaben um. Deutschland hingegen, das sich militärisch auf seine Bündnispartner verlässt, nimmt das Internet vornehmlich als Gefahr durch Kriminalität und Terrorismus wahr. ‹‹‹‹

Sören Ludwig *studiert den Master Public Policy an der Universität Erfurt.*

Quellen und Links:

Bericht der *Washington Post* vom 27. Januar 2013

Bericht der *Financial Times Deutschland* vom 5. Juni 2012

»Strategy for Operating in Cyberspace« des US-Verteidigungsministeriums vom Juli 2011

Gesetz zur Stärkung der Sicherheit in der Informationstechnik des Bundes vom 14. August 2009

Ein alter Hut

von Michael Seibold

Cybersicherheit ist kein neues Problem – schon seit den 1960er Jahren befassen sich amerikanische Geheimdienste, Militärs und Wissenschaftler damit. >>

Ein Magnetband-Massenspeicher der US Navy von IBM, Typ 729, im Jahr 1969. Foto: US DoD

>> Keine Frage: Cybersicherheit ist eines der wichtigsten gegenwärtigen Sicherheitsprobleme, denn aufgrund ihrer zunehmenden Abhängigkeit von Informationstechnologien ist die Gesellschaft anfälliger für Cyberangriffe als jemals zuvor. Als »Stunde Null« der Cyberkriegsgeschichtsschreibung gilt oft die US-Übung »Eligible Receiver«, in der 1997 zum ersten Mal ein »Team Rot« gezielt Angriffe auf die US-Computerinfrastruktur startete. Die Übungsleitung brach die Simulation damals vorzeitig ab, so groß war der simulierte Schaden, den die Pseudohacker mit einfachsten Mitteln erzeugen konnten – das Ergebnis schien zu deprimierend, um es noch länger zu ertragen.

Stuxnet ließ 1995 schon von sich grüßen.

In einem Beitrag im Fachjournal *Intelligence and National Security* hat Michael Warner, Historiker des Pentagon, jüngst die historischen Wurzeln von Cybersicherheit aufgezeigt. Amerikanische Geheimdienste, Wissenschaftler und – mit zeitlichem Abstand – auch Politiker beschäftigen sich seit rund fünfzig Jahren mit Gefährdungen im und aus dem digitalen Raum.

In den 1960ern kam die Gefahr nicht aus dem Internet, sondern sie resultierte aus der gemeinsamen Benutzung der teuren und seltenen Computer. Großrechenmaschinen wurden stundenweise an Firmen und Einrichtungen vermietet; es fehlte aber noch an Schutzmaßnahmen, um sensible Daten vor Zugriff durch andere zu schützen. Insbesondere Experten der National Security Agency (NSA) warnten vor den Gefahren, die hieraus entstehen könnten. Untermauert wurde das Ganze durch die Entdeckung eines DDR-Spions, der Daten von Rechnern der IBM Deutschland stahl. »EDV abgezapft«, titelte 1969 der *Spiegel*.

Mit der Vernetzung von Computern stieg auch deren Verwundbarkeit. US-Verteidigungsplaner fürchteten nun um die Integrität ihrer nuklearen Steuersysteme. Neben Freizeithackern, die bald täglich und tausendfach versuchten, auf militärische Netzwerke zuzugreifen, begannen die Strategen zunehmend, ausländische Mächte zu fürchten, die die Schwächen der amerikanischen Systeme ausnutzen könnten, vorrangig, um sich Daten zu beschaffen.

In den frühen 1990ern begannen die US-Militärs, Cybertechnologie als Waffe zu begreifen. Die Luftwaffe gründete 1993 ihr »Information War Center«, Marine und Heer folgten 1994. Im Strategiepapier »Cornerstones of Economic Warfare« illustrierten 1995 hochrangige Vertreter der US Air Force, wie einfach die neuen Cyberkrieger die Kontrollsoftware von Raffinerien manipulieren und letztere damit lahmlegen könnten – Stuxnet ließ grüßen. Ein Bericht der nationalen Akademie der Wissenschaft hatte zudem bereits 1991 gewarnt: »Der moderne Dieb kann mehr mit einem Computer stehlen, als mit einer Waffe erbeuten. Die Terroristen von heute könnten mehr Schaden mit einer Tastatur anrichten als mit einer Bombe.«

Während die anfänglichen Bedenken vor allem in Expertenkreisen – Geheimdienste und Militär – die Runde machte, erlangte das Thema nach Ende des Kalten Krieges öffentliche Aufmerksamkeit. 1992 löste der Computervirus »Michelangelo« eine erste Panikwelle aus; 1996 legten Angreifer mit dem ersten bekannten »Denial of service«-Angriff den Internetzugang in New York lahm. Im gleichen Jahr setzte Präsident Bill Clinton eine Kommission zum Thema »Schutz kritischer Infrastrukturen« ein, die – unter großem medialen Interesse – noch einmal die Gefahren durch Cyberangriffe unterstrich: »Heutzutage kann der richtige Befehl die Steuerung eines Kraftwerks genauso zerstören wie ein Rucksack voller Sprengstoff; und es ist schwerer, den Angreifer zu ermitteln und festzunehmen.«

Mit der Übung »Eligible Receiver«, die alle diese Befürchtungen bestätigte, rückte das Thema 1997 dann endgültig ins Bewusstsein der höchsten Regierungskreise und der Öffentlichkeit an. Knapp dreißig Jahre später als bei den Experten. ◂◂◂◂

Quellen und Links:

Strategiepapier »Cornerstones of Information Warfare« des US Secretary of the Air Force aus dem Jahr 1995

Bericht »EDV abgezapft« im *Spiegel* vom 14. April 1969

Vom Spielzeug zum Codebrecher

von Stefan Dölling

Vom E-Mail-Konto bis zur Kritischen Infrastruktur – im digitalen Zeitalter setzen wir zur Sicherung wichtiger Daten und Netze seit langem vor allem auf Passwörter.

Doch zweckentfremdete Hochleistungsgrafikkarten gepaart mit neuen Erkenntnissen zu Mustern bei der Passwortvergabe stellen diese Praxis zunehmend in Frage. Unsere Passwörter sind nicht mehr sicher.

Nur für harmloses Vergnügen gedacht? Eine Grafikkarte vom Typ AMD Radeon 6990 Foto: AMD

>> Am 12. Oktober 2012 war die Aufregung unter den Computerspielebegeisterten Europas groß – ein schwedisches Online-Computermagazin wollte herausgefunden haben, dass die EU ab 2014 ein Verbot besonders leistungsfähiger Grafikkarten plane. Um der Erfüllung der Klimaschutzziele ein wenig näher zu kommen, sollten diese Stromfresser – derzeitige Spitzenmodelle verbrauchen unter Last mehr als 550 Watt – angeblich künftig nicht mehr als Grafikantrieb immer realistischerer Computerspiele dienen. Zur Erleichterung der Spieler stellte sich das Ganze bereits wenige Tage später als Falschmeldung heraus. Dabei gäbe es durchaus gute Gründe, einmal über Beschränkungen besonders leistungsfähiger Grafikkarten nachzudenken – sicherheitspolitische Gründe. Denn diese leistungsfähigen Rechnerbauteile eignen sich nicht nur dazu, optischen Glanz auf den Bildschirm zu zaubern, sondern können auch ganz hervorragend Passwörter knacken.

Während der Hauptprozessor eines Computers darauf getrimmt ist, möglichst viele unterschiedliche und unterschiedlich komplexe Rechenoperationen zu bewältigen, sind die Grafikchips darauf spezialisiert, vergleichsweise einfache und immer gleichartige Berechnungen wie am Fließband abzuarbei- >>

ten. Damit fehlt ihnen zwar die Flexibilität des Hauptprozessors, aber in dem, was sie tun, sind die Grafikchips hunderte Male schneller als der Computerkern. Genau das macht sie so interessant für Menschen, die fremde Passwörter mit so genannten »Brute force«-Attacken entschlüsseln wollen.

Die etwas martialische Bezeichnung – »brute force« bedeutet wörtlich »rohe Gewalt« – rührt daher, dass hier wenig Finesse im Spiel ist. Eine entsprechende Software probiert einfach so lange alle möglichen Passwortkombinationen durch, bis die richtige gefunden ist. Theoretisch kann mit dieser simpel-brutalen Methode jedes Passwort irgendwann geknackt werden. Je länger und komplexer das angegriffene Codewort ist, desto mehr mögliche Varianten müssen allerdings durchprobiert werden und desto länger dauert folglich die Suche nach der richtigen Kombination.

Mit Grafikkarten und roher Gewalt Passwörter knacken

Kurze und wenig komplexe Passwörter, wie zum Beispiel die vierstellige Geheimzahl der EC-Karte mit ihren theoretisch 10.000 verschiedenen Kombinationen, sind daher nicht sonderlich sicher und könnten selbst von einem Smartphone-Prozessor praktisch sofort gebrochen werden. An einem typischen achtstelligen Passwort aus Groß- und Kleinbuchstaben und Zahlen mit seinen 218 Billionen (10^{12}) möglichen Varianten würde ein aktueller Vierkern-Hauptprozessor, etwa aus der Intel i7-Reihe, hingegen deutlich länger rechnen. Mit seinen rund 20 Millionen Versuchen pro Sekunde würde er bei einer reinen »Brute-Force«-Attacke beispielsweise das Passwort »Inge1967« nach 126 Tagen gebrochen haben. Enthielte das Passwort bei acht Stellen zusätzlich noch ein typisches Sonderzeichen – wie in »Inge196%« – so bräuchte der Prozessor ganze 23 Jahre, um alle 7,2 Billiarden (10^{15}) Kombinationen durchzuprobieren. Achtstellige Passwörter mit Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen galten daher bislang als relativ sicher.

Das hat sich geändert, da heutige Hochleistungsgrafikkarten die für »Brute-Force«-Attacken notwendigen Berechnungen drastisch schneller abwickeln können als Hauptprozessoren. So schafft eine ältere Grafikkarte des Typs »Radeon 6770«, derzeit erhältlich für unter 100 Euro, schon fast 200 Millionen Versuche pro Sekunde – und knackt »Inge196%« damit in etwas mehr als einem Jahr. Investiert man rund 800 Euro in das Topmodell dieser älteren Reihe, die »Radeon 6990«, so liegt das Passwort bei 772 Millionen Versuchen pro Sekunde bereits nach 107 Tagen offen.

Eine Eigenart der neueren Grafikkarten ist zudem, dass man mehrere Exemplare in Reihe schalten kann. Während Computerspieleenthusiasten diese Möglichkeit gerne dazu nutzen, noch mehr Grafikleistung zu erzielen, brechen Hacker und »Penetration-testing«-Spezialisten Passwörter so noch

PENETRATION-TESTING

Als »Penetration-Testing« oder kurz »Pen-Testing« werden alle Aktivitäten bezeichnet, bei denen Hacker, beispielsweise im Auftrag einer Firma, versuchen, in deren Systeme einzudringen oder ihre Passwörter zu brechen. Die so entdeckten Sicherheitslücken können dann beseitigt werden, bevor Cyberkriminelle sie nutzen können.

DAS MOORESCHE GESETZ

Der Physiker und Intel-Mitbegründer Gordon Moore sagte 1965 voraus, dass sich die Leistung integrierter Schaltkreise auf Grund des technischen Fortschritts in Zukunft jährlich verdoppeln würde. Angesichts neuerer Daten hat Moore selbst 1975 den Zeitraum auf etwas weniger als zwei Jahre korrigiert.

>>

schneller. Ein System aus drei »Radeon 6990« berechnet beispielsweise 2.094 Millionen mögliche Passwörter pro Sekunde und knackt »Inge196%« so in unter 40 Tagen, die Variante ohne Sonderzeichen in knapp 29 Stunden. Passwörter mit weniger als sieben Stellen fallen bei Einsatz dieser Technik in wenigen Minuten oder gar Sekunden!

Bei einem Preis um 3.000 Euro dürften die wenigsten Otto-Normalbürger derzeit ein solches System besitzen. Da sich allerdings nach »Moores Gesetz« etwa alle 20 Monate die Leistung von Prozessoren verdoppelt, ist es bei derzeitigem Stand nur eine Frage der Zeit, bis komplexe achtstellige Passwörter von jedem Kinderzimmer mit Spiele-PC aus in wenigen Stunden gebrochen werden können und auch neunstellige Passwörter in Gefahr geraten. Und weil die entsprechenden Programme wie »Hashcat« oder »Cain&Abel« samt ausführlichen Anleitungsvideos im Netz frei verfügbar sind, wird diese Fähigkeit künftig auch technischen Laien problemlos offen stehen.

348 Milliarden Versuche pro Sekunde: Professionelle Systeme wie dieses von Jeremi Gosney mit insgesamt 25 Grafikkarten brechen »Inge196%« in weniger als sechs Stunden.

Foto: Jeremi M. Gosney

Abhilfe schaffen nur längere, komplexe Passwörter mit derzeit mehr als zehn Stellen. Hier lauert aber schon das nächste Problem, denn während sich beispielsweise »$Inge1967%« noch relativ einfach merken lässt und mit seinen zehn Stellen, Groß- und Kleinbuchstaben, Sonderzeichen und Zahlen theoretisch auf 66,4 Trillionen (10^{18}) mögliche Kombinationen kommt, ist dieses Passwort in Wirklichkeit deutlich schwächer.

Könnten Sie sich ein Passwort wie »2&%-_mI0o-4« merken?

Denn in den vergangenen Jahren gelangten durch schlecht gesicherte Server bei Dating-, Social-Media- und Informationsdiensten mehrfach millionenfach Passwortdaten an die Öffentlichkeit. Die Analyse solcher Passwörter, beispielsweise von den Microsoft-Forschern Dinei Florêncio und Cormac Herley, konnte gebräuchliche Muster bei der Passworterstellung identifizieren, welche Nutzer bewusst oder unbewusst weltweit anwenden. So sind beispielsweise Kombinationen aus Namen und Geburtstagen – so wie »Inge1967« – immer noch sehr häufig. Und sofern Sonderzeichen überhaupt verwendet werden, tauchen sie gemeinhin am Anfang oder am Ende des Passworts auf. Dadurch werden solche Passwörter allerdings deutlich schwächer, da zum Brechen nun nicht mehr alle möglichen Kombinationen probiert werden müssen.

Typische Programme zum Knacken von Passwörtern verlassen sich daher nicht mehr allein auf »rohe Gewalt«, sondern testen anhand der erkannten Muster zunächst gängige Kombinationen mit Hilfe von Wörterbüchern, Namenslisten sowie üblicherweise den Zahlen, die gängigen Geburtsdaten entsprechen. Anstelle von etwa 1.007 Jahren, welche das System mit drei Rade- >>

on 6990 für »$Inge1967%« theoretisch brauchen würde, wäre das Passwort – wie auch alle anderen genannten Beispielpasswörter – so vermutlich innerhalb von Sekunden oder Minuten gebrochen worden.

Nur wirklich zufällig erstellte Passwörter, die keine gebräuchlichen Wörter, Namen oder Jahreszahlen enthalten, haben gegen diese Angriffe überhaupt eine Chance. Doch wer könnte sich beispielsweise ein Passwort wie »2&%-_mI0o-4« merken? Und das, da man ja für jedes E-Mail-Konto, jede Social-Media-Plattform und jeden Rechner idealerweise ein separates Passwort hat, gleich noch mehrfach? Im Alltag werden solche sicheren Passwörter schnell erst zum Hindernis, dann zum Ärgernis und landen schließlich – sichtbar für jedermann – per Post-it am Bildschirmrand oder als Notiz auf der Schreibtischunterlage. Das dies der Sicherheit nicht unbedingt zuträglich ist, erschließt sich von selbst. Mit fortschreitender Leistungsfähigkeit der Technik, wenn in naher Zukunft zwölf oder vierzehnstellige Passwörter zum Mindeststandard werden (müssten), wird dieses Problem nicht kleiner werden.

Es ist daher an der Zeit, einmal grundsätzlich darüber nachzudenken, ob und wie Passwörter mittel- und langfristig im Alltagsbetrieb überhaupt noch sinnvoll für die Absicherung von Daten, Konten und Netzwerken genutzt werden können. Und höchste Zeit, einmal die eigenen Passwörter zu überprüfen und gegebenenfalls den heutigen Erfordernissen anzupassen. ◂◂◂◂

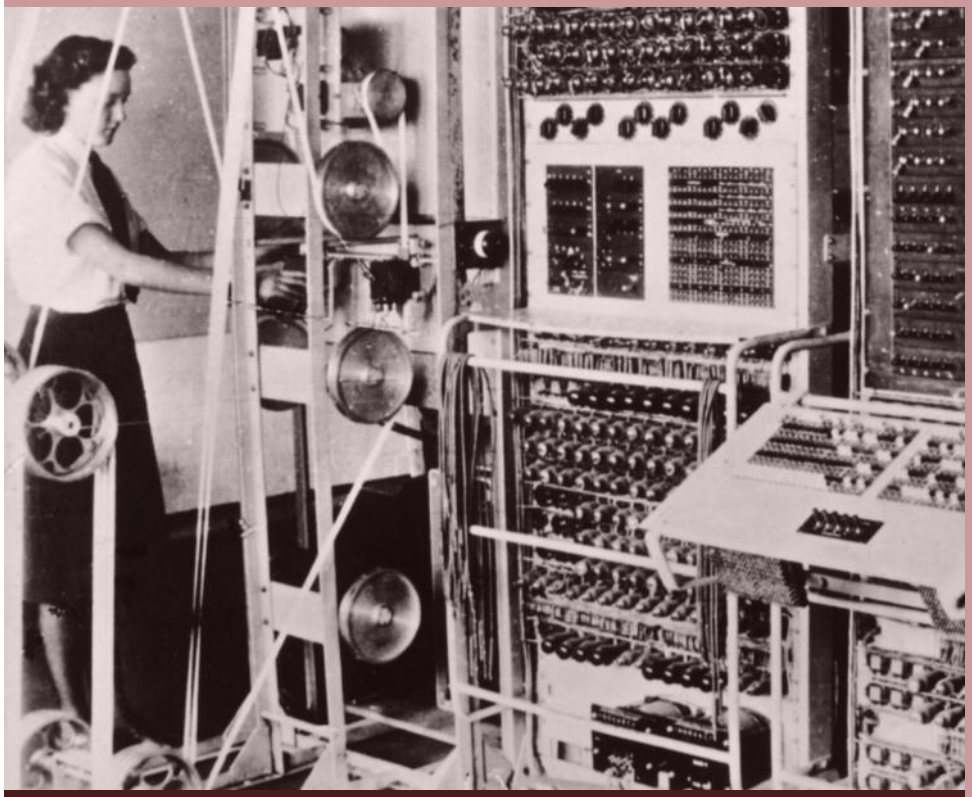
Quellen und Links:

Informationsseite des Bundesamts für Sicherheit in der Informationstechnik zu sicheren Passwörtern

Übersicht zur Sicherheit von Passwörtern auf *Lockdown.co.uk*

Hintergrundbericht auf *arstechnica.com* vom 21. August 2012

Bericht der BBC über den Codebrecher »Colossus« vom 2. Februar 2010



Gigantische Anfänge: Zu Zeiten des Zweiten Weltkriegs konnte nur eine Großmacht wie Großbritannien in großem Maßstab Codes knacken. »Colossus« war der erste Computer, der für nur eine Aufgabe bestimmt war: deutschen Funkverkehr dechiffrieren. Foto: National Archives UK

Akkord unbefriedigend

von Nedife Arslan

Mit der 2001 unterzeichneten »Convention on Cybercrime» des Europarats haben insgesamt 48 Staaten den Kriminellen im Netz den Kampf angesagt. Sie verpflichten sich darin, ihren Strafverfolgungsbehörden umfangreiche Befugnisse zum Abhören der Kommunikation via Internet und zum grenzüberschreitenden Datenaustausch einzuräumen.

Doch bis heute ist ein Rückgang der Computerkriminalität nicht feststellbar – während Bürgerrechte in Gefahr geraten.

Foto: MPD01605 / lizensiert gemäß CC-AS 2.0 Generic

>> Als Reaktion auf die seit Jahren steigende Computerkriminalität unterzeichneten die 26 Länder des Europarats sowie die USA, Kanada, Japan und Südafrika im Jahr 2001 die »Convention on Cybercrime«. Ziel der Konvention war es, zur Bekämpfung der zunehmenden Computerkriminalität wirksame, länderübergreifende Standards für die länderspezifischen Computerstrafrechtsregelungen zu vereinbaren. Dabei wurde in Kauf genommen, dass wichtige Rechte wie die Informationsfreiheit und das Recht auf Privatsphäre im Netz eingeschränkt werden.

Die Notwendigkeit für ein solches, internationales Abkommen ergab sich aus einer einfachen Beobachtung: Ohne Computer und Internet funktionieren viele Bereiche in Gesellschaft und Wirtschaft heutzutage einfach nicht mehr. Ob nun unterwegs mit dem Smartphone, dem Tablet oder daheim mit dem Computer: Ende 2011 nutzten weltweit gut 2,1 Milliarden Menschen das Internet. Dies ist im Vergleich zu 2000 mit gut 360 Millionen Internetnutzern eine siebenfache Steigerung innerhalb eines Jahrzehnts! Ob Online-Banking, Online-Shopping oder E-Mails – zentrale Aspekte des täglichen Lebens erledigen wir heute im Netz, mit einem Mausklick weiß ich als Bürger, was genau >>

zur selben Zeit an anderen Orten der Welt geschieht. Die Vorzüge von Computer und Internet liegen auf der Hand: die Möglichkeit der weltweiten Kommunikation und der Zugang zu einer historisch einmaligen Bandbreite an Informationen. Wo aber viel Licht ist, sind auch die Schatten tief.

Mit »Cybercrime«, also der Kriminalität im digitalen Raum verknüpfte Begriffe wie Spam, Virus, Phishing und Cyber-Angriff haben nicht ohne Grund mittlerweile Einzug in die Alltagssprache gefunden und sorgen für Verunsicherung beim einzelnen Nutzer aber auch der Wirtschaft und beim Staat. So stieg allein in Deutschland die Zahl der polizeilich erfassten Fälle von Computerkriminalität von 1995 mit 27.902 Fällen bis 2011 auf 84.981 Straftaten. Dies hat auch gravierende finanzielle Folgen für viele Unternehmen. Einer Studie von Hewlett-Packard zufolge, beträgt der jährliche Schaden für deutsche Unternehmen gut 4,8 Millionen Euro, für US-amerikanische Unternehmen gar 6,9 Millionen Euro. Die Dunkelziffer dürfte hingegen um ein Vielfaches höher sein, da erfahrungsgemäß nur wenige Unternehmen Cyberattacken – und damit Schwächen in ihrer IT-Infrastruktur – öffentlich machen. Die Tendenz ist steigend. Der Präsident des Bundesamtes für Sicherheit in der Informationstechnik (BSI), Michael Hange, nennt die Computer- und Internetkriminalität daher auch eine »massive Bedrohung«.

Viele Staaten haben diese Kriminalitätsphänomene und die Folgen für Bürger, Unternehmen und Staat erkannt, nationale Strategien entwickelt und gehen dagegen vor. Anders als bei der traditionellen Kriminalität erfordert die Bekämpfung der virtuellen Variante mit ihrem transnationalen Charakter allerdings eine internationale Herangehensweise. Denn wenn, um nur ein Beispiel zu nennen, Islamisten oder Rechtsradikale von im Ausland stehenden Servern über das Internet ihre – in Deutschland unter Strafe gestellte – Propaganda verbreiten oder zu Straftaten aufrufen, dann stoßen rein nationale Strukturen der Strafverfolgung oft schnell an ihre Grenzen. Die Notwendigkeit internationaler Regelungen und Abkommen zur besseren Kooperation der Zusammenarbeit auf diesem Sektor ist augenfällig.

Das erste und bis dato auch einzige international verbindliche Rechtsabkommen für den Bereich der digitalen Kriminalität ist die » EU Convention on Cybercrime«. Primär dient sie den Unterzeichnerstaaten als gemeinsame Leitlinie bei der Ausarbeitung der jeweiligen nationalen Gesetzgebungen gegen Computerkriminalität. Bereits in der Präambel ist das Ziel der Konvention festgeschrieben: »protection of society against cybercrime« – der Schutz der Gesellschaft vor Cyberkriminalität.

Um 304.5 Prozent in sechs Jahren ist die Cyberkriminalität in Deutschland gewachsen.

Dabei werden aber für jeden Bürger grundsätzliche Fragen aufgeworfen. Wollen Sie zum Beispiel, dass Geheimdienste und staatliche Behörden im In- und Ausland in Zukunft wissen, wann Sie online waren und welche Seiten Sie zu welcher Zeit besucht haben? Die »Convention on Cybercrime« macht dies möglich. Sie geht sogar noch einen Schritt weiter: Diese Aktivitäten sollen schriftlich dokumentiert und die gesammelten Daten für eine Vielzahl in- und ausländischer Behörden verfügbar gemacht werden. Daher ist die Konvention unter Menschenrechtlern und Datenschützern höchst umstritten, obwohl die Wahrung einer Balance zwischen den Anforderungen einer wirksamen Strafverfolgung auf der einen und von Freiheits- und Menschenrechten auf der anderen Seite explizit in die Konvention aufgenommen wurde: »respect for fundamental human rights«.

Aus Sicht der Datenschützer ist dabei insbesondere der Artikel 16 der Konvention problematisch. Demnach sind gespeicherte Computerdaten längstens 90 Tage vom Dienstanbieter vorzuhalten, damit bei einem eventuellen Kriminalfall mithilfe üblicher Ermittlungs- und Rechtshilfemaßnahmen durch die Strafverfolgungsbehörden auf diese Daten zugegriffen werden kann. Auch eine >>

Verlängerung der Speicherung ist auf Wunsch einer Vertragspartei möglich. Außerdem haben die Vertragsstaaten nationalstaatliche Möglichkeiten für eine Echtzeitüberwachung nicht nur der Verkehrs- beziehungsweise Verbindungsdaten – also wer wann mit wem kommuniziert – sondern auch der Inhalte dieser Kommunikation zu schaffen. Die Konvention ermöglicht es außerdem, dass von Dienstanbietern eine ganze Reihe persönlicher Informationen – beispielsweise Namen, Adresse, Telefonnummer und Kontoverbindungsdaten – über ihre Kunden an die Strafverfolgungsbehörden herausgegeben werden müssen. Und dies bereits beim bloßen Anfangsverdacht einer Straftat.

Der Bundesbeauftragte für Datenschutz, Peter Schaar, sieht diese Entwicklung kritisch: »Gerade im Kampf gegen den Terrorismus werden die Grenzen immer mehr verlagert. Wir gehen mit hoher Geschwindigkeit in Richtung gläsernen Bürger. Ich fürchte um unseren Rechtsstaat«.

Der »Hackerparagraf« ist ein zweischneidiges Schwert.

Neben diesen grundsätzlichen Einwänden stellte sich zudem schnell heraus, dass auch die Umsetzung der Konvention in nationales Recht der Unterzeichnerstaaten nicht völlig problemlos verlaufen würde und zum Teil erhebliche Unterschiede festzustellen waren. So haben sich beispielsweise die USA, welche die Cybercrime-Konvention 2006 ratifizierten, einem Zusatzprotokoll des Abkommens nicht angeschlossen, das unter anderem die Verbreitung rassistischer Propaganda unter Verbot stellt. Denn dann müssten die US-Strafverfolger gemäß der Konvention auch gegen eigene Bürger ermitteln, selbst wenn die ihnen zur Last gelegte Tat nach nationalem US-Recht nicht strafbar wäre. Dies ist einer der Gründe, warum gerade Staaten wie die USA, aber auch Russland oder China erhebliche Vorbehalte dagegen haben, anderen Staaten in solchen Fällen im Sinne der Konvention Unterstützung bei der Strafverfolgung zu gewähren.

In anderen Fällen schoss man bei der Umsetzung der Konvention zum Teil weit über das Ziel hinaus – was dann nicht mehr, sondern weniger digitale Sicherheit zur Folge hatte. So wurde beispielsweise in Deutschland mit dem im Mai 2007 im Bundestag mit großer Mehrheit verabschiedeten »Hackerparagrafen« – Paragraf 202c des Strafgesetzbuches, Vorbereiten des Ausspähens und Abfangens von Daten – Artikel 6 der Konvention in nationales Recht umgesetzt. Das Gesetz stellt unter anderem die Herstellung und die Verbreitung so genannter »Hackertools« unter Strafe. Sicherheitsexperten kritisierten das Gesetz bereits im Vorfeld, da es nicht klar definiert, welche Software genau in Zukunft illegal sein sollte. Es wurde außer Acht gelassen, dass Software zum »Ausspähen und Abfangen von Daten« gleichzeitig auch dazu genutzt werden kann, die Sicherheit eines Systems zu testen um dann Angriffe besser abwehren zu können. Die Unterscheidung zwischen Hackertool und Sicherheitswerkzeug kann in der Realität daher eigentlich erst in Verbindung mit der Intention des Nutzers getroffen werden. Da das Gesetz dies nicht ausdrücklich vorsieht, sahen sich IT-Sicherheitsexperten in Deutschland mit Inkrafttreten des Gesetzes ihrer Arbeitsmittel beraubt – oder mit einem Bein im Gefängnis. Ein Beleg für die Problematik dieser nationalen Umsetzung der Konvention war die unmittelbar nach Inkrafttreten 2007 wegen Verstoß gegen Paragraf 202c erstattete Strafanzeige – gegen das BSI.

Zudem zeigt die Entwicklung seit der Verabschiedung der Konvention, dass die Kriminalität im Netz trotz allem weiter ansteigt. Ein reines Verbot von »Hackertools« schreckt die eigentlichen Kriminellen offenbar nicht ab. Wichtige Faktoren, welche Cyberkriminalität oft überhaupt erst ermöglichen – beispielsweise zum Teil gravierende Sicherheitsmängel in Netzen und Systemen oder der leichtsinnige Umgang vieler Nutzer mit persönlichen Daten – werden von der Konvention überhaupt nicht berührt. Wie in fast allen Feldern der Kriminalitätsbekämpfung wäre allerdings Vorbeugung das vermutlich wirksamste Mittel – beispielsweise durch die gesetzliche Verpflichtung von Netzbetreibern und Softwareherstellern auf Sicherheitsmindeststan- >>

dards ihrer Produkte und Netze oder die bessere Information der Nutzer über den sicheren Umgang mit dem Internet.

Die Herstellung von Sicherheit vor digitaler Kriminalität und die Bekämpfung von rassistischen und menschenverachtenden Inhalten im Netz sind erhebliche globale Probleme, die es zu meistern gilt. Letztlich ist die Abwägung zwischen den beiden Extremen »Freiheit« und »Sicherheit« eine enorm schwierige Aufgabe. Mit der massiven Einschränkung von jahrhundertelang erkämpften Freiheits- und Bürgerrechten wird das tatsächliche Problem aber nicht zu lösen sein. Daher liefert die Konvention des Europarates letztlich keine befriedigenden Lösungen für die Herausforderung durch Cyberkriminalität, da das hier hergestellte Mehr an Sicherheit fast zwangsweise zu einem erheblichen Verlust von Freiheit führt. Und kaum jemand dürfte sich wünschen, dass Vater Staat einem beim Schreiben einer einfachen E-Mail über die digitale Schulter schaut. Das Internet ist kein rechtsfreier Raum. Es darf auch kein bürgerrechtsfreier Raum werden. ◂◂◂◂

Nedife Arslan *hat 2011 ihren Master in »Europäische Studien« an der Universität Osnabrück abgeschlossen.*

Quellen und Links:

Studie von Hewlett-Packard zu den Kosten von Cyberkriminalität vom Oktober 2012

Stellungnahme des Chaos Computer Club e.V. vom 21. Juli 2008 zu Paragraf 202c des Strafgesetzbuchs

Informationsseite des Chaos Computer Club e.V. zur »Convention on Cybercrime« des Europarats

Text der »Convention on Cybercrime« des Europarates vom 23. November 2001

Spätzünder

von Andrea Pretis

Jahrzehntelang hatte die Nato klar umrissene Gegner, die sie mit der Abschreckungswirkung realer Waffen im Zaum halten konnte. Nun muss das Verteidigungsbündnis auf schwer fassbare, doch zum Teil folgenreiche Angriffe aus dem Cyberspace reagieren. Erst vor wenigen Jahren ist die neuartige Bedrohung ganz oben auf der Agenda der Allianz angekommen.

Rechtzeitig reagiert? Nato-Generalsekretär Anders Fogh Rasmussen erklärt auf dem Gipfel von Lissabon 2010 das neue strategische Konzept des Bündnisses Foto: Nato

>> Spätestens mit dem Cyber-Angriff auf den Nato-Mitgliedstaat Estland im April 2007 hat beim Verteidigungsbündnis ein Bewusstseinswandel eingesetzt. Es war ein Schock, dass Cyber-Attacken – in diesem Fall ein sogenannter Distributed Denial of Service (DDoS) -Angriff – in der Lage waren, die Server und Internetseiten wichtiger staatlicher Institutionen sowie Banken und Telekommunikationsfirmen tagelang lahmzulegen und somit das Leben einer ganzen Nation zum Stillstand zu bringen. Bis zu einer Million »fremdgesteuerte« Computer in 75 verschiedenen Ländern hatten estländische Server und Internetseiten mit permanenten Datenanfragen gezielt überlastet und außer Gefecht gesetzt.

Ein Jahr später verdeutlichte ein Cyber-Angriff im Zuge des Georgien-Kriegs der Allianz, dass Cyber-Attacken auch Bestandteil militärischer Kriegführung sein können. Ähnlich wie bei zuvor bei dem Angriffen auf Estland, wurden georgische Server und Internetseiten lahmgelegt, jedoch mit dem Unterschied, dass sich das Land zu diesem Zeitpunkt in einem Krieg befand, dem so genannten Fünftagekrieg mit Russland. >>

Bereits 2002 hatten sich die Regierungschefs der Nato in Prag als Reaktion auf eine Cyber-Attacke während der Operation »Allied Force« im Kosovo – pro-serbische Hacker hatten versucht, die Nato mit Cyber-Angriffen zu schwächen – geeinigt, ein Cyber-Verteidigungsprogramm ins Leben zu rufen. Bis zu dem Vorfall in Estland war man davon ausgegangen, dass Cyber-Angriffe nur beschränkten Schaden anrichten könnten und technische Lösungen zu dessen Behebung ausreichend wären. Binnen weniger Jahre hatte die Abhängigkeit öffentlicher, militärischer und wirtschaftlicher Infrastrukturen von leicht verwundbaren Kommunikationssystemen jedoch dermaßen zugenommen, dass Cyber-Angriffe auf diese Systeme nicht mehr nur rein technisch zu lösen und zu beantworten sind.

Darüber hinaus wurde dem Militärbündnis klar, dass es nicht genügte, sich nur auf den Schutz Nato-eigener Netzwerke zu konzentrieren. Auch eine Strategie zum Schutz der Kommunikationssysteme der einzelnen Mitgliedstaaten war dringend erforderlich geworden. Die Allianz brauchte auf politischer Seite dringend eine offizielle Position beziehungsweise Strategie, wie sie auf Cyber-Angriffe in Zukunft reagieren würde – und aus technischer Sicht bessere Kapazitäten, um auf Angriffe auf Strukturen der Nato und ihrer Mitgliedstaaten antworten zu können.

Deshalb stellten die Nato-Regierungschefs in Bukarest 2008 und in Lissabon 2010 die Weichen dafür, die bisherige Cyber-Verteidigungs-Policy zu überarbeiten und effektiver zu machen. Das neue Strategische Konzept der Nato, das in Lissabon beschlossen wurde, hat zum Ziel, die Fähigkeit des Bündnisses weiter zu entwickeln, Cyber-Attacken zu verhindern und sie zu entdecken, sich gegen sie zu verteidigen und ihre Schäden wieder beheben, »including by using the Nato planning process to enhance and coordinate national cyber-defence capabilities, bringing all Nato bodies under centralized cyber protection, and better integrating Nato cyber awareness, warning and response with member nations.«

Darüber hinaus betont das Konzept das erhöhte Gefahrenpotential von Cyber-Angriffen für das Bündnis und die Bevölkerung seiner Mitgliedstaaten: Diese Bedrohung gehe sowohl von staatlichen Akteuren – wie Militär oder Geheimdienste – als auch von nicht-staatlichen Akteuren – wie organisierte Kriminalität, Terroristen und Extremisten – aus.

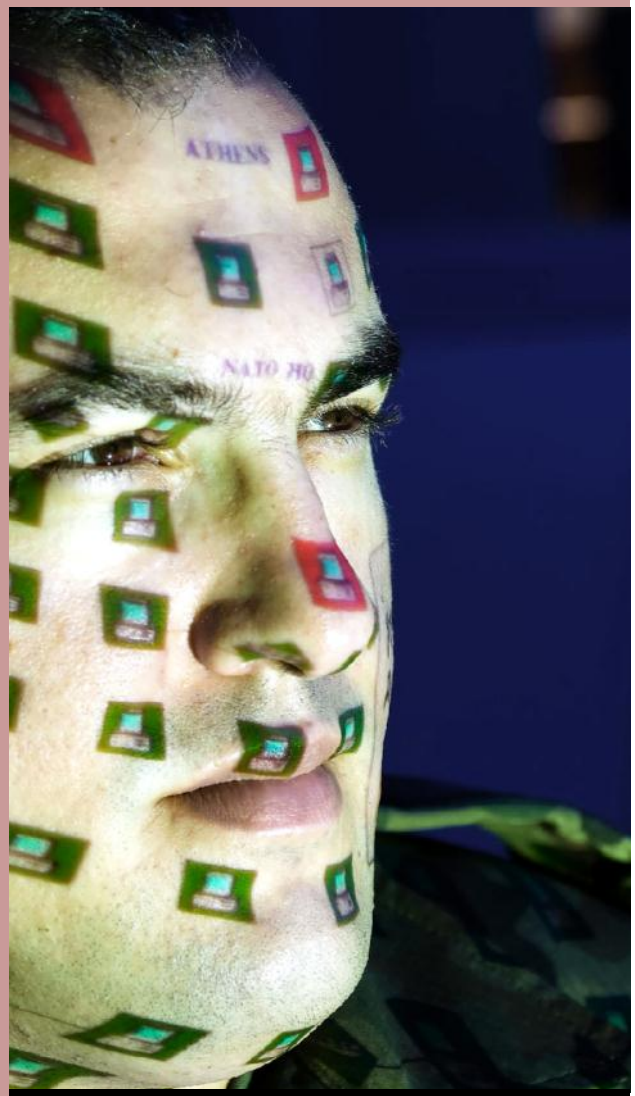
Entsprechend den Leitlinien des Strategischen Konzepts von 2010 vereinbarten die Verteidigungsminister der Nato-Partner am 8. Juni 2011 eine überarbeitete »cyber defence policy« zusammen mit einem Aktionsplan zu deren Implementierung. Dieses neue Cyber-Verteidigungsprogramm unterscheidet – anders als vorherige – klar zwischen operativen und politischen Mechanismen bei der Reaktion auf Angriffe aus der Netzwelt.

Erst ab Anfang 2013 sollen die Nato-Netzwerke rund um die Uhr geschützt sein.

Der letzte Nato-Gipfel in Chicago im Mai 2012 hat dieses derzeit geltende – aber in seinen Einzelheiten nicht öffentlich einsehbare – Programm mit dem Fokus auf folgende zwei Aspekte nochmals bekräftigt:

1. Der Schutz aller Nato-Strukturen, also auch derjenigen, die sich außerhalb des Bündnisterritoriums befinden, was etwa bei Auslandseinsätzen der Fall ist, soll zentralisiert geschehen. Nationale Strukturen, die Nato-Informationen verarbeiten oder Zugang zu diesen haben, müssen in Zukunft gewisse Minimalstandards erfüllen, die sich allerdings noch in der Entwicklung befinden.

2. Die neue Policy hält die Mitgliedstaaten an, beim Schutz kritischer nationaler Infrastruktur eng mit der Nato zusammenarbeiten, wobei auf Prävention, Belastbarkeit und die Vermeidung von Doppelstrukturen ihrer Kommunikations- >>



Im Nato INFOSEC Technical Centre in Mons, Belgien Foto: Nato

und Informationssysteme besonderer Wert gelegt werden soll.

Was den ersten Aspekt betrifft, so befinden sich die Nato-eigenen Strukturen der Cyber-Abwehr weiterhin im Aufbau. Nach mehrjähriger Umstrukturierung ist nun das Cyber Defence Management Board (CMDB) das zentrale Experten-Gremium, das die Partnerstaaten in technischen und politischen Fragen berät sowie den Informationsaustausch und das Management bereits bestehender Cyber-Verteidigungseinheiten koordiniert. Das CMDB entwickelt daneben operationelle Konzepte, führt Simulationen durch und unterhält Kontakte zu wichtigen Partnern wie zu internationalen Organisationen, zum Privatsektor oder zur Wissenschaft.

Die im Juli geschaffene »Communication & Information Agency« ist für die technische Seite der virtuellen Verteidigung zuständig. Ihr untersteht die »Nato Computer Incident Response Capability« (NCIRC), die für die Erkennung und Abwehr von Cyber-Angriffen auf die Netzwerke der Allianz zuständig ist. Der Aufbau dieses Elements des zentralisierten Sicherheitsmanagements hat vor zehn Jahren begonnen und sollte Anfang 2013 fertig gestellt werden. Erst dann werden die Nato-Netzwerke umfassend, also rund um die Uhr, geschützt sein. Die Zeit läuft, denn laut Generalleutnant Kurt Herrmann, Direktor der »Nato Communication and Information Systems Services Agency«, ließe sich »eine quantitative, aber auch qualitative Zunahme« der Cyber-Angriffe auf die Nato beobachten, meist durch E-Mails, die von Schadsoftware infiziert seien.

Trotz stärkerer Koordination unter den Partnerstaaten und der Aufnahme von Cyber-Verteidigung in den Verteidigungsplanungsprozess der Nato, bleiben ihre Mitglieder in erster Linie selbst dafür verantwortlich, ihre nationalen Kommunikations- und Informationssysteme zu schützen. Um den Informationsaustausch, die Lageerkennung und die Interoperabilität zwischen den Mitgliedstaaten und den bündniseigenen Strukturen zu optimieren, vereinbaren die nationalen Cyber-Abwehr-Behörden mit dem CMDB entlang eines Rahmenplans der Allianz gemeinsame Absichtserklärungen. Dies soll auch die Fähigkeit der Nato verbessern, im Falle eines konkreten Hilfsgesuchs eines oder mehrerer Partnerstaaten koordinierte Hilfe zu leisten.

Neben der strategischen, strukturellen und operativen Anpassung der Nato an die sich rasant wandelnden Herausforderungen der Cyber-Welt ist die wohl kritischste Frage der Allianz, ab welcher Schwere ein Cyber-Angriff den Bündnisfall nach Artikel 5 des Nordatlantikvertrags auslöst. Dafür gibt es bisher keine eindeutigen Kriterien, sondern lediglich das vertragliche Erfordernis, einstimmig den Bündnisfall im Nordatlantikrat auszurufen. »A cyber attack invokes individual and collective self-defense if it rises to the threshold of an ›armed attack‹«, ordnet Rechtsexpertin Eneken Tikk vom Nato Cooperative Cyber Defence Centre of Excellence in Tallinn die Vo- >>

raussetzungen für einen bewaffneten Gegenangriff der Allianz im Verteidigungsfall rechtlich ein. »The assessment of whether a cyber attack is, by its effects, consequences or nature, equivalent to such an attack will be made by national authorities or, for collective action, by international partners.« Laut Tikk könne ein militärischer Gegenschlag dann legal sein, wenn er notwendig wäre, um dem Cyber-Angriff ein Ende zu setzen, und in seiner Art sowie in seinen Auswirkungen verhältnismäßig wäre.

Folgt man dem klassischen Abschreckungsprinzip, scheint es fraglich, ob diese abstrakten Kategorien – gekoppelt mit dem Erfordernis des politischen Konsens – für in der Regel asymmetrisch angreifende und schwer identifizierbare »Cyber-Krieger« abschreckend wirken. Voraussichtlich ist eher das Gegenteil der Fall: Virtuelle Angreifer haben bestenfalls mit »deterrence by denial« zu rechnen, wenn ihre Attacken technisch von den Angegriffenen erkannt und sie dementsprechend abgewehrt werden können. Die Nato selbst besitzt derzeit auch keine offensiven virtuellen Cyber-Kapazitäten, die nötig wären, um einen Cyber-Angriff zu vergelten – im Sinne einer »deterrence by punishment«. Während bei »deterrence by denial« also etwa nur das Eindringen von Schadsoftware erkannt und verhindert wird, würde bei »deterrence by punishment« der Angreifer einen Gegenangriff zu befürchten haben. Einzelne Mitglieder arbeiten an der Entwicklung solch offensiver Möglichkeiten und könnten sie der Allianz in einem schwerwiegenden Fall zur Verfügung stellen . ◂◂◂◂

Ein Cyberangriff wird zum »bewaffneten Angriff«, wenn die Betroffenen es so bestimmen.

Andrea Pretis *hat 2010 in Berlin ihren Master der Internationalen Beziehungen erworben und arbeitet als Ausschuss-Koordinatorin bei der Parlamentarischen Versammlung der Nato in Brüssel.*

Quellen und Links:

Webpräsenz des Nato Cooperative Cyber Defence Centre of Excellence

Vincent Joubert: »Five years after Estonia's cyber attacks: lessons learned for Nato?«, Forschungspapier des Nato Defence College vom Mai 2012

Bericht: »Nato kämpft gegen Flut von Cyber-Attacken« des *Spiegel* am 25. April 2012

Bericht »Nato Doesn't Yet Know How To Protect Its Networks« im Blog *Danger Room* vom 1. Februar 2012

Eneken Tikk: »Ten Rules for Cyber Security«, in der *Survival*, Ausgabe 3/2011

Thomas Michael Jopling: »Information and National Security«, Bericht 171 CDS 11 E rev. final vom Oktober 2011

Infoblatt »Nato Policy on Cyber Defence« vom September 2011

»Nato Strategic Concept« vom 19./20. November 2010

Der falsche Zuständige

von Julian Schibberges

Kann die Nato im Zeitalter des Cyberwar ihre Aufgaben erfüllen? Gelang ihr im Kalten Krieg noch, Verteidigung flächendeckend glaubwürdig zu machen, lässt sich das heute bezweifeln.
Ein anderer Sicherheitsakteur bietet sich aber an: Europa.

Diffuses Ziel Infrastruktur: Kraftwerk in Datteln

Foto: E.ON

>> »Bedingt abwehrbereit« sei die Bundeswehr, so das kritische Urteil der Nato anlässlich der Übung Fallex 62, die niedrigstmögliche Bewertung der Einsatzbereitschaft. Zum 50. Jubiläum der Spiegel-Affäre, die durch den gleichlautenden Artikel im *Spiegel* angestoßen wurde, hätte man vergangenes Jahr das gleiche Urteil auch über die Nato und ihre Fähigkeit, auf Cyberangriffe zu reagieren, fällen können. Anders als damals hat dieses Urteil jedoch wenig mit den Anstrengungen zu tun, die das Bündnis in diesem Feld unternimmt, als vielmehr mit den institutionellen Begrenzungen der Nato, die es ihr nur unzulänglich ermöglichen, auf die Herausforderungen, vor die Cyberwar die Staatengemeinschaft stellt, einzugehen.

Die Nato hat mit der Cyber Defense Management Authority (CDMA), dem Cooperative Cyber Defence Centre of Excellence (CCD CoE) und dem Nato Computer Incident Response Capability Technical Centre (NCIRC TC) durchaus Organisationen geschaffen, die in der Lage sind, auf Angriffe aus dem virtuellen Raum zu reagieren. Das Problem ist jedoch fundamentalerer Natur: Bis zu den Cyberattacken auf Estland 2007 lag der Fokus >>

der Nato vor allem auf dem Schutz der bündniseigenen Infrastruktur, was sicherlich im Rahmen der ihrer Kapazitäten liegt. Jedoch zeigen die »Nato Policy on Cyber Defense« von 2011 und die »Lissabon-Erklärung« von 2010, dass diese Konzentration nicht mehr exklusiv ist, sondern zunehmend die einzelnen Mitgliedsstaaten und deren kritischen Infrastruktureinrichtungen Berücksichtigung finden. Gewissermaßen ist das logisch, da die Nato schließlich auf das Funktionieren dieser Strukturen aufbaut. Betrachtet man jedoch das Cyberspace-Umfeld und sich abzeichnende Charakteristika eines Cyberwars, so muss man sich fragen, ob die Nato diesen Anspruch erfüllen kann.

»Cyberwar«, dem US-Politologen Adam Liff folgend, bezieht sich auf computerbasierte netzwerkgestützte Operationen, die nicht der psychologischen Kriegsführung zuzuordnen sind, und die der Erreichung eines militärischen oder politischen Zieles dienen. Eine solche klare Definition ist wichtig, da der Begriff in den letzten Jahren sehr schwammig gebraucht worden ist. Das mag auch daran liegen, dass die praktische Unterscheidung schwer fällt: Beispielsweise das Eindringen in einen Server oder ein Netzwerk kann einer ganzen Reihe von Zwecken dienen, die sich jedoch nicht alle als kriegsähnlich klassifizieren lassen. Website-Vandalismus, Cyber-Spionage oder Hacken aus wirtschaftlichen Interessen sind nicht mit »Krieg« gleichzusetzen, ebenso wie es die »Offline«-Äquivalente auch nicht sind. Ebenso lassen sich elektronische Kampfführung oder ein kinetischer Angriff auf Cyberstrukturen – etwa der Abwurf von Bomben auf ein Rechenzentrum – klar abgrenzen. Schlösse man diese ein, würde der Begriff beliebig und könnte kaum noch als analytische Kategorie dienen.

Den Aspekt der Zielsetzung zu betonen, unterstreicht die Verwandtschaft zum konventionellen Krieg, der nach Clausewitz ja ebenfalls der Durchsetzung letztendlich politischer Interessen dient. Durch Cyberwar soll der Gegner also ebenfalls zu einem bestimmten gezwungen werden.

Cyberwar dürfte sich vor allem auf einer strategischen Ebene abspielen und taktisch nur von begrenztem Nutzen sein: Das prominente Beispiel Stuxnet zeigt, wie zumindest für hochwertige Ziele eine gründliche Vorbereitung notwendig ist, die ad-hoc nicht zu bewältigen wäre. Als Ziele von Cyberattacken dürften deswegen vor allem Objekte von strategischer Bedeutung, die schon angesprochenen kritischen Infrastrukturen, in Frage kommen: beispielsweise Einrichtungen der Energie- und Gesundheitsversorgung oder Verkehrs- und Kommunikationsinfrastrukturen.

Zumindest in Europa befindet sich ein Großteil dieser Anlagen in Privatbesitz oder ist zumindest teilprivatisiert – was im Gegensatz zu konventionellen Bedrohungen im Cyberwar bedeutsam ist. Vereinfacht ausgedrückt konnte man ein Kraftwerk vor wenigen Jahrzehnten noch dadurch schützen, indem man ein Flugabwehrgeschütz daneben und einen Panzer vor das Tor stellte. Dieser Schutz war kaum von der Zustimmung oder Kooperation mit dem Betreiber des Kraftwerks abhängig und griff auch nur geringfügig in den Betriebsablauf ein.

Im Gegensatz dazu lässt sich ein Cyberangriff durch solche »simplen« Maßnahmen nicht abwehren, sondern erfordert, dass man sich tiefgreifend mit der vorhandenen IT-Infrastruktur auseinandersetzt. Dies ist ohne Zustimmung und Kooperation des Betreibers genauso wenig möglich, wie es ohne Auswirkungen auf den Betrieb bleiben dürfte. Während eine Luftabwehr außerdem auch auf regionaler, nationaler oder gar multinationaler Ebene einheitlich organisiert werden kann – wie die Nato es im Kalten Krieg getan hat –, erfordert der Schutz der kritischen IT-Infrastruktur auf- >>

Der Begriff »Cyberwar« ist in den letzten Jahren zu schwammig geworden.

grund der unterschiedlichen Systeme der einzelnen Unternehmen ein sehr individuelles Vorgehen. Ein Schutz kritischer Infrastrukturen ist demzufolge nur in Kooperation mit der Privatwirtschaft möglich. Dies geschieht auf nationalstaatlicher Ebene bislang vor allem auf der Basis von Public-Private-Partnerships (PPP).

Die Perspektive der betroffenen Firmen auf den Komplex Cyberdefense ist allerdings naturgegeben ein anderer: Schutzmaßnahmen verursachen vor allem Kosten und wirken sich deswegen, außer vielleicht im Ernstfall, eher negativ auf die Wettbewerbsfähigkeit aus. Sowohl für die Sicherheit – im Sinne eines Risk Management und nicht absoluter Sicherheit – als auch für die Unternehmen ist es deshalb notwendig, möglichst einheitliche Standards und Regulierung zu schaffen, aufgrund der vernetzten Infrastruktur in Westeuropa und dem transnationalen Charakter vieler Unternehmen am besten auf internationaler Ebene.

Dies ist der Punkt, an dem die Nato an ihre Grenzen stoßen wird: Sie verfügt als intergouvernementale militärische Organisation nicht über den benötigten »Werkzeugkasten«, um flächendeckend und übernational PPPs zum Cyberschutz einzugehen. Zwar gäbe es durchaus die Möglichkeit, die Allianz entsprechend umzubauen – die Sinnhaftigkeit einer solchen Konstruktion dürfte allerdings in Frage zu stellen sein, da es zumindest auf europäischer Ebene tatsächlich eine Organisation gibt, die diese Fähigkeiten hat: die Europäische Union.

Die EU besitzt sowohl die Möglichkeit der direkten Regulierung, als auch reichhaltige Erfahrung in der Kooperation mit Unternehmen. Im Bereich Cyberdefense besteht mit der »European Network and Information Security Agency« (ENISA) auch eine Organisation mit entsprechender inhaltlicher Kompetenz. Die Nato sollte sich also fragen, ob sie im Bereich Cyberdefense wirklich über den Schutz der bündniseigenen Netzwerke hinausgehen möchte oder ob sie nicht lieber der EU hier eine größere Rolle zusprechen möchte, wenigstens in Form einer Kooperation. Absoluten Schutz wird es in keinem Fall geben, aber zumindest könnte die EU die notwendigen Bemühungen effektiver und effizienter gestalten. ◂◂◂◂

Julian Schibberges *schließt gegenwärtig seinen Masterstudiengang in Politikwissenschaften an der Freien Universität Berlin ab.*

Für die privaten Betreiber kritischer Infrastrukturen wirken sich Schutzmaßnahmen zunächst einfach nur negativ auf die Wettbewerbsfähigkeit aus.

Quellen und Links:

Webpräsenz der ENISA

Adam P. Liff: »Cyberwar: A New ›Absolute Weapon‹?«, im *Journal of Strategic Studies*, Ausgabe 3/2012

Miriam Dunn Cavelty: »Cyber-Allies«, in der *Internationale Politik Global Edition* vom 1. Mai 2011

Miriam Dunn Cavelty und Manuel Suter: »Public-Private Partnerships are no silver bullet«, im *International Journal of Critical Infrastructure Protection*, Ausgabe 2/2009

NOTIZ

Googlefail

Eine außereheliche Affäre kostete CIA-Chef David Petraeus den Job. Eigentlich hätte man ihn wegen Unfähigkeit feuern müssen.

David Petraeus und Paula Broadwell 2008. Foto: ISAF

Kaum wiedergewählt, musste sich US-Präsident Barack Obama gleich um den ersten Skandal kümmern. Ausgerechnet CIA-Direktor David Petraeus musste seinen Hut nehmen: Nun lässt sich darüber streiten, ob eine außereheliche Affäre im 21. Jahrhundert noch ein zwingender Grund für den Verlust des Jobs sein sollte – bei nachgewiesener Unfähigkeit als dringlichem Rücktrittsgrund hingegen dürfte Einigkeit herrschen. Nachdem herauskam, wie stümperhaft Petraeus die Kommunikation mit seiner Liebhaberin gehandhabt hatte, war er als Chef des vermutlich mächtigsten Geheimdienstes der Welt nicht mehr tragbar.

Dabei hatte Petraeus durchaus versucht, seinen Briefwechsel mit Paula Broadwell zu verschleiern. Er nutzte den bekannten Kniff, E-Mails nicht zu verschicken, sondern nur als Entwurf zu speichern. Da Broadwell über die Zugangsdaten zu seinem inkognito angelegten Googlemail-Konto verfügte, konnte sie die Nachrichten im Entwurfsordner einsehen, ohne dass diese zuvor durchs Netz gegangen wären. Problematischer war Petraeus' Entscheidung, für seine delikaten Nachrichten auf Googlemail zu setzten – ein Dienst, der bekanntlich die Kommunikation seiner Nutzer systematisch für Werbezwecke durchsucht. Kaum der geeignete Ort für einen Geheimdienstchef, um potenziell brisante Mitteilungen abzulegen.

Dass Googlemail-Konten auch gern einmal gehackt werden und man bei einem Cloud-basierten Dienst nie so genau weiß, wo die eigenen Daten genau gespeichert sind und wer gegebenenfalls mitliest, machen die Sache nicht besser. Dass Petraeus zudem nicht wenigstens auf frei verfügbare Verschlüsselungsmethoden wie »PGP« oder »Truecrypt« zurückgriff, um seine Kommunikation mit Broadwell für Fremde unlesbar zu gestalten, zeigt sein absolutes Unverständnis für grundlegende Regeln der IT-Sicherheit. Deswegen – und nicht wegen seiner Affäre – war er als Geheimdienstchef untragbar. **doe**

Quellen und Links:

Bericht der *InformationWeek* vom 13. November 2012

Bericht der *Washington Post* vom 10. November 2012

Webseiten der freien Verschlüsselungsprogramme Truecrypt und GnuPG

Misstrauen säen, Aussteiger ermutigen

von Guido Steinberg

Die Bekämpfung des islamistischen Terrorismus am Übergang von der Internetpropaganda zur blutigen Tat ist alles andere als einfach.

Für die deutschen Behörden ist es aber an der Zeit, neue Wege zu beschreiten.

Al-Quaidas Webmagazin *Inspire*. Quelle: Wikimedia Commons

>> In den letzten Monaten warnten deutsche Sicherheitsbehörden immer wieder vor einigen Dutzend deutschen »Salafisten«, die seit dem Verbot der Gruppierung »Millatu Ibrahim« im Juni 2012 nach Ägypten gezogen sind. Es wird berichtet, dass die jungen Männer dort versuchen, neue Strukturen aufzubauen. Nachrichtendienste und Polizei befürchten, dass einige von ihnen auch in Richtung der Krisengebiete in Libyen, Mali, Syrien und auf dem Sinai ziehen.

An der Spitze der deutschen Gruppe in Ägypten steht mit dem Österreicher Mohamed Mahmoud der Doyen der jihadistischen Internetszene in Deutschland. Sein Fall zeigt wie kein anderer die Bedeutung des Internets bei der Ausbildung einer deutschen Unterstützerszene auf und verdeutlicht, dass >>

im Netz die Trennlinien zwischen Terroristen einerseits und ihren Unterstützern und Sympathisanten andererseits immer mehr verwischen. Die deutsche Terrorismusbekämpfung muss dieser Entwicklung angepasst werden.

Mohamed Mahmoud begann seine Karriere als Chef der deutschsprachigen Sektion der *Globalen Islamischen Medienfront* (GIMF). Dabei handelte es sich um eine der wichtigsten jihadistischen Medienstellen, die Material von al-Qaida und anderen Organisationen im Netz verbreitete. Die Ende 2005 gebildete deutsche GIMF wurde vor allem durch ein im März 2007 veröffentlichtes Drohvideo bekannt, in dem sie einen Abzug der deutschen und österreichischen Truppen aus Afghanistan forderte. Obwohl Mahmoud im September 2007 in Wien verhaftet wurde, führte eine kleine Gruppe deutscher Freiwilliger die Öffentlichkeitsarbeit der GIMF bis 2008 fort. Als auch diese verhaftet wurden, übernahmen teils sehr professionell agierende Einzelpersonen die Verbreitung des jihadistischen Propagandamaterials in Deutschland.

Als Mahmoud im September 2011 schließlich aus österreichischer Haft entlassen wurde, stellte er sofort den Kontakt zu Gleichgesinnten in Deutschland her und zog zunächst nach Berlin. Die deutsche jihadistische Internetszene gewann enorm an Dynamik. Sein wichtigster Helfer wurde der Berliner Ex-Rapper Denis Cuspert (alias Abu Maleeq oder Abu Talha), der damals bereits als Sänger jihadistischer Hymnen, so genannter »anashid« bekannt war. Gemeinsam verbreiteten sie jihadistische Propaganda auf der Webseite *millatu-ibrahim.com*. Dabei war der Name ebenso Bezeichnung für eine kleine Gruppe von Propagandisten wie auch deren religiös-politisches Programm: »Gemeinschaft (des Propheten) Abrahams« oder »Millat(u) Ibrahim« nämlich lautet der Titel eines der einflussreichsten Werke der jihadistischen Literatur, das von dem Palästinenser Abu Muhammad al-Maqdisi verfasst wurde. Mit der »Gemeinschaft Abrahams« bezieht sich Maqdisi auf einen Koranvers (60:4), aus dem er das jihadistische Konzept der Loyalität gegenüber dem einzigen Gott und der Lossagung vom Polytheismus und seinen Anhängern ableitet. Demzufolge sei es die Pflicht des Gläubigen, den Unglauben vieler nomineller Muslime als solchen zu benennen und ihnen gegenüber eine offen feindselige Haltung einzunehmen. Mahmoud und seine Anhänger übernahmen diese Lehre für die Diaspora und forderten auch hier von den Muslimen, offene Feindschaft gegenüber den nicht gleichgesinnten Muslimen und der Mehrheitsgesellschaft zu leben.

Die Gruppe »Millatu Ibrahim« gelangte im Juni 2012 zu bundesweiter Bekanntheit, als das Bundesinnenministerium sie verbot und ihre Webseite schließen ließ. Mahmoud und viele seiner Anhänger reisten nach Ägypten, wo deutsche Salafisten bereits seit Jahren Zuflucht gesucht hatten, um dem Verfolgungsdruck deutscher Behörden zu entgehen. Sie setzen von dort ihre Propagandaaktivitäten mit Zielrichtung Deutschland fort, sollen laut Angaben der deutschen Sicherheitsbehörden aber gleichzeitig versuchen, sich jihadistischen Netzwerken in der Region anzuschließen.

Die jihadistische Karriere eines Österreichers in Berlin

Die Karriere Mahmouds zeigt die großen Schwierigkeiten der Terrorismusbekämpfung am Übergang von der Internetpropaganda zur terroristischen Tat. Vor allem nach der Entlassung Mahmouds zeigte sich, dass seine Inhaftierung nur bedingt zielführend war. Denn im Gefängnis hatte er sich zu einem Star der Unterstützerszene entwickelt und betrieb nun sehr viel offener jihadistische Propaganda als noch 2007. Das anschließende Verbot von »Millatu Ibrahim« führte in erster Linie zu einem Ausweichen der Gruppe nach Ägypten, wo es für die deutschen Behörden kaum möglich sein dürfte, auch nur den Überblick über ihre Aktivitäten zu bewahren.

Zwar ist die Inhaftierung wichtiger Aktivisten ein probates Mittel, um die jihadistische Öffentlichkeitsarbeit im Internet zu beeinträchtigen. Auch ein >>

Verbot von Gruppen, die wie »Millatu Ibrahim« Propaganda betreiben, kann kurzfristige Erfolge zeitigen. Doch darf die deutsche Politik hier nicht stehenbleiben. Die Ideologie des Autoren Maqdisi und anderer bekannter Jihadisten ist in Deutschland angekommen. Die Aktivitäten im Internet werden nach Inhaftierungen immer wieder von neuen Propagandisten übernommen. Immer neue Webpräsenzen sorgen für eine stetige Verfügbarkeit von Material.

Langfristig sollte es den deutschen Behörden deshalb vor allem darum gehen, Misstrauen zu säen. Denn das jihadistische Internet lebt vom Vertrauen in die Authentizität des Materials und die (jihadistische) Integrität des virtuellen Gegenübers. Wo dieses Vertrauen verloren geht und eine Manipulation durch Sicherheitsbehörden vermutet wird, stockt auch die Internetkommunikation.

Die deutsche Terrorismusbekämpfung darf nicht bei Inhaftierungen und Verboten stehenbleiben.

Darüber hinaus ist es die vielleicht vordringlichste Aufgabe zu verhindern, dass die jetzt schon in großer Zahl im Gefängnis einsitzenden Jihadisten nach ihrer Freilassung als neue Stars der Szene auftreten und Anhänger gewinnen. Dabei sollte man sich nicht darauf beschränken, ihnen den Weg zurück ins bürgerliche Leben zu ebnen.

Vielmehr sollten potentielle Aussteiger identifiziert werden, die einerseits im jihadistischen Milieu so bekannt sind, dass sie nach ihrer Haft Sympathisanten überzeugen können, ebenfalls auszusteigen. Andererseits sollten sie ideologisch so wenig gefestigt sein, dass sich die Chance bietet, sie zu einer Zusammenarbeit zu bewegen. Das Internet wäre ein geeignetes Medium, über das sie Anhänger der jihadistischen Szene überzeugen könnten, dass der bewaffnete Kampf ein Irrweg ist. ◂◂◂◂

Dr. Guido Steinberg *ist wissenschaftlicher Mitarbeiter der Forschungsgruppe Naher/Mittlerer Osten und Afrika der Stiftung Wissenschaft und Politik (SWP) und war davor Referent im Referat Internationaler Terrorismus im Bundeskanzleramt.*

Quellen und Links:

Studie der Stiftung Wissenschaft und Politik »Jihadismus und Internet: Eine deutsche Perspektive« vom Oktober 2012

Guido Steinberg: »Wer sind die Salafisten? Zum Umgang mit einer schnell wachsenden und sich politisierenden Bewegung«, SWP-Aktuell vom Mai 2012

Krieg den Narcobloggern

von Hanna Pütz

Der mexikanischen »Drogenkrieg« verändert sich: Das World Wide Web wird zum Instrument im Kampf der Kartelle gegen kritische Berichterstattung.

Unvorsichtige Nutzer werden ermordet und auch das Hacker-Kollektiv Anonymous greift in diesen Krieg ein.

»Super-stummer Mexica«: Protest indianischer Anonymous-Aktivisten in der Stadt Puebla im Süden Mexicos im Juni 2012
Foto: Plumerio Pipichas / lizensiert gemäß CC-A NonCommercial-NoDerivs 2.0 Generic

>> In Morelia, der Hauptstadt des mexikanischen Bundesstaates Michoacán, fliegen bei einer Veranstaltung zum Unabhängigkeitstag am 15. September 2008 zwei Handgranaten in die versammelte Menschenmenge. Mindestens zwölf Personen werden getötet, mehrere hundert verletzt. Auf einer Schnellstraße nahe Monterrey im Norden Mexikos entdecken Sicherheitskräfte 49 enthauptete Leichen. Größtenteils verpackt in schwarze Plastiksäcke, wurden sie hier im Mai 2012 publikumswirksam drapiert. Und der »Suppenkoch«, der für das Kartell von Sinaloa innerhalb von zwei Jahren mindestens 300 Leichen in Salzsäure auflöste, hat mittlerweile nicht nur in Mexiko traurige Berühmtheit erlangt.

Seit Präsident Felipe Hinojosa Calderón am 11. Dezember 2006 den »Krieg gegen die Drogen« und gegen die Organisierte Kriminalität verkündete, starben dabei in Mexiko rund 60.000 Menschen; etwa weitere 25.000 werden ver- >>

misst: Im Drogenkrieg stehen sich das mexikanische Militär, unterstützt von der Bundespolizei, und diverse Drogenhandelsorganisationen gegenüber. Letztere liefern sich auch untereinander Gefechte um Handelsrouten und Gebiete. Beinahe täglich berichtet die Presse von neuem über Verbrechen und Korruption während die Wellen der Gewalt das Land unaufhaltsam überrollen. Mit Enthauptungen und Folter versuchen die Gruppen der Organisierten Kriminalität ihre Machtansprüche deutlich zu machen – je blutiger, desto besser. Diese Strategie der Einschüchterung feindlicher Kartelle und der Presse, der Einflussnahme auf die Zivilbevölkerung und nicht zuletzt auch auf den Staat scheint zu fruchten. Journalisten üben Selbstzensur, und zivilgesellschaftliches Engagement endet unter Umständen mit dem Tod. Allerdings eröffnet sich in zunehmend eine neue Dimension in dem gewaltsamen Konflikt. Denn über traditionelle Formen der Konfliktaustragung hinaus erweitern die Beteiligten ihre Auseinandersetzungen nun auch in den Cyberspace.

Ganz neu ist diese Entwicklung nicht: Bereits seit Jahren spielen die »Neuen Medien« eine Rolle im mexikanischen Konfliktgeschehen. Drogenhandelsorganisationen zeichnen ihre Gewaltakte auf, stellen sie in Internetportale oder schicken die Videos direkt an die einschlägigen Fernsehsender Mexikos. »An Schaurigkeit kaum zu überbieten« sind solche Aufzeichnungen, so Politikwissenschaftler Karl-Dieter Hoffmann, der als Geschäftsführer des Zentralinstituts für Lateinamerikastudien bereits seit Jahren zum mexikanischen Konfliktgeschehen forscht.

Journalisten üben Selbstzensur und zivilgesellschaftliches Engagement endet unter Umständen mit dem Tod.

Neben Brasilien und Honduras ist Mexiko das Land mit der eingeschränktesten Pressefreiheit in Lateinamerika. Die kunstvollen Verflechtungen zwischen Medien, Politik und Gesetzgebung, das oft tödliche Wechselspiel zwischen Transparenz und Methoden der Zensur und Selbstzensur erschweren eine neutrale Berichterstattung und Analyse. »Wenn du über Chapo Guzmán [*Anführer des Sinaloa-Kartells, d. Red.*] schreibst, passiert dir nicht viel. Aber wenn du darüber schreibst, wie er die Polizeichefs kauft und offiziellen Schutz erhält, werden sie dich töten!«, beschreibt etwa die Journalistin Marta Durán die Lage. Mexikos Drogenkartelle hatten schon häufig Zeitungsredaktionen angegriffen und Reporter bedroht, entführt oder getötet. Die durch Selbstzensur entstandene Lücke in der Berichterstattung wird zunehmend durch Blogs gefüllt. Diese können aus der Anonymität heraus betrieben werden und sind so vor Vergeltungsmaßnahmen sicher. Die damit einhergehende Freiheit wurde zum Beispiel im international bekannten *Blog del Narco* genutzt, um schonungslos über die Verbrechen der Kartelle zu berichten.

Allerdings ist Anonymität im Netz keine simple Angelegenheit. Die Fehlerquellen sind zahlreich und das technische Verständnis dafür hat nicht jeder. Dies wurde im November 2011 drei Foristen zum Verhängnis. Das für seine Brutalität bekannte mexikanische Drogenkartell Los Zetas ging als eine der ersten Gruppen des organisierten Verbrechens gezielt gegen Internet-Nutzer vor. Ziel der Aktion war es, die Berichterstattung im Netz zu kontrollieren. Mindestens drei Nutzer des Chatrooms »Nuevo Laredo en Vivo«, in dem sich Kommentare zu den Umtrieben der Zetas und anderer Kartelle in der Stadt Nuevo Laredo finden, wurden ermordet und die Opfer zur Warnung an einer Brücke aufgehängt. Die Botschaft des Kartells am Tatort war eindeutig: »Das hier droht allen Internet-Wichtigtuern.«

Der Versuch von Akteuren, Diskurs und Kommunikation zu kontrollieren, findet überall statt. Aber Mexiko sticht heraus durch die Brutalität und Vehemenz mit der Informationen buchstäblich aufgelöst werden. Was sich in Nuevo Laredo ereignete, ist im Grunde genommen ein Frontalangriff auf die Öffentlichkeit. Diese bleibt trotz gestiegenen Sicherheitsbewusstseins der Internetnutzer und Warnungen, keine persönlichen Informationen preiszugeben, höchst verwundbar. Der Informationspfad über Cookies, Server-Adressen, Login- und Kontoinformationen ist leicht sichtbar zu machen, und für die Zetas mit ihrem Geld aus dem Drogenhandel stellt es kein Problem dar Spuren von Chatteilnehmern zu verfolgen. Von der Utopie des Internet als Ort, in dem sich Öffentlichkeit und Zivilgesellschaft organisieren können, bleibt unter diesen Umständen wenig übrig. >>

Dennoch zeigte die Aktion zuerst, dass trotz aller Gefahren und trotz der Angst großes Interesse daran herrschte, die Akteure der Organisierten Kriminalität nun erst recht zu enttarnen. Nach dem Nuevo Laredo Vorfall holten zahlreiche Bürger zu einer Gegenattacke aus: Der bereits seit 2010 existierende und wohl bekannteste *Blog del Narco* hatte Zulauf wie selten zuvor, und über neue blutige Taten der Kartelle wurde getweetet und gebloggt, als gelte es, mit Worten die tödlichen Übergriffe zu rächen.

Im selben Zeitraum stieß noch eine weitere Konfliktpartei an die Cyberfront vor: Das Anonymous-Kollektiv. Dass die beiden Organisationen, die Los Zetas und Anonymous, eines Tages aufeinanderprallen würden, war seit den tödlichen Übergriffen des Kartells auf kritische Internetnutzer wahrscheinlich. Schon zuvor bauten sich Spannungen zwischen den Kartellen und Anonymous Mexiko auf: Letztere recherchierten intensiv zu mexikanischen Drogenkartellen und korrupten Politikern, und zwar insbesondere im Bundesstaat Veracruz. Dort vermuteten nicht nur die mexikanische Zivilgesellschaft, sondern augenscheinlich auch Anonymous eine besonders starke Verflechtung der dortigen Landesregierung mit den Zetas.

Zum Zeichen des Protests gegen diesen Umstand organisierte das Internetkollektiv eine groß angelegte Protestaktion, genannt »Paperstorm«. Dabei verteilten die Aktivisten Flugblätter und stellten Videos online, in denen die Landesregierung für ihre Kooperation mit den Zetas denunziert wurde. Die Folge der öffentlichen Bloßstellung war ein erneuter Gewaltakt der kriminellen Vereinigung, diesmal in Form von Entführungen. Noch während des »Paperstorms« schlugen die Zetas zu und verschleppten mindestens ein Anonymous-Mitglied.

»Es war ein großer Fehler von euch, einen von uns zu entführen. Lasst ihn frei!« So lautete kurz nach der Entführung die Forderung des maskierten Anonymous-Sprechers in einem Video. Andernfalls werde man die Namen von Taxifahrern, Polizisten, Politikern und Journalisten veröffentlichen, die mit dem Kartell zusammenarbeiten. Die Zetas drohten im Gegenzug damit, zehn Personen zu töten, und zwar für jeden einzelnen von den Hackern veröffentlichten Namen. Der mexikanische Blogger Wikichava stellte an dieser

Die Kartelle beginnen, Hacker für sich arbeiten zu lassen.

Stelle die entscheidende Frage: »Was wissen die Zetas vom Hacken einer Website? Und was wissen die Anonymous-Leute von Waffen und den Millionen von Dollar, die da im Spiel sind? Wissen Sie, was sie tun?«

Ganz klar lassen sich diese Fragen auch ein Jahr nach dem Zwischenfall nicht beantworten, fest steht aber, dass beide Seiten zunächst relativ glimpflich davongekommen sind. Zwar wurde ein Bruchteil der verfilzten Strukturen des »Drogenkrieges« freigelegt und die Homepage von Gustavo Rosario gehackt. Dieser wurde als Zeta enttarnt – fatal für einen Obersten Staatsanwalt, der diese Organisation eigentlich bekämpfen soll. Aber mehr wurde scheinbar nicht veröffentlicht, und der Aktivist, einer von insgesamt vier bis fünf entführten Personen, wenige Wochen später wieder freigelassen.

Die Geschehnisse haben trotzdem auf verschiedenen Ebenen zu Veränderungen geführt. So richtete die mexikanische Regierung eine zehntausende Mails umfassende Datenbank ein, in der nach Hinweisen auf Korruption in >>

Zwei User, die in einem Internetforum die Kartelle kritisiert haben, wurden im November 2011 in Nuevo Laredo von Kriminellen hingerichtet.

Bildquelle: hoylaredo.net (abgerufen am 27.01.2013)

Mexikos Verwaltung und Regierung gesucht werden kann. Dieses Vorhaben kommt der Zivilbevölkerung vermutlich entgegen, ist doch das Vertrauen in den Regierungsapparat in einer akuten Krise. Es lässt sich in Mexiko aber auch eine sichtliche Unterstützung der Anonymous-Aktivisten durch die Bevölkerung spüren. Denn die ist von Politik, Justiz und Polizei bitter enttäuscht. Damit wird die Datenbank zu einem Paradoxon, haben doch solche, eigentlich vertrauensbildende Maßnahmen oft einen gegenteiligen Effekt. So treten Fälle von schwerer Korruption und Unterwanderung des Staates gerade bei der Bekämpfung des Drogenhandels immer wieder auf.

Ein besonders prägnantes Ereignis war die »Operación Limpieza«, zu Deutsch »Operation Reinigung«. Im Rahmen dieser 2008 durch die Regierung eingeläuteten Antikorruptionsmaßnahme wurde durch staatliche Ermittler die Zusammenarbeit zwischen dem Beltrán-Leyva-Kartell und zwei ehemaligen Direktoren der Interpol Mexiko aufgedeckt. Anonymous mag daher für viele wie ein Hoffnungsträger erscheinen, der effektiver und unabhängiger als der Staat für Transparenz und gegen Korruption eintritt.

Von der Utopie des Internet als Ort, in dem sich Öffentlichkeit und Zivilgesellschaft organisieren, bleibt wenig übrig.

Wie es im mexikanischen Ringen um Drogen, Daten und Demokratie weitergeht, ist noch offen. In den Jahren seit der Verkündung des »Drogenkrieges« wurde mehr als deutlich, wie schnell die dortige Konfliktdynamik sich ändern kann. Es lassen sich zahlreiche Zukunftsszenarien ausmalen. Die Kartelle könnten versuchen mehr Mitglieder von Anonymous ausfindig zu machen und einzuschüchtern. Vielleicht auch zu diesem Zweck beginnen die Kartelle selbst Hacker zu engagieren. Geld genug haben sie. Tatsächlich hat das amerikanische Unternehmen Stratfor in einer Sicherheitsanalyse davon berichtet. Der Zugang zum *Blog del Narco* ist seit einigen Monaten massiv erschwert ist. Auch eine neue, ähnlich konzipierte Seite, *MilCincuenta* , weist zunehmend technische Störungen oder Blockaden auf.

Und Anonymous? Vielleicht haben die Hacker nur gespielt, ihre Grenzen und Möglichkeiten getestet. Vielleicht sind sie bereits eine fest etablierte Kriegspartei, die aber noch im Untergrund agiert und irgendwann die Informationsbombe zum Platzen bringt. Vielleicht, so spekulierte die »Zeit«, bekommt der transnationale Drogenhandel zum ersten Mal einen Gegner, der ebenfalls transnational vernetzt ist und an jedem Ort der Welt zuschlagen kann.

Mexiko könnte schlussendlich ein Paradebeispiel dafür sein, dass die Relevanz Neuer Medien und Cyberkriminalität in den multidimensionalen Konflikten des 21. Jahrhunderts rasant wächst – und dafür, dass Konfliktakteure weniger greifbar werden. Anonymous jedenfalls drücken es so aus: »Das ist jetzt global. Ihr könnt versuchen, Anonymous in Mexiko, Mittelamerika und vielleicht auch in den USA aufzuhalten. Aber Ihr könnt [...] nicht auf den globalen Geist schießen und ihn nicht in Säure auflösen.« ◂◂◂◂

Hanna Pütz *hat in Bonn Politologie, Ethnologie und Geschichte studiert. In ihrer Magisterarbeit analysierte sie die Strukturen des »Drogenkriegs« in Mexiko.*

Quellen und Links:

Blog del Narco (Website auf Spanisch)

Robert J. Bunker: »The Growing Mexican Cartel and Vigilante War in Cyberspace«, Kurzessay im *Small Wars Journal* vom 3. November 2011

Interview mit dem Autor des *Blog del Narco* vom 14. September 2010 im Blog *Boing Boing*

Digitales Dilemma

von Constantin Schüßler

Eigenschaften der digitalen Welt wie Anonymität und Nicht-Attribuierung belasten auch die Beziehungen zwischen Staaten in der realen Welt. Schlimmstenfalls könnten Cyberattacken sogar bald Grund für kriegerische Auseinandersetzungen werden.

Beschwört das längst vergessen geglaubte Zeiten der Anarchie wieder herauf? >>

Titelblatt von Thomas Hobbes' »Leviathan« aus dem Jahr 1651

>> Ist ein USB-Stick militärisches Gerät? Sind Computerspezialisten Soldaten? Augenscheinlich nicht, jedoch gewinnen beide zunehmend an sicherheitspolitischer Bedeutung, wodurch auch viele althergebrachte Denkmuster und Handlungsweisen in Frage gestellt werden. Das für die internationale Sicherheitspolitik geradezu konstitutive Sicherheitsdilemma bleibt davon nicht unberührt. Ein solches Dilemma entsteht, wenn ein Staat sein Überleben besonders durch die militärische Überlegenheit eines anderen Staates bedroht sieht.

Wenn dann die ergriffenen Vorbeuge- oder Verteidigungsmaßnahmen von der Gegenseite als aggressiver Akt missverstanden werden, und dort wiederum zu entsprechenden Gegenmaßnahmen führen, kann schnell eine paradoxe Eskalationsspirale im Namen der Sicherheitsvorsorge entstehen. Entgegen der grundlegenden Absicht des sich bedroht fühlenden Staates seine eigene Sicherheit zu gewährleisten, führten seine Anstrengungen nur zu weiterer Verunsicherung und Erschaffung von größerem Bedrohungspotenzial durch beide Seiten.

Das Sicherheitsdilemma: Unsicherheit durch Sicherheit

Der deutsch-amerikanische Politologe John Herz führte dieses Konzept 1950 in den sicherheitspolitischen Diskurs ein und legte so eine bedeutende Grundlage zur Analyse von Konflikten. 2003 resümierte er, dass das Dilemma mehr denn je von größter Bedeutung sei. Griff Herz mit »mehr denn je« auch auf die gegenwärtigen Entwicklungen im Cyberspace vor? Vieles deutet darauf hin. So wies der US-Sicherheitssoftwarehersteller McAfee 2010 bezeichnenderweise darauf hin, dass der Cyberspace in vielen Bereichen die Weltanschauung von Thomas Hobbes widerspiegelt, der die Natur als »einen Krieg aller gegen alle« begriff.

In der Auseinandersetzung mit den internationalen Beziehungen wird klassischerweise die Anarchie als systemprägende Grundbedingung angenommen. Ohne eine höhere regulative Autorität verbleiben Staaten gegenüber den Intentionen anderer Staaten grundlegend ahnungslos und unsicher. Auch internationale Organisationen und das Völkerrecht können diese Anarchie nicht aufheben, sondern höchstens mildern. Damit erscheint das Prinzip der Selbsthilfe zur herausragenden Überlebensstrategie zu werden. Versuchen Staaten auf diesem Weg – durch militärische Aufrüstung ihr Überleben und ihre Sicherheit gegenüber anderen Staaten zu gewährleisten – erzeugen sie allerdings nur weitere Verunsicherung in diesen Staaten, welche dann wiederum selbst aufrüsten, um dem neugeschaffenen Drohpotential zu begegnen. Die Staaten erschaffen so im Namen der Sicherheit durch wechselseitige Aufrüstung das Sicherheitsdilemma.

Dieses setzt drei entscheidende Bedingungen voraus: erstens strukturelle Anarchie, zweitens eigene Ungewissheit, ob Absichten von und Bedrohungen durch andere Staaten richtig interpretiert werden und drittens Akkumulation von Macht. Letztere basiert auf einer Nullsummenlogik, nach der ein Zugewinn an Macht eines Staates nur auf Kosten eines anderen erfolgen kann.

In konventionellen Konflikten waren Anarchie und Unsicherheit stets maßgebende Aspekte. Das Deutsch-Britische Flottenwettrüsten vor dem Ersten Weltkrieg oder die Abschreckungslogik des Kalten Kriegs sind herausragende Beispiele dafür. In beiden Fällen waren allerdings die Konfliktgegner und Bedrohungspotentiale eindeutig zu identifizieren. Im Cyberspace hingegen ist eine solche Zuweisung von Bedrohung und Gegner hingegen nicht ohne weiteres möglich, wodurch der Unsicherheitsfaktor für den betroffenen Staat noch zunimmt und sich das Sicherheitsdilemma womöglich verschärft.

Dies beginnt bereits mit der Unklarheit darüber, was der Begriff des Cyberspace eigentlich benennt. Die Komplexität des Begriffs wird beispielsweise in einem Bericht des UN Office of Disarmament Affairs deutlich, in dem der Cyberexperte James Lewis ihn folgendermaßen umreißt: »It is very fluid and the technology changes rapidly. It is an environment tilted towards anonymity. It is complex. It is millions, even hundreds of millions of devices each with different systems and software all connected to each other. It is opaque. [...] Finally, it is an environment that is marked by competition and mistrust«. Ein solides technisches Verständnis seiner Funktionsweise ist daher die Grundvoraussetzung, um eine konstruktive Diskussion über den Cyberspace und seine sicherheitspolitischen Implikationen führen zu können. >>

Sandro Gaycken, Wissenschaftlicher Mitarbeiter am Institut für Informatik der FU Berlin, monierte im *ADLAS* (Ausgabe 1/2012), dass durch mangelnde technische Kompetenz etablierte Konzepte oft unkritisch auf neue Situationen übertragen werden und einer genaueren Betrachtung nicht Stand halten. Dieses Problem kommt bei der sicherheitspolitischen Erschließung des Cyberspace bereits in grundlegenden Fragen zum Tragen. So ist vor allem ungeklärt, was genau eine »Cyberwaffe« ist, wohingegen nukleare, biologische oder chemische Waffen klar und international anerkannt definiert sind.

Folglich laufen Vorschläge zur Regulierung oder Nonproliferation von Cyberwaffen Gefahr, irreführend oder praxisuntauglich zu sein. Sollte ein USB-Stick, eine Onlineapplikation oder sonstige kommerzielle Software als digitale Waffe bezeichnet werden, nur weil sie für einen kriminellen oder gar kriegerischen Akt missbraucht wurde? Der Wurm »Stuxnet« infizierte das Zielsystem über einen handelsüblichen USB-Stick. Auch gezielte DDoS-Attacken gegen einen bestimmten Server sind nur eine beabsichtigte Überlastung durch die Versendung einer Vielzahl fehlerhafter IP-Pakete, wie diese sonst im gewöhnlichen Internetverkehr vorkommen kann. Während Definitionsfragen unbeantwortet bleiben, nutzen diverse Akteure den Cyberspace seit Jahren für Angriffe unterschiedlicher Art.

Der Öffentlichkeit sind vornehmlich die Attacken der vergangenen Jahre wie in Estland 2007, in Georgien 2008 und im Iran 2010 ein Begriff. Dabei wurden zumeist DDoS-Attacken oder Würmer eingesetzt, die Systeme ausspionieren oder temporär zum Erliegen bringen. Erst unlängst erkennen hochtechnisierte Industriestaaten den Cyberspace als Schlachtfeld der Zukunft an und bereiten sich auf bevorstehende Auseinandersetzungen in dieser Sphäre vor. Die Errichtung von Cyber Commands, Cybereinheiten und vergleichbaren Dienststellen in verschiedenen Streitkräften bezeugt dies. Insbesondere die USA folgen dabei einer Philosophie der aktiven Verteidigung und versuchen, feindliche Hacker zu jagen, ihre Techniken zu verstehen und sie bestenfalls genau zu identifizieren. Die Aspekte der Anarchie, Unsicherheit und Nicht-Attribuierung kommen hierbei voll zum Tragen.

Gesetze und internationale Abkommen könnten diesen Zustand durch ansatzweise Regulierung mildern. Neben der »Convention on Cybercrime« des Europarats existieren aber nur wenige internationale Abkommen, da die meisten Regelungen allein auf nationaler Ebene verabschiedet wurden. Der reizvolle Schutz, den Anonymität und Nichtnachweisbarkeit im Cyberspace bieten, würde international ratifizierte Abkommen in ihrer Umsetzung stark erschweren oder gar unmöglich machen.

Ein Cartoon des Politikmagazins *The New Yorker*, in welchem ein Hund einen PC bedient und einem anderem Vierbeiner erklärt, dass im Internet niemand wisse, dass er als Benutzer ein Hund sei, beschreibt die grundlegende Problematik treffend. Zudem ist die Rolle der Anonymität im Cyberspace zweischneidig. Einerseits würde ein Verlust der Anonymität die Privatsphäre verletzen, während andererseits ein völlig anonymes Internet immense Chancen für Missbrauch bis hin zum Verbrechen böte. Folglich kumuliert eine Debatte über die Internetanonymität schnell in Grundsatzfragen über das Spannungsverhältnis zwischen Freiheit und Sicherheit.

Der Hobbessche »Krieg aller gegen alle« 2.0 findet im Cyberspace statt.

In der realen Welt ist es für einen Staat über weite Strecken unmöglich, sich hinter dem Deckmantel der Anonymität und Nicht-Attribuierung zu verstecken. Im Cyberspace ist die Attribuierung hingegen deutlich schwieriger. Verena Diersch zeigte im *ADLAS* (Ausgabe 2/2012), dass ohne eine genaue Zuordnung eines Angriffes und die Identifizierung des Angreifers keine Optionen zum Gegenschlag, geschweige denn eine wirkungsvolle Verteidigung oder Abschreckung, entwickelt werden könne.

Das Zwei-Ebenen-Problem der Attribuierung bleibt bestehen: Kann erstens ein Angriff eindeutig interpretiert sowie einem Täter zugewiesen werden und wenn ja, kann eine gezielte Antwort darauf erfolgen? Wenn zweitens die Möglichkeit eines Gegenschlags besteht, in welcher Form kann und sollte dieser erfolgen? Mit konventionellen oder digitalen Waffen? Aufgrund dieser Tatsache warnt das britische Forschungsinstitut »Chatham House« in einem im Zuge der Entwicklung der nationalen britischen Cyberstrategie er- >>

stellten Report davor, dass die Überwindung der Nichtattribuierung das größte Hindernis sei, die Anarchie im Cyberspace zu relativieren.

Die fehlende eindeutige Nachweisbarkeit der Identität eines Angreifers sowie die ihm inhärente Anonymität stellen auch den Begriff der Kriegsführung als eine notwendigerweise zielgerichtete und gegenseitige Aktivität in Frage. Denn entgegen der klassischen Auffassung von Kriegsführung nach von Clausewitz mangelt es im Cyberspace an einer unmittelbaren und offensichtlichen Beziehung zwischen Angreifer und Angegriffenem oder Verteidiger. Somit weiß nur der Angreifer, dass er einen Angriff ausführte. Das Opfer kann zwar von einem kriegerischen Akt sprechen, aber keine gezielten Kriegshandlungen initiieren, da der Angreifer sich stets im Schutz der Anonymität und Nichtnachweisbarkeit verstecken kann.

Der »kriegerische Akt« verliert seine Eindeutigkeit.

Die Erfahrungen aus Estland, Georgien und dem Iran verdeutlichen, dass die angegriffenen Staaten die Attacke erst bemerkten, als diese bereits im Gange war und die betreffenden Regierungen nicht wussten, ob und wie sie gegen wen hätten reagieren können. Die unmissverständliche Identifikation eines Gegners war unmöglich, und das Risiko, lediglich auf Vermutungen und Wahrscheinlichkeiten basierend, zurückzuschlagen blieb zu hoch. Martin Libicki, der als Mitglied der RAND Corporation zur Cyberkriegsführung forscht, formulierte trefflich, dass kein größerer Kontrast zwischen der Klarheit einer nuklearen Explosion und der Doppeldeutigkeit eines Cyber-Schlags bestehe.

Die genannten Angriffe bestätigten zwei elementare Eigenschaften des Sicherheitsdilemmas: die strukturelle Anarchie im Cyberspace sowie die dreifache Unsicherheit eigener Interpretationen, Antworten und der eigentlichen Absichten des Gegners. Man kann sogar argumentieren, dass die Natur des Cyberspace mit seiner bisweilen völligen Anonymität und Nicht-Attribuierun das Sicherheitsdilemma noch verschärft, denn die Machtakkumulation von Staaten in Form forcierter Cyberspace-Aktivität ist deutlich schwieriger zu beweisen als gängige, nachrichtendienstlich auswertbare Indikatoren insbesondere militärischer Macht. Neben der anzunehmenden Verschärfung stellt sich somit allerdings auch die Frage, inwiefern das klassische Konzept von Macht, auf dem das Sicherheitsdilemma basiert, sich eigentlich in eine Welt, die zunehmend vom Cyberspace geprägt ist, übertragen lässt.

Anonymität und Anarchie stellen in einer grenzenlosen Sphäre einen bedrohlichen Paradigmenwechsel dar. Beide Eigenschaften verschärfen das Sicherheitsdilemma gefährlich. Der Cyberspace beeinflusst oder verändert sogar das klassische Verständnis von Macht, da digitale Fähigkeiten konventionelle Machtsymbole, wie militärisches High-Tech-Gerät durch die Abhängigkeit zum Cyberspace, stark einschränken oder nivellieren könnten. Im schlimmsten Falle könnten Cyberattacken als Grund für reelle militärische Auseinandersetzungen (aus)genutzt werden. Durch die Anonymität und Nicht-Attribuierung besteht eine große Gefahr, dass unbeteiligte oder unschuldige Staaten in eine reelle militärische Auseinandersetzung geraten. ◂◂◂◂

Constantin Schüßler *hat International Security Studies an der University of St. Andrews studiert und dort seine Masterthese über Cyberkrieg und das Sicherheitsdilemma verfasst.*

Quellen und Links:

Studie »On Cyber Warfare« des Chatham House vom November 2010

Studie »In the Crossfire. Critical Infrastructure in the Age of Cyber War« von McAfee aus dem Jahr 2009

Studie »Cyberwarfare and its Impact on International Security« des United Nations Office for Disarmament Affairs vom 19. Februar 2009

Konfliktzone **Ostasien**

Wirtschaftsdominanz
und Geopolitik
im »pazifischen Jahrhundert«

ADLAS – Magazin für Außen- und Sicherheitspolitik zieht es zum Stillen Ozean: Mit der nächsten Ausgabe beginnt unsere neue Reihe, die wir das Jahr über verfolgen: »Konfliktzone Ostasien – Wirtschaftsdominanz und Geopolitik im ›pazifischen Jahrhundert‹«.

Wer sind die wichtigen Akteure im Raum Asien-Pazifik? Wie empfindlich ist das Gleichgewicht zwischen China und den USA? Und welche Rolle spielt eigentlich Europa? ***ADLAS*** **freut sich über alle Beiträge, die uns helfen, diese und mehr Fragen zu beantworten**.

Der Zankapfel

von Ingmar Zielke

Im Mittelmeer stationierte Aegis-Zerstörer der US Navy sollen mit der »Standard Missile« SM-3 feindliche ballistische Raketen abfangen.

Foto: US Navy

>>

Eine Kooperation der USA mit Russland im Bereich der Raketenabwehr wird auch nach der Wiederwahl von Barack Obama nur schwer zu realisieren sein. Zu fest sitzt das Denken in Dimensionen des Kalten Krieges in Moskau, zu sehr hat sich Washington bereits davon entfernt.

>> Es begann mit einem Lapsus: Unbeabsichtigt vor offenen Mikrofonen hat US-Präsident Barack Obama im März 2011 dem russischen Präsidenten Dmitri Medwedjew ein amerikanisches Entgegenkommen im Raketenabwehrstreit im Falle seiner Wiederwahl signalisiert. Seither wird darüber spekuliert, welche konkreten Schritte Washington einleiten könnte, um die russischen Sorgen zu zerstreuen. Warum haben es Washington und Moskau nicht verstanden, eine Lösung im Bereich der Raketenabwehr zu finden?

Erklärungen, die auf eine unterschiedliche Gefahrenanalyse der Kapazitäten des Iran, ein Fortbestehen der Mentalitäten des Kalten Krieges auf amerikanischer und russischer Seite oder innenpolitische Konstellationen eingehen, haben zwar allesamt ihre Berechtigung. Sie verkennen jedoch, dass diese Faktoren eher Symptome des bilateralen Verhältnisses zwischen Moskau und Washington im weitesten Sinne sind. Beispielsweise ist das politische Gewicht russischer Generäle oder russischer Rüstungsunternehmen, die fortwährend auf eine nukleare »Superwaffe« gegen die europäische Raketenabwehr drängen, nur durch die antagonistischen Beziehungen Russlands und Amerikas zueinander denkbar. Gleiches gilt für die populäre anti-amerikanische Rhetorik Wladimir Putins, die es der jetzigen Regierung erlaubt, eine »Belagerungsmentalität« zu erzeugen, um von der eigenen Legitimitätsfrage abzulenken.

Die Reaktionen Russlands auf die Fortschritte der US-Raketenabwehr rühren auch nicht allein von streng sicherheitspolitischen Überlegungen her. Zwar befürchtet man bahnbrechende amerikanische Entwicklungen. Dennoch gibt es einen Konsens im russischen Militär, nach dem die amerikanische Raketenabwehr im kommenden Jahrzehnt keine Gefahr für Russlands nukleare Zweitschlagfähigkeit darstellen würde.

Zum einen handelt es sich bei dem Verlust der realen (Verhandlungs-)Macht Russlands um eine psychologische Herausforderung, die bisher alle absteigenden Großmächte vor Probleme gestellt hat. Großbritannien hat sich etwa bis zum Ende der Suezkrise 1956 geweigert, den postkolonialen Charakter der Nachkriegswelt einzugestehen. Bei Frankreich dauerte es sogar bis zum Algerienkrieg 1963. Zum anderen sind »Anerkennung« für Moskau seitens des Westens und eine historisch gewachsene Angst vor »Einkreisung« wichtige Merkmale der russischen Diplomatie. Bereits die >>

VON KOOPERATION ZU KONFRONTATION:

Foto: George Bush Presidential Library

Raketenabwehr und Diplomatie 1990 bis 2000

Dass die Raketenabwehrkontroverse im letzten Jahrzehnt eine so prominente Stellung erlangen konnte, war zu Beginn der 1990er keinesfalls gewiss. George Bush senior und Michail Gorbatschow, später Bill Clinton und Boris Jelzin, sprachen gar von einem »globalen Raketenabwehrsystem«, bei dem die USA und Russland gemeinsam technologische Entwicklungen vorantreiben wollten.

Gleichzeitig versuchte Russland bereits, die von Clinton geförderte und von Moskau als ungefährlich eingestufte Kurzstreckenabwehr, die »Theater Missile Defense« (TMD), in ihrem Potential einzuschränken: Daher auch Moskaus Zögern, den START-2-Vertrag zu ratifizieren: Die

Bezeichnung des russischen Reiches als »Drittes Rom« in der Zarenzeit war vom Wunsch nach Status im westlichen Europa geprägt.

Erschwerend kommt hinzu, dass das ehemalige Imperium sich auf lediglich drei Faktoren stützt, die den eigens angestrebten Status einer Großmacht rechtfertigen: erstens der ständige Sitz im UN-Sicherheitsrat – dessen Relevanz von den USA in den letzten zwei Jahrzehnten zunehmend in Frage gestellt wurde –, zweitens der vom Weltmarkt abhängige Ressourcenreichtum Sibiriens sowie drittens und nicht zuletzt der Besitz von Nuklearwaffen. Russland scheint nicht gewillt, sein strategisches Gleichgewicht gegenüber den USA zu verlieren, zumal Atomwaffen durch die Erosion seiner konventionellen Streitkräfte nach Ende des Kalten Krieges für den Kreml noch an Bedeutung gewonnen haben.

Ein entscheidender, aber wenig beachteter Grund für die anhaltenden Spannungen betrifft die unterschiedlichen strategischen Ziele beider Staaten. Bei der diesjährigen Raketenabwehrkonferenz des »Royal United Services Institutes« (RUSI) wies der amerikanische Nato-Botschafter, Ivo Daalder, darauf hin, dass »wir nicht im Kalten Krieg, sondern im 21. Jahrhundert leben. Neue Zeiten verlangen neue Lösungen.« Demnach messen die USA dem Verhältnis zu Russland weitaus weniger Bedeutung bei, als dem Schutz ihres Landes und dem amerikanischer Verbündeter gegen neue Bedrohungen. Für Russland bleiben die USA dagegen der Hauptbezugspunkt der Außenpolitik. Die Prioritäten Amerikas sind expansiv und global, diejenigen Russlands hingegen beschränken sich auf die Sicherung des Status quo der internationalen Ordnung und (zumindest zunächst) die Eindämmung der USA im russischen »Hinterhof« in Osteuropa und Zentralasien.

Ein zweiter politischer »Stolperstein«, der damit einhergeht, ist die von Amerika dominierte Weltordnung. Letztlich verkörpert die Raketenabwehr die unipolare »Pax Americana« jenseits sämtlicher Verträge und einen besonders Anfang der 2000er Jahre offen ausgesprochenen Anspruch auf »absolute Sicherheit«. Wladimir Putin hat dann auch mehrfach auf das so genannte Sicherheitsdilemma der internationalen Beziehungen hingewiesen: Absolute Sicherheit für einen Staat kann nur mit dem Verlust von Sicherheit anderer Staaten einhergehen.

Die Raketenabwehr verkörpert die unipolare »Pax Americana« jenseits sämtlicher Verträge.

Aus seiner Position der Schwäche setzt sich Russland nun gegen die Erosion der internationa- >>

Neuauflage des »Strategic Arms Reduction Treaty« hätte Russland gezwungen, seine gegen die amerikanische Raketenabwehr wirksamste Waffe – landgestützte Langstreckenraketen mit nuklearen Mehrfachsprengköpfen – zu vernichten.

Ebenfalls parallel hatte die Clinton-Regierung im »Missile Defense Act« von 1999 bereits festgelegt, dass die USA den Aufbau einer für Russland problematischen Langstreckenraketenabwehr, die »National Missile Defense« (NMD), zum Schutz vor »unbeabsichtigten« chinesischen und russischen Angriffen und Attacken von »Schurkenstaaten« frühestmöglich beginnen sollten. Nach der Kündigung des ABM-Vertrags 2001 durch die Regierung unter George W. Bush begann 2004 der Aufbau von Abfangraketen in Alaska und Kalifornien.

Dennoch war die Reaktion Moskaus auf die Kündigung des zentralen Waffenkontrollvertrages des Kalten Krieges gedämpft. Wladimir Putin, Kremlchef seit 2000, hoffte im Gegenzug auf eine verhaltene Rhetorik Washingtons in Bezug auf den russischen Tschetschenien-Krieg sowie Unterstützung für Russlands Wunsch, der Welthandelsorganisation beizutreten. Dies sollte auch eine freundschaftliche Umgangsweise nach den Terroranschlägen des 11. September erreichen, als Moskau amerikanischen Militärbasen in Zentralasien zustimmte und eigene Militärbasen in Vietnam und Kuba auflöste.

Bereits davor hatte Putin Signale ausgesandt, die eine dramatische nukleare Abrüstung der USA und Russlands im Sinne Gorbatschows als

Noch unter George W. Bush war die landgestützte »Theatre High Altitude Area Defense« THAAD Bestandteil der Raketenabwehr. Unter Barack Obama verlagert sich die Infrastruktur mehr und mehr auf See.

Foto: US Missile Defense Agency

len (Nachkriegs-) Ordnung ein. Zwar ist das Abkommen »New START«, das Barack Obama und Putins Vorgänger Dmitri Medwedjew im April 2010 unterzeichnet haben, als eine teilweise Rückkehr zur Rüstungskontrolle des Kalten Krieges zu werten; dennoch insistierte die Obama-Administration darauf, dass die Raketenabwehr in keinerlei Weise eingeschränkt würde.

Die Raketenabwehrproblematik aber steht stellvertretend für die Gesamtproblematik: Washington stellt im Bewusstsein seiner gegenwärtigen Überlegenheit einzelne, aus dem Kalten Krieg herrührende Beschränkungen in Frage; Moskau hält an der Ordnung des Kalten Krieges fest und will gleichberechtigt behandelt werden – eine Forderung, die den realen militärischen und politischen Machtverhältnissen entgegensteht.

Zudem geht es auch um geostrategische Aspekte. Bereits die drei Nato-Erweiterungsrunden haben Tatsachen geschaffen, während sie Russlands Rolle in Europa nicht abschließend geklärt haben. Davor haben zahlreiche amerikanische Russlandexperten – unter anderem der »Vater der amerikanischen Eindämmungspolitik« George Kennan – bereits in den 1990er Jahren gewarnt. Hinzu kam der Drang der Administration von George W. Bush, das Militärbündnis bis in die Ukraine und nach Georgien auszuweiten: Russland befürchtete, die USA könnten dann auch Kiew in das System der Raketenabwehr einspannen. In der Tat: Die Stationierung solcher strategischer Abwehrwaffen nach der Erweiterung kann man als Versuch der »Zementierung« der amerikanischen Einflusssphäre in (Ost-) Europa sehen.

>>

erstrebenswert bezeichneten. So sprach der russische Präsident, wie zuvor der letzte sowjetische Staatschef, von einer wünschenswerten »minimum sufficiency« der russischen Nukleardoktrin und tiefgreifenden nuklearen Abrüstungen. Die diplomatische Ouvertüre Putins war von ökonomischen Zwängen beeinflusst, die eine nukleare Modernisierung der russischen Streitkräfte nicht wünschenswert erscheinen ließen.

Der Vertrag von Moskau, offiziell »Strategic Offensive Reductions Treaty« (SORT), im Jahr 2002 war dann auch eine amerikanische Konzession an den russischen Wunsch, an der bilateralen Abrüstungstradition festzuhalten – auch wenn sich das bewusst knapp gehaltene Dokument stark an die Wünsche Washingtons anlehnte und sich so fundamental von den langwierigen Konsultationen des Kalten Krieges unterschied. Beispielsweise sah SORT, im Gegensatz zu START II, keine Verifikationsmechanismen oder einen konkreten Zeitplan zum Abbau von Sprengköpfen vor. Beide Seiten betonten zudem ihre Bereitschaft, in Sachen Raketenabwehr eng zu kooperieren. Allerdings hat weder das mittlerweile von den USA abgebrochene Projekt eines

Zurück in die Zukunft? Die US-Raketenabwehr war schon einmal vertraglich gebunden.

Angesichts der unterschiedlichen globalen Zielsetzungen und geostrategischen Überlegungen, die sich teils diametral gegenüberstehen, ist nicht verwunderlich, dass eine Problemlösung, geschweige denn eine Kooperation im Bereich der Raketenabwehr bisher ausgeblieben ist. Nato-Generalsekretär Anders Fogh Rasmussen betont zwar kontinuierlich die Potentiale einer verstärkten Raketenabwehr-Kooperation mit Russland. Allerdings liegen zwischen den Vorstellungen der Nato und Moskaus Welten. Letzteres drängt auf eine volle Gleichberechtigung, auch um mehr Mitspracherechte in Angelegenheiten europäischer Sicherheit zu erlangen und die eigene Isolation aufzubrechen.

Die USA unterscheiden dagegen zwischen dem Schutz ihrer Verbündeten und dem Russlands. Sie befürworten lediglich einen minimalen Datenaustausch zwischen zwei getrennten Abwehrschirmen. Die meisten vergangenen Versuche zur Zusammenarbeit sind zudem an restriktiven Technologietransfers, mangelndem Vertrauen und fehlender Kooperationsbereitschaft auf diversen bürokratischen Ebenen gescheitert. Auch ist unklar, inwiefern Russland überhaupt sinnvoll zum westlichen Abwehrschirm beitragen kann.

Die »Wiedergeburt« der amerikanischen Raketenabwehr nach Ende des Kalten Krieges nun ist auch Teil einer unilateralen außenpolitischen Tendenz der USA, die sich auch im Bereich des internationalen Rechts wiederfinden lässt: Sie wirkt sich in der Distanzierung zu Abrüstungsverträgen, des »marktwirtschaftlich-demokratischen Kreuzzugs« und der präventiven Kriegsführung unter Umgehung des UN-Sicherheitsrats seit Ende der 1990er Jahre aus.

Moskau klammert sich an die Ordnung des Kalten Krieges.

Diese Tendenz ähnelt auch denen anderer ehemaliger Imperien, wie beispielsweise des britischen Empire im 19. Jahrhundert. Wie Robert Jervis, Professor für Internationale Beziehungen an der Harvard-Universität betont: »No matter how secure states are, only rarely can they be secure enough, and if they are currently very powerful, they will have strong reasons to act now to prevent a deterioration that could allow others to harm them in future.«

Dennoch steht hinter dem Nutzen der Raketenabwehr ein Fragezeichen – insbesondere für Europa. Die Nichtratifizierung des START II-Vertrags und die damit ausbleibende Vernichtung russischer Mehrfachsprengköpfe, die Eskalation des Streits im Jahr 2007 und der ein Jahr >>

russisch-amerikanischen Satellitensystems, noch ein Datenzentrum zur gemeinsamen Frühwarnung zu einem echten Durchbruch geführt.

Die bilateralen Beziehungen verschlechterten sich deutlich, als die US-Regierung unter George W. Bush Anfang 2007 bilaterale Verträge mit Polen und Tschechien zur Stationierung von Abfangsystemen für Langstreckenraketen und einer Radaranlage anstrebte. Gleichzeitig haben Spannungen in anderen Bereichen für eine kühlere Beziehung gesorgt – die amerikanische Invasion im Irak, die von den USA unterstützten »coloured revolutions« in Georgien und der Ukraine, die amerikanischen Nato-Erweiterungspläne um eben jene Staaten sowie die im Raum stehende staatliche Anerkennung des Kosovo. Kooperationsvorschläge Putins, nach denen eine gemeinsame Radaranlage in Aserbaidschan den Aufbau des Systems in Polen und Tschechien hätte ersetzen sollen, stießen in Washington auf taube Ohren, auch weil der russische Vorschlag offen ließ, wie die US-Raketen in Polen ersetzt werden könnten.

Dementsprechend enthusiastisch nahm Dmitri Medwedjew nach seiner Amtsübernahme Barack Obamas Pläne die Pläne für einen neuen Abrüstungsvertrag (»New START«) und eine amerikanische Abkehr von den Raketenabwehrplänen in Polen und Tschechien wieder auf. An die Stelle der von Russland so vehement kritisierten Langstreckenraketenverteidigung in Polen und einer Radaranlage in Tschechien traten ein für den Kreml zunächst unproblematisches

Verstehen sich blendend: der wiedergewählte Barack Obama und der abgetretene Dmitri Medwedjew

Foto: White House

später folgende Georgien-Krieg sowie die allgemeine Verhärtung der diplomatischen Fronten stehen in keinem Verhältnis zu fragwürdigen Vorteilen. So ist eher noch kritisch zu hinterfragen, in welchem Ausmaß die Raketenabwehr zur Modernisierung russischer Nuklearstreitkräfte beigetragen hat. Zweifelhaft bleibt ebenfalls, ob sich aus einem Entgegenkommen der USA gegenüber Russland nicht sogar tatsächlicher Nutzen, beispielsweise bei der schrittweisen Eliminierung taktischer Nuklearwaffen in Russland, ergeben könnte.

Die Chancen auf eine Zusammenarbeit würden sich vergrößern, sollten die USA erkennen, dass ihre »unipolarer Moment« uneingeschränkter Macht seine Grenzen erreicht hat, und eine realistischere Grundhaltung in Washington einzieht. So hat Zbigniew Brzezinski, der ehemalige Nationale Sicherheitsberater Jimmy Carters, im Hinblick auf die wachsenden Herausforderungen in Asien festgestellt, dass eine amerikanisch-russische Annäherung im eigentlichen Interesse der USA liege.

Demnach könnte eine Annäherung im Raketenabwehrstreit nur dann erfolgen, wenn es mit einem strategischen Wandel der USA einhergeht und sich Russland als wichtiger strategischer Partner erweist. Einiges deutet darauf hin, dass Barack Obama genau deshalb eine engere Zusammenarbeit mit Moskau anstrebt, jedoch gleichzeitig unter innenpolitischem Druck steht. In der Tat bleibt »Russophobie« in Washington auch zwei Dekaden nach dem Fall der Sowjetunion stark ausgeprägt. >>

seegestütztes System zum Abfangen von Kurz- und Mittelstreckraketen und eine Radaranlage in der Türkei. Dennoch: Auch Obama rückte nicht von einer späteren Stationierung von Langstreckenabwehrsystemen in Osteuropa ab.

Russland behauptet nun, dass die letzte, für 2020 avisierte Ausbaustufe der europäischen Raketenabwehr seine strategische Abschreckung gefährden könnte. Zwar begrüßt der

Die Machtlosigkeit Moskaus gegenüber dem »globalen Leviathan« aus Washington ist deutlich erkennbar.

Kreml die Feststellung im »New START«-Abkommen von 2010, dass offensive und defensive Waffen in einem wechselseitigen Verhältnis stünden und auch die Raketenabwehr als Gefahrenquelle gewertet werden könne. Allerdings greift diese Passage nur auf die Erkenntnisse des ABM-Vertrags zurück.

Immerhin scheint ein Ausstieg Russlands aus New START möglich zu sein, sollte Moskau entscheiden, seine vertraglichen Abrüstungsverpflichtungen aufgrund der US-Raketenabwehr nicht einhalten zu können. Russland wünscht sich ferner ein völkerrechtliches Dokument, welches dem Kreml garantieren soll, dass sich die Raketenabwehr niemals gegen Russland richten wird. Das würde eine qualitative und quantitative

Ein löblicher Lösungsansatz wie das kürzlich von der »Euro-Atlantic Security Initiative« der »Carnegie Endowment for International Peace« ausgearbeitete Konzept eines gemeinsamen Russland-Nato-Frühwarnsystems greift zwar konstruktiv auf die Idee einer multilateralen Kooperation zurück. Es überschätzt jedoch die Entscheidungsbefugnisse des Militärbündnisses. Die Wurzel des Problems sowie dessen Lösung liegt in den bilateralen Beziehungen zwischen Washington und Moskau.

Viel wäre bereits gewonnen, wenn zwischen beiden ein Dialog ähnlich dem der 1990er Jahre zustande käme, der darauf ausgelegt ist, technologische Begrenzungen der US-Raketenabwehr auszuloten. Das könnte ein neuer nuklearer Abrüstungsvertrag in der Nachfolge von New Start fixieren: Er könnte die taktischen Nuklearwaffen Russlands und der USA, konventionelle Langstreckenpräzisionswaffen und eben Raketenabwehr in einem Dokument bündeln.

Bis dahin ist es noch ein langer Weg. Kurzfristig scheint die Möglichkeit einer Annäherung eher in einem realpolitischen Quid-pro-Quo zu liegen. So könnte ein Ausgleich, ähnlich wie bei den jüngsten Iran-Resolutionen, in einer russischen Kooperation im Syrien-Konflikt bei einem gleichzeitigen Entgegenkommen Washingtons im Bereich der Raketenabwehr liegen. ◂◂◂◂

Zementiert die Stationierung von strategischen Abwehrwaffen die amerikanische Einflusssphäre?

Ingmar Zielke *ist Doktorand am »War Studies Department« des King's College in London.*

Quellen und Links:

Website der »Euro-Atlantic Security Initiative« der »Carnegie Endowment for International Peace«

Tom Z. Collina: »Failure to Launch – Why did America just spend $30 billion on a missile defense system that doesn't work?« in der *Foreign Policy* vom 12. September 2012

Nikolai Sokov: »Nato-Russia Disputes and Cooperation on Missile Defense« in *James Martine Center for Nonproliferation Studies* vom 14. Mai 2012

Dirk Schuchhardt: »Theologie statt Technik – Überzogene Erwartungen an eine territoriale Raketenabwehr für Europa« in den *Atlantischen Beiträgen* Nr. 4, Mai 2012

Begrenzung des US-Raketenabwehrsystems bedeuten und Amerika und seinen Verbündeten die Freiheit nehmen, flexibel auf Gefahren zu reagieren. Washington lehnt ein solches Dokument ab.

Moskaus Reaktionsschema lässt seine Machtlosigkeit gegenüber der Politik des »globalen Leviathans« aus Washington deutlich erkennen. Im vergangenen Jahrzehnt wiederkehrende Drohungen, den Intermediate-Nuclear-Forces-Vertrag (INF), der den Bau atomarer Mittelstreckenraketen in den USA und Russland seit 1988 verbietet, zu kündigen, oder die Aussetzung des Vertrags über konventionelle Streitkräfte in Europa (KSE) sind für Russland von zweifelhaftem strategischem Nutzen. Noch unglaubwürdiger ist das nukleare Säbelrasseln russischer Generäle.

Eine Hauptsorge des Kremls scheint dann auch eher eine gefürchtete »Isolation« von Europa zu sein. Dies würde teilweise erklären, warum Moskau zwar beständig die Dringlichkeit eines Schutzes vor »Schurkenstaaten« – die Russland im Übrigen nicht im Iran oder Syrien, sondern in Pakistan und Saudi-Arabien sieht – bezweifelt, um gleichzeitig jeder Art von Raketenabwehr-Kooperation mit Europa und den USA zuzustimmen, sollte der Westen Russland als gleichberechtigten Partner einbeziehen. Andererseits ist der Kreml der Gefahr ausgesetzt, bei einer weitgehenden Kooperation mit den USA China zu verprellen, zumal die russisch-chinesische Annäherung der letzten Jahrzehnte auch auf einer Kritik der amerikanischen Raketenabwehr fußte. <<

Radikal, brutal, erfolgreich

von Nils Metzger

Neben der »Freien Syrischen Armee« kristallisiert sich mit »Jabhat al-Nusra« im blutigen Kampf gegen das Assad-Regime eine islamistische Gruppe heraus, die mit Autobomben und Selbstmordattentaten von sich reden macht und immer mehr Rekruten anzieht.

Für die USA ist sie der Beweis, dass Al-Qaida im syrischen Bürgerkrieg kräftig mitmischt.

>> Keine Fotos, keine Videoauftritte – eine verzerrte Stimme ist das einzige Lebenszeichen von dem Menschen, der sich Abu Muhammad al-Golani nennt. Und doch horchen Diplomaten, Terrorexperten und Militärs gleichermaßen auf, wenn sich die mysteriöse Stimme der syrischen »*Jabhat al-Nusra*« (»Unterstützungsfront«) zu Wort meldet. Der mysteriöse Sprecher der islamistischen Miliz hat den Dschihad gegen Baschar al-Assad ausgerufen. Aber existiert er überhaupt? Ist Golani eine einzelne Person, oder nutzen ihn voneinander unabhängige Gruppen inzwischen als Pseudonym, damit der Glanz der wohl kompromisslosesten Miliz im syrischen Bürgerkrieg auf sie abfärbt? >>

Fakten gibt es wenige, denn Jabhat al-Nusra ist im Kampf gegen das Regime von Bashar al-Assad so allgegenwärtig wie öffentlichkeitsscheu. Im Januar 2012 tauchten ihre Kämpfer erstmals in einem dreiviertelstündigen Propagandavideo auf, das in Dschihadisten-Netzwerken kursiert. Die Gruppe sei erstklassig vernetzt, schreibt der Journalist und Terrorismusforscher Aron Lund in einem Bericht des »Schwedischen Instituts für Internationale Angelegenheiten«: »Die Al-Nusra-Front ist die Organisation, die am ehesten Anerkennung von Al-Qaida erwarten kann«, lautet sein Resümee. Gleichzeitig hat Jabhat al-Nusra im Laufe des Jahres einen rasanten Wandel durchlaufen.

Gründete ihr Ruhm ursprünglich noch auf Selbstmordattentaten und Autobomben in Damaskus und anderen Städten, so wirbt sie inzwischen immer mehr Kämpfer anderer Brigaden aus Aleppo und Umgebung ab, wodurch auch der Anteil ausländischer Rekruten in ihren Reihen sinkt, insbesondere aus dem Libanon und Jordanien. Sollen ihre Anhänger noch Anfang 2012 nur ein Prozent der Kämpfer der »Freien Syrischen Armee« (FSA) gezählt haben, so machen sie, laut Angaben von moderaten syrischen Aufständischen gegenüber der *Washington Post*, inzwischen bis zu neun Prozent der losen Koalitionstruppe aus. Dabei ist die Front finanziell unabhängig von der FSA: Privatpersonen von der arabischen Halbinsel unterstützen sie meist direkt. In dem umkämpften Aleppiner Stadtteil Saif al-Daula, wo die Islamisten einen wahrnehmbaren Teil der Kämpfer stellen, operiert sie aber teils gemeinsam mit FSA-Verbänden – was nicht immer reibungslos verläuft. Wiederholt endeten Versuche einzelner Milizen, Angehöriger anderer Verbände wegen Plünderungen oder Diebstahl zu verhaften, in wilden Schießereien. Nusra-Anhänger ignorierten mehrfach die Anweisung der FSA-Führung, nicht in kurdische Gebiete einzudringen

Foto: Zyzzzzzy / lizensiert gemäß Creative Commons Attribution 2.0 Generic

Am 3. Oktober 2012 explodierten am »Saadallah-Al-Jabiri-Platz« in Aleppo unweit eines Offiziersclubs der syrischen Armee drei Autobomben. Mindestens 34 Menschen starben, Jabhat al-Nusra übernahm die Verantwortung.

Welche Rebellengruppe möchte nicht, dass der Glanz der wohl kompromisslosesten Miliz auf sie abfärbt?

Die Erklärung des ominösen Sprechers der Dschihadistengruppe, den Waffenstillstand, den UN-Sonderbotschafter Lakhdar Brahimi für das islamische Opferfest Ende Oktober verhandelt hatte, nicht achten zu wollen, zeigte, wie unberechenbar die Gruppe selbst für andere Rebellen ist und wie unklar ihre politischen Ziele sind. Um- >>

stände, die zu betonen die staatlichen syrischen Medien nicht müde werden. Zur Frage nach einer möglichen Nachkriegsordnung etwa trug Sprecher Golani bislang nicht mehr als die Forderung nach einem »Gottesstaat« bei.

Jabhat al-Nusras Erfolg tut das keinen Abbruch: War die Front vor einem Jahr noch ein radikales Randphänomen, das mit brutalen Anschlägen auch auf Zivilisten und Journalisten – mit bis heute circa 150 Toten – viele verschreckte, kämpfen heute einigen Schätzungen zufolge bis zu 10.000 Kämpfer »diszipliniert«, wie der *Christian Science Monitor* befürchtet, unter ihrem Banner an vorderster Front. Zuletzt machten die Islamisten in Aleppo damit von sich reden, dass sie in der hungernden Millionenstadt Aleppo Teile der Brotvergabe übernahmen, nachdem sich Teile der kriegsmüden Bevölkerung über die Arbeit der FSA beklagtendie Unfähigkeit der FSA beklagten, ihnen eine zuverlässige Versorgung mit alltäglichen Bedarfsgütern zukommen zu lassen.

Noch weiter im Norden, nahe der kurdischen Stadt Ras al-Ayn, kommt es immer wieder zu Zusammenstößen kurdischer Milizen mit Jabhat al-Nusra. Dass sich die Kurden aus dem Bürgerkrieg weitgehend heraus halten, legen ihnen viele radikale Gruppen als Unterstützung des Regimes aus.

Anscheinend auch auf die zunehmend alarmierenden Berichte über die Gruppe hin haben die USA mittlerweile Konsequenzen gezogen: Sie erklärten die »Unterstützungsfront« am 11. Dezember zur terroristischen Organisation, indem sie sie zum Ableger von Al-Qaida gemacht haben. »Al-Nusra hat versucht, sich selbst als Teil der legitimen syrischen Opposition darzustellen«, erklärte die Sprecherin des amerikanischen Außenministeriums, Victoria Nuland. »Tatsächlich ist sie aber der Versuch von Al-Qaida im Irak, den Kampf des syrischen Volkes für die eigenen bösen Absichten auszunutzen.« Weder Al-Qaida noch Jabhat al-Nusra haben diese vermutliche Verbindung bisher bestätigt. ◂◂◂◂

Quellen und Links:

Interview des *Time Magazine* mit Abu Adnan, einem Offiziellen von Jabhat al-Nusrah, vom 25. Dezember 2012

Aron Lund: »Aleppo and the Battle for the Syrian Revolution's Soul«, Bericht der Carnegie Endowment for International Peace vom 4. Dezember 2012

Bericht von *Aljazeera* vom 11. Dezember 2012
Presseerklärung des US Department of State vom 11. Dezember 2012

Kommentar von David Ignatius in der *Washington Post* vom 30. November 2012

Bericht des *Christian Science Monitor* vom 27. November 2012

Aron Lund: »Syrian Jihadism«, Forschungsbericht des Swedish Institute of International Affairs vom 14. September 2012

Illustration: »Syria Violence« von Surian Soosay / lizensiert gemäß Creative Commons Attribution 2.0 Generic

Foto: CIA

Von bösen Mächten gut behütet

von Michael Seibold

Wie viel Böses darf man tun, um Gutes zu erreichen? Dieses Grunddilemma internationaler Beziehungen findet seine Zuspitzung in der Halbschattenwelt der Geheimdienste. Bei der Terrorabwehr oder beim Ausspionieren fremder Mächte helfen manchmal nur Mittel, die rechtlich und moralisch fragwürdig sind.

Das Thema beschäftigt Philosophen bereits seit Jahrhunderten – und Kritiker der amerikanischen Central Intelligence Agency nach dem Tod Osama Bin Ladens erneut.

>> Wenige Monate nach dem Tode Osama bin Ladens bestätigte die US-Regierung Berichte, denen zufolge sich amerikanische Agenten bei der Suche nach dem Terrorchef auch als Polio-Impfteam getarnt hatten. Geheimdienstliche Quellen ließen vermuten, dass sich bin Laden in der pakistanischen Garnisonsstadt Abbottabad versteckt hielt; die falschen Impfteams sollten nun mittels Impf-Wattestäbchen DNS-Spuren um den vermuteten Aufenthaltsort herum sammeln. Hätte der Gentest zumindest auf Verwandte bin Ladens hingedeutet, wäre das der endgültige Hinweis auf dessen Versteck gewesen. Am Ende blieb die Aktion wirkungslos: Die CIA entdeckte keine eindeutigen Genspuren; aber andere, »normalere« Quellen waren eindeutig genug für den späteren Zugriff.

Das Bekanntwerden der Aktion sorgte dennoch für Aufruhr: Gesundheits- und humanitäre >>

Organisationen beklagten den Rückschlag für die Bemühungen, Polio auch in Pakistan auszurotten. Durch die Aktion der CIA sei das Impfprogramm vollends in Verruf geraten, denn schon lange ging das Gerücht in Pakistan um, die westlichen Ärzte seien nicht im Auftrag der Menschlichkeit, sondern als Handlanger der USA unterwegs. Neben diesen konkreten Auswirkungen hagelte es Kritik aber vor allem auf moralischer Ebene: »Es hätte einen besseren, einen ethischeren Weg geben müssen«, kommentierte etwa der britische *Guardian*. Für Tom Scocca vom *Slate Magazine* enthüllte der Skandal »den moralischen Bankrott der amerikanischen Schlapphüte.«

Der Vorfall von Abbottabad lenkt den Blick auf das ethische Dilemma, in denen Nachrichtendienste stecken. Was ist ethisch erlaubt, um an Informationen zu gelangen, von denen vielleicht hunderte Menschenleben abhängen? Zugespitzt stellt sich diese Frage besonders deutlich im so genannten »ticking bomb«-Szenario: Darin konnten die Behörden ein Mitglied einer Terrorzelle, die unmittelbar einen Anschlag plant, festnehmen. Wo die Gruppe zuschlagen will – wo also die Bombe tickt und wann sie detonieren soll – ist unklar. Welche Mittel dürfen und sollten die Ermittler nun anwenden, um von dem Festgenommenen diese Informationen zu erlangen? Dramatische Wirklichkeit wurde das Szenario im September 2002, als Frankfurter Polizisten dem Kindesentführer Magnus Gäfgen körperliche Gewalt androhten, sollte er den Aufenthaltsort des Kindes nicht verraten – zu spät, wie sich herausstellte: Gäfgen hatte sein Opfer bereits kurz nach der Entführung ermordet. Die Androhung von Folter, das machten Gerichte danach aber deutlich, war auch in diesem Fall eine unmenschliche Behandlung und ohne Ausnahme verboten.

Nicht immer sind die Fälle so extrem, und selten eine einzelne Information so offensichtlich entscheidend, um eine Straftat zu verhindern oder Leben zu retten. Aber auch weniger einschneidende Maßnahmen – beispielsweise beim »Verwanzen« von Räumen oder beim Erschleichen von Informationen – können Rechte anderer verletzen.

Die amerikanische Politikwissenschaftlerin Toni Erskine unterscheidet zwischen drei Herangehensweisen an das Problem: eine »realistische«, eine »konsequentialistische« und eine »deontologische« Sicht der Dinge. Für Realisten steht das Handeln und die Staatsräson der eigenen Nation im Mittelpunkt ihrer Weltanschauung. Sie handeln aber keineswegs komplett amoralisch – für Realisten ist Handeln im Sinne des Staates moralisches Handeln. Darauf hatte schon Thomas Hobbes abgezielt: Herrscher dürften demnach zur Wahrung der Sicherheit der Bürger nicht nur Spione aussenden, es wäre im Gegenteil sogar ein schweres Versäumnis, dies nicht zu tun! Aus den anderen beiden Perspektiven dürfte der realistische Ansatz dennoch unmoralisch sein, kommt doch der schwammige Begriff des Staatsinteresses einem – oft missbrauchten – Freibrief gleich.

Konsequentialisten bewerten ihr Handeln – wie schon der Name verrät – nach dessen Konsequenzen, so Erskine: »Der richtige Weg zu handeln ist der, der am meisten Gutes tut.« Informationsgewinnung ist moralisch gerechtfertigt, wenn die Ergebnisse zu positiven Entwicklungen führen; oder anders ausgedrückt: Der Zweck kann die Mittel heiligen, wenn er denn wichtig genug ist. Positiv ist dabei aber nicht nur auf den eigenen Staat bezogen, sondern auf die Allgemeinheit. Für Michael Herman, ehemals hochrangiges Mitglied der britischen Intelligence Community, muss Nachrichtengewinnung moralisch daran gewertet werden, »ob sie eine bessere Welt oder eine schlechtere Welt erzeugt«. Die Logik der Konsequentialisten ist aber brüchig: was ist »gut«, was »schlecht«? Eine Frage, die in vielen Kulturräumen dieser Welt unterschiedlich beantwortet werden dürfte.

Und selbst wenn es einen allgemein verbindlichen Gut-und-Böse-Katalog gäbe, so wäre es >>

»Nichts – nicht einmal Menschenleben zu retten – rechtfertigt Folter«, erklärte die ehemalige MI5-Chefin dem britischen Oberhaus.

immer noch unmöglich, jede letzte Konsequenz des eigenen Handelns vorab zu wissen und zu messen. Oft wissen Geheimdienstangehörige vor Ort noch gar nicht, wozu das Wissen einmal dienen wird. Und im Falle der Impfteams von Abbottabad etwa ist heute noch gar nicht abzusehen, welche Langzeitfolgen der Plan für die Bemühungen, flächendeckende gesundheitliche Versorgung einzurichten und für die Stabilität der Region noch haben wird. Die Vereinten Nationen zogen sich beispielsweise nach mehreren Anschlägen islamischer Extremisten auf (echte) Impfteams im Dezember 2012 aus dem Impfprogramm gegen Polio zurück – ein schwerer Rückschlag für die weltweiten Bemühungen, diese Krankheit endgültig auszurotten.

Der dritte, deontologische Ansatz, ist absolut: Gewisses Handeln ist moralisch immer falsch und unter keinen Umständen vertretbar. Prinzipien sind hier ausschlaggebend, nicht das Abwägen zwischen relativem Gut und Böse. Eine schlechte Tat wird danach nicht durch deren gute Wirkung gerechtfertigt. Immanuel Kant vertrat 1797 diese Ansicht in seinem Aufsatz »Über ein vermeintes Recht aus Menschenliebe zu lügen«. Und in seiner »Metaphysik der Sitten« aus dem gleichen Jahr bezog er sich ausdrücklich auch auf Agenten: Zu den nicht erlaubten Mittel im Kriege gehört demnach »seine eigne Untertanen zu Spionen, diese, ja auch Auswärtige zu Meuchelmördern, Giftmischern […] oder auch nur zur Verbreitung falscher Nachrichten, zu gebrauchen: mit einem Wort, sich solcher heimtückischen Mittel zu bedienen, die das Vertrauen, welches zur künftigen Gründung eines dauerhaften Friedens erforderlich ist, vernichten würden.«

Das moralische Dilemma der Geheimdienste lässt sich nicht im stillen Kämmerlein lösen.

Die Central Intelligence Agency wirbt mit freundlichen Mitarbeitern um Nachwuchs. Der Nachrichtendienst legt dafür bei den Bewerbern Wert auf »Ehrlichkeit und einen hohen Standard persönlicher Ethik.«

Foto: CIA

Das im Fall Gäfgen bekräftigte absolute Folterverbot entspricht der deontologischen Sichtweise – kein Zweck kann Folter rechtfertigen. Eine Sicht, die auch die ehemalige Direktorin des britischen Inlandsgeheimdienstes MI5, Eliza Manningham-Buller, teilt: »Nichts – nicht einmal Menschenleben zu retten – rechtfertigt Folter«, erklärte sie 2010 im britischen Oberhaus. Das Kant'sche Verbot gilt aber auch für weniger schlimme Taten: Spionieren, Abhören, Unterwandern sind ebenfalls nicht erlaubt – für den Philosophen widersprach selbst eine Notlüge den deontologischen Anforderungen an einen mora- >>

lisch unanstößigen Lebenswandel. Das aber würde in seiner Konsequenz nicht nur nachrichtendienstliche, sondern letztlich auch die polizeiliche Arbeit erschweren, ja unmöglich machen.

Keine der drei Sichtweisen bietet daher eine handhabbare Lösung für das moralische Dilemma von Nachrichtengewinnung und Geheimdiensten. Was stattdessen notwendig ist – und auch von Praktikern wie Manningham-Buller gefordert wird – ist ein intensiver gesellschaftlicher Dialog über die Ziele und Mittel der Geheimdienste, der in Gesetzen mündet, die durch einen breiten Konsens legitimiert sind. Auf dem Fundament unveräußerlicher Menschenrechte können nur so die schützenswerten Ziele und die nicht immer ganz einwandfreien Mittel in Einklang gebracht werden. ◂◂◂◂

Quellen und Links:

Meldung des *National Public Radio* vom 20. Dezember 2012 über den Ausstieg der Vereinten Nationen aus dem Polio-Impfprogramm in Pakistan

Kommentar von Heidi Larson im *Guardian* am 27. Mai 2012 zur Aktion der CIA

Hintergrundbericht von *Slate* vom 25. Juli 2011 über den »moralischen Bankrott« der US-Geheimdienste

Auszug aus Immanuel Kants »Metaphysik der Sitten« aus dem Jahr 1797 zum Völkerrecht

Kein Einsatz, nirgends

von Sebastian Hoffmeister

Für Missionen wie in Mali wurden die EU-Battlegroups einst geschaffen. Und doch sitzen sie jetzt weiter zuhause in den Kasernen. Mehr Handlungsfähigkeit traut sich die Politik einfach nicht zu.

Die Straße nach Timbuktu war frei, aber Frankreichs Verbündete Deutschland und Polen ließen sich nicht blicken.

Foto: Annabel Symington / lizensiert gemäß CCA 2.0 Générique

>> Die »Kampfgruppe Weimar« ist einsatzbereit – theoretisch. Der martialische Name, erdacht von den Außenministern Polens, Frankreichs und Deutschlands, bezieht sich auf das »Weimarer Dreieck«. So nennt sich das regelmäßige trilaterale Treffen zwischen den drei Staaten – die im ersten Halbjahr 2013 auch die Truppen für die in Bereitschaft stehende »Battlegroup« der Europäischen Union stellen.

Nach ursprünglicher Planung sollten freilich zu jeder Zeit gleich zwei Battlegroups bereit stehen – doch die Mitgliedsstaaten der Union meldeten nur ausreichend Truppen für einen einzigen Verband. Europas militärische Feuerwehr muss also mit halber Stärke auskommen. Und obwohl es im Hinterhof lichterloh brennt, darf sie nicht ausrücken.

Das einst hochtrabend begonnene Vorhaben ist damit weitgehend auf dem Boden der Realpolitik angekommen. Eigentlich sollten die Battlegroups den Weg aus der Handlungsunfähigkeit Europas in sicherheitspolitischen Fragen aufzeigen: Auf dem Balkan, in Ruanda war schmerzhaft klargeworden, dass ohne die Vereinigten Staaten für Europa eine eigenständige militärische Handlungsfähigkeit nicht gegeben war.

Die Geburtsstunde der Battlegroups schlug 2004. Die Aufstellung der Verbände verfolgte zwei Ziele: Zum einen sollten sie der EU die Fähigkeit verleihen, unabhängig von Nato und Amerika rasch eigenständige begrenzte Operationen durchzuführen. Zum anderen sollten sie Antreiber der Transformation sein. Die Ermutigung der Staaten, ihre Streitkräfte rasch in ein einsatzfähiges Format zu bringen, war erklärtes Ziel des Beschlusses einer europäischen »Military Capability Commitment Conference«.

Eine EU-Battlegroup umfasst etwa 1.500 Soldaten. Im Kern handelt es sich um ein verstärktes Infanteriebataillon, von Kampfunterstützungstruppen und weiteren Kräften flankiert. Hinzu kommt ein Hauptquartier. Luftstreitkräfte oder Logistikelemente sind nicht mit umfasst, diese müssen individuell »dazubestellt« werden.

Frankreich hat seit Mitte Januar in Mali etwa 2.500 Soldaten im Einsatz. In dieser Dimension wird deutlich: Es wäre ohne weiteres möglich, jedenfalls einen Teil dieser Kräfte durch eine EU-Battlegroup zu stellen. Hätten sich die europäischen – wie ursprünglich vereinbart – sogar dazu durchringen können, zwei Battlegroups aufzu- >>

stellen, wäre sogar der gesamte Einsatz im EU-Rahmen bestreitbar.

Doch was hat einen gemeinsamen Einsatz bisher verhindert und verhindert ihn weiter? Offene oder selbst versteckte Kritik am französischen Vorgehen findet sich kaum. Es scheint sich um einen grundsätzlich konsensfähigen und überschaubaren Einsatz zu handeln – hier will niemand in ein zweites Afghanistan hineinschlittern. Völkerrechtlich ist der Einsatz ohnehin unbedenklich, schließlich hat die malische Regierung selbst um Hilfe gebeten.

Warum eigentlich noch nicht einmal »zur Debatte«? Vollständig raushalten will man sich in Rest-Europa schließlich auch nicht. Eine Reihe Verbündeter verspricht Unterstützung – beinahe ausschließlich in Form von Transportflugzeugen. Das ist billig, sieht gut aus und lässt sich – vor allem in Deutschland – ohne Parlamentsmandat und öffentlichen Diskurs der Bevölkerung verkaufen. Von einem zeugt es aber allemal nicht: dem Willen zu einer gemeinsamen europäischen Verantwortung.

Was verhindert es also, mit der EU-Battlegroup gemeinsam militärische Handlungsfähigkeit zu beweisen und die Last des Einsatzes gerechter zu verteilen? Die Stiftung Wissenschaft und Politik, der Think-Tank der Bundesregierung, fasste bereits 2010 – akademisch korrekt und mit fortdauernder Gültigkeit – zusammen: »Einen Einsatz haben vor allem die unterschiedlichen strategischen Kulturen der EU-Staaten bislang verhindert.« Dabei erscheint heute, im ersten Halbjahr 2013, die Situation historisch günstig: In der »Weimar Battlegroup« stellen nur drei verschiedene Staaten die Kräfte – zu anderen Zeiten sind es bis zu sechs. Und doch unterscheiden sich die strategischen Kulturen im »Weimarer Dreieck« mit Deutschland, Polen und Frankreich so fundamental, dass selbst ein Einsatz in Mali nicht den kleinsten gemeinsamen Nenner darstellt. Für die weiterhin in Afghanistan stark engagierten Polen, analysiert der britische *Economist*, sei Mali einfach ein ferner Krieg zu viel. Und die Deutschen seien ja ohnehin immer dann zögerlich, wenn »boots on the ground« gefragt sind.

Ob Paris willens gewesen wäre, die Battlegroup zum Einsatz zu bringen, ist nicht überliefert. Möglicherweise war auch dort das Interesse von vornherein gering. Denn wie sie eindrucksvoll beweisen, sind die französischen Streitkräfte auch allein handlungsfähig. Hinzu kommt, dass nach der französischen Verfassung allein der Präsident über den Einsatz der Streitkräfte entscheidet. Das Parlament wird einige Tage später informiert – das ist alles. Gemeinsam mit zwei zögerlichen und flatterhaften Verbündeten in einen Krieg zu ziehen, den man auch alleine führen und gewinnen kann – das erschien François Hollande offenbar als die unattraktivere Option.

Damit zeigt sich der fundamentale Fehler im Konzept der EU-Battlegroups: Die handlungswilligen Staaten – Frankreich und Großbritannien – können auch alleine agieren. Die wankelmütigen Partner einschließlich Deutschlands können aber nur gemeinsam – nur wollen sie nie alle zur selben Zeit. ◂◂◂◂

Die strategischen Kulturen im »Weimarer Dreieck« unterscheiden sich zu fundamental.

Selbst die Motive für den Einsatz können nicht ernstlich in Zweifel gezogen werden: Der Schutz der malischen Bevölkerung vor dem weiteren Vormarsch marodierender Milizen islamischer Gotteskrieger, die Zerschlagung von Al-Qaida-Strukturen in der Sahara und ein Strauß postkolonialer Interessen haben Frankreich zum Eingreifen bewogen. Selbst Bundesaußenminister Guido Westerwelle, sonst steter Mahner des »politischen Prozesses«, kann dem französischen Einsatz nichts Schlechtes abgewinnen: »Es war richtig, dass Frankreich dem Hilfsersuchen der malischen Regierung gefolgt ist.« Und doch schiebt er gleich nach: »Ein Einsatz deutscher Kampftruppen steht nicht zur Debatte.« In welchem Rahmen auch immer.

Quellen und Links:

Bericht des *Economist* vom 19. Januar 2013

Studie »EU-Battlegroups« der Stiftung Wissenschaft und Politik vom August 2010

Ein Zwischenruf in eigener Sache

von Michael Seibold

Seit nun mehr sechs Jahren begleitet ADLAS die deutsche außen- und sicherheitspolitische Debatte. Die Diskussionskultur lässt dabei manchmal nicht nur Interesse, sondern auch Freundlichkeit vermissen – beides Eigenschaften, die wir uns erhalten möchten.

>> Gerade in einem so heiklen Themengebiet wie Sicherheits- und Außenpolitik ist es nicht nur legitim, sondern sogar äußerst wichtig, anderer Meinung zu sein – und diese auch zu vertreten. Wo und wie sollte Deutschlands Sicherheit verteidigt werden? Was sind deutsche Interessen? Gibt es eine »Responsibility to Protect«, die dazu zwingt, andernorts bei erheblichen Menschenrechtsverstößen zu intervenieren? Was sind überhaupt die wirklichen sicherheitspolitischen Bedrohungen – Terrorismus, Atomkrieg, Umweltverschmutzung, Pandemien oder gar Wirtschaftskrisen? Und in welchem Umfang sind militärische Mittel überhaupt in der Lage, diese Probleme auch nur ansatzweise zu lösen – gibt es nicht andere, bessere Instrumente? Die Grundfragen von Sicherheits- und Außenpolitik gehören in der Öffentlichkeit diskutiert, nicht hinter verschlossenen Türen.

Das setzt aber zwei Dinge voraus, für die sich *ADLAS* seit nunmehr sechs Jahren einsetzt: Zum einen die Bereitschaft, sich einem ernsthaften Dialog zu stellen und andere Meinungen zu akzeptieren. Diese Forderung richtet sich an alle Beteiligten, egal welchen Hintergrund und welche Weltanschau- >>

ung sie haben mögen. In Göttingen blockierte im Januar eine »antimilitaristische« Aktionsgruppe einen Vortrag der lokalen Hochschulgruppe des »Bundesverbands Sicherheitspolitik an Hochschulen« zum Thema Cybersicherheit – es hätte sich dabei um eine Undercover-Werbeveranstaltung der Bundeswehr gehandelt. Statt aber auf die eigene Überzeugungskraft und das Streitgespräch zu vertrauen, verhinderte die Gruppe jede wirklich kritische Auseinandersetzung.

Zwar flogen – wie noch in den 1980ern – keine Wasserhähne durch die Gegend. Erschreckend ist es dennoch, wenn gerade im universitären Umfeld das Recht auf Meinungsäußerung (selbstverständlich auf dem Boden des Grundgesetzes und der allgemeinen Menschenrechte) nicht gelten darf. Irgendetwas kann nicht stimmen, wenn vermeintliche Militaristen reden wollen und vermeintliche Pazifisten Gewalt anwenden, um dies zu verhindern. Der Appell, andere Meinungen ernst zu nehmen und anzuerkennen, richtet sich aber auch an jene Praktiker, die in wissenschaftlichen Erkenntnissen und Theorien oft nur hochtrabendes Geschwätz sehen.

Wie sehr die wissenschaftliche Betrachtung eines zunächst abstrakten Themas zu höchstinteressanten Erkenntnissen führen kann, glaubt etwa *ADLAS* 3/2012 gezeigt zu haben: Das Thema Frauen und Gender ist viel mehr als die Frage, ob Frauen an der Waffe dienen können oder sollten. Es berührt grundsätzliche Fragen der Außen- und Sicherheitspolitik. Sich den Erkenntnissen verschließen, die Wissenschaft und Theorie bieten können, bedeutet, einen Großteil der Lage nicht zu erfassen.

Gerade das bisweilen sehr abstrakte Thema Gender verdeutlicht aber auch die zweite Voraussetzung für einen ausreichenden gesellschaftlichen Dialog: Die Beteiligten müssen sich über Fakten und Hintergründe nicht nur informieren wollen, sondern auch können. Kritik an Wissenschaft ist dann berechtigt, wenn sich Forschung hinter Worthülsen und Satzungetümen verschanzt. Hier will *ADLAS* seit sechs Jahren Abhilfe schaffen. Das Magazin will Wissenschaft in verständliches Deutsch übersetzen und damit einen Zugang zur Diskussion ermöglichen.

Mehr noch: *ADLAS* will überhaupt Interesse wecken an Sicherheits- und Außenpolitik und zeigen, dass das Thema mehr umfasst als Militär und Krieg. Das zeigen auch die Schwerpunkte der vergangenen Jahre: Neben einigen wenigen »klassischen« Themen wie Streitkräftetransformation oder Europas Sicherheit hat *ADLAS* versucht, mit dem Fokus auf Kultur, Wirtschaft, Medien, Gesundheit, Spiele und Simulationen sowie Gender die Bandbreite des Themas anzudeuten und Bereiche zu erfassen, die in den Augen vieler Leser sicherheitspolitisches Neuland waren.

Daneben gab es aber auch Dauerbrenner, die sich abseits der Schwerpunkte immer wieder in den Heften fanden: Religion, Geheimdienste, Völkerrecht oder der Komplex Afghanistan. Insbesondere letzteres Thema zeigt sehr deutlich die Möglichkeiten und Grenzen unserer Arbeit der vergangenen Jahre auf. Als unabhängiges Journal mit wissenschaftlichem Hintergrund ist *ADLAS* nicht an *political correctness* gebunden, und früher als mancher andere konnten wir den Konflikt in Afghanistan als das bezeichnen, was er ist: als Krieg. Darauf aufbauend über Sinn, Unsinn, Ziel und Zweck der Missi-

Kritik an Wissenschaft ist dann berechtigt, wenn diese sich hinter Worthülsen und Satzungetümen verschanzt.

on am Hindukusch immer wieder zu diskutieren – das kann *ADLAS* aber nur anregen, nicht erzwingen. Dabei entbindet uns alle der Abzug aus Afghanistan keineswegs von dieser Pflicht, denn vergleichbare Fragen und Probleme stellen sich auch in Syrien oder in Mali.

Sicherheitspolitik steht immer noch im Randbereich der öffentlichen Wahrnehmung. Es ist ein Thema, das sporadisch aufflammt, etwa wenn eine neue Bundeswehrreform beschlossen wird, oder deutsche Firmen Panzer ins Ausland verkaufen. Die grundlegenden Fragen bleiben dahinter im Dunkeln verborgen. Allein kann *ADLAS* das natürlich nicht ändern. Aber das Magazin kann versuchen, einen möglichst effektiven Beitrag dazu zu leisten, dass die Gesellschaft über Sicherheitspolitik diskutiert, und dass sie es in Kenntnis möglichst vieler Fakten und Informationen tut. Es bleibt also noch viel zu tun für die Redaktion. ◂◂◂◂

Der Unterschied zwischen Peking und Berlin

Ohne Panikmache ist es Toshi Yoshihara und James R. Holmes gelungen, mit **»Der Rote Stern über dem Pazifik«** eine zwar kurze, aber äußerst aufschlussreiche, sachliche Analyse über Chinas maritimen Aufstieg vorzulegen.

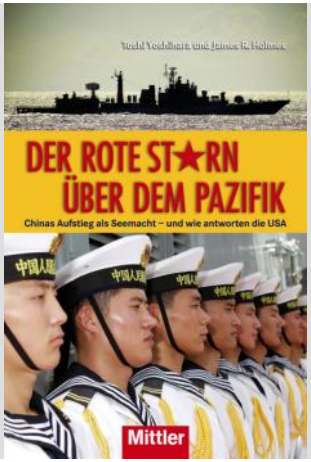
>> Heutzutage besteht wahrlich kein Mangel an Meldungen, Artikeln und Büchern über Chinas Ambitionen zur See. Dennoch sollte man »Der Rote Stern über dem Pazifik. Chinas Aufstieg als Seemacht – und wie antworten die USA« von Toshi Yoshihara und James R. Holmes nicht gleich zur Seite zu den anderen legen. Anstatt Schiffstypen und Waffen aufzuzählen, konzentrieren sich die Autoren auf eine Analyse der Strategie Pekings und kommen zu dem Schluss, dass die Volksrepublik momentan die Basis für eine ernsthafte und nachhaltige Bedrohung der amerikanischen Vorherrschaft im Raum Asien-Pazifik legt.

Interessant und neu ist hierbei ihre Vorgehensweise. Dank chinesischer Sprachkenntnisse haben beide Autoren vornehmlich die Debatte zur Strategieausrichtung in der Volksrepublik analysiert, und sich nicht, wie bei vielen anderen Publikationen üblich, auf englischsprachige Quellen verlassen. Dabei zeigen sie auf, dass chinesische Strategen inzwischen den amerikanischen Theoretiker für Seemacht des 19. Jahrhunderts, Alfred T. Mahan, nicht nur für sich entdeckt, sondern auch verinnerlicht haben.

Einen Vergleich, der in der Literatur äußerst beliebt ist, – der zwischen Pekings momentaner Situation und der des kaiserlichen Deutschlands im Flottenwettrüsten mit Großbritannien vor dem Ersten Weltkrieg – entkräften Yoshihara und Holmes: China befinde sich gegenüber den Vereinigten Staaten in einer weitaus komfortableren geostrategischen Lage als es das Deutsche Reich jemals war.

Abgerundet wird die strategische Analyse durch Kapitel zu den Themen Flottentaktiken, Raketenabwehr auf See und nukleare Abschreckmittel unter der Meeresoberfläche. Dabei verfallen die Autoren nicht in das Erklären von zum Beispiel unterschiedlichen Raketentypen, sondern stellen vielmehr heraus, welche Auswirkungen ballistische Antischiffsraketen auf die Strategie Chinas und der USA im Pazifik haben.

Allerdings merkt man den Autoren an, dass sie als Dozenten am Institut für Strategie und Politik des US Naval War College arbeiten und vornehmlich akademische Artikel verfassen. Es lassen sich immer wieder schwer verständliche Schachtelsätze finden, die die deutsche Übersetzung leider beibehält. Dafür überzeugt der Anhang von über 40 Seiten, der es dem Leser hervorragend ermöglicht, sich weiter in das Thema zu vertiefen . **dim**



Toshi Yoshihara und James R. Holmes

»Der Rote Stern über dem Pazifik. Chinas Aufstieg als Seemacht – und wie antworten die USA«

Hamburg (E.S. Mittler & Sohn) 2011, 258 Seiten, 24,95 Euro

Weiche Männer, leise Boote, coole Frauen

Larry Bonds neuester Schmöker **»Exit Plan«** bedient alle Geschmäcker der militärischen Unterhaltungsliteratur: Verfolgungen auf See, zu Land und unter Wasser. Obendrein ist die Hintergrundstory brandaktuell: Es geht um Irans Atomprogramm.

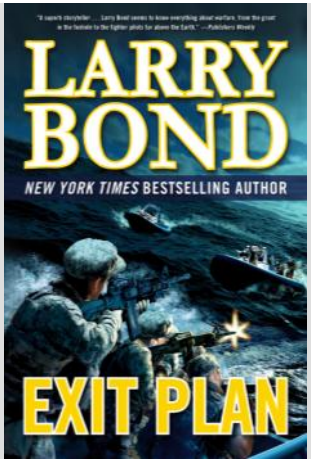
>> In seinem jüngsten Werk beweist Larry Bond wieder einmal sein Talent, spannende Militärthriller zu verfassen. Der Autor und ehemalige US-Marineoffizier ist dafür bekannt, seine Ideen aus der Tageszeitung zu gewinnen, und so verwundert es nicht, dass es um den Iran und sein angebliches Atomwaffenprogramm geht.

Die Geschichte von »Exit Plan« ist recht einfach gestrickt: In der Urananreichungsanlage Natanz geschieht ein Unfall, der Irans Atomprogramm um Jahre verzögern wird. Da die Führung in Teheran nicht so lange warten will, beschließt sie kurzerhand zu verkünden, eine Atombombe in wenigen Tagen testen zu wollen, um so einen Angriff Israels zu provozieren. Die muslimische Welt würde sich daraufhin dem Iran anschließen und dessen Träume einer Hegemonialmachtstellung im Nahen Osten Geltung verschaffen.

Allerdings deckt eine junge iranische Wissenschaftlerin namens Shirin dieses Komplott auf und versucht, zu den USA überzulaufen, um den israelischen Angriff zu verhindern. Die Amerikaner entsenden das Atom-U-Boot USS »Michigan« mit einem SEAL-Team zur iranischen Küste, um die Wissenschaftlerin aus dem Land zu holen. Dass bei der Rettungsaktion einiges schief laufen wird, versteht sich von alleine.

Bond besticht insbesondere durch seine hervorragende Recherche. Taktiken von U-Booten und Navy SEALs, Atomtechnologie, iranische Revolutionsgarden, aber auch die Küstenlandschaft des Irans beschreibt er detailgetreu und stimmig. Dabei bleibt seine Erzählung durchweg spannend und wartet mit vielen überraschenden Wendungen auf. Dem einen oder anderen SEAL-Fan wird jedoch die Emotionalität des Teamführers sauer aufstoßen. Es verwundert schon, wenn eine junge Iranerin einen kühleren Kopf bewahrt als ein ausgebildeter US-Elitesoldat.

Ein Wermutstropfen ist, dass Bonds sämtliche Werke bisher leider nur auf Englisch erhältlich sind. Eine deutsche Übersetzung ist laut Autor vorerst nicht geplant. Das sollte aber nicht vom Lesen abhalten. Bonds Schreibstil lässt sich leicht lesen, vor allem da er Fachbegriffe recht selten verwendet. Und wenn doch, bietet »Exit Plan« ein umfangreiches Glossar, das äußerst hilfreich ist. Definitiv ein lesenswertes Buch. **dim**



Larry Bond

»Exit Plan«

New York (Forge) 2012,
412 Seiten, 26,99 US$

***ADLAS* Magazin für Außen- und Sicherheitspolitik**

ist aus dem »Aktualisierten Dresdner InfoLetter für Außen- und Sicherheitspolitik« des Dresdner Arbeitskreises für Sicherheits- und Außenpolitik hervorgegangen und besteht seit 2007. Er erscheint seit 2010 als bundesweites, überparteiliches, akademisches Journal für den Bundesverband Sicherheitspolitik an Hochschulen (BSH).

Der *ADLAS* erscheint quartalsweise und ist zu beziehen über www.adlas-magazin.de.

Herausgeber: Michael Seibold
c/o Bundesverband Sicherheitspolitik an Hochschulen
Zeppelinstraße 7A, 53177 Bonn

Redaktion: Stefan Dölling (doe), Sophie Eisentraut (eis), Sebastian Hoffmeister (hoff), Dieter Imme (dim) (V.i.S.d.P.), Christian Kollrich (koll), Marcus Mohr (mmo), Sebastian Nieke (nik), Michael Seibold (msei), Stefan Stahlberg (sts)

Layout: mmo

Autoren: Nedife Arslan, Sören Ludwig, Nils Metzger, Andrea Pretis, Hanna Pütz, Thomas Reinhold, Julian Schibberges, Constantin Schüßler, Isabel Skierka, Guido Steinberg, Ingmar Zielke

Danke: S.

Fotos Seite 49: (von lins oben nach rechts unten) Fotos: US Navy / Chad J. McNeeley, US Navy / Denver Applehans, David W. / CCA 2.0 Generic, Vladimir V. Samoilov CCA-SA 2.5 Generic

DER BUNDESVERBAND SICHERHEITSPOLITIK AN HOCHSCHULEN

verfolgt das Ziel, einen angeregten Dialog über Außen- und Sicherheitspolitik zwischen den Universitäten, der Öffentlichkeit und der Politik in Deutschland herzustellen. Durch seine überparteilichen Bildungs- und Informationsangebote will der BSH vor allem an den Hochschulen eine sachliche, akademische Auseinandersetzung mit dem Thema Sicherheitspolitik fördern und somit zu einer informierten Debatte in der Öffentlichkeit beitragen. Unterstützt wird der BSH durch seine Mutterorganisation, den Verband der Reservisten der Deutschen Bundeswehr. ◂◂◂◂

Weitere Informationen zum BSH gibt es unter www.sicherheitspolitik.de.

Foto: US Marine Corps / Marco Mancha

Ausgabe 2/2013

Schwerpunkt
VON WINDMÜHLEN UND MAGISCHEN DRACHEN
Der Kampf gegen die Drogen