Kühler Krieg

Verteidigung Nicht Panzer oder Flugzeuge werden in Zukunft über Sieg und Niederlage entscheiden, sondern Software und Computer. Die neuen Cyberwaffen sind ein sicherheitspolitischer Albtraum – und bedrohen schon jetzt die Demokratien des Westens.

GETTY IMAGES (2) STOYAN NENOV / REUTERS / MONTAGE DER SPIEGEL

Die Angreifer zielen auf das Herz Amerikas. In Michigan, Pennsylvania und Ohio bricht nacheinander die Stromversorgung zusammen. Millionen Amerikaner sitzen im Dunkeln. Klimaanlagen, Waschmaschinen, Computer, Fernseher, Telefone und Handys fallen aus, in den Krankenhäusern wird der Diesel für die Notstromaggregate knapp.

In Tennessee reagieren Ampeln, Straßenanzeigen und die Mautstationen der Highways nicht mehr. Eine Cyberattacke hat die zentrale Verkehrssteuerung lahmgelegt. Im texanischen Port Arthur fällt das Kontrollsystem einer riesigen Raffinerie aus, mit katastrophalen Folgen für die Umwelt. Vor der Golfküste schwappt ein kilometerbreiter Ölteppich, die Gouverneure von Texas und Louisiana rufen den Notstand aus.

Ein Stromausfall in Arizona löst eine Kettenreaktion aus, die auch Los Angeles erfasst. In mehreren Häfen im Süden Kaliforniens sind die hydraulischen Systeme lahmgelegt, Dutzende Containerschiffe können nicht entladen werden.

Unbekannte dringen in das Computernetzwerk der US-Luftfahrtbehörde ein und stehlen dort Software, mit der sie die Positionen aller Kampfflugzeuge im amerikanischen Luftraum orten können. Auf den Bildschirmen der Abwehrspezialisten verwandeln sich die Eingaben in unverständliches Gebrabbel.

Das Chaos, das sich Mitte Juni in einem streng bewachten Militärkomplex in Suffolk in Virginia ausbreitet, ist eine sorgfältig inszenierte Katastrophe. Neun Tage lang lässt das Pentagon, streng abgeschirmt von der Öffentlichkeit, 800 Experten aus 100 militärischen und zivilen Organisationen die Zukunft des Krieges üben.

Simuliert wird ein Hackerangriff auf die amerikanische Infrastruktur. „Cyber 9/11“ nennen die Militärs das Szenario, denn so könnte ein digitaler 11. September aussehen. „Für uns stellt sich nicht die Frage, ob so etwas passiert, sondern wann“, so zitiert das Fachblatt „Military Times“ Konteradmiral Kevin Lundsay vom U. S. Cyber Command.

Die Administration in Washington ist nicht die einzige Regierung, die sich mit großem Aufwand auf den digitalen Ernstfall vorbereitet. Die Einschläge nähern sich. Hochgerüstete Hacker bewiesen, dass sie praktisch jedes Netzwerk ausspionieren, sabotieren und manipulieren können.

Am vergangenen Donnerstag wurde bekannt, dass bei einem Hackerangriff auf den Internetkonzern Yahoo im Jahr 2014 die Daten von mindestens 500 Millionen Nutzern gestohlen wurden. Cyberangreifer drangen in die Parteirechner der Demokraten ein und mischten den amerikanischen Präsidentschaftswahlkampf auf. Unbekannte stahlen Digitalwaffen des US-Supergeheimdienstes NSA, und in Deutschland geriet ein gewisser „Heinrich Krammer“ ins Visier der Behörden.

Mit diesem Absender wurden an zwei Augusttagen zahllose Mails quer durch Deutschland geschickt, die scheinbar aus dem Brüsseler Nato-Hauptquartier kamen. Wer darin einen Link anklickte, um Informationen über den Militärputsch in der Türkei oder das Erdbeben in Italien zu bekommen, öffnete in Wahrheit seinen Rechner für eine Hackerattacke.

Der Angriff richtete sich nach Angaben der Bundesregierung gegen Bundestagsabgeordnete, mehrere Unternehmen und vor allem die Büros aller großen Parteien. Die Angreifer hätten „wie mit der Schrotflinte“ überall hingezielt, um wahllos Informationen zu sammeln, heißt es. Viel Mühe, dabei unentdeckt zu bleiben, gaben sie sich nicht.

Der Schaden hält sich offenbar in Grenzen, auch weil die NSA die Deutschen frühzeitig auf den Angriff hinwies. Und da die gleiche Schadsoftware bereits für den Cyberangriff auf den Bundestag im vergangenen Jahr eingesetzt worden war, war zumindest das Parlament dieses Mal besser gerüstet.

DAVID FLOCK / IMAGO

Angriffsziel Bundestag in Berlin
„Wie mit der Schrotflinte“

Fest steht, dass es sich wieder um eine Kampagne des russischen Kollektivs „Sofacy“ handelte, das viele Virenschutzprogramme inzwischen entdecken. Denkbar, dass die Russen noch einmal wahllos abfischen wollten, bevor ihre Software völlig wertlos ist. Oder dass sich jemand Fremdes das Werkzeug geschnappt hat. Beunruhigend sind beide Szenarien.

Disruption nennt man es in der Wirtschaft, wenn eine Innovation die bisherige Welt auf den Kopf stellt. Die Digitalisierung hat in den vergangenen 20 Jahren schon ganze Branchen vernichtet, sie ändert auch die Spielregeln des Krieges. Ein Angreifer kann mit einem billigen Laptop das Steuerungssystem eines milliardenteuren Raketenabwehrsystems lahmlegen. Größe und Ressourcen allein reichen nicht mehr aus, um militärische Überlegenheit zu garantieren.

Während die Preise für Kampfflugzeuge oder Panzer steigen, werden Computer, Software oder Drohnen billiger. Potenzielle Kriegswaffen werden damit zur Massenware, die es auch armen Staaten oder nicht staatlichen Angreifern erlaubt, die Großen herauszufordern. Ein sicherheitspolitischer Albtraum für die westlichen Demokratien.

Kampfhubschrauber, Streitkräfte und Kriegsschiffe wird es weiter geben, doch entscheiden sie in Zukunft nicht mehr allein über Sieg und Niederlage, sondern auch Drohnenschwärme, autonome Waffensysteme und vor allem: Software.

Im 21. Jahrhundert ist das Internet neben Land, Luft, See und Weltraum zum neuen Kriegsschauplatz geworden, der vieles, was für die Kriege vergangener Jahrhunderte galt, in Zweifel zieht. „Der Cyberspace stellt jede historische Erfahrung infrage“, schreibt Henry Kissinger in seinem Buch „Weltordnung“.

Der Doyen der amerikanischen Außenpolitik befürchtet einen Rückfall in den „Naturzustand“, den sich der englische Philosoph Thomas Hobbes im 17. Jahrhundert als „Krieg aller gegen alle“ vorgestellt hat. Eine Welt ohne Regeln, rechtlos und voller Gewalt, weil die technischen Möglichkeiten den politischen weit vorausgeeilt sind. „Das Konzept der internationalen Ordnung könnte in wachsendem Maß gefährdet werden“, warnt Kissinger.

Der Krieg der Zukunft unterscheidet nicht zwischen innerer und äußerer Sicherheit, zwischen zivilen und militärischen Zielen, nicht einmal zwischen Krieg und Frieden. Er ist ein hybrider Krieg ohne Kriegserklärung, ohne Anfang und Ende.

Wahrscheinlich waren es russische Hacker, die in den USA in die Rechner der Demokratischen Partei eindrangen, interne Unterlagen veröffentlichten und so versuchten, den amerikanischen Präsidentschaftswahlkampf zu beeinflussen. Das ist zwar noch nicht Krieg, aber auch nicht mehr wirklich Frieden.

„Wir befinden uns in einem permanenten Zustand des Konflikts zwischen einzelnen Staaten, der nur selten zum offenen Krieg wird“, sagt Joel Brenner, der frühere Spionageabwehrchef der USA. „Cool War“ nennt David Rothkopf, der Chefredakteur von „Foreign Policy“, diese neue Form der Auseinandersetzung – kühler Krieg.

Er ist total, denn er zielt ins Herz der Gesellschaft. Sein Ziel ist es, die politische Ordnung zu unterminieren oder den gesellschaftlichen Frieden zu zerstören. Alles kann zum Kriegsschauplatz werden: Eisenbahn- und Stromnetze, Wasserwerke und Atommeiler oder Fernsehsender wie der französische Kanal TV5 Monde, der im

vergangenen Jahr von Hackern lahmgelegt wurde.

Die Regeln des Krieges änderten sich, erklärte der russische Generalstabschef Walerij Gerassimow Anfang 2013 in einer Rede, denn „nicht militärische Mittel sind zum Erreichen politischer und strategischer Ziele in vielen Fällen wirksamer als Waffen“. Ein blühendes Gemeinwesen könne sich so „innerhalb von Monaten, sogar von Tagen in die Arena eines heftigen bewaffneten Konflikts verwandeln, das Opfer einer fremden Invasion werden und im Chaos, in einer humanitären Katastrophe, im Bürgerkrieg versinken“.

Im Westen spricht man schon von einem „Informationskrieg“ des Kreml. Es gehe Mächten wie Russland darum, so Wolfgang Ischinger, Chef der Münchner Sicherheitskonferenz, „das Grundvertrauen des Bürgers in das Funktionieren demokratischer Institutionen zu unterminieren und zu sabotieren“.

Der Kalte Krieg war vergleichsweise überschaubar. Während damals nur wenige Länder im Besitz der Atombombe waren, ist heute die Zahl der potenziellen Cyberangreifer riesig. Das kann genauso ein russisches Verbrechersyndikat sein wie auch islamistische Terroristen, ein anonymes Hackerkollektiv oder die Digitaltruppen eines Staates. Allein China soll mittlerweile eine Armee von über 100 000 Cyberkriegern unterhalten. Peking weiß, dass es beim konventionellen Rüstungswettlauf mit der Supermacht USA nicht mithalten kann. Washington wird in den nächsten Jahren allein für die Anschaffung eines neuen Kampfflugzeugs, des „Joint Strike Fighter“, etwa 400 Milliarden Dollar ausgegeben haben. Länder wie China, Russland oder Nordkorea verlagern den Konflikt deshalb auf eine Ebene, wo sie selbst stark sind und der Gegner besonders verletzlich ist.

Eine Cyberattacke ist relativ billig, doch es ist sehr aufwendig und teuer, sie abzuwehren. Der deutsche Verfassungsschutzpräsident Hans-Georg Maaßen fordert mittlerweile eine partielle Remechanisierung, etwa von Steuerungsanlagen in Atomkraftwerken, um die Gefahr eines Cyberangriffs abzuwehren. „Ich glaube, es ist notwendig, bestimmte Teile der Infrastruktur aus dem Netz herauszunehmen“, so Maaßen. Eine digitale Attacke auf eine Nuklearanlage ist das Schreckensszenario von Sicherheitsexperten. Dass sie schwierig, aber möglich ist, ist seit Jahren bekannt.

Die Wahrscheinlichkeit, dass es zu so einem Katastrophenszenario kommt, ist zuletzt deutlich gestiegen. Seit einigen Wochen kursieren im Netz Digitalwaffen aus dem Bestand des amerikanischen Geheimdienstes NSA. Jeder, der will, kann sich die Hackerwerkzeuge mit so bizarren Codenamen wie „Epicbanana“ oder „Extrabacon“ herunterladen. IT-Experten haben das getan und getestet: Die Werkzeuge waren noch einsatzbereit.

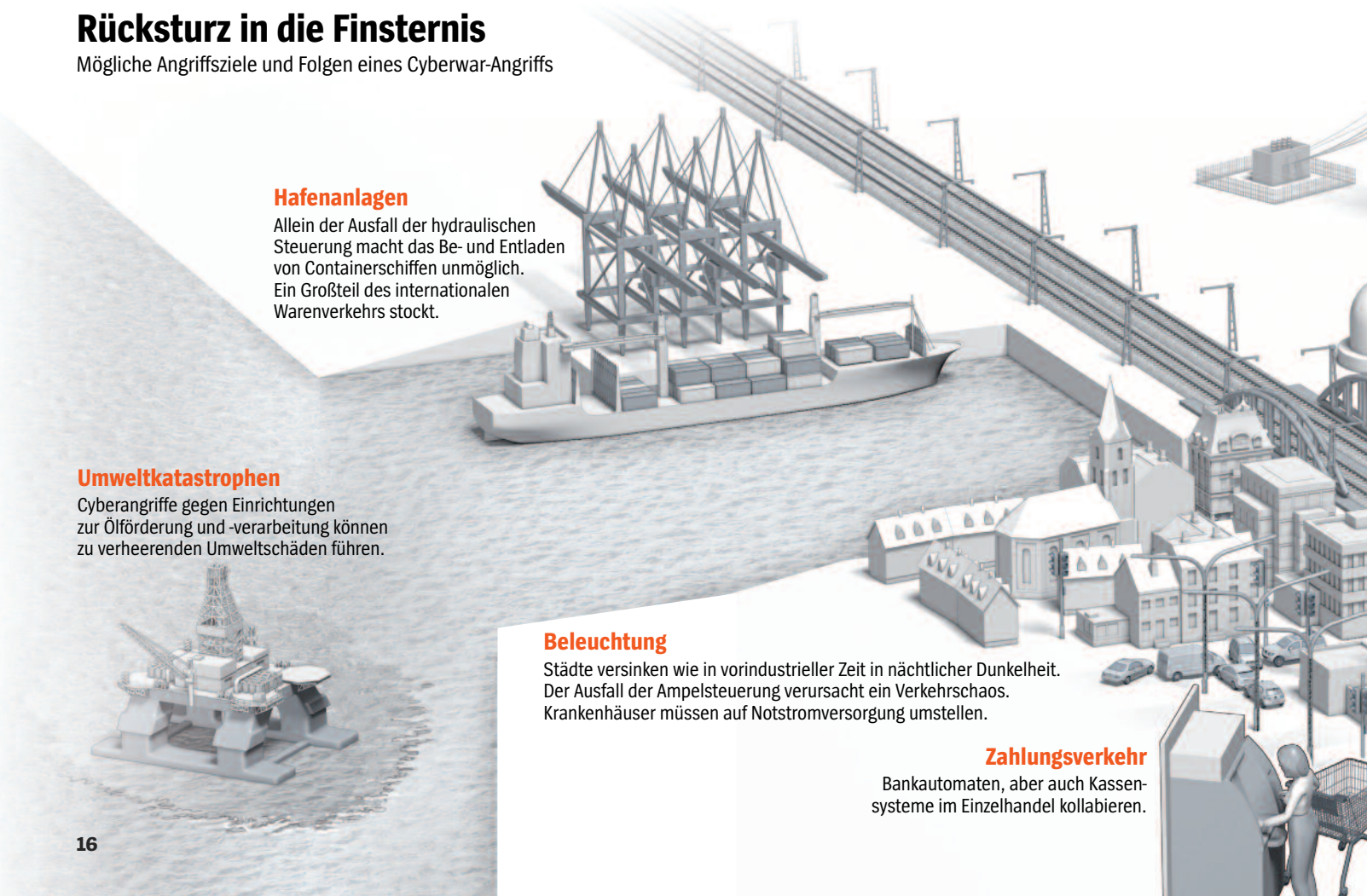
Ein futuristischer Albtraum, der allzu schnell Wirklichkeit geworden ist. Als würde die internationale Rüstungsindustrie ihre modernsten Waffensysteme inklusive der Baupläne auf den Hof stellen, und jeder könnte sich bedienen. Militärs, Geheimdienste, Terrororganisationen, und zwar weltweit.

Die NSA konnte die Angriffssoftware nutzen, um zum Beispiel die Sicherungssysteme des Netzausrüsters Cisco zu überwinden. Der amerikanische IT-Konzern stattet weltweit Behörden, Banken und Großunternehmen mit seiner Hard- und Software aus. Wer sich den Zugang zu diesen Netzen verschafft, hat den Zugriff auf Infrastruktureinrichtungen, die für das Überleben moderner Gesellschaften unverzichtbar sind.

Der SPIEGEL veröffentlichte bereits Ende 2013 einen geheimen NSA-Katalog

Rücksturz in die Finsternis

Mögliche Angriffsziele und Folgen eines Cyberwar-Angriffs



Hafenanlagen

Allein der Ausfall der hydraulischen Steuerung macht das Be- und Entladen von Containerschiffen unmöglich. Ein Großteil des internationalen Warenverkehrs stockt.

Umweltkatastrophen

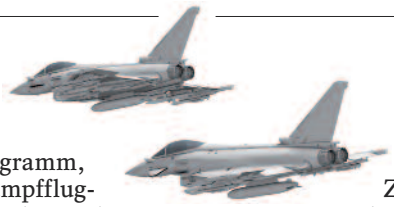
Cyberangriffe gegen Einrichtungen zur Ölförderung und -verarbeitung können zu verheerenden Umweltschäden führen.

Beleuchtung

Städte versinken wie in vorindustrieller Zeit in nächtlicher Dunkelheit. Der Ausfall der Ampelsteuerung verursacht ein Verkehrschaos. Krankenhäuser müssen auf Notstromversorgung umstellen.

Zahlungsverkehr

Bankautomaten, aber auch Kassensysteme im Einzelhandel kollabieren.



für Cyberwaffen und Hackerwerkzeuge, in dem es auch Hinweise auf die Geheimwaffen gab, die nun im Netz kursieren. Offenbar wurden einige von ihnen erfolgreich gegen Ziele in Pakistan und dem Libanon eingesetzt. Experten halten das NSA-Leck und seine Folgen für das Cyberkriegsprogramm der Amerikaner für mindestens so schwerwiegend wie die Enthüllungen des früheren Geheimdienstmitarbeiters Edward Snowden. Die Programme sind der „Schlüssel zum Königreich“, zitiert die „Washington Post“ einen ehemaligen Hacker der NSA.

Bisher sind nur erste Kostproben im Umlauf. „Shadow Brokers“ („Schattenhändler“) nennt sich die Gruppe, die im Netz die NSA-Waffen anbietet. Dabei ist immer noch unklar, wer in die hochgeheimen Rechner der NSA eingedrungen ist. Es ist nicht ohne Ironie, dass nun ausgerechnet geheime Cyberwaffen des US-Geheimdienstes auf dem Markt sind, denn es war Washington, das den Rüstungswettlauf im Cyberraum überhaupt erst anfeuerte.

2007 machten die Amerikaner das Städtchen Oak Ridge in Tennessee zu einem der Schauplätze eines einzigartigen Experiments. Im „National Laboratory“ testeten Fachleute der NSA einen Angriff auf das iranische Atomprogramm, ohne Raketen, ohne Kampfflugzeuge oder bunkerbrechende Bomben. Der Angreifer war ein Computervirus. Er sollte die Drehzahl der Zentrifugen, mit denen Uran angereichert wird, manipulieren und so weit erhöhen, bis sie zerbersten.

Das Experiment war erfolgreich. Die NSA-Leute kratzten die Trümmer der Zentrifugen zusammen, luden sie in ein Flugzeug und flogen damit nach Washington. Im Weißen Haus kippten sie den Metallschrott auf den Konferenztisch im „Situation Room“, um dann den Präsidenten anzurufen.

Als George W. Bush wenig später die Reste einer Zentrifuge in der Hand hielt, war er davon überzeugt, die iranische Bombe verhindern zu können, ohne einen weiteren Krieg im Nahen Osten führen zu müssen. „Versucht es“, sagte er. So jedenfalls beschreibt es ein Zeuge in Alex Gibneys Dokumentarfilm „Zero Days“.

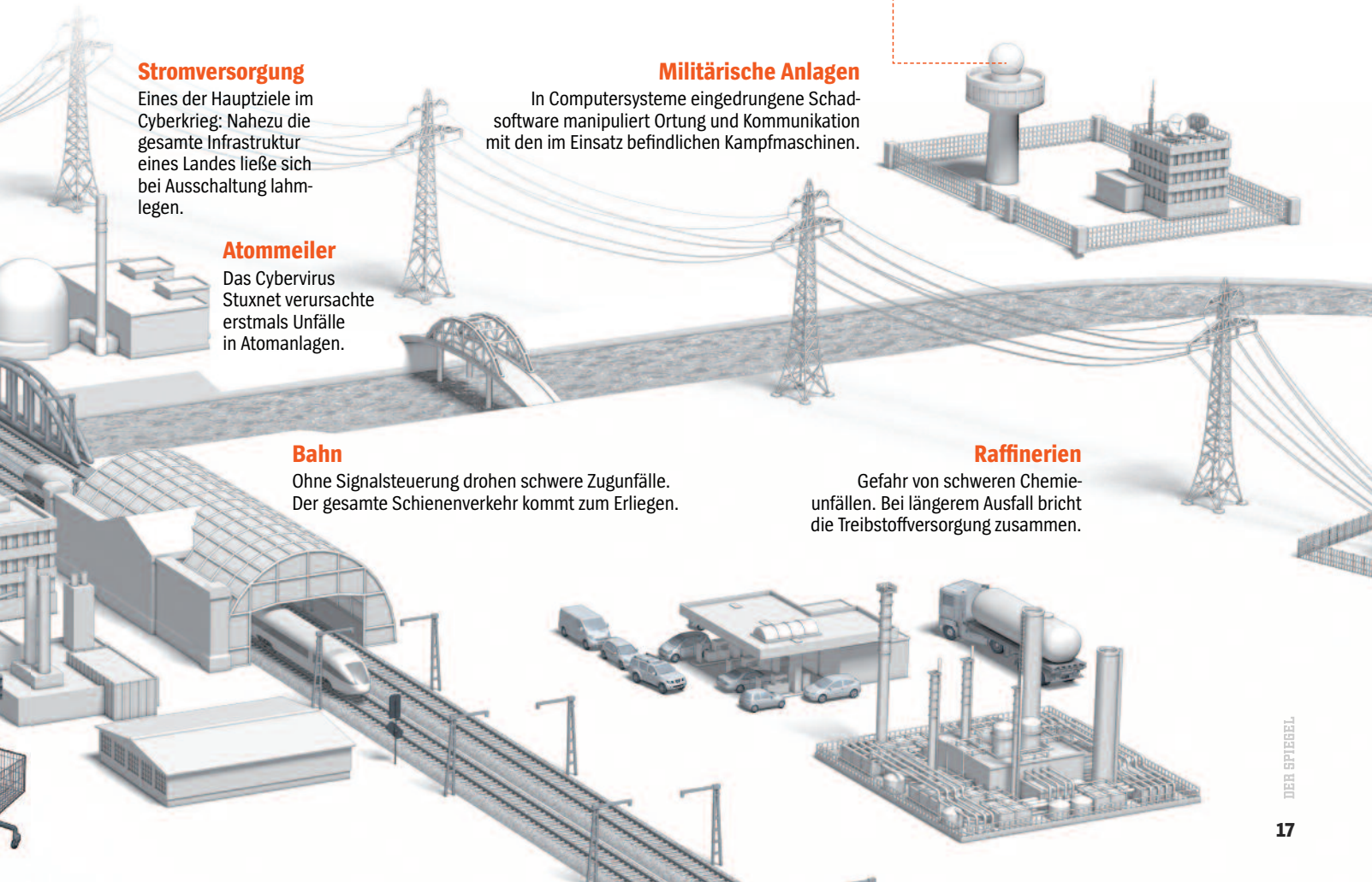
Es ist die Geburtsstunde von „Stuxnet“, dem Computervirus, der am Ende etwa tausend iranische Zentrifugen unbrauchbar gemacht haben soll. Die amerikanische Cyberexpertin Leslie Harris nennt diese Stunde null der Cyberkriegführung den „ersten Schuss eines Krieges, den wir alle verlieren werden“.

Zum ersten Mal dient eine staatlich eingesetzte Software als offensive, digitale Waffe, die materielle Zerstörung anrichtet.

Die Sabotage an den Zentrifugen ist Teil eines größeren Plans. Unter dem Codenamen „Nitro Zeus“ haben Hacker im Dienst der NSA große Teile der iranischen Infrastruktur mit Schadsoftware infiziert: Stromversorgung, Telekommunikation, Luftabwehr. Bush-Nachfolger Barack Obama wollte offenbar auf der sicheren Seite stehen, falls die Nuklearverhandlungen mit Teheran scheitern sollten. Im Falle eines iranischen Angriffs auf Israel hätten die US-Cyberkrieger auf Befehl des Präsidenten wichtige Rechner in Iran lahmlegen oder manipulieren können.

Die Iraner nutzen „Stuxnet“ inzwischen offenbar als Modell für eigene Cyberwaffen. Nur gut zwei Jahre nachdem der amerikanische Virus die iranischen Zentrifugen zerstört hatte, legte im August 2012 eine Schadsoftware 30 000 Computer des saudischen Ölkonzerns Saudi Aramco lahm. Die Aktion gilt als der erste Vergeltungsschlag in der Geschichte des Cyberwar.

Und noch etwas zeigt der Fall: Die USA haben keine Hemmungen, Cyberwaffen



zu entwickeln und einzusetzen, obwohl sie sich bis heute nicht offen zu dem Angriff bekannt haben. Wenn es um die eigenen militärischen Fähigkeiten geht, lassen sich Weißes Haus, Pentagon und Geheimdienste ungern in die Karten blicken.

Für ein wenig Transparenz hat erst jener Mann gesorgt, den sie bei der CIA in Anlehnung an den Harry-Potter-Bösewicht Voldemort nennen. Die Dokumente, die Edward Snowden an die Öffentlichkeit spielte, zeigen, dass die NSA bereits 1996 die militärische Bedeutung der Informationsrevolution mit jener der Atombombe gleichsetzte.

Wer die Datenverarbeitung kontrolliere, besitze die Schlüssel zur Macht im 21. Jahrhundert, schrieb der damalige NSA-Direktor Kenneth Minihan in einem Memorandum an seine Mitarbeiter. Daher gehe es fortan darum, die „informationelle Vorherrschaft für Amerika“ zu erlangen und zu sichern.

Die geheimen Snowden-Dokumente zeigen, dass die NSA und die Streitkräfte dieser Vision einer „globalen Dominanz“ offenbar sehr nahe gekommen sind. Die Cyberkrieger gehen nach einem Mehrphasenmodell vor. In einer ersten Stufe suchen sie nach Schwachstellen im gegnerischen System, die dann mit der eigenen Schadsoftware infiltriert werden. Von diesem Moment an schlummern auf den Rechnern der Angegriffenen Trojaner, also eine Art digitale Schläferzellen.

Bei Bedarf können die Spezialisten im „Remote Operations Center“, dem Fernbedienungszentrum, diese Schläfer aktivieren. Die Kommandozentrale für den Cyberwar ist in einem abgeschirmten Bereich des NSA-Hauptquartiers in Fort Meade, Maryland, untergebracht. Dort arbeiten Nachrichtendienstler und Militärs eng zusammen. Die Hacker im Dienste der NSA können mit der Schläfersoftware „kritische Daten der Gegner bei Bedarf manipulieren“, um eigene militärische Operationen zu unterstützen oder die der Gegner zu stören.

In der Dominanzphase soll es dann möglich sein, kritische Systeme der Gegner in der Wirtschaft, den Transportwegen und der Telekommunikation nach Belieben zu kontrollieren oder zu zerstören; um so den „Kampfeswillen“ des Gegners zu brechen, wie es in den geheim eingestuften Dokumenten heißt.

Die USA gehören zu den wenigen Ländern, die bereits eine ausgefeilte Cyberdoktrin entwickelt haben. Im Falle eines schweren Computerangriffs auf ihre eigenen kritischen Infrastrukturen behält sich Washington ausdrücklich vor, mit einem konventionellen Erstschlag zu kontern.

Gleichzeitig rüsten die Vereinigten Staaten massiv zum Cyberwar. Im Snowden-Archiv fand sich eine Direktive des Präsidenten vom Oktober 2012, in der Obama die Chefs der Geheimdienste anwies, eine Liste mit möglichen Zielen für amerikanische Cyberattacken zu erstellen.

In Israel hat Premierminister Benjamin Netanjahu das Thema zur Chefsache erklärt. Sein Acht-Millionen-Einwohner-Staat soll Cyberweltmacht werden. Die legendäre Einheit 8200, das israelische Pendant der NSA, besteht aus mehreren Tausend Experten. Neben weitreichender technischer Überwachung von Palästinensern im Westjordanland und im Gazastreifen arbeiten die Elitehacker dort an elaborierten Digitalwaffen.

Im April gab Verteidigungsministerin Ursula von der Leyen bekannt, auch die Bundeswehr werde in Zukunft alle Cyberaktivitäten in einem neuen militärischen Organisationsbereich zusammenfassen. Zum 1. April 2017 sollen knapp 14 000 Soldaten und Zivilisten dem neuen Inspekteur des Kommandos Cyber- und Informationsraum in Bonn unterstellt werden, einem Dreisternegeneral.

In der abgeschirmten Tomburg-Kaserne in Rheinbach bei Bonn spielen 60 Bundeswehrhacker der geheimnisvollen Einheit Computer Netzwerk Operationen (CNO) schon seit Jahren Cyberangriffe und Gegenattacken durch, nicht verbunden mit dem Internet. Die wichtigste Aufgabe der neuen Digitaltruppen wird der Schutz des riesigen Bundeswehrnetzes sein. Moderne Waffensysteme wie der „Eurofighter“ sind schon heute mehr Soft- als Hardware. In dem Kampfflugzeug sind 80 Computer und 100 Kilometer Kabel verbaut. Der „Eurofighter“ ist damit ein potenzielles „Hochwertziel“ für digitale Angreifer, eines von vielen.

Unter dem Spardiktat der vergangenen Jahrzehnte wurde die Armee wie viele westliche Streitkräfte Schritt für Schritt nach dem Vorbild von Großunternehmen auf Effizienz getrimmt. Eine einheitliche Datenverarbeitung oder standardisierte Logistiksoftware sparen Geld, aber sie machen es Angreifern einfacher, mit einer erfolgreichen Attacke gleich das ganze System zu beherrschen. Mehr Effizienz kann deshalb zu weniger Widerstandsfähigkeit führen. Wem es gelänge, die SAP-Software zu kapern, mit der die Bundeswehr ihren zentralen Nachschub organisiert, der könnte die Barcodes für Millionen Produkte manipulieren und dafür sorgen, dass die Truppen im Einsatz in ihren Containern Klopapier statt Granaten fänden.

Dass die Bundeswehr und die westlichen Partnerarmeen die Cyberbedrohung so ernst nehmen, hat auch mit Freitag, dem 27. April 2007, zu tun. Damals fielen in Tallinn einige Geldautomaten aus, und ein technischer Fehler legte die Kartenlesegeräte in den Supermärkten lahm. Für die Bürger der estnischen Hauptstadt war das ärgerlich, aber nicht zu ändern, denn der Fehler erwies sich als hartnäckig.

Doch dann häuften sich in dem kleinen Land im Baltikum die Merkwürdigkeiten. Onlinedienste blieben gesperrt, Rundfunksender gingen offline, Kommunikationskanäle im estnischen Parlament waren blockiert. Am 9. Mai verstummte auch die Website des Premierministers. Innerhalb von zwei Wochen hatten Unbekannte die Bürger von einem Teil ihres Lebens abgeschnitten. „In Estland“, erklärte Ministerpräsident Andrus Ansip, „wurde das Modell eines neuen Cyberkriegs getestet.“

Wer die Angreifer waren, ist bis heute nicht zweifelsfrei geklärt. Für den Premier war es „keine Frage“, dass Russland da-

JESSE A. HYATT / DOD NEWS

Cyberübung in den USA: Sorgfältig inszenierte Katastrophe

JIM LO SCALZO / DPA

NSA-Zentrale in Fort Meade: Amerikas „informationelle Vorherrschaft“ sichern

hintersteckte. Denn die Attacke hatte genau an jenem Tag begonnen, an dem Estland allen Protesten des Kreml zum Trotz ein russisches Kriegsdenkmal aus dem Stadtzentrum von Tallinn verlegte.

Zwei Jahre später brüstete sich ein Führer der Putin-treuen Jugendorganisation „Naschi“ damit, den Angriff orchestriert zu haben. Das offizielle Moskau bestreitet bis heute eine Verstrickung.

Die Bundesregierung hält vier Staaten für die größte Bedrohung des Westens im virtuellen Raum: China, Russland, Iran und Nordkorea, wobei alle unterschiedliche Ziele verfolgen. Während Peking zum größten Teil Industriespionage betreibt, setzt der Kreml seine mindestens 4000 hoch spezialisierten Cybersoldaten vor allem für politische Spionage und zunehmend auch Sabotage ein. Nordkorea gilt als Gefahr, weil es seine Cyberkrieger offenbar auch als Söldner vermietet.

Mehr als 15 Staaten sollen inzwischen in der Lage sein, mit digitalen Waffen die Energie-, Kommunikations- und Verkehrsnetze, das Finanzsystem und die Lebensmittellogistik ganzer Staaten zu torpedieren. Mit gewaltigem finanziellen und personellen Aufwand entwickeln sie dafür maßgeschneiderte Schadsoftware, die das digitale Nervensystem von Behörden und Firmen zerstören kann.

„Advanced Persistent Threat“ (APT) nennen Experten solche Cyberangriffe, die wie der Computervirus „Stuxnet“ so komplex sind, dass ihre Urheber nur Staaten oder deren Helfer sein können. Allein Chinas berüchtigte Einheit 61398 verantwortet seit 2006 mehr als 140 solcher Großangriffe auf Organisationen aus den USA und anderen englischsprachigen Ländern, um sie auszuspionieren.

Wie erfolgreich und hartnäckig die staatlich gesponserten Digitalwaffen sein können, zeigt beispielhaft APT28 alias „Sofacy“. Seit spätestens 2007 attackierte die dahinterstehende Gruppe unter anderem osteuropäische Ministerien, Rüstungsmessen, Nato-Organisationen und das Weiße Haus. Getarnt als „News Bulletin“ der Vereinten Nationen schlich sich die Schadsoftware im Frühjahr 2015 ins Netzwerk des Deutschen Bundestags und fischte dort unbemerkt große Datenmengen ab.

Auch der Cyberangriff auf die CDU-Bundeszentrale im April soll das Werk von „Sofacy“ sein. So wie der spektakuläre Sabotageakt auf den französischen Sender TV5 Monde im vergangenen Jahr. Hacker hatten den Sendebetrieb zum Erliegen gebracht, auf der Website des Fernsehkanals islamistische Botschaften platziert und damit den Eindruck erweckt, es handle sich um einen Angriff durch das „Cyber Kalifat“ des „Islamischen Staats“.

IT-Experten sind sich heute sicher, dass hinter „Sofacy“ in Wahrheit russische Cyberaktivisten stehen. Denn zu den Opfern gehörten nicht nur auffällig viele russische Dissidenten und ukrainische Aktivisten. Abwehrspezialisten stellten auch fest, dass die Gruppe vor allem zu den üblichen Moskauer und St. Petersburger Bürozeiten aktiv ist und dass entscheidende Zeilen des Softwarecodes mit kyrillischen Tastaturen verfasst wurden. Keine Beweise, aber starke Indizien.

Die Attacke auf TV5 Monde verblüffte westliche Militärbeobachter auch aus einem anderen Grund. Fast allen APT-Angreifern ging es in den vergangenen Jahren darum, die Opfer so lange und intensiv wie möglich auszukundschaften und dabei möglichst unerkannt zu bleiben. Die unverfrorene Attacke auf den französischen Fernsehsender war jedoch ein Fall offener Sabotage. Wollte der Kreml der Welt demonstrieren, wozu er in der Lage ist?

Mit dem digitalen Gruß aus Moskau könnte ein Szenario Wirklichkeit geworden sein, vor dem Sicherheitsexperten wie Hans-Georg Maaßen schon länger warnen. Mit komplexen Cyberwaffen platzierten die Täter „digitale Zeitbomben“ bei ihren Gegnern, die scharf gestellt werden könnten, wenn es politisch opportun erscheint. Droht also tatsächlich irgendwann ein „Cyber Pearl Harbor“, wie es der ehemalige US-Verteidigungsminister Leon Panetta schon 2012 an die Wand malte?

Es ist eine Lehre der Kriegsgeschichte, dass neue Erfindungen die alte Technik nur sehr langsam ersetzen. Sie erweitern zunächst nur das Arsenal um weitere, gefährliche und möglicherweise kriegsentscheidende Waffen. Und so glaubt der Bundesnachrichtendienst, dass Schadsoftware in einem bewaffneten Konflikt als „flankierendes Wirkmittel“ eingesetzt werden könnte. Also potenziell gegen jedes Ziel, das mit einem Netzwerk verbunden ist. Für die Ära des „Internets der Dinge“, in der schon eine vernetzte Zahnbürste eine fatale Kettenreaktion auslösen kann, sind das beunruhigende Nachrichten.

Wer einen Eindruck davon bekommen will, wie verletzlich ein voll vernetztes Gemeinwesen ist, kann nach Saarbrücken reisen. Dort sitzt Marco Di Filippo an einem sonnigen Tag in seinem Büro und hat die Wahl. Er könnte irgendwo in Süddeutschland Kirchturmglocken läuten lassen, hundert Kilometer entfernt die Pumpen eines Wasserwerks hochfahren oder die Beleuchtung des Berliner Doms ausknipsen.

Stattdessen dringt er mühelos und ganz legal in ein Privathaus ein. „Schauen Sie hier“, sagt Di Filippo, die Temperatur liegt bei 21,7 Grad. „Etwas zu warm, finden Sie nicht?“ Er könnte das ändern, doch sicherheitshalber klappt er sein Notebook zu. Di Filippo hat sich einer großen Aufgabe verschrieben. Er sammelt Schwachstellen.

Die Deutschlandkarte in seinem Büro ist mit Tausenden roten Punkten übersät. Jeder steht für eine Fabrik, eine Schleuse, ein Wohnhaus oder eine Schule, die ein halbwegs versierter Computernutzer problemlos manipulieren könnte, weil sie nicht geschützt sind, noch nicht einmal per Passwort. Es ist eine Karte flächendeckender Sorglosigkeit. „Gegen Cyberattacken“, sagt Di Filippo, „sind wir in Deutschland nicht besonders gut gewappnet.“

Er arbeitet für das Forschungsprojekt „RiskViz“, „Risikolagebild der industriellen IT-Sicherheit in Deutschland“, zu dem sich im April 2015 mehrere Universitäten, Institute und Unternehmen zusammengeschlossen haben, darunter Di Filippos Koramis GmbH.

Als sich das Bundesamt für Sicherheit in der Informationstechnik im vergangenen Jahr unter deutschen Unternehmen und Institutionen nach dem Stand der Cybersicherheit erkundigte, stießen die Beamten auf ein Paradox. Fast 60 Prozent der Firmen gaben im Schutz der Anonymität zu, 2014 und 2015 Opfer von Cyber-

U.S. AIR FORCE / TECH. SGT. EFFRAIN LOPEZ / HANDOUT / REUTERS

US-Drohne: Wer über die modernsten Waffen verfügt, ist am verletzlichsten

attacken geworden zu sein. Nahezu jeder zweite Angriff war erfolgreich.

Doch nur die wenigsten Unternehmen strengen sich an, ihr digitales Nervensystem zu schützen. Besonders absurd: Jede sechste Firma antwortete auf die Frage, wie viele Mitarbeiter mit Datensicherheit befasst seien, mit einem Wort: keiner.

Di Filippo wundert sich deshalb nicht, wenn er sich nahezu beliebig durch Wasserwerke und vernetzte Eigenheime klicken kann. Einmal hätte er in Norddeutschland das Babybecken eines Schwimmbads problemlos auf brühend heiße 88 Grad erhitzen können.

Im vergangenen Jahr startete seine Firma das Projekt „Honeytrain“. Sie erfand ein fiktives kommunales Verkehrsunternehmen, die „Nahverkehr Saar“, stellte eine professionelle Website online und schützte die Steuerungssysteme mit einer Standard-Firewall. Innerhalb von sechs Wochen registrierten Di Filippo und seine Experten fast 2,8 Millionen feindselige Zugriffsversuche aus aller Welt, die meisten automatisiert und erfolglos. In acht Fällen allerdings schafften es die Angreifer, die Sicherheitsbarrieren zu überwinden. Sie übernahmen die Steuerung von Zügen oder änderten Signale von Rot auf Grün. Bei einer Attacke aus Malaysia lotsten die Hacker einen Personenzug auf ein Nebengleis und ließen ihn mit einem anderen kollidieren.

Di Filippo ist sicher, dass sich digitale Sorglosigkeit rächen kann. Man könne fast von Glück reden, dass für Terroristen bisher Bomben und Kalaschnikows die Mittel der Wahl seien.

Es gehört zu den Absurditäten der Netzwelt, dass die Staaten, die über die modernsten Digitalwaffen verfügen, auch die verletzlichsten sind. „Wenn die Nation heute in einen Cyberkrieg ziehen müsste, würden wir verlieren“, sagte Mike McConnell in einer Anhörung vor dem US-Senat. Der Mann muss es wissen. In seiner Zeit als Nationaler Geheimdienstdirektor investierten die USA zwischen 2007 und 2009 Milliarden in ihre Cyberkriegsfähigkeiten. Und dennoch war sich McConnell sicher: „Wir sind besonders verwundbar. Wir sind am stärksten vernetzt. Für uns steht am meisten auf dem Spiel.“

Anders als viele seiner Gegner ist das US-Militär fast vollständig von seinen Computernetzen abhängig. Eine Cyberattacke gleicher Stärke hätte in den USA damit ungleich größere Auswirkungen als in einem Land wie China, dessen Armee sehr viel weniger vernetzt ist. Von einem Digitalzwerg wie Nordkorea ganz zu schweigen, das sich nie an das weltweite Netz angekoppelt hat.

Vor sieben Jahren schnappten amerikanische Soldaten im Irak einen Anführer der Aufständischen. Als sie seinen Laptop durchsuchten, machten sie eine erstaunliche Entdeckung. Der Mann hatte beobachtet, wie er von den Amerikanern beobachtet wurde. Den Aufständischen war es gelungen, sich in den Datenstrom der Aufklärungsdrohnen zu hacken, mit denen das US-Militär jede ihrer Bewegungen verfolgte. Wie ein Bankräuber, der illegal den Polizeifunk mithört, konnten die Aufständischen die Videos mitverfolgen, die die Drohnen an ihre Bodenstation funkten.

Doch noch erschreckender war die Erkenntnis, wie leicht sie die amerikanischen Drohnen knacken konnten. Sie benutzten eine Billigsoftware, die ursprünglich von amerikanischen Collegestudenten entwickelt worden war, um im Netz illegal Videos runterzuladen. Auf einer russischen Website wurde sie für 25,95 Dollar verramscht.

Später wurde bekannt, dass die Computer der US-Luftwaffe in Nevada, mit denen die Drohnenflotte gesteuert wird, von einem Virus infiziert waren, der sich nicht entfernen ließ. „Wir löschen ihn, und er kommt immer wieder“, so zitierte das Magazin „Wired“ einen Fachmann, der an dem Problem arbeitete, „wir glauben, dass er harmlos ist, aber wir wissen es nicht.“

Cyberwaffen revolutionieren die Kriegführung, doch wird der Krieg der Zukunft dadurch „humaner“ sein, mit weniger Toten und weniger Zerstörung? Die Antwort auf diese Frage ist unbefriedigend: Es kommt darauf an. Waffen sind ethisch neutral. Entscheidend ist, wer sie wie einsetzt.

Der „Stuxnet“-Virus zeigt, wozu digitale Waffen in der Lage sind. Im Vergleich zu einem konventionellen Angriff war die physische Wirkung minimal. Der Virus war so gezielt, dass er ausschließlich die iranischen Uranzentrifugen zerstörte, es gab keine Toten. Als die israelische Luftwaffe 1981 eine irakische Atomforschungsanlage bombardierte, legte sie noch ein komplettes Gebäude in Schutt und Asche und tötete zehn Soldaten und einen Zivilisten.

Öffnete „Stuxnet“ also die Tür in eine Zukunft der „humanen“ Kriegführung? Der Test steht noch aus, die historische Erfahrung spricht dagegen. Die Wahrscheinlichkeit ist hoch, dass neue Cyberwaffen oder Drohnen ein globales Wettrüsten in Gang setzen. „Wir sind bereits mitten im Cyberkrieg“, sagt ein hoher deutscher Regierungsbeamter.

Die Nato-Partner haben sich inzwischen darauf geeinigt, dass Cyberangriffe den Bündnisfall nach Artikel 5 des Nordatlantikpakts auslösen können. Aber dafür müsste klar sein, wer der Angreifer ist, und genau diese Zuordnung ist das Problem.

Kann sein, dass der Angreifer in einem Internetcafé in Südafrika sitzt, einen Computer in Argentinien kapert, mit dem er in ein chinesisches System eindringt, das von Rechnern kontrolliert wird, die sich physisch in Großbritannien befinden.

25 Prozent der Computer, die 2007 die Netze in Estland angriffen, standen in den USA, obwohl die Attacke wahrscheinlich von russischen Hackern gefahren wurde. Der Server für die jüngste Attacke auf Deutschlands Parteien soll auf Bali gestanden haben. Selbst die aufwendigsten Cyberanalysen enden meist beim angreifenden Rechner, ohne dass klar ist, ob er ferngesteuert wurde und, wenn ja, von wem.

Nie war es leichter als im Digitalen, seine Spuren zu verwischen. Und nie war es schwerer, den wirklichen Gegner und damit das Ziel eines möglichen Gegenschlags eindeutig und sicher zu identifizieren. Gut möglich, dass die amerikanischen Cyberwaffen, die seit zwei Wochen im Netz kursieren, bereits eingesetzt wurden. Wäre der Datendiebstahl nicht entdeckt worden, hätte im Falle einer neuen Attacke alles auf einen einzigen Urheber hingedeutet: den US-Geheimdienst NSA.

Matthias Gebauer, Konstantin von Hammerstein, Christiane Hoffmann, Marcel Rosenbach, Jörg Schindler

Video: Hackerangriff auf ein Smart-Home

spiegel.de/sp392016hacker
oder in der App DER SPIEGEL