

03 2013

DOSSIER

KRIEG DER ZUKUNFT

ZEIT
WISSEN

s 00 BIS s 00

Der unsichtbare Gegner



DIE FRONT löst sich auf, die großen Heere von einst verschwinden. *Drohnen und Software*, Spezialeinheiten und Guerillakrieger übernehmen den Kampf. Wie sieht der KRIEG DER ZUKUNFT aus?

42 **Drohnen** – *Das Wettrüsten mit ferngesteuerten Bombern.*

45 **Killermaschinen** – *Wann dürfen Roboter selbstständig töten?*

46 **Cyberkrieg** – *Was Schadsoftware wirklich anrichten kann.*

48 **Atombomben** – *Neue Risiken einer alten Technologie.*

Seit Jahrtausenden quält sich die Menschheit mit einer tödlichen Plage: dem Krieg. In mehr als 30 Ländern wird derzeit gekämpft, teils in Guerilla-, teils in Bürgerkriegen. Weder Friedensforscher noch Militärexperten gehen davon aus, dass sich dies jemals ändern wird. Aber der Krieg des 21. Jahrhunderts wird anders aussehen als seine Vorgänger. »Er wird fraktaler«, sagt der Hamburger Friedensforscher Götz Neuneck. Will heißen: Die Front löst sich zunehmend auf, das Schlachtfeld, auf dem große Armeen gegeneinander kämpften, weicht einem unüberschaubaren Mosaik von Konfliktpunkten. Der Krieg könnte irgendwann überall und nirgends sein, in Los Angeles, Taipeh und der uigurischen Steppe zugleich. Ohne klassische Heere. Mehrere Entwicklungen sprechen dafür.

Zum einen ist Krieg immer weniger eine Frage der Truppenstärke, wie der US-Militärhistoriker Max Boot in seinem Buch *War Made New* mit nüchternen Zahlen belegt. Im Amerikanischen Bürgerkrieg wurden knapp 3900 Soldaten pro Quadratkilometer Frontgebiet eingesetzt, im Ersten Weltkrieg waren es noch 404, im Zweiten Weltkrieg 36 und im Golfkrieg von 1991 ganze zwei. Im Industriezeitalter ging die Vernichtungskraft auf Maschinen über, die von Soldaten bedient werden: Maschinengewehre, Panzer, Kampffjets, Raketen.

Zweitens sind die Kriege der Gegenwart zunehmend »asymmetrisch«. Eine staatliche Streitmacht sieht sich mit einem schlecht ausgerüsteten, aber gewieften Gegner konfrontiert, der keinen Staatsapparat hinter sich hat und an vielen Orten operiert. Hightech kämpft gegen Lowtech – und kann dabei verwundbar sein. »Die Al-Kaida, deren gesamte finanzielle Mittel nicht für den Kauf eines F-22-Jets ausreichen würden, kann dem reichsten Land der Welt enormen Schaden zufügen«, schreibt Boot über die Anschläge des 11. September 2001.

Drittens sind die westlichen Industrienationen – nicht erst seit 9/11 – dazu übergegangen, Waffen zu entwickeln, die präziser sein sollen. Je kritischer ihre Bürger es beurteilen, wenn Zivilisten und eigene Soldaten getötet werden, desto mehr versuchen sie, nur die militärischen Ziele des Gegners zu treffen. Die Präzision erscheint auch in der Logik des Krieges als Notwendigkeit: Wo sich der Gegner über das ganze Land verteilt oder in Städten versteckt, bringen klassische Kampfverbände wenig. Die sogenannte Drohne, ein unbemanntes und ferngesteuertes Fluggerät, tritt ihren Siegeszug an. Im Kosovo-Krieg noch ein Aufklärungsinstrument, ist sie etwa für die USA zur Waffe der Wahl geworden, um im Bergland an der afghanisch-pakistanischen Grenze Al-Kaida- oder Taliban-Kämpfer zu liquidieren. Dass die Genauigkeit von Drohnenangriffen aller-

dings nur ein frommer Wunsch ist, zeigen die zahlreichen zivilen Opfer.

Der nächste Schritt könnte von der »präzisen« zur »intelligenten« Waffe führen, die, mit Roboter-technik ausgerüstet, selbsttätig über ihr Ziel entscheidet. Neuere Studien zeigen, dass sogar Drohnenpiloten unter Traumatisierungen leiden, obwohl sie den Angriff nur aus der Ferne steuern. Also entledigt man sich am Ende gänzlich des Menschen, dieses labilen Anhängsels der Maschine.

Drohnen und mögliche Roboterwaffensysteme sind ohne die moderne Computertechnik nicht denkbar. Vielmehr sind sie – der vierte Trend – Teil einer Informationssphäre, die nicht nur in Form von Satelliten den Erdball umspannt, sondern auch den Alltag und die Infrastruktur der alten und der neuen Industriestaaten durchzieht. Für deren Militärs ist sie Fluch und Segen zugleich. Segen, weil den elektronischen Augen von Satelliten und Drohnen nur wenig zu entgehen scheint und weil manche hoffen, staatliche Gegner allein mittels Software schädigen zu können. Der Computerwurm Stuxnet, der Uran-Zentrifugen des iranischen Atomprogramms zerstörte, war womöglich der Anfang einer solchen Taktik. Fluch, weil selbst kleine Gegner dasselbe versuchen könnten – mit großem Effekt.

Ob sich hieraus ein Cyberwar entwickeln wird, ist umstritten. Der frühere Sicherheitskoordinator der US-Regierungen Clinton und Bush, Richard Clarke, mahnt: »Wir befinden uns bereits im Netzkrieg.« Thomas Rid, Cybersicherheitsforscher am King's College, widerspricht: Man dürfe Cyberspionage und -sabotage nicht mit Krieg verwechseln (siehe Seite 46). Das ist aber vielleicht kein Widerspruch. Dass Großmächte in den kommenden Jahrzehnten offenen Krieg gegeneinander führen werden, ist unwahrscheinlich. Weil ihre Ökonomien über globale Zulieferketten und Produktionsnetze verwoben sind, könnten sie Cyberwaffen als Nadelstiche einsetzen, um in Zeiten politischer Spannung Druck auf andere Staaten auszuüben.

Eine Unbekannte bleibt die atomare Bedrohung. Noch immer gibt es Tausende von nuklearen Sprengköpfen weltweit, und die martialischen Gesten des nordkoreanischen Diktators Kim Jong Un erinnern daran, dass auch unberechenbare Staaten in ihrem Besitz sind. Selbst wenn sich hier doch Vernunft durchsetzen sollte, bleibt die Tatsache, dass Krieg eine Konstante der menschlichen Zivilisation ist. Zwar haben Rüstungsabkommen und eine bessere Krisendiplomatie ein großes Gemetzel nach dem Zweiten Weltkrieg verhindert. Waffenhandel und Militärbudgets sind jedoch nicht geschrumpft. Die düstere Einschätzung des spanischen Philosophen George Santayana dürfte weiterhin gelten: »Nur die Toten haben das Ende des Krieges gesehen.«

Niels Boeing

Vom Faustkeil zur Drohne

In der Kriegstechnik gibt es viel Innovation. Sie macht das Töten effizienter.

Ab 2000 v. Chr.



Das Schwert entwickelt sich in der Bronzezeit als Langform des Dolches.

Ab 2000 v. Chr.



Der Streitwagen kommt in Zentralasien auf. Auch in Mesopotamien werden Schlachten damit geführt.

Ab 1200 v. Chr.



Die Kavallerie verdrängt seit Beginn der Eisenzeit den Streitwagen.

Ab 1200 v. Chr.



Das Kriegsschiff verlagert den Krieg auf die Meere. In der Antike wird es von Sklaven gerudert (Galeere).

Der ferngesteuerte Krieg

DROHNEN könnten bald autonom über *Leben und Tod* entscheiden.
Wer trägt dann die Verantwortung für KRIEGSVERBRECHEN?

Ab 400 v. Chr.



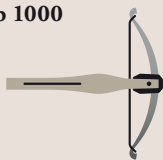
Das Katapult entwickelt sich zur wichtigen Waffe für Stadtbelagerungen.

Ab 600 n. Chr.



Der Steigbügel ermöglicht einen wendigeren Reistil, Voraussetzung für Ritterheere im Mittelalter.

Ab 1000



Die Armbrust bringt die ersten Scharfschützen der Geschichte hervor.

1346



Aus der Kanone, in der Schlacht von Crécy von England eingesetzt, entwickelt sich die Artillerie.

Explosionen dröhnen, Rauch steigt auf, Maschinengewehre knattern. Kurz vor 14 Uhr beginnt das tägliche Gefecht in Abu Dhabi. Panzer fahren Rampen hinauf, gefolgt von Haubitzen, die ihre Geschützrohre aufrichten. Elitesoldaten seilen sich von Hubschraubern ab, und Kampfjets donnern über das Showgelände der International Defence Exhibition & Conference (Idex), der wirtschaftlich bedeutendsten Rüstungsmesse der Welt. Die Streitkräfte der Vereinigten Arabischen Emirate führen den Besuchern ihr Arsenal vor.

Das Drehbuch zu der Waffenshow scheint Hollywood geschrieben zu haben. Und doch wirken die Kriegsszenen wie aus einem Film der neunziger Jahre. Denn es fehlt ein Waffentyp, der das Militärwesen des 21. Jahrhunderts revolutioniert: bewaffnete ferngesteuerte Flugzeuge, besser bekannt als Drohnen.

Am Boden sind auf der Messe in Abu Dhabi zahlreiche solcher Modelle zu sehen. Für die unbemannten Systeme wurde in diesem Jahr ein eigener Bereich aufgebaut, der stets gut besucht ist. Etwas entfernt vom Showgelände, getrennt durch eine Schnellstraße, stehen einige hellgrau gestrichene Kleinflugzeuge. UAV nennen die Militärs die Maschinen: *unmanned aerial vehicles*, unbemannte Flugsysteme. Vor allem ein Modell zieht die Blicke auf sich: Predator heißt der Flieger, Raubtier oder Räuber. Der Name ist Programm.

Weltweit streiten Befürworter und Gegner von Drohnen über das gezielte Töten. Doch auf der Idex finden kritische Töne kein Gehör. Hier wird deutlich, dass nicht mehr nur reiche Industriestaaten auf Drohnen setzen. Heute will jeder aufstrebende Staat seine Kampfdrohnen haben.

Am Stand von General Atomics sind die Broschüren zur Predator zeitweilig vergriffen. Das Unternehmen wirbt mit mehr als zwei Millionen Flugstunden, dem automatischen Start- und Landesystem, der Reichweite von mehr als 1000 Meilen und einer Einsatzzeit von rund 30 Stunden. An Bord der Predator XP befinden sich hochauflösende Videokameras mit Infrarot und Bildanalysesoftware sowie ein Schlechtwetter-Radargerät. Die Predator XP könne jederzeit und an jedem Ort Ziele aufspüren, sie identifizieren, verfolgen und bekämpfen, verspricht der Hersteller.

Der amerikanische Geheimdienst CIA und die U. S. Army haben mit Kampfdrohnen bereits Hunderte Einsätze gegen Terrorverdächtige und andere Gegner in Pakistan, Afghanistan, dem Jemen, Libyen und Somalia geflogen. Allein in Pakistan und im Jemen sollen US-Drohnen 420 Mal zugeschlagen haben, errechnete der US-Thinktank New America Foundation. Dabei wurden bis zu 3967 Menschen getötet. So kamen bei verschiedenen Luftschlägen gegen Terroranführer auch deren Kinder, Frauen und andere Unbeteiligte ums Leben. »Gezieltes Töten« nennen das amerikanischen Sicherheitsexperten. »Finger Gottes« heißt die Steuerungstechnik der Drohnen bei den Soldaten.

Während amerikanische Politiker die Erfolgsquote des Drohnenprogramms im »Krieg gegen den Terror« loben, kritisieren Menschenrechtler die hohe Zahl der durch die Predator getöteten Zivilisten und die »feige« Kriegsführung. »Der Drohnenkrieg ist kein fairer Kampf«, schrieb Byung-Chul Han, Philosophie-Professor an der Berliner Universität der Künste, in der *ZEIT*. »Dem Gegner wird nicht einmal die Möglichkeit gewährt, sich zu ergeben oder sich zu verteidigen, es gilt ja, ihn auf jeden Fall zu töten, zu vernichten, zu liquidieren.«

Tatsächlich sind die Drohnenpiloten gleichzeitig Agent, Soldat und Scharfrichter. Sie suchen nach Terroristen, identifizieren und liquidieren sie. Ihre Opfer sind Verdächtige, deren Schuld nicht bewiesen ist, die nicht vor einem Richter standen. Dank moderner Satellitentechnik können die Drohnen, von den USA aus gesteuert, in Tausenden Kilometern Entfernung zuschlagen. Die Gegner der ferngelenkten Flugzeuge sprechen von »Killermaschinen«. Das Töten sei damit so leicht wie bei einem Computerspiel. Sie fürchten eine Automatisierung des Krieges, eine Verrohung der Militärs und ein Herabsinken der Hemmschwelle beim Töten. Byung-Chul Han findet es »pervers, vor dem Bildschirm sitzend eine ganze Region, eine ganze Bevölkerung in Angst und Schrecken zu versetzen«.

Allerdings ist es ein Klischee, dass Drohnenpiloten das Töten leicht von der Hand geht. Eine Studie

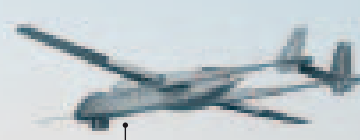
Das Schlachtfeld der Zukunft

Euro Hawk Die Aufklärungsdrohne kann in 20 Kilometer Höhe drei Tage lang in der Luft bleiben.



MQ-9 Reaper Diese Kampfdrohne ist bewaffnet. Die USA setzen sie in Afghanistan und Pakistan ein.

Cyberkrieger
Rund 30 Staaten haben Kommandostäbe eingerichtet, um sich auf Cyberangriffe vorzubereiten.



Heron TP Die Aufklärungsdrohne aus Israel kann 400 Kilometer von der Steuerzentrale entfernt operieren.

Packbot (iRobot)
Der Packbot kann Bomben, Sprengstoff und Chemikalien aufspüren. 2000 sind in Irak und Afghanistan im Einsatz.

A small, tracked robot with a sensor arm and a camera, used for detecting explosives and chemicals.

Mikado Die Mikrodrohne eignet sich etwa zur Überwachung eines Stützpunkts.



MAARS Der bewaffnete Roboter soll Menschenmengen in Schach halten.



LS3 Als eine Art Roboter-Esel schleppt das Gerät bis zu 180 Kilogramm Material.



Throwbot Der kleine Spion dient vor allem der Aufklärung in Häusern und Straßen.

A small, cylindrical robot with a camera lens, used for reconnaissance in buildings and streets.

Exoskelett Mit seiner Hilfe können Soldaten höher springen, schwerer tragen und weiter laufen.



Ende 14. Jahrhundert

Die Arkebuse ist die erste (nicht besonders zielsichere) Handfeuerwaffe auf dem Schlachtfeld.

1588

Mit Batterien von Schiffskanonen vernichten die Engländer die spanische Armada und revolutionieren den Seekrieg.

18. Jahrhundert

Aus dem Hinterlader entwickelt sich das Gewehr.

1854

Seeminen werden erstmals im Krimkrieg gegen feindliche Flotten eingesetzt.

1914

Mit dem Flugzeug entsteht der Luftkrieg. Es wird eine der Hauptwaffen der modernen Kriegsführung.

im Auftrag des US-Verteidigungsministeriums ergab, dass sie durchschnittlich genauso oft an psychischen Krankheiten wie der posttraumatischen Belastungsstörung leiden wie ihre Kollegen, die Kampffjets über dem Irak oder Afghanistan steuerten.

Die USA setzen ihre Drohnen beim »gezielten Töten« im Hoheitsgebiet anderer Länder ein. Philip Alston, Professor an der New York University School of Law und spezialisiert auf Menschenrechte, stellte 2010 als UN-Sonderbeauftragter fest, dass die Vereinigten Staaten damit zunehmend internationales Recht verletzen. Artikel 2 der UN-Charta untersagt den Militäreinsatz auf fremdem Territorium. Und Artikel 51 toleriert die Anwendung von Gewalt in Konflikten nur, wenn ein UN-Mandat das gestattet oder es um Selbstverteidigung geht. »Werden Drohnen direkt durch Geheimdienste eingesetzt, so führt dies zudem in eine juristische Grauzone, was die Definition regulärer Kriegsparteien und die Legitimation nichtmilitärischer Gewalt betrifft«, stellte die Berliner Stiftung Wissenschaft und Politik (SWP) fest.

Internationale Abkommen über den Einsatz der ferngesteuerten Waffensysteme gibt es nicht, ebenso wenig wie Exportbeschränkungen für Drohnen. Selbst Terroristen und radikale Gruppen wie Hisbollah im Libanon sollen darüber verfügen: Mit Sprengstoff beladen, könnten die Drohnen zu Anschlägen genutzt werden. Wissenschaftler haben nun das International Committee for Robot Arms Control« gegründet, das gegen die Aufrüstung mit Roboterwaffen kämpft. Die Organisation befürchtet, dass Drohnen eher zu Kriegen verführen als herkömmliche Waffensysteme und dass sie Konflikte eskalieren lassen.

Trotz aller Kritik will auch die Bundesrepublik nun Kampfdrohnen anschaffen. Bisher verfügen die deutschen Streitkräfte nur über unbemannte Aufklärer wie die »Luftgestützte unbemannte Nahaufklärungsausstattung« (Luna) und das Kleinflugzeug Zielortung (KZO). Seit März 2010 kommt zudem die Heron 1 in Afghanistan zum Einsatz. Diese unbewaffnete Drohne hat Deutschland von Israel geleast. Im Oktober 2014 endet der Leihvertrag, dann soll eine bewaffnete Version folgen. Laut Bundesregierung sind die mit Raketen bestückten Drohnen »Ausdruck eines technologischen Vorsprungs, der einen Sicherheitsgewinn vor allem durch glaubhafte Abschreckung zu bewirken vermag«.

Verteidigungsminister Thomas de Maizière sieht auch andere die Vorteile der Drohnen: Sie werden nicht müde und kennen keine körperliche Belastung. Ihre Einsatzzeiten sind länger als die von herkömmlichen Kampffjets. Sie können in die gefährlichsten Missionen geschickt werden, ohne eigene Soldaten zu gefährden. Ihre Wartung ist billiger als die der größeren Kampfflugzeuge, und der Stückpreis fällt niedriger aus: Ein F-35-Kampffjet, das neueste Mehrzweck-

Hightech-Kampfflugzeug der USA, kostet rund 100 Millionen Dollar, eine Predator-Drohne 4,5 Millionen Dollar.

Dafür bekommt der Käufer mehr als die Fähigkeit zum »gezielten Töten«. Drohnen wie die Predator unterstützen bei Gefechten die Truppen am Boden mit Informationen in Echtzeit und Waffeneinsatz, klären Routen von Patrouillen auf, begleiten Konvois, leisten Langzeitbeobachtungen von Zielen, suchen nach Hinterhalten sowie Sprengfallen und bewachen Objekte. Aber: Wenn es nicht möglich sei, den Angreifer zu töten, der die Drohne lenkt, schreibt der Philosoph Han, werde der Kriegsbegriff obsolet.

Vielleicht werden Menschen künftig für Kampfeinsätze gar nicht mehr gebraucht. Schon jetzt können Drohnen den idealen Ort für ihre Beobachtungseinsätze selbst finden. Beim Abbruch der Funkverbindung kehren sie per Autopilot zu einem definierten Punkt zurück. Sie landen und starten eigenständig und werden dank neuer Sensoren künftig mehrere Ziele gleichzeitig beobachten können. »Da die Komplexität der Operation für den Menschen in Echtzeit dann nicht mehr nachvollziehbar ist, bleibt ihm lediglich die Bestätigung oder Verweigerung einer von der Maschine vorgeschlagenen Lösung«, heißt es in einer SWP-Studie. »Eine wirkliche Entscheidungsautonomie des Menschen – auch zur Zielauswahl – wäre unter diesen Umständen nicht mehr gegeben.«

Längst arbeiten Ingenieure an der völligen Autonomie der Waffensysteme. Drohnen sollen unter anderem lernen, den automatischen Angriff bei verdächtigem Verhalten von Zielpersonen eigenständig umzusetzen. Allein die Software an Bord der Maschinen identifiziert dann die Gegner. Ein Szenario dafür: Eine Drohne entdeckt nachts Gestalten am Straßenrand, die Männer könnten Sprengfallen vergraben. Kommen weitere Verdachtsmomente hinzu, etwa dass sie mit Gewehren bewaffnet sind oder fliehen, sobald sie die Drohne bemerken, dann greift das Flugzeug autonom an. Zudem sollen Drohnen künftig mit Software zur Gesichtserkennung ausgestattet werden, um festgelegte Zielpersonen selbstständig finden zu können. Computer als Entscheider über Leben und Tod – das bringt enorme rechtliche und ethische Probleme mit sich: Wer übernimmt die juristische und moralische Verantwortung, wenn Maschinen Kriegsverbrechen begehen?

Die Drohnenkrieger lassen sich davon nicht beirren. Die Vereinigten Arabischen Emirate verkündeten gerade, dass sie Drohnen von General Atomics anschaffen werden. Auf der nächsten Rüstungsmesse in Abu Dhabi dürfte die Predator XP dann eine Hauptrolle in der täglichen Show spielen. —

Dürfen Roboter automatisch töten?



Sie haben eine Ethiksoftware für autonome Killerroboter geschrieben.

ben. Was macht die?

Der Algorithmus entscheidet aufgrund von Logik, Anweisungen und Verboten, welche Ziele angegriffen werden dürfen – und welche nicht, etwa weil das völkerrechtswidrig wäre. Es geht nicht darum, Killerroboter zu bauen, sondern darum, dass diese Roboter keine Zivilisten oder Verwundeten töten.

In einer Simulation auf Ihrer Website fliegt eine

Drohne über einen Friedhof, auf dem sich feindliche Kämpfer aufhalten. Was empfiehlt das Ethikprogramm?

Das Szenario entspringt einer wahren Begebenheit, bei der eine Drohne angefordert wurde, um Taliban-Kämpfer auf einer Beerdigung zu attackieren. Die Einsatzregeln verbieten das. Trotzdem ging die Anfrage hoch bis zum Pentagon, wo sie abgelehnt wurde. Für ein automatisches System wäre es kinderleicht, mithilfe des GPS Zonen zu definieren, wo nicht geschossen werden darf. **Die Maschine entschei-**

det also schneller.

Sie handelt am Ende auch menschlicher als ein Soldat aus Fleisch und Blut, denn sie kennt keine Angst oder Rachegefühle. Sie hat kein Recht auf Selbstverteidigung.

Sie ist aber dumm. Human Rights Watch schildert ein Szenario, in dem eine Mutter laut schreiend auf Soldaten zuläuft, weil ihre Kinder nur mit Plastikgewehren spielen. Ein autonomer Roboter würde das nicht erkennen.

Dann dürfte er auch nicht schießen. Natürlich werden diese Systeme Fehler machen. Aber

wenn sie weniger Fehler machen als menschliche Kämpfer, dann haben wir am Ende Leben gerettet.

Wie schätzt eine Maschine ein, ob ein Angriff im Sinne des Völkerrechts verhältnismäßig ist?

Das Militär nutzt heute schon Programme, um die Verhältnismäßigkeit abzuschätzen. Bug Splat etwa berechnet die Schäden aus der Explosionskraft der Munition. In Zukunft wird man den Schaden in Echtzeit kalkulieren – bevor das Feuer eröffnet wird. Maschinen werden das ebenso gut oder besser können als Soldaten.

Autonome Roboter könnten aber die Hemmschwelle senken, einen Krieg zu führen.

Diese Möglichkeit gibt es zweifellos, das gilt für jede neue Technik. Was ist die Alternative? Die Entwicklung neuer Technologien für das Militär verbieten? **Die Ächtung der Waffen.** Die Waffen sollten nicht eingesetzt werden, bevor sie sicher sind. Muss man sie dafür ächten? Ich denke nicht. Das Völkerrecht reicht dafür aus.

Ronald Arkin leitet das Mobile Robot Laboratory am Georgia Institute of Technology in Atlanta.

Die Legende vom Cyberkrieg

Medien und Politiker überbieten sich in CYBER-WAR-FANTASIEN.

Das Gerede *verschleiert die wahren Probleme*, meint Thomas Rid.

Anonymous hackt Sony. Die chinesische Armee hackt die *New York Times*. US-Agenten hacken das iranische Atomprogramm. Ist es nur noch eine Frage der Zeit, bis Cyberkrieger Züge entgleisen lassen und Flugzeuge zum Absturz bringen? Wird der nächste Weltkrieg womöglich ein Cyberkrieg sein?

Wohl kaum. Die Rede vom Cyberkrieg ist irreführend und lenkt von den wirklichen Problemen ab. Immerhin wurde noch nie ein Mensch durch einen Computerangriff verletzt oder getötet. Statt diffus von virtueller Kriegstreiberei zu reden, sollten wir das, was wirklich passiert, beim Namen nennen: Spionage, Sabotage und Subversion. Mit dieser Unterscheidung werden drei Effekte erkennbar.

Der erste Effekt betrifft die Gewalt. Bei näherem Hinsehen haben Computerangriffe unerwartete Folgen: Sie machen bisher gewaltsame Handlungen weniger gewalttätig. Geheimdienste können heute riesige Datenmengen auswerten, ohne ein Land mit Spionen zu infiltrieren. Streitkräfte legen gegnerische Luftabwehrsysteme lahm, ohne feindliche Soldaten zu verletzen. Und politische Aktivisten mobilisieren Menschenmassen, ohne zuvor durch politische Gewalt das herrschende Regime zu unterminieren. Der Konflikt selbst wird dadurch natürlich nicht gewaltfrei. Doch Staaten und Bürger haben neue Instrumente an die Hand bekommen. Nur in höchst seltenen Ausnahmefällen werden diese Instrumente zu gewaltsamen Waffen.

Der zweite Effekt betrifft die technischen Hürden. Subversion und politischer Aktivismus erfordern wenig technisches Know-how. Es braucht eine frustrierte Zielgruppe, eine gute Idee zur Mobilisierung sowie Facebook, Twitter oder andere soziale Medien. Der Flashmob oder die gemeinsame Attacke auf verwundbare Internetseiten sind mit Freeware schnell zu organisieren. Spionage dagegen will gekonnt sein. Angreifer haben hier üblicherweise ein bestimmtes Ziel im Visier. Zuerst muss das Opfer ausgetrickst werden, zumeist durch unverdächtige E-Mails mit verwanztem Anhang. Die virtuellen Einbrecher müssen dann die gesuchten Daten finden, heimlich eine Kopie fortschaffen und dabei ihre Spuren verwischen. All das ist leichter gesagt als ge-

tan. Attraktive Ziele zu knacken, etwa das Pentagon oder Google, erfordert ein sehr hohes Maß an Kompetenz und Kreativität.

Sabotage ist noch schwieriger. Die Angreifer müssen ihr Ziel im Vorfeld genau kennen. Wer komplexe Anlagen wie etwa ein Kraftwerk oder eine Raffinerie lahmlegen will, muss die Prozesssteuerung verändern und darf nicht bloß eine Fehlfunktion herbeiführen, die sofort behoben werden kann. Zudem sind besonders empfindliche Ziele womöglich gar nicht mit dem Internet verbunden. Sabotage erfordert möglicherweise Probeangriffe in einer Testumgebung sowie Komplizen vor Ort. Der Aufwand an Zeit, Aufklärung, Ressourcen und nötigem Fachwissen ist beträchtlich. Und echte Cyberwaffen sind am Ende so zielspezifisch programmiert, dass deren breiter Nutzen sehr fragwürdig erscheint.

Der dritte Effekt schließlich betrifft das Risiko. Subversion und politischer Aktivismus mögen eine Bedrohung für autoritäre Regime darstellen, wie der Arabische Frühling gezeigt hat. Doch die Situation in freien Gesellschaften ist eine andere: Demokratie und Kapitalismus leben von einem gesunden Maß an Subversion und permanenter Erneuerung. Die große digitale Herausforderung des Westens ist es, konstruktive von gefährlicher Subversion zu unterscheiden und Erstere zu schützen. Computerspionage stellt das größte unmittelbare Risiko dar. Das 21. Jahrhundert ist das goldene Zeitalter der *signal intelligence*, wie der ehemalige CIA-Direktor Michael Hayden einmal sagte. Derzeit profitiert vor allem China von diesem Goldrausch. Unvorstellbare Mengen von intellektuellem Eigentum werden heimlich in Form von Einsen und Nullen nach Fernost gepumpt. Die wirtschaftlichen Kosten dieses Wissenstransfers sind noch nicht abzuschätzen. Sabotage bleibt die Ausnahme. Es gibt weniger als eine Handvoll ernsthafter Fälle.

All das könnte sich ändern. Doch absurde Science-Fiction-Szenarien, rhetorisch zum Cyberkrieg zugespitzt, dürfen nicht länger den Blick auf die wirklichen Probleme versperren.



Thomas Rid ist Professor im Fachbereich War Studies am King's College in London. Sein neues Buch »Cyber War Will Not Take Place« erscheint am 18. April.

1939



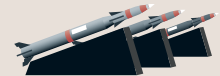
Der Panzer ermöglicht raumgreifende Feldzüge statt Stellungskriegen.

1945



Die Atombombe ist mit ihrer Vernichtungskraft ein dramatischer Einschnitt in der Militärgeschichte.

1957



Die erste Interkontinentalrakete hebt im russischen Baikonur ab. Ein globaler Atomkrieg wird zum denkbaren Szenario.

1964



Die Drohne wird erstmals im Vietnamkrieg von den USA zur Luftaufklärung eingesetzt.

1/1

GANZE SEITE

Gefährliche Grauzonen

Der *Nuklearschmuggel* und das Szenario eines regionalen ATOMKRIEGS beunruhigen Friedensforscher. Auch *an Deutschland gibt es Kritik*.

Es klingt seltsam, dass Wissenschaftler einen Brief an den amerikanischen Präsidenten schreiben, nur weil sie eine Uhr stellen, aber in diesem Fall ging es um ein besonderes Exemplar: die Weltuntergangs-Uhr. Seit 1947 diskutiert eine Gruppe von Forschern regelmäßig, wie nah die Menschheit am Abgrund steht, und stellt dann symbolisch den Minutenzeiger. Für 2012 entschieden sie: Es bleibt fünf Minuten vor zwölf, wie im Vorjahr. »2012 war das Jahr der ungenutzten Möglichkeiten, das nukleare Waffenarsenal zu reduzieren, die Verbreitung radioaktiven Materials zu kontrollieren und dem Nuklearterrorismus Einhalt zu gebieten«, schrieben sie im Januar an Barack Obama. Eine Bestätigung ihrer düsteren Einschätzung bekamen sie einen Monat später: Nordkorea machte seinen dritten Atombombentest.

Knapp 17 300 atomare Sprengköpfe befinden sich derzeit im Besitz von neun Staaten (siehe Grafik). Bis zu 300 davon sind in der Hand von Indien, Pakistan, Israel und Nordkorea, die nicht Mitglied des Atomwaffensperrvertrags sind und keiner Kontrolle durch die Atomenergiebehörde IAEA unterliegen.

In einem Schreckensszenario hat der Meteorologe Alan Robock berechnet, welche Klimafolgen ein begrenzter Atomkrieg hätte: Würden etwa Indien und Pakistan mit je 50 Atombomben die Städte des Gegners angreifen, gäbe es nicht nur dort zahlreiche Opfer, sondern obendrein gelangten Millionen Tonnen Ruß in die oberen Atmosphärenschichten. Die Durchschnittstemperatur würde weltweit jahrelang um 1,25 bis 2 Grad absinken. »Die Erde würde stärker abkühlen als in der Kleinen Eiszeit«, sagt Robock. Weltweit würden Menschen unter Ernteausfällen leiden.

100 Atombomben? Das sei gar nicht so abwegig, meint der Sicherheitsforscher Zia Mian von der Universität Princeton: »In den 50er und 60er Jahren sah die militärische Planung der USA vor, im Ernstfall alle Atombomben einzusetzen.« Das waren viele Hundert. Im Jahr 2000 wurde bekannt, dass die USA innerhalb von zwei Minuten knapp 1800 Atombomben auf Ziele in Russland abfeuern könnten. Warum sollten Indien und Pakistan andere Strategien verfolgen? Ein schwacher Trost: Nordkorea, dessen Außenministerium im Februar mit einem Präventivschlag drohte,

besitzt derzeit weniger als zehn Sprengköpfe. Nach dem jüngsten Atomwaffentest rätseln Experten noch, ob dies eine kompakte Atombombe der zweiten Generation war, wie man sie für Raketen braucht.

Eine weitere Sorge gilt dem Nuklearschmuggel. Seit 1993 registrierte die IAEA weltweit 615 Fälle von Diebstahl oder Verlust, meist von radioaktiven Stoffen aus Krankenhäusern oder Industrieunternehmen. »Einige Fälle« deuteten auf organisierten Handel mit radioaktivem Material hin, schreibt die Behörde. 16 Mal wurde hochangereichertes Uran (HEU) oder Plutonium beschlagnahmt, Bombenrohstoff.

Weltweit befinden sich 20 Tonnen HEU in Nichtatomwaffenstaaten. Das Material wird in Forschungsreaktoren verwendet, schon vier Kilo würden für den Bau einer Atombombe genügen. Seit Jahren gibt es deshalb Bemühungen, HEU aus dem zivilen Kreislauf zu verbannen. Auch der Münchner Forschungsreaktor FRM II sollte bis 2010 von HEU auf harmloses Uran umrüsten, darauf einigten sich die Bundesregierung und Bayern 2003. Daraus wurde nichts, nun wird 2018 anvisiert. Deutschland sei ein »unrühmliches Beispiel«, klagt Friedensforscher Matthias Englert von der Technischen Universität Darmstadt. »Wir warten nur darauf, dass der Iran dieses Argument entdeckt und auch einen Forschungsreaktor mit HEU bauen will.« Max Rauner

Der Münchner Forschungsreaktor sollte eigentlich von 2010 an weniger gefährliches Uran verwenden. Nun ist von 2018 die Rede.

Das nukleare Waffenarsenal (2012)

