



CYBERWAR

Ausweitung der Kampfzone

Kriege werden auch auf digitalen Schlachtfeldern ausgetragen. Internationale Völkerrechtler haben deshalb Regeln für den Cyberwar festgelegt. Darf der künftig mit militärischen Mitteln beantwortet werden?

Die Attacke steckte in der alltäglichen Post: Bei ausgewählten südkoreanischen Firmen landeten Mitte vorvergangener Woche E-Mails mit angeblichen Kreditkarteninformationen.

Empfänger, die die Mail öffneten, holten sich den Feind ins Haus. Hinter der elektronischen Post verbarg sich ein Angriff aus dem Internet. Statt der erhofften Kreditkarteninformationen luden sich die Empfänger eine Zeitbombe auf ihre Rechner, deren Zünder auf Mittwoch, 14 Uhr koreanischer Ortszeit programmiert war.

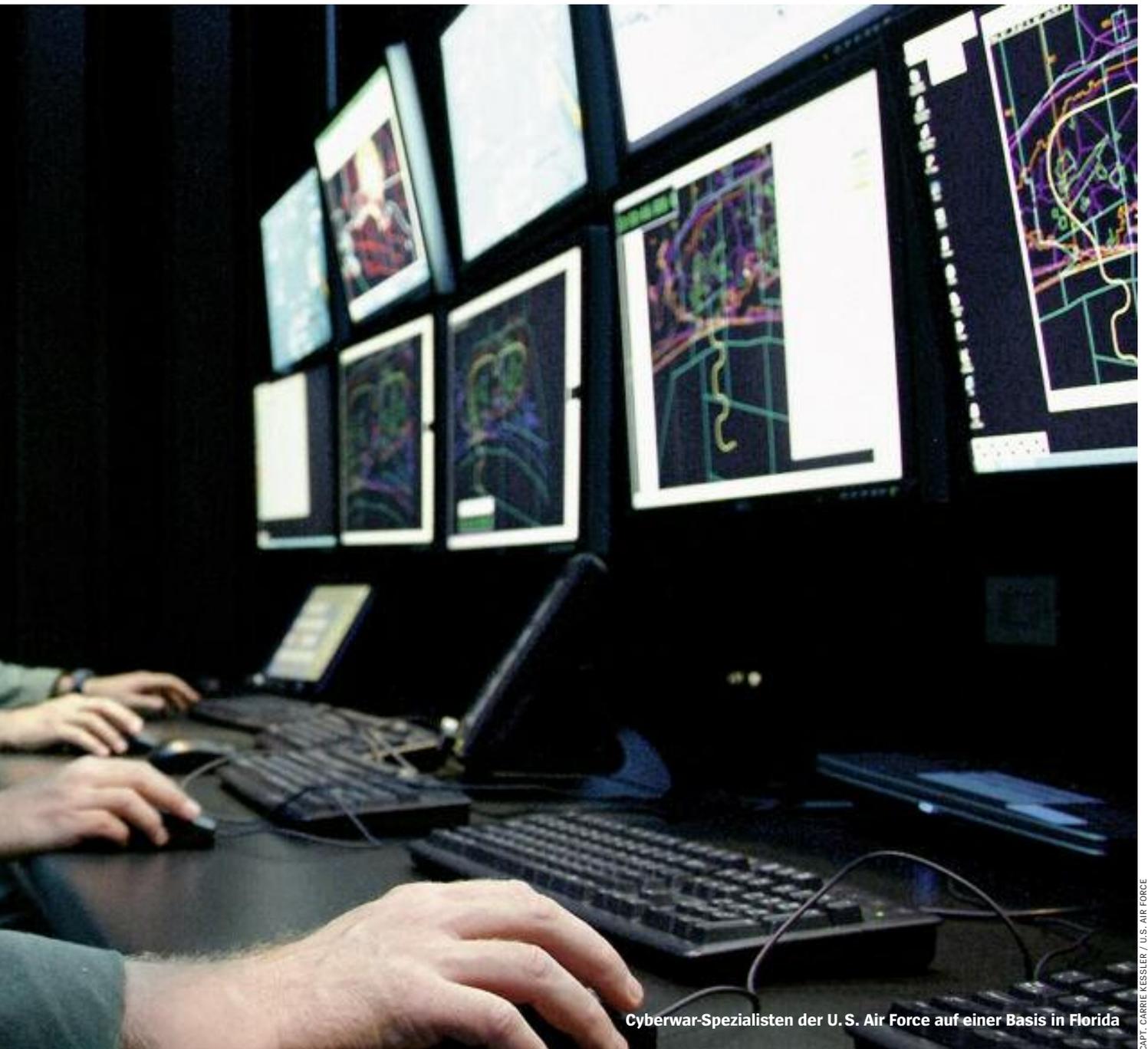
Pünktlich auf die Minute brach auf mehr als 30 000 Computern in südkoreanischen Fernsehstationen und Banken dann das Chaos aus. „Installieren Sie ein

Betriebssystem“, meldeten betroffene Rechner, Geldautomaten stellten ihren Service ein. Das Schadprogramm, das Experten mittlerweile „DarkSeoul“ getauft haben, löschte Daten von den Festplatten, so dass die infizierten Computer nicht mehr hochgefahren werden konnten.

DarkSeoul war einer der schwersten digitalen Angriffe, von denen die Welt in diesem Jahr heimgesucht wurde. Doch nahezu wöchentlich erreichen neue Alarmmeldungen die Cyber-Abwehrzentren in den Hauptstädten westlicher Nationen. Die bislang heftigste Attacke kam aus Amerika: 2010 schmuggelten Hightech-Krieger auf Befehl des US-Präsidenten den zerstörerischen Angriffscodename „Stuxnet“ in iranische Atomanlagen.

Dabei wird es nicht bleiben. Militärführer in den Vereinigten Staaten und bei den europäischen Nato-Partnern rüsten neue Bataillone für die bevorstehende Datenschlacht. Und weltweit streiten Völkerrechtler mit Politikern über die Art der neuen Bedrohung: Ist das bereits Krieg? Oder handelt es sich um Sabotage und terroristische Akte? Und wenn es tatsächlich eine neue Art von Krieg sein sollte, ist er auch mit militärischen Mitteln zu beantworten?

Wenige Tage vor dem Computerdesaster von Seoul erschien unter der Schirmherrschaft der Nato ein schmales, blaues Büchlein. Es gibt gefährliche Antworten auf all diese Fragen. Das „Handbuch des internationalen Rechts für die Cyber-



Cyberwar-Spezialisten der U.S. Air Force auf einer Basis in Florida

CAPT. CARRIE KESSLER / U.S. AIR FORCE

Kriegsführung“ dürfte kaum dicker als der Daumen des amerikanischen Präsidenten sein. Es ist kein offizielles Nato-Dokument, doch in der Hand Barack Obamas kann es die Welt verändern.

Was einflussreiche Völkerrechtler da an Regeln zusammengefügt haben, ist geeignet, die Grenzen zwischen Krieg und Frieden zu verwischen und eine heftige Datenattacke blitzschnell in einen echten Krieg mit Bomben und Raketen eskalieren zu lassen. Militärs könnten es auch als Einladung zu einem präventiven Erstschiß im Cyberwar lesen.

Auf Einladung eines Think-Tanks der Nato im estnischen Tallinn und unter Vorsitz eines Pentagon-nahen US-Militärjuristen hatten führende Völkerrechtsexper-

ten über die Regeln des Kriegs der Zukunft diskutiert. Völkerrecht ist großenteils Gewohnheitsrecht. Und was als Gewohnheitsrecht gilt und gelten kann, das stellen Experten fest.

Das „Tallinn-Manual“, das dabei entstand, gilt als erstes, informelles Gesetzbuch für den Krieg der Zukunft. Aber es hat keine beruhigende Wirkung – ganz im Gegenteil. Denn es erlaubt, Datenattacken mit den Waffen des realen Kriegs zu beantworten.

Wohin das führen kann, machte das Pentagon schon vor zwei Jahren klar: Wer beispielsweise versuche, der mächtigsten Nation der Welt per Schadprogramm den Strom auszuschalten, müsse mit einer Rakete als Antwort rechnen.

Deutlich wie selten wurden in den vergangenen Wochen die Gefahren eines Cyber-Kriegs in Washington beschworen. Im Situation Room, dem geheimsten aller geheimen Konferenzräume im Keller des Weißen Hauses, versammelte Obama Mitte März 13 führende Vertreter der US-Wirtschaft, darunter die Bosse von UPS, JPMorgan Chase und Exxon Mobil. Einziges Thema: Wie kann Amerika den Krieg im Netz gewinnen?

Am Tag zuvor hatte der nationale Geheimdienstdirektor James Clapper die Cyber-Bedrohung als die „größte Gefahr weltweit“ eingestuft.

Was genau die Wirtschaftsbosse und der Präsident im Situation Room berieten, wollte das Weiße Haus nicht verraten.

„Doch es ging vor allem darum, den Firmen klarzumachen, wie bedroht auch sie sind – und so ihre Bereitschaft zur Kooperation zu stärken“, sagt Christopher Bronk, IT-Experte an der Rice University.

Auf diese Kooperation ist der Präsident auch dringend angewiesen. Denn die USA haben ihre digitale Infrastruktur dem Gesetz des Marktes überlassen. Alle Netzwerke werden von privaten Unternehmen betrieben. Sollte es einen Krieg im Netz geben, dann werden sich Schlachtfelder wie Waffen in Privatbesitz befinden.

Das Weiße Haus bereitet deshalb nun mit großem Aufwand mögliche Gegenangriffe vor. „Wir müssen unseren Feinden wirklich Angst einjagen“, so der ehemalige General James Cartwright, Autor der gültigen Cyber-Strategie des Pentagons.

Zuständig ist das vor drei Jahren gegründete Cyber Command des Pentagons mit 900 Mitarbeitern. Es sitzt in Fort Meade in unmittelbarer Nähe der Natio-

lege im US-Bundesstaat Rhode Island, der ältesten Marineakademie der Welt, müssen drei Sicherheitsschleusen passieren.

„Man muss doch ehrlich sein“, sagt Michael Schmitt. „Jedermann hat das Internet als eine Art Wilden Westen angesehen, als einen rechtsfreien Raum. Internationales Recht muss für Online-Waffen aber genauso gelten wie für herkömmliche Waffen.“

Leicht gesagt. Doch wann wird eine Schadsoftware zur Waffe? Wann ein Hacker zum Krieger? Wann grober Unfug oder Spionage zum „bewaffneten Angriff“ im Sinne des Völkerrechts? Detailfragen, die über Krieg und Frieden entscheiden können.

Eher skeptisch beurteilt James Lewis, einer der führenden Cyberwar-Experten der USA von der Washingtoner Denkfabrik Center for Strategic and International Studies (CSIS), das neue Werk. Lewis liest daraus „den Versuch, die Hürden für militärische Gegenschläge niedriger anzusetzen“. Mit militärischen Mit-

nes „bewaffneten Angriffs“ wird, das Recht zu, sich mit Waffengewalt zu verteidigen. Der Artikel kam nach dem 11. September 2001 zu neuer Bedeutung, als die USA den Einmarsch in Afghanistan als Selbstverteidigung gegen al-Qaida deklarierten und die Nato den „Bündnisfall“ ausrief, um der Weltmacht zu Hilfe zu eilen.

Die Frage, wie böse ein Schadprogramm sein muss, um das Recht des Gegenschlags zu begründen, ist friedensentscheidend. Nur solche Angriffe, so die neue Doktrin, seien von völkerrechtlichem Gewicht, die an ihrem Ziel beim Gegner physische Schäden oder Personenschäden, aber nicht virtuelle Schäden auslösen. Der Ausfall eines Rechners oder der Verlust von Daten allein reicht nicht, von einem „bewaffneten Angriff“ zu sprechen.

Doch was ist, wenn, wie häufig, der Ausfall von Rechnern zwar nicht zu physischen Schäden, aber zu erheblichen Vermögensschäden führt? Ein Cyber-Angriff auf die Wall Street mit mehrtägigem Ausfall der Börse war der Casus Belli unter den Experten in Tallinn. Die US-Vertreter wollten dies als Verteidigungsfall anerkennen, die Europäer lieber nicht. Doch die US-Militärjuristen blieben dabei: Ökonomische Schäden begründen dann ein Recht zum Gegenschlag, wenn sie „katastrophal“ sind.

So bleibt es letztlich jedem Staat überlassen, welche wirtschaftlichen Schäden ihm als ausreichend erscheinen, einen Krieg zu wagen. Einen „Dammbruch“ für das völkerrechtliche Gewaltverbot befürchtet Kriegerrechtler Kreß.

War es also ein bewaffneter Angriff, der am 20. März über Südkorea hereinbrach? Die Vermögensschäden, die der Ausfall der Bankcomputer ausgelöst hat, sind noch nicht abschließend berechnet. Ob sie „katastrophal“ sind, werden Politiker entscheiden, nicht Juristen.

Wie schnell das Internet zum Schauplatz massiver Auseinandersetzungen werden kann, zeigte sich auch diesen Monat: Wie aus dem Nichts gerieten plötzlich zwei große Anbieter unter digitales Dauerfeuer.

Hauptangriffsziel war die Website Spamhaus.org – das Projekt macht seit 1998 Jagd auf die großen Spamversender im Netz. Es unterstützt andere Anbieter mit schwarzen Listen von bekannten Spammern dabei, Mail-Müll zu filtern. Damit macht sich die Organisation mächtige Feinde und war schon mehrfach Ziel von Angriffen. Doch die aktuelle Angriffswelle stellt alles in den Schatten. Sie legte nicht nur Spamhaus lahm, sondern zog zeitweise sogar das US-Unternehmen CloudFlare in Mitleidenschaft, das bei der Abwehr der Attacke half. Analysten bezifferten die Angriffsstärke auf 300 Gigabit pro Sekunde – und damit auf ein Vielfaches des Wertes, mit dem 2007 estnische Be-



U.S.-Cyber-Command-Chef Alexander: „Die größte Gefahr weltweit“

nal Security Agency (NSA), des größten Geheimdienstes der Vereinigten Staaten. Beide Einrichtungen haben denselben Chef: General Keith Alexander. Das Cyber Command soll innerhalb weniger Jahre rund 4900 Mitarbeiter umfassen und sich künftig in verschiedene „Cyber Mission Forces“ für Verteidigung und Angriff aufteilen.

Es ist wohl kein Zufall, dass das Tallinn-Manual ausgerechnet jetzt erscheint. Entstanden ist es unter Federführung von Michael Schmitt. Nato-Vertreter bezeichnen es als das „wichtigste rechtliche Dokument der Cyber-Ära“.

Der US-Militärjurist prüfte schon die Rechtmäßigkeit des Einsatzes streng vertraulicher Atomwaffensysteme und das Für und Wider der US-Drohnenattacken. Besucher seines Büros im Naval War Col-

lekteln auf eine „Denial of Service“-Attacke zu antworten ist für den Experten „eine verrückte Vorstellung“. Die Wegweisung aus Tallinn sei „etwas ziellos“.

Der Völkerrechtler und Direktor des Instituts für Friedenssicherungsrecht der Kölner Universität, Claus Kreß, sieht in dem Handbuch eine „Weichenstellung“ mit „Folgewirkungen für das gesamte Recht des Krieges“. Wichtige „Hemmschwellen“, die bislang vor kriegsrischer Eskalation politischer Konflikte oder terroristischer Akte schützen sollten, würden „zur Disposition gestellt“.

Der entscheidendste Punkt sei dabei die „Anerkennung eines staatlichen Selbstverteidigungsrechts gegen Cyber-Angriffe“, so Kreß. Das entspricht dem Verteidigungsfall: Artikel 51 der Uno-Charta billigt jedem Staat, der Opfer ei-



PETE SOUZA / CNP / POLARIS / STUDIO X

Präsident Obama in Arlington*: Wie kann Amerika den Krieg im Netz gewinnen?

hörden „beschossen“ wurden. Der Angriff wirkte sich sogar auf den Datenverkehr im gesamten Internet aus. Die Gruppe „Stophaus“ bekannte sich als Verursacher und rechtfertigte ihre Tat als Vergeltung dafür, dass Spamhaus sich in die Geschäfte mächtiger russischer und chinesischer Internetfirmen eingemischt habe.

Zivile Kräfte, gelenkt von wirtschaftlichen Interessen, spielen Cyber-Krieg – und stellen damit alle bisherige Kriegslage auf den Kopf.

Wie real die Bedrohung ist, zeigt ein Feldversuch in den USA. Um potentielle Angreifer aus der Reserve zu locken, baute die IT-Firma Trend Micro in einer amerikanischen Kleinstadt eine virtuelle Pumpstation auf – zumindest sollte es für „Besucher“ aus dem Netz so aussehen: Sie nannten es einen „Honeypot“, einen Honigtopf, der potentielle Angreifer im Netz anlocken sollte.

Die Fallensteller installierten dafür Server und industrielle Steuersysteme, wie sie Stadtwerke dieser Größenordnung betreiben. Um die Versuchsanordnung realistisch aussehen zu lassen, hinterlegten sie auf den Rechnern sogar täuschend echt aussehende Dokumente der Stadtverwaltung.

Nach nur 18 Stunden registrierten die Analysten bereits den ersten Angriffsversuch. Innerhalb der folgenden vier Wochen gab es 39 Attacken aus 14 Ländern. Die meisten kamen von Rechnern aus China (35 Prozent), gefolgt von den USA (19 Prozent) und Laos (12 Prozent).

Viele Angreifer versuchten, Spionagewerkzeuge in die vermeintliche Wasser-

pumpstation einzuschleusen, um die Anlage nach Schwachstellen abzuklopfen. Spionage verbietet das Völkerrecht nicht. Aber einige gingen weiter: Sie wollten die Steuerungsanlagen manipulieren oder sogar zerstören.

„Manche versuchten die Drehzahl der Wasserpumpen so zu erhöhen, dass sie in der realen Welt nicht überlebt hätten“, so Trend-Micro-Mitarbeiter Udo Schneider, der diese Fälle als „klassische Sabotage“ einordnet.

„Es ist keine Frage, ob es einen katastrophalen Cyber-Angriff gegen Amerika geben wird. Die Frage ist nur, wann.“ Das sagt Terry Benzel, die Frau, die Amerika vor einem solchen Angriff schützen und seine Rechnernetze sicherer machen soll. Die gelernte Computerspezialistin ist Leiterin von DeterLab in Kalifornien. Ein Projekt, das 2003 auch mit Mitteln des US-Heimatschutzministeriums gegründet wurde und eine Simulationsplattform bietet, um Reaktionen auf Cyber-Attacken durchzuspielen.

Benzels Stimme schwankt nicht, wenn sie von einem Kriegsszenario spricht, das sie „Cyber Pearl Harbor“ nennt. Und so könnte es aussehen: „Stromausfälle über längere Zeiträume, ein Zusammenbruch des Elektrizitätsnetzes, irreparable Störungen des Internets.“ Mit einem Schlag kämen Lebensmittel nicht rechtzeitig in die Läden und keine Geldscheine mehr aus dem Bankautomaten. „Alles hängt doch heute von Computern ab, selbst die Lieferung der Brötchen um die Ecke“, sagt sie.

Terry Benzel hat noch weitere Krisenszenarien parat: Sie verweist auf Programme, die Fluttore an amerikanischen Tal-

Der digitale SPIEGEL

Jetzt auch für Windows 8



In dieser Ausgabe:

- Der Tonzauberer** – Video-Spezial über Richard Wagners Musik
- Auf dem Abstellgleis** – Eine Video-Fahrt im Pannenzug der Deutschen Bahn
- Schlacht im Netz** – Video über Cyberwar

Die neue Art zu lesen.

- Mit zusätzlichen Hintergrundseiten.
- Mit exklusiv produzierten Videos.
- Mit 360°-Panoramafotos, interaktiven Grafiken und 3-D-Modellen.
- Alles immer schon **ab Sonntag 8 Uhr!**

www.spiegel.de/digital



Einfach scannen und Testangebot sichern – Nutzen Sie dafür unsere App **DER SPIEGEL** mit integriertem QR-Code-Scanner



* Mit Generalstabschef Martin Dempsey.

sperren öffnen und schließen und potentiell verwundbar sind. Ein geschickter Hacker könnte, so Benzels Befürchtung, Amerikas Dämme nach Belieben öffnen.

Solche und andere Fälle werden derzeit in Cyber City geprobt, einer Modellstadt, die US-Experten in ihren Rechnern in New Jersey aufgebaut haben, um die Folgen von Datenangriffen durchspielen zu können. Einen Wasserturm gibt es da, eine Bahnstation – und 15 000 Einwohner. Alles ist realistisch vernetzt. So lässt sich ausprobieren, welche Verheerungen unter den Bewohnern durch Datenattacken angerichtet werden könnten.

In Europa sind es vor allem Geheimdienste, die digitale Kriegsspiele proben. Auch beim Bundesnachrichtendienst arbeitet eine Einheit an den Details der künftigen Kriege. Bezeichnend ist, dass nicht nur der Verteidigungsfall durchgespielt wird, sondern zunehmend auch Angriffsszenarien – um zumindest für eine Art digitalen Zweitschlag gerüstet zu sein (SPIEGEL 9/2013).

„Offensive Cyber Operations“, sogenannte OCOs, sind in mehreren Nato-Staaten Teil der Strategie für künftige Cyber-Kriege. Das Tallinn-Manual eröffnet nun auch die rechtliche Grundlage für mögliche „preemptive strikes“, also Präventivschläge. Sie sind im Kriegsrecht ein Thema, seit Präsident George W. Bush im März 2003 vorsorglich den Irak überfiel.

Wann ein Offensivschlag als Akt der präventiven Selbstverteidigung gegen Cyber-Angriffe zulässig ist, war der umstrittenste Punkt der Beratungen in Tallinn. „Imminent“, unmittelbar bevorstehend, so die bisherige Lehre, müsse ein Angriff sein, um das Recht auf Selbstverteidigung präventiv auszulösen. Das Tallinn-Manual ist da großzügiger: Auch wenn eine digitale Waffe ihre unheilvolle Wirkung erst später entfalte, könne schon ein Erstschlag gerechtfertigt sein.

Die doppelte Moral wird deutlich am Umgang der Völkerrechtler mit Stuxnet, dem bislang verheerendsten Schadprogramm, das wohl auf Obamas Befehl in iranische Atomanlagen geschmuggelt wurde. Der Datenangriff zerstörte zahlreiche Zentrifugen für die Urananreicherung in der Aufbereitungsanlage Natans. Nach den Kriterien des Tallinn-Manuals wäre das ein kriegerischer Akt.

Die USA als Täter eines völkerrechtswidrigen Angriffskrieges? Für eine „Handreichung für das Pentagon“ hält der Kölner Völkerrechtler Claus Krefß, was die Autoren bei der schriftlichen Erörterung des Falles Stuxnet in Klammern schrieben: Denn dort wird Obamas digitaler Übergriff als „Akt der vorbeugenden Selbstverteidigung“ gegen das Atomprogramm der Ajatollahs gesehen.

Als Brandbeschleuniger nach der Tallinn-Lesart könnten zahllose virtuelle

Spionagevorfälle wirken, von denen mittlerweile alle Industrienationen fast täglich betroffen sind. Reine Cyber-Spionage, im Sprachgebrauch amerikanischer Politiker ebenfalls „attack“ genannt, ist zwar auch nach den Regeln von Tallinn nicht als Kriegshandlung zu betrachten. Doch die Erörterungen der Völkerrechtler erlauben es, auch solche Spähattacken als Vorbereitung eines zerstörerischen Angriffs zu werten. Deshalb könne es legitim sein, sich mit einem präventiven Schlag gegen den Spion zur Wehr zu setzen.

Besondere Sorge bereitet es manchen, dass nach den Tallinn-Vorschlägen auch die Regeln des „Kriegs gegen den Terror“ ausgeweitet werden könnten. So haben die Autoren des Manuals die Forderung des US-Geostrategen Joseph Nye, Vorsorge gegen ein „Cyber-9/11“ zu treffen, übernommen. Danach könnte die Supermacht sogar lose organisierten Hackergruppen den Krieg erklären. Kampfdrohen gegen Hacker? Kriegsrechtler Krefß sieht bei der Ausweitung der Kampfzone auf die Laptops von Privatleuten „Menschenrechte in Gefahr“.

Bedenken gegen die Weiterungen digitaler Waffengänge werden mittlerweile auch bei der Bundeswehr laut. Nachdenkliche Militärs wie Karl Schreiner, Brigadegeneral bei der Führungsakademie der Bundeswehr in Hamburg, sieht die Notwendigkeit von „ethischen Regeln“ für das Schlachtfeld Internet und hält einen internationalen Kanon für die Verwendung digitaler Waffen für erforderlich.

Neu nachdenken müssen die Militärs vor allem über die wichtigste Frage der Verteidigung im Cyberspace: Wer ist der Angreifer? „In den meisten Fällen“, so heißt es optimistisch im Tallinn-Manual, sei die Quelle von Datenattacken zu ermitteln. Das aber deckt sich nicht mit den Erfahrungen vieler IT-Sicherheits-Experten.

Der typische Nebel des Cyber-Kriegs zeigte sich zuletzt wieder am Beispiel Südkorea. Erst hieß es, DarkSeoul sei sicher ein Angriff aus dem Norden, dann wurden angeblich Spuren nach China, Europa und in die USA entdeckt. Manche Analysten haben inzwischen patriotisch motivierte Hacker in Nordkorea in Verdacht, aufgrund der vergleichsweise schlichten Schadprogramme. Gegen wen also sollte Südkorea nun zurückschlagen?

Der Kölner Völkerrechtler Krefß sieht daher schon ein „neues ungelöstes Problem“ auf die Juristen zukommen: den „Krieg auf Verdacht“.

THOMAS DARNSTÄDT,
MARCEL ROSENBACH, GREGOR PETER SCHMITZ



**Video: Digitalwaffen
gegen Raketen**

spiegel.de/app142013cyberwar
oder in der App DER SPIEGEL