„Der Krieg bleibt nicht in

US-Sicherheitsberater Richard Clarke warnte als einer der Ersten vor al-Qaida. Nun hält er den Cyberwar für eine größere Bedrohung als den Terrorismus

Interview **DIRK LIEDTKE, ULF SCHÖNERT, MICHAEL STRECK**
Foto **JULIANE WERNER**

Mister Clarke, Sie haben für vier US-Präsidenten als Sicherheitsberater gearbeitet, vor al-Qaida gewarnt, als das noch niemand hören wollte, die 9/11-Untersuchungskommission mit geleitet, aber in Ihrem neuen Buch* erwecken Sie den Eindruck, die größte Gefahr für die Menschheit komme aus dem Netz. Sind wir schon mittendrin in diesem virtuellen Krieg?

Wenn Sie die Definition eines Kriegs auf Spionage und Diebstahl erweitern: Ja. Jede große Firma in den USA, in Europa und in Asien ist schon infiltriert worden und hat Informationen verloren – trotz des vielen Geldes, das sie in den Schutz ihrer Netze investiert haben. Und Beispiele für Cyberwar gibt es auch. Die USA etwa hackten sich auf experimenteller Basis in ein Stromnetz und ließen den Generator in die falsche Richtung laufen. Das Ding wäre glatt explodiert, wenn sie den Test nicht abgebrochen hätten.

Ein digitales Sandkastenmanöver ist kein Krieg. Howard Schmidt, Barack Obamas Beauftragter für Netzsicherheit, sagt: „Es gibt keinen Cyberwar." Übertreiben Sie nicht?

Wenn es den Cyberkrieg nicht gäbe, könnte er ja das U. S. Cyber Command auflösen und Milliarden Dollar sparen. Das ist nun wirklich Blödsinn. Stuxnet, das Virus, das vergangenen Sommer die Zentrifugen in iranischen Atomanlagen lahmlegte, hat doch aller Welt gezeigt, was heute möglich ist. Die Internationale Atomenergiebehörde geht davon aus, dass durch Stuxnet 1000 Zentrifugen zerstört wurden. Und Stuxnet ist immer noch eine Gefahr.

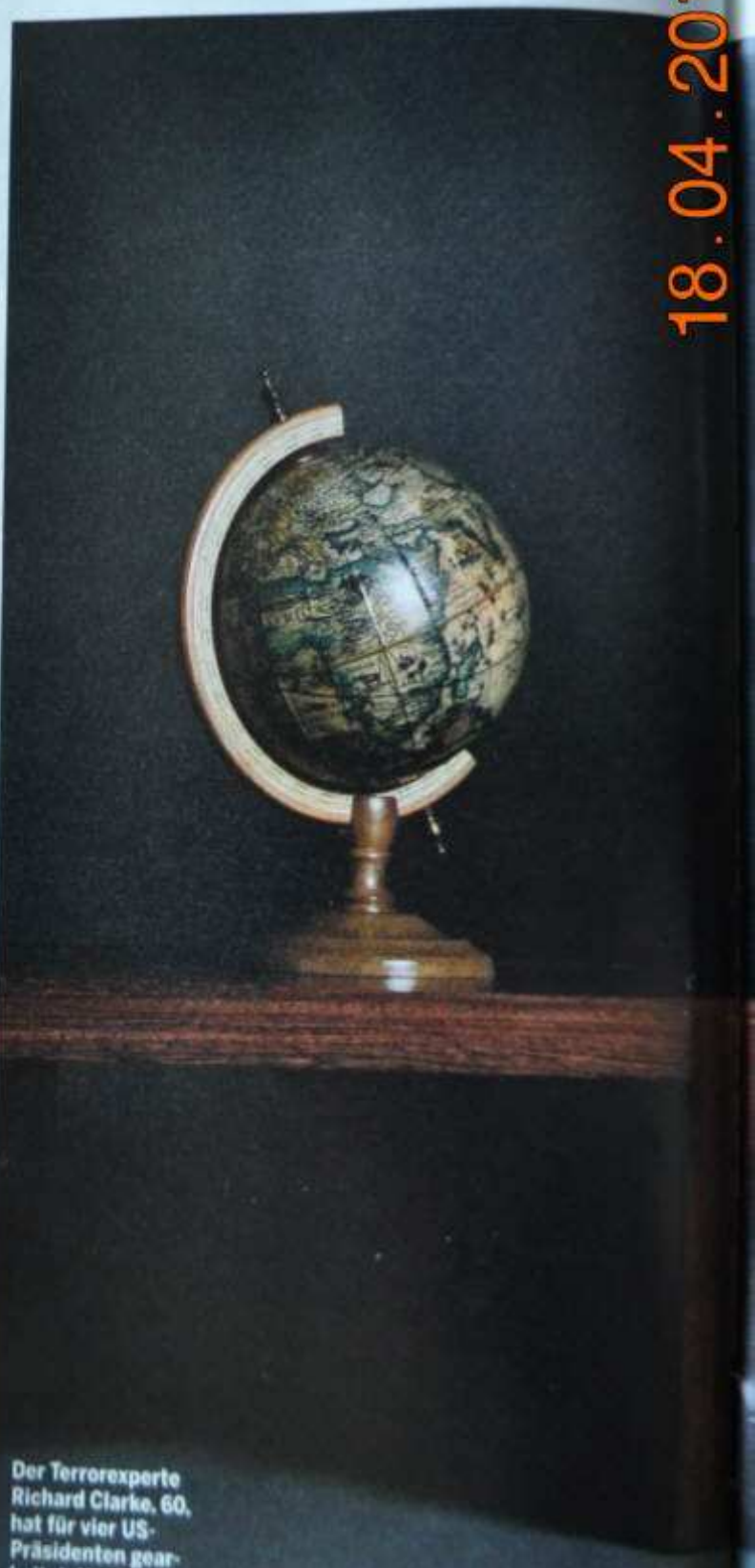
Inwiefern immer noch?

Zunächst mal: Ich hielt es für eine gute Nachricht, dass das iranische Nuklearprogramm gebremst wurde. Eine ausgesprochen schlechte Nachricht allerdings ist, dass Stuxnet in die Cyberwelt freigesetzt wurde und von vielen Menschen abgefangen und der Quellcode analysiert werden konnte. Der normale Quellcode einer Schadsoftware, also der Bauplan eines Computervirus, umfasst 200 bis 500 Zeilen, Stuxnet hat aber rund 15000. Stuxnet ist also eine sehr ausgefeilte Waffe. Und jetzt, da es so viele Menschen haben, können sie davon lernen. Vielleicht modifizieren sie das Virus. Nehmen wir das Ziel: Siemens-Steuerungsanlagen. Die Sicherheitslücken wurden angeblich mit Software-Updates gestopft. Gesetzt den Fall, Sie haben eine Kopie von Stuxnet, dann können Sie Programmierzeilen, die sich auf die Siemens-Anlage beziehen, einfach herausnehmen und durch andere Befehle ersetzen. Schon haben Sie eine perfekte Waffe für ein neues Ziel.

Und diese Waffe, sagen Sie, könnte bereits außer Kontrolle sein?

Jedenfalls haben auch nichtstaatliche Akteure den Code. Es ist nicht möglich zu sagen, wann das passieren wird. Aber es ist der nächste Schritt im Cyberkrieg. Staaten haben meist gute Gründe, Kriege nicht zu beginnen. Das ist bei Terroristen anders. Viele so

*Richard Clarke: „World Wide War: Angriff aus dem Internet", Hoffmann und Campe, 352 Seiten, 22 Euro.



Der Terrorexperte Richard Clarke, 60, hat für vier US-Präsidenten gearbeitet. Nun warnt er vor Angriffen aus dem Internet

virtuellen Raum“

eine Waffe in die Hände krimineller Kartelle oder Individuen, wäre das eine ganz neue Dimension.

Wer, glauben Sie, hat Stuxnet in die Cyberwelt gesetzt? Die Israelis, wie oft gemutmaßt wird?

Auf jeden Fall jemand, der wirklich gut ist. Ich weiß es nicht, aber die Fingerabdrücke deuten eher auf einen amerikanischen Angriff hin.

Im aktuellen Libyen-Konflikt spielt der virtuelle Krieg keine erkennbare Rolle. Warum nicht?

In Libyen erleben wir deshalb keine Cyberattacken, weil es einfachere Alternativen gibt.

Die Alliierten könnten den Ölfluss stoppen ...

Wenn das tatsächlich das Ziel der Koalition wäre, könnten sie das. Aber das ist nicht das Ziel.

In Ihrem Buch behaupten Sie, konventionelle Kriege würden durch Informationskriege ersetzt.

Ersetzt ist nicht der richtige Ausdruck. Ich glaube, dass sich in Zukunft zwei souveräne Staaten zunächst im Cyberspace bekämpfen können – dass ein solcher Krieg aber nicht im virtuellen Raum bleiben wird. Darüber mache ich mir die größten Sorgen. Eines Tages werden Entscheidungsträger womöglich denken, ein Cyberwar sei sauber und ordentlich, klinisch, keiner stirbt. Eine „easy option“. Ich befürchte, dass künftige Staatslenker eher für diese scheinbar einfache Option votieren und gar nicht realisieren, dass sie einen richtigen Krieg beginnen. Denn das attackierte Land ist vermutlich versucht, nicht nur mit virtuellen Waffen zurückzuschlagen. Sondern mit echten.

Der Cyberkrieg wäre also ...

... die Vorstufe des echten Waffengangs, ganz genau. Denn der zweite entscheidende Punkt im Cyberwar ist der Anreiz, als Erster loszuschlagen. Das wiederum setzt zwingend voraus, das Schlachtfeld zeitig zu präparieren – indem man sich in die Systeme des anderen Landes hackt. Es dauert Monate, manchmal Jahre, sich dort reinzuschleichen, digitale Falltüren zu öffnen, einen Hinterausgang zu planen und so weiter. Und das Resultat dieser virtuellen →

Kriegsvorbereitungen ist, dass Länder feststellen werden, dass irgendjemand ihr System penetriert hat. Stellen Sie sich vor, ein fremdes Land hat sich in Ihre Kontrollsysteme für, sagen wir, Pipelines oder das Stromnetz gehackt. Und Sie wüssten auch, welches Land das war. Was dann? So etwas destabilisiert die Beziehungen. Sollten dann politische, militärische oder ökonomische Umstände eine Krise zwischen diesen Ländern generieren, könnte das sehr leicht eskalieren.

Sie implizieren sogar, dass die Chinesen womöglich schon sogenannte Logikbomben in amerikanische Versorgungsnetze platziert haben, also Sabotage-Software, die auf Befehl losschlägt.

Ja, ich halte das für wahrscheinlich. Lassen Sie mich aber auch klar sagen: Ich glaube nicht, dass sich die USA und China den Krieg erklären, bloß weil sie die Fähigkeit dazu besitzen. Dass die amerikanischen Militärs besorgt sind und deshalb entsprechende Planspiele abhalten, ist nur legitim. Das ist ihr Job. Aber ich möchte nicht als jemand abgestempelt werden, der die chinesische Bedrohung hochspielt oder sagt, ein Krieg sei unvermeidlich. Die USA und China sind wirtschaftlich voneinander abhängig.

Dennoch skizzieren Sie immer wieder eine chinesische Bedrohung. Warum?

Mit der Bedrohung meine ich vor allem Industriespionage. Die Chinesen sind ziemlich aggressiv beim Angriff auf IT-Firmen und eigentlich alle anderen Branchen. Sie stahlen nicht nur Software-Codes, sondern auch chemische Formeln, Diagramme von Ingenieuren, pharmazeutische Informationen. Im Prinzip alle intellektuellen Besitztümer von Wert. Sie konnten das ziemlich ungestraft tun. Sie mussten dafür nicht einmal einen diplomatischen oder wirtschaftlichen Preis zahlen. Aus ihrer Perspektive stellt sich die Frage: Warum sollten wir nicht einfach so weitermachen?

Sie haben Obama im Wahlkampf beraten. Was sagt der dazu?

Na ja, während des Wahlkampfes haben sich die Chinesen in sein Kampagnennetzwerk gehackt. Obama weiß also aus erster Hand Bescheid. Unsere Regierung muss sich entscheiden, ob sie diese Art von Diebstahl ernst genug nimmt, um daraus Konsequenzen für die Chinesen zu ziehen. Mit einem „So what?" kommen wir nicht weiter. Wenn wir den Chinesen sagen: „Wir mögen es nicht, dass ihr unsere Software klaut, und wir mögen es auch nicht, dass ihr unsere Netzwerke infiltriert", dann müssen wir auch sagen: „Wenn ihr damit weitermacht, gehen wir den Weg x." Tatsache ist doch, dass wir – genauso wie Europa – gigantische Summen an geistigem Eigentum verlieren.

Ein Computervirus legte 2010 vorübergehend das Nuklearprogramm des iranischen Präsidenten Ahmadinedschad lahm

„Tatsache ist, dass wir gigantische Summen an geistigem Eigentum verlieren"

Können Sie das beziffern?

Nicht in Zahlen. Aber ich glaube, dass Staaten wie Deutschland oder die USA schon jetzt mehr Verluste durch Cyberspionage erleiden als durch Terrorismus.

Wird der von Ihnen beschworene Cyberkrieg also immer noch unterschätzt?

Sagen wir so: Das Pentagon ist zunehmend besorgt. Spätestens seit sie dort feststellen mussten, dass die Russen das geheime Netz des Verteidigungsministeriums geknackt hatten. Das war ein Weckruf. Und sie sind sich inzwischen auch darüber im Klaren, dass die meisten Computerchips in amerikanischen Waffensystemen nicht in den USA produziert wurden und die Herstellerkette nicht unbedingt vertrauenerweckend ist. Die beginnen zu kapieren, dass sie irgendwann in den Krieg marschieren und nichts funktioniert. Außerhalb des Pentagons aber herrscht in meinem Land ein ziemlicher Unwille, viel dagegen zu tun. Die Leute mögen keine staatlichen Regularien für das Netz. Viele denken gleich an Big Brother.

Und was schlagen Sie vor, gewissermaßen als friedensstiftende Maßnahme in diesem Cyberkrieg?

Lassen Sie uns die Regierung außen vor lassen und die Internetdienste-Anbieter die Aufgabe der Netzsicherheit übernehmen. Die Technologie existiert, die Daten, die durchs Netz laufen, nach den Mustern bekannter Attacken zu durchsuchen. Das Schlüsselwort ist dabei „bekannt". Die Anbieter könnten per Gesetz verpflichtet werden nachzuschauen, was durch ihre Netze fließt, und bekannte Angriffsmuster zu scannen und zu bekämpfen. Die Kosten dafür würden sich – umgelegt auf alle Internetnutzer – auf Pennys belaufen. Die Firmen müssten dann die Angriffsmuster untereinander austauschen. Und die Regierung könnte Muster mit den Firmen teilen, die diese noch nicht kennen. Würde das alle Attacken stoppen? Nein. Aber einen Großteil sehr wohl.

Wir reden über Virusattacken, digitale Falltüren und Hintereingänge. Und dann kommt der US-Soldat Bradley Manning daher, lädt alle möglichen Geheimnisse herunter, gibt sie Wikileaks und blamiert die USA bis auf die Knochen ...

So ist es. Wirklich frustrierend an der Wikileaks-Affäre ist aber, wie leicht man sie hätte verhindern können. Es gibt sehr, sehr schlichte Software, die auffälliges Verhalten von Mitarbeitern automatisch meldet. Wenn der Italien-Sachbearbeiter auf einmal ganz viel über Brasilien herunterlädt, dann merkt die Software das und meldet dem Vorgesetzten: Vorsicht, da läuft was falsch. Das Verteidigungsministerium und viele Unternehmen haben solche Software. Der Computer, aus dem Manning die Daten gezogen hat, hatte sie offensichtlich nicht.

Ist es in manchen Fällen nicht sinnvoll, ganz den Stecker zu ziehen?

Tja, das haben die Iraner ja gemacht in ihrer Nuklearanlage. Sie haben den Stecker gezogen, und die Fabrik war nicht ans Internet angeschlossen. Und Stuxnet konnte trotzdem zuschlagen. Im Sicherheitsbusiness kursiert ein Witz: Es gibt drei Regeln in unserem Beruf – erste Regel: Schaff dir gar nicht erst einen Computer an. Zweite Regel: Wenn du doch einen Computer brauchst, schalte ihn nicht an. Dritte Regel: Wenn du einen Computer hast und dich gezwungen fühlst, ihn einzuschalten: Vernetze ihn nicht.

Sie reden die ganze Zeit vom Cyberkrieg. Ist so etwas wie Cyberfrieden überhaupt noch vorstellbar?

Seit ich das Buch geschrieben habe, haben erste Debatten über Cyberwaffenkontrolle begonnen. Das kann aber dauern. In jedem neuen Bereich braucht es erst einmal fünf oder zehn Jahre, bis es erste Vereinbarungen über Waffenkontrolle gibt. Das war bei strategischen Atomwaffen so und auch bei biologischen und chemischen Waffen. Ich fürchte, wir werden weiter mit ansehen müssen, wie Unternehmen aus Europa und Nordamerika wichtige Informationen verlieren. Ich weiß auch nicht, wie sich das so schnell ändern lässt. ✖