DROEMER

YVONNE HOFSTETTER

DER UNSICHTBARE KRIEG

WIE DIE DIGITALISIERUNG SICHERHEIT UND STABILITÄT IN DER WELT BEDROHT

DROEMER

Besuchen Sie uns im Internet:
www.droemer.de

Originalausgabe Oktober 2019

Dieses Werk wurde vermittelt durch die
Literarische Agentur Michael Gaeb.

Ein Imprint der Verlagsgruppe
Droemer Knaur GmbH & Co. KG, München

Covergestaltung: Martin Steiner
Coverabbildung: youworkforthem / Colorpong
Emoji im Innenteil: popicon / Shutterstock.com
Satz: Adobe InDesign im Verlag
Druck und Bindung: CPI books GmbH, Leck
ISBN 978-3-426-27786-7

2 4 5 3 1

Triggerwarnung

Dieses Sprachwerk enthält Informationen zu politischer Macht und militärischer Gewalt, die beim Leser Angst oder Empörung auslösen können.

Inhalt

[VORWORT]

Mitten im Frieden

Digital First. Bedenken Second.

Wahlkampfplakat der FDP 2017

Von: Anonymous Hacker
Gesendet: 30. Juli 2019
An: yvonnehofstetter@web.de

Hallo, Opfer.
Ich kenne dein Passwort: torno2001.
Das ist meine letzte Warnung.
Ich schreibe dir, weil ich einen Trojaner auf einer Pornografie-Webseite installiert habe.
Und du hast die Webseite besucht.
Meine Malware hat all deine persönlichen Daten aufgezeichnet.
Dann hat der Trojaner deine Kontaktliste gespeichert und deine Webcam eingeschaltet.
Du warst unanständig, und dabei habe ich dich gefilmt.
Das schmutzige Video und deine Daten werde ich löschen, wenn du mir 500 US-Dollar in Bitcoin bezahlst.
Hier ist die Wallet-Adresse für deine Zahlung:
135qVXXBZb3v2tQcLJRA8UAndiUYNybh3J
(Du kannst googeln: »Wie man Bitcoin kauft.«)
Ich gebe dir 24 Stunden Zeit ab dem Moment, in dem du meine Nachricht liest.
Und ich weiß sofort, dass du meine Nachricht gesehen hast.
Du kannst die Polizei alarmieren, aber sie wird dir nicht helfen.

Wenn du versuchst, mich zu betrügen, sehe ich es sofort! Stell dir nur die Peinlichkeit vor: Ich kann dein Leben ruinieren!

* * *

Nein, ich habe nie eine Pornografie-Webseite besucht, und bei mir gibt es auch nichts zu sehen oder zu hören, wenn ein Hacker Kamera oder Mikrofon an meinem Laptop oder Tablet einschaltet. Denn schon viele Jahre lang klebe ich die Sensoren meiner elektronischen Geräte ab. Deshalb ist die E-Mail-Drohung nichts weiter als ein Bluff. Sollten Sie ähnliche Erpresser-Mails erhalten, zahlen Sie nichts. Und wenn auf die Drohbotschaft eine weitere E-Mail mit Anhang folgt, hüten Sie sich, den Anhang zu öffnen! Er könnte Schadsoftware auf Ihrem Rechner installieren.

Während ich an diesem Buch schreibe, werde ich von Computerkriminellen einmal erpresst, einmal bestohlen und einmal gehackt. Obwohl ich für die Sicherheit meiner eigenen Rechneranlagen bis jetzt selbst sorgen konnte: Der Schutz von Informationen, die ich anderen Unternehmen überlassen musste, entzieht sich meiner eigenen Sorgfalt. Zum Beispiel bei Dropbox. Der Datenspeicher wurde angegriffen und die E-Mail-Daten der Nutzer gestohlen. Oder bei der Hotelkette Marriott. Adressen von 500 Millionen Hotelgästen wurden entwendet, viele Kreditkartendetails eingeschlossen. Auch ich bin Kundin bei Marriott. Nur wenn die Bank Verdacht schöpft – »Wir haben Ihre Kreditkarte gesperrt, weil wir eine verdächtige Transaktionsanfrage der *Air Nigeria* erhalten haben« –, verursacht der Datendiebstahl keinen unmittelbaren finanziellen Verlust beim Kontoinhaber. Trotzdem ist der volkswirtschaftliche Schaden durch Online-Betrügereien beträchtlich, weil er völlig unproduktiven Arbeitsaufwand verursacht.

Wenn Hackerangriffe publik werden, stellen sich Bürger wie Unternehmen gerne vor, die Angriffe würden von 18-jährigen Sonderlingen aus dem Schlafzimmer heraus geführt. Oft haben sie damit

auch recht. Doch nun findet ein Bewusstseinswandel statt: Ermittler stellen immer häufiger fest, dass digitale Angriffe von Regierungen anderer Staaten beauftragt oder orchestriert sind, die sich privater Helfer bedienen, um online zu spionieren, Sabotageakte vorzubereiten und subversiv zu handeln. Der Angriff auf die Marriott-Hotelkette soll auf das Konto chinesischer Hacker gehen, die für das chinesische Regime spionieren.[1] Peking streitet die Angriffe ab – ein ganz typisches Verhalten, um sich von illegalen Aktionen auf fremdem Staatsgebiet zu distanzieren und Vergeltungsmaßnahmen der Staatengemeinschaft vorzubeugen. Die Externalisierung staatlicher Angriffe an Hacker, Internettrolle und Roboter, kurz: an die privaten Subunternehmer des Staates, erleichtert das Leugnen jedweder Regierungsbeteiligung.[2]

Die Digitalisierung hat nicht nur unser Privatleben und unseren Arbeitsalltag fest im Griff, mit ihr durchläuft auch die Kriegsführung die nächste Stufe der Evolution. Für Politik und militärische Gewaltausübung sind die allgegenwärtige Vernetzung, unsere permanente Ansprechbarkeit, die Geschwindigkeit der Kommunikation und immer intelligenter werdende Maschinen lohnende Mittel einer Art *Soft War*. Sie erlauben, Druck auf Staaten und deren Bevölkerung – selbst bei so etablierten Mächten wie den USA – auszuüben und trotzdem das Risiko von Vergeltung und Eskalation zum heißen Krieg klein zu halten. Ganz ausschließen lässt es sich aber nicht, wie wir noch sehen werden. Denn die sogenannten asymmetrischen oder hybriden Bedrohungen, zu denen digitale Spionage, Sabotage und Subversion zählen, sind zum erschwinglichen Kriegsersatz geworden.[3] Und weil digitale Angriffe billiger kommen als ein heißer Krieg, nehmen immer mehr Staaten – auch die ökonomisch schwachen mit geringen Militärausgaben und schlecht ausgerüsteten Truppen sowie die neuen globalen Aufsteiger – eifrig daran teil und stören die internationale Ordnung und ihr früheres Gleichgewicht.

Deshalb werden für die Kriegsführung im 21. Jahrhundert Universaltechnologien wie künstliche Intelligenz für kognitive Maschi-

nen immer wichtiger. Einige Nationen haben klar erkannt: Digitale Technologien bringen nicht nur wirtschaftlichen Nutzen, sondern auch politische und militärische Überlegenheit. Wer geostrategische Einsatzkonzepte der Digitalisierung findet, wird im neuen Wettbewerb des Kräftemessens der Großmächte in Führung gehen.

Die Vereinigten Staaten, bisher unbestritten digitale Führungsmacht, sehen ihren einstigen Vorsprung rasch schmelzen und geben unfreiwillig Einfluss an kraftstrotzende Parvenüs, besonders China, ab. Der Rückzug Amerikas und die Vehemenz, mit der sich konkurrierende Mächte räumlich ausdehnen, haben ein neues, beängstigendes Wettrüsten eingeläutet, das sich nicht nur auf Datendiebstahl, Sabotage und Subversion beschränkt. Durch die Vernetzung von allem mit allem zum *Internet of Everything* erfasst das digitale Wettrüsten auch die physische Welt, die noch smarter werden wird als unsere Smartphones, smarten Häuser oder Autos: Kampfroboter, Drohnenschwärme, intelligente Implantate, vernetzte Nuklearwaffen und hypersonische Trägerplattformen intelligenter Munition, die ihre Ziele mit einer Überschallgeschwindigkeit von bis zu 33 000 Stundenkilometern innerhalb weniger Minuten erreichen.

Die Ausbreitung des *Internet of Everything* macht die Mittel des Krieges im 21. Jahrhundert unüberschaubar, weshalb ich mir erlaubt habe, eine thematische Auswahl zu treffen.

Kapitel 1 beginnt damit, dass Staaten digital spionieren und sabotieren. Die Frage nach ähnlichen Operationen, die nicht staatliche Akteure im eigenen Interesse ausführen – etwa Kriminelle oder Terroristen –, wird bewusst ausgeklammert, weil wir Folgendes reflektieren wollen: Ist das, was wir gedankenlos als »Cyberkrieg« bezeichnen, wirklich Krieg? Eine völkerrechtlich ausdrücklich geforderte Voraussetzung des Krieges ist zwischenstaatliches Handeln. Geht Gewalt indes von Privaten aus, wie es Freiheitskämpfer, Aufständische, Terroristen oder private Hacker ohne staatliches Mandat sind, ist die völkerrechtliche Voraussetzung im strikten Wortsinn nicht erfüllt.

Steter Begleiter der Machtkontrolle in Zeiten von Krieg und Frieden ist die Unterminierung des Vertrauens einer Bevölkerung in ihre Regierung. Meisterstück einer solchen Subversion waren die koordinierten Angriffe Moskaus auf den amerikanischen Präsidentschaftswahlkampf 2016, die vom amerikanischen Sonderermittler Robert Mueller akribisch nachvollzogen und beschrieben wurden. Möglich wurde die Subversion erst durch die Geschäftsmodelle von Facebook, Twitter und Co. Wie der Informationsraum des 21. Jahrhunderts die Gesellschaft spaltet und den Humus für den Aufstieg von Demagogen bildet, ist Gegenstand der Überlegungen in **Kapitel 2.**

Kapitel 3 verlässt die virtuelle Welt und begibt sich hinaus in die physische Realität tödlicher autonomer Waffensysteme. Nicht nur Deutschland will gemäß Koalitionsvertrag der 19. Legislaturperiode bis 2021 letale autonome Waffensysteme ächten, auch andere Staaten ringen um eine Regulierung der bedrohlichen neuen Waffen, die aus dem Nichts auftauchen, ihren *Kill Cycle* aktivieren und ohne menschliches Zutun töten können. Doch die Chancen für ein Verbot stehen schlecht, auch weil Deutschland nicht reglementieren will, was es laut eigener Feststellung noch gar nicht gibt: selbstbestimmte Waffen, deren kritische Funktionen dem Menschen ganz entzogen sind. Liegt die Lösung eines Verbots dann vielleicht nicht beim Recht, sondern in der Aufrüstung von Gegenmaßnahmen der elektronischen Kampfführung?

Wen ein digitaler Angriff trifft, der will am liebsten Rache nehmen.

»Wenn ich je einen Hacker zwischen die Finger bekomme, drehe ich ihm den Hals um«, höre ich von seriösen Programmierern, die immer wieder mit Zusatzarbeit als Folge digitaler Angriffe konfrontiert sind. Immer mehr Unternehmen wünschen sich daher, eigene Kompetenzen für das *Hacking Back* aufzubauen. Aber ist das Zurückhacken überhaupt erlaubt? Trifft die Vergeltung tatsächlich auch den wahren Angreifer oder vielleicht nur einen Unbescholtenen in einem alliierten Land, dessen Rechner für einen Angriff missbraucht wurde? Und wenn *Hacking Back* erlaubt sein soll, ist der Verteidiger

auch auf die Folgen einer Eskalation vorbereitet? Die Verteidigung gegen digitale Angriffe ist eine heikle politische Angelegenheit und kann ernstliche diplomatische Verwicklungen nach sich ziehen. Wie das Völkerrecht zur Verteidigung in digitalen Zeiten steht, erörtern wir in **Kapitel 4.**

Wenn einige Staaten erkannt haben, dass die Technologien der digitalen Ära auch Geopolitik unterstützen, werden sie ihre Technologiestrategie darauf abstimmen. **Kapitel 5** stellt fest, dass es Unterschiede zwischen dem Westen einerseits und China und Russland andererseits gibt, was Digitalstrategien angeht. Abhängig vom politischen System wird insbesondere die künstliche Intelligenz als Schlüsseltechnologie für das 21. Jahrhundert anders eingesetzt – hier für mehr wirtschaftliche Wettbewerbsfähigkeit, dort für die politische und militärische Kontrolle wirtschaftlich relevanter Ressourcen. Die Unterschiede beim Einsatz künstlicher Intelligenz sind das Ergebnis zweier ungleicher Systemalternativen, die erstmals aufeinanderprallen: der Neoliberalismus und der chinesische Traum von der Weltherrschaft.

Zwischen beiden Systemalternativen ist Europa herausgefordert. Was bedeutet das neue Großmachtstreben Asiens für unseren europäischen Erdteil? Das Amerika Donald Trumps will jedenfalls nicht mehr für die Sicherheit Europas eintreten. Der Kontinent ist somit stärker auf sich selbst gestellt – gegen den Druck und die Spaltungsbemühungen aus dem Osten von nah wie fern. Kann Europa eine eigene Weltpolitik formulieren und auch leben? Die neuen Technologien könnten dabei unterstützend wirken. Eine kleine Auswahl an Ideen dafür betrachtet **Kapitel 6.**

Als ich begann, mich mit digitalen Technologien im Kontext politischer Macht und militärischer Gewalt zu beschäftigen, traf ich zunächst auf ein scheinbar kapitales Denkhindernis. Wer die bessere Waffe hat, so der erste Reflex, der setzt sich politisch oder militärisch durch. Erst langsam erschlossen sich mir die politischen Feinheiten und die Bedeutsamkeit des außerordentlichen Umbaus der Weltord-

nung, der sich vor unseren Augen vollzieht. Atemberaubendes geschieht, will gesehen, gewusst und thematisiert werden. Technologie steht dabei nicht nur am Spielfeldrand – sie ist ein, wenn nicht der wichtigste, Schlüssel dafür, welche Ordnung unser digitales 21. Jahrhundert dominieren wird.

[EINS]

Code als Waffe

Moderne Kriege sind anders,
in manchen Fällen so sehr,
dass die alten NATO-Handbücher
auf den Müll gehören.

Judy Dempsey

»Der Angeklagte Marcus Hutchins alias Malwaretech hat sich wissentlich mit dem Angeklagten N. N. verschworen und mit diesem vereinbart, die folgende Straftat gegen die Vereinigten Staaten von Amerika zu begehen: innerhalb eines Jahres vorsätzlich Computerprogramme, -codes und -befehle auf zehn oder mehr geschützte Computer zu übertragen, um Schaden zu verursachen.«[1]

So lautet die Anklage des United States District Court, Eastern District of Wisconsin, Aktenzeichen 17-CR-124, gegen den 23-jährigen britischen Staatsangehörigen Marcus Hutchins, ein Blogger zum Thema Schadsoftware und Mitarbeiter der US-amerikanischen Firma Kryptos Logic.

Auf dem Heimweg von der Teilnahme an den beiden amerikanischen Hackerkonferenzen Black Hat Briefings und DEF CON im August 2017 wartet der junge Mann in der Lounge des Flughafens Las Vegas McCarran International gerade auf seinen Rückflug nach Großbritannien, als er festgenommen, aus dem Flughafen eskortiert und zur FBI-Außenstelle Las Vegas geschafft wird. Dort konfrontiert man ihn mit dem Vorwurf der Verschwörung: Er habe den Banktrojaner Kronos, der Zugangsdaten zu Bankkonten stiehlt, programmiert und für wenige Tausend US-Dollar verkauft.

Was sich in die juristisch-trockene Sprache der Anklageschrift kleidet, die selbst nur Behauptungen aufstellt, aber keine Beweise vorlegt, kann dem jugendlich wirkenden Programmierer bis zu 40 Jahre Freiheitsstrafe einbringen. Schon im Teenageralter soll er als Black-Hat-Hacker ohne ethische Standards im Auftrag Dritter tätig gewesen sein, dann aber um das Jahr 2013 zu den White-Hat-Hackern, den »guten« Hackern, gewechselt haben. Aber sicher ist man sich nicht.

Je nach Beobachter pikant, verstörend oder strategisch unklug an der Anklage der amerikanischen Justiz ist, dass es ausgerechnet Marcus Hutchins war, der erst im Mai 2017 einen »Notausschalter« im Programmcode der Erpressersoftware WannaCry gefunden und betätigt hatte. Rein zufällig sei das geschehen, sagen die einen. Nein, er kannte den *Kill Switch* nur, weil er die Erpressersoftware mitentwickelt habe, behauptet hingegen das amerikanische FBI. Monate später sollte sich herausstellen, dass Marcus Hutchins, der seine Unschuld beteuerte, die Wahrheit gesagt hatte.

»Es ist offiziell«, titelt das *Wall Street Journal* im Dezember 2017. »Nordkorea steckt hinter dem Cyberangriff mit WannaCry.«[2] Ein Staat und seine Hacker hatten zahlreiche andere Staaten angegriffen.

Doch den Vorwurf, er sei für den Banktrojaner Kronos verantwortlich, konnte Hutchins nicht entkräften. Im April 2019 bekannte er sich schuldig, die Schadsoftware programmiert und vertrieben zu haben. Immerhin: Die restlichen Anklagen wurden fallen gelassen.

Sicherheitslücken

»Uuups, Ihre Daten wurden verschlüsselt! Überweisen Sie den Gegenwert von 300 US-Dollar in Bitcoin an die folgende Adresse.«[3] Was folgt, ist ein langer Schwanz aus Ziffern und Buchstaben – und etliche getätigte Überweisungen an die Erpresser. Im Sturm hatte

sich die Erpressersoftware WannaCry seit dem frühen Morgen des 12. Mai 2017 auf dem ganzen Globus ausgebreitet und 99 Länder infiziert, darunter auch China und Russland, regelmäßig die ersten Verdächtigen, denen man die Urheberschaft von Hackerangriffen unterstellt. Die Schadsoftware nützt eine Sicherheitslücke im Microsoft-Betriebssystem aus, verschlüsselt wichtige Daten des infizierten Computers und gibt den Zugriff auf die Daten erst nach Zahlung eines Geldbetrags wieder frei.[4]

Lange war die betroffene Microsoft-Sicherheitslücke nur der US-amerikanischen Heimatschutzbehörde NSA bekannt. Nicht nur die NSA, auch andere westliche Sicherheitsbehörden sammeln Sicherheitslücken von Computerprogrammen – im Hackerjargon *Zero Days* genannt –, um bei Bedarf in jeden Rechner weltweit einbrechen zu können. Normalerweise sind Sicherheitslücken strikt geheim. Doch mit der Geheimhaltung war es schnell vorbei, als die NSA selbst Opfer eines Datenklaus wurde. Eine Hackergruppe mit dem Namen Shadow Brokers, die die NSA erfolgreich überrumpelt hatte, machte die gestohlene Information über die Microsoft-Sicherheitslücke im April 2017 im Internet öffentlich bekannt. Es dauerte nur wenige Tage, und WannaCry trat seinen Raubzug rund um die Erde an.

Von WannaCry geschädigt waren zunächst britische Krankenhäuser, dann auch das US-Logistikunternehmen FedEx, russische Banken, das russische Innen- und Gesundheitsministerium, die staatliche russische Eisenbahn und das zweitgrößte Mobilfunknetz Russlands. In Deutschland wurde schnell für jeden Bahnreisenden offenbar, dass auch die Bahn AG Opfer war, so prominent prangte auf Zugzielanzeigen deutscher Bahnhöfe die Erpresserbotschaft.

Microsoft zeigte sich besorgt, machte aber gleichzeitig sorglose und leichtsinnige Nutzer mitverantwortlich für den entstandenen Schaden. Denn außer der NSA war auch Microsoft selbst auf die Sicherheitslücke in seinen Betriebssystemen gestoßen – und hatte seinen Nutzern schon im März 2017 eine Softwarekorrektur geliefert, die die Lücke schließen sollte. Nur: Millionen Nutzer hatten ihre

Rechner nicht aktualisiert und blieben weiter angreifbar. Schlimmer noch, zahlreiche Behörden nutzen für kritische staatliche Infrastrukturen noch heute ein veraltetes, vom Softwarehersteller seit April 2014 nicht weiter gepflegtes Betriebssystem: Windows XP.

Der erpresserische Angriff vom Mai 2017 offenbart ein Dilemma. Es ist die Ratlosigkeit der öffentlichen Hand bei der Beschaffung von Softwaresystemen. Bei der Digitalisierung kritischer Infrastrukturen – Verkehr, Energie, Verteidigung, Gesundheit, Ernährung, Finanzmärkte oder die staatliche Verwaltung – stehen die Behörden vor der Frage: *Make or Buy?* Soll man die Software für den Betrieb von Panzern, Atomkraftwerken oder Krankenhäusern bei Google, Microsoft, Amazon, SAP & Co. einkaufen oder lieber selbst bauen? Die Fachwelt spricht hier von *Commercial off-the-Shelf*, also von kommerzieller Fertig-Software, kurz: COTS. Auf den ersten Blick ist der Kauf von der Stange immer billiger, weil niemand nachbauen will, was ein anderer längst erfunden hat. Aber es gibt eine große Einschränkung. Standardsoftware ist sehr unsicher. Sicherheitslücken werden schnell weltweit bekannt und auch ausgenutzt. Die Folgen von Cyberangriffen auf den Betrieb kritischer Infrastrukturen können verheerend sein, denn obligate Sicherheitsstandards gibt es bisher keine.[5]

Was die Sache zusätzlich erschwert: Oft ist für die Digitalisierung kritischer Infrastrukturen oder für Kriegsgerät eine Zulassung nötig, so etwas wie ein Pendant zum TÜV-Siegel. Normalerweise erfolgt eine solche Zertifizierung für eine im Detail spezifizierte Zielplattform, etwa ein Waffensystem, ein Messsystem oder ein Röntgengerät samt Software. Wird eine neue Softwareversion geladen, um die Zielplattform zu aktualisieren, entfallen genau aus diesem Grund häufig sowohl die Betriebserlaubnis als auch Garantien für andere Computerprogramme, die mit der früher zertifizierten Zielplattform integriert waren. Zeiten, in denen wir, die Konsumenten, aufgefordert werden, uns unablässig und in Echtzeit zu erneuern, sind deshalb schlechte Zeiten für den Betrieb kritischer Infrastrukturen des

Staates, die über eine Lebensdauer von 20 Jahren und länger verfügen. Bislang ist unklar, wie und ob der gordische Knoten lösbar ist, der durch den Konflikt zwischen zwei inkompatiblen Paradigmen entsteht: zwischen der geforderten und aus Sicherheitsgründen auch notwendigen Daueraktualisierung und der Langlebigkeit gemeinschaftlich genutzter Infrastrukturen.

Dennoch bleiben die Firma Microsoft und mit ihr viele Technologiegiganten dabei: Computersicherheit obliegt auch der Verantwortung des Nutzers, der (moralisch) verpflichtet sei, seine Rechner stets auf neuesten Stand zu bringen. Was die Haftung für einen sicheren Rechnerbetrieb betrifft, sehen die Hersteller also ihren Kunden gleichermaßen in der Pflicht – immerhin läge es in dessen Macht, seine betriebliche Sicherheit selbst zu beeinflussen. Dass aber insbesondere staatliche Nutzer ein zertifiziertes System nicht ohne Weiteres aktualisieren können, ignorieren die Anbieter, während ebendiese Nutzer nur allzu gerne vergessen, wie wartungsintensiv ihre digitalisierte Infrastruktur tatsächlich ist.

Dass Fragen rund um die Sicherheit digitalisierter Infrastrukturen nicht leichtfertig auf den Nutzer abgewälzt werden sollten, liegt darin begründet, dass Unternehmen wie Regierungen auf die digitalen Angebote Dritter dringend angewiesen sind. Millionen von Nutzern gebrauchen die Rechnerwolken von Technologiegiganten wie Amazon oder IBM. Ihre Sicherheit, ihre Verfahren, ihr Know-how hängen sämtlich davon ab, dass die Betreiber von Rechenzentren ihre Clouds gegen Hackerangriffe absichern. Das kann aber nie ganz gelingen. Jeder Softwarecode, auch der in Rechenzentren, hat Fehler oder Lücken, die sogenannten *Bugs*. Softwarefehler, die Zugriffe auf Rechner ermöglichen, sind Gold wert und werden, sofern sie noch nicht öffentlich bekannt sind und sich noch niemand auch nur einen Tag lang mit ihrer Korrektur beschäftigt hat (daher der Name *Zero Day*), mit bis zu sechsstelligen Dollarbeträgen gehandelt.

Microsoft erhebt aus diesem Grund nachvollziehbare Vorwürfe gegen die NSA. Der amerikanische Staat hortet Sicherheitslücken

kritischer Computerprogramme, kann sie aber selbst nicht geheim halten. In den Händen von Datendieben würden Sicherheitslücken so zu zerstörerischen Waffen, erklärt Brad Smith, Microsoft Chief Legal Officer, ja sogar zu Massenvernichtungswaffen. Dem stimmt auch Michael Rogers, der frühere NSA-Chef, zu. Computerwürmer und Virensoftware, so schlägt er vor, sollten dem Kriegsvölkerrecht unterliegen: »Cyberwaffen sind nur eine andere technische Möglichkeit, um in einigen Fällen dieselben Schäden hervorzurufen wie konventionelle Waffen.«[6]

»Der Diebstahl der Microsoft-Sicherheitslücke bei der NSA ist mit dem Diebstahl einiger Tomahawk-Raketen beim US-amerikanischen Militär vergleichbar«, schlussfolgert Brad Smith ähnlich entschieden.[7] »Der jüngste Angriff stellt ein völlig unbeabsichtigtes und höchst beunruhigendes Bündnis zwischen den beiden schwerwiegendsten Formen weltweiter Sicherheitsbedrohungen dar – den staatlichen Aktionen einerseits und kriminellem Vorgehen andererseits.«[8]

Zwei Wege zur Macht

Wenn im 21. Jahrhundert zur Waffe wird, was nicht zum klassischen Waffenarsenal früherer Jahrzehnte gehört, weil es sich um neue Technologien handelt, ist es Zeit zu reflektieren, wie sich die Natur des Krieges durch die Digitalisierung verändert und unser Verständnis von Krieg und Frieden fundamental infrage stellt.

Krieg gehört zur Grunderfahrung des Menschen und ist »so alt wie die dokumentierte Menschheitsgeschichte«[9]. Die Gründe militärischer Gewalt sind vielfältig. Aus Misstrauen oder der Angst vor eigener Machtlosigkeit streben die Stärksten, die Fittesten, nach Macht.[10] Neben dem Sozialdarwinismus sind es wirtschaftliche Zwänge, geografische Ansprüche, militärstrategische Überlegungen

oder technologische Entwicklungen, die das auslösen, was wir als »Krieg« bezeichnen, und zu einer sehr besonderen sozialen und auch rechtlichen Beziehung zwischen Menschen führen. Krieg gilt als fundamentales soziales System und als »prinzipielle strukturierende Kraft der Gesellschaft, um Wirtschaftssysteme, politische Ideologien und Rechtssysteme zu erhalten«[11].

Krieg, so formulierte einst der Generalmajor und Militärtheoretiker Carl von Clausewitz (1780–1831) zu Beginn des 19. Jahrhunderts, sei die »Fortsetzung von Politik mit anderen Mitteln«[12]. Nach geltendem Kriegsvölkerrecht erfolgt diese Fortsetzung von Politik durch Kriegserklärung eines Staates gegenüber einem anderen Staat. Damit ist Krieg rechtlich als zwischenstaatlicher Vorgang definiert. Im Fall eines solch interstaatlichen Konflikts spricht das Völkerrecht von einem internationalen bewaffneten Konflikt – eben einem bewaffneten Konflikt zwischen Nationen.

Politik und Krieg sind ein ungleiches Paar, ein Entweder-oder, das dennoch unzertrennlich zu sein scheint. Beide nehmen Einfluss auf den Willen von Menschen,[13] und beide verfolgen denselben Zweck: Menschen zu einem gewünschten Verhalten zu bewegen. Doch die Methoden unterscheiden sich grundlegend: Der Krieg arbeitet mit Instrumenten militärischer Gewalt, die Politik mit schierer Überzeugungskraft.

Tatsächlich bestätigen Veteranen die klare Unterscheidbarkeit von Krieg und Politik. Der Unterschied, versichern sie, läge in der Wahl der Mittel, sodass Krieg nicht einfach Politik unter einem anderen Namen sei.[14] Ein Messer an der Kehle zu spüren habe eben eine ganz andere Überzeugungskraft als eine politische Debatte zur Meinungsbildung. Denn wenn der Krieg auch keine rechtsfreie Zone ist, weil die Grundsätze der Humanität immer zu beachten sind (und dennoch so oft mit Füßen getreten werden), gilt im Krieg faktisch das Recht des Stärkeren, das kein Leben schont. Ein Kombattant darf einen anderen Kombattanten straflos töten, denn eine Sanktion für eine solche Tötung ist nicht vorgesehen.

In Zeiten politischer Machtausübung gelten andere Regeln, und die Tötung eines anderen Menschen ist immer strafbewehrt. Doch die Androhung rechtlicher Sanktionen bedeutet keinen Zwang zur Unterordnung wie während eines kriegerischen Konflikts. Vielmehr garantieren die normativen Systeme politischer Herrschaft den so Beherrschten Freiheit, weil sich jeder aus freien Stücken entscheiden kann, ob er geltende Normen befolgen oder lieber dagegen verstoßen will. Worauf Politik hofft, ist also die Freiwilligkeit der Unterordnung der Beherrschten. Daher kann sie auf physischen Zwang verzichten. Deshalb trennt auch Hannah Arendt, die große politische Theoretikerin des 20. Jahrhunderts, säuberlich zwischen (politischer) Macht und (militärischer) Gewalt: »Macht und Gewalt sind Gegensätze: wo die eine absolut herrscht, ist die andere nicht vorhanden.«[15] Dieser Dichotomie, die sich prinzipiell auf den Vers aus Goethes Erlkönig reduzieren lässt – »Und bist du nicht willig, so brauch' ich Gewalt« –, hängen im Kern auch heute noch zahlreiche Politiker und Militärstrategen an.

Weil es aber auch in der Politik nicht bei einem einmal erreichten Zustand bleibt, weil »gesamtheitliches Wollen nicht ein für alle Male im Voraus hergestellt und gegeben ist, (…) die Macht sorgfältig erst zu bilden und immer wieder neu zu gliedern ist, (…) rein mechanisch laufende Staatstätigkeit überhaupt erst ausgeschlossen ist«[16], muss auch die Politik Macht immer wieder neu gewinnen und legitimieren. Wo der politische Prozess von Überzeugung und Normgebung nicht zum Erfolg führt, haben nicht wenige Machthaber beide Wege beschritten und zur politischen Machterlangung nicht allein auf ihre Überzeugungskraft, sondern auch auf die technischen Werkzeuge militärischer Gewaltausübung gesetzt, wie es Mao Zedong zynisch auf den Punkt bringt: »Macht entspringt einem Fass Schießpulver.«[17] »Alle Politik ist ein Kampf um die Macht, und die ultimative Machtausübung ist die [militärische] Gewalt«, räumt deshalb auch der Soziologe C. Wright Mills völlig zutreffend ein.[18]

Dem Frieden verpflichtet

Mit Friedensverträgen werden Kriege wieder beendet. Frieden, so die Auffassung der Militärtheoretiker, ist die Beendigung eines Krieges und damit ein Endzustand, den es zu erreichen gilt. Frieden und Krieg stünden im Wechsel zueinander; sie bildeten einen Zyklus, bei dem auf einen Krieg der Frieden folge und auf den Frieden der Krieg, auch wenn die Zyklen von hoher zeitlicher Unregelmäßigkeit zeugten.

Nach unserem europäischen Verständnis ist der Frieden ein Wert, den es zu erhalten und zu vertiefen gilt, damit gesellschaftlicher Fortschritt möglich wird. Frieden, so glauben wir Europäer, müsse zu immer tieferem Frieden führen. Frieden in Europa ist die politische Idee der Europäischen Union, wofür sie 2012 mit dem Friedensnobelpreis ausgezeichnet wurde.

Heute, wenige Jahre später und nach Konflikten wie in Syrien, im Jemen oder mit dem Islamischen Staat scheint offenkundig, dass die Idee, Frieden müsse immer weiter vertieft werden, wohl eine sehr europäische Vorstellung ist. Insofern ist die Ablehnung militärischer Gewalt auch eine kulturell geprägte, ethnozentrische Sicht auf die Kriegsführung. Denn für andere Kulturen gilt keineswegs, wozu sich Europa so sehr verpflichtet fühlt. Das hat der Außenminister des 3. Kabinetts von Angela Merkel, Sigmar Gabriel, bei seiner Rede anlässlich der 54. Münchner Sicherheitskonferenz 2018 so ausgedrückt: »Als einziger Vegetarier werden wir es in der Welt der Fleischfresser verdammt schwer haben.«[19]

Dabei sei Frieden dauerhaft zu stiften, wenn man nur die Grundsätze der Vernunft befolge, meinte schon Immanuel Kant in seiner Schrift *Zum ewigen Frieden* aus dem Jahr 1795. Tatsächlich strahlt Kants Schrift bis in das 21. Jahrhundert hinein, weil sie der Charta der Vereinten Nationen, die sich für ein ganz ausdrückliches Gewaltverbot ausspricht, zugrunde gelegt ist.

Auf ebenjene Karte der Vernunft haben die Vereinigten Staaten

nach Ende des Zweiten Weltkriegs gesetzt: dass der Krieg nicht neben dem Handel bestehen kann. Oder anders gesagt: Wer kauft, schießt nicht. Ungeachtet der Kosten und Investitionen in Billionenhöhe hatten sich die Amerikaner bereit erklärt, in die Rolle der globalen Ordnungsmacht zu schlüpfen. Sie wollten »sicherstellen, dass der Welthandel blühte und die Vereinigten Staaten nicht erneut in große regionale zwischenstaatliche Konflikte wie die beiden Weltkriege hineingezogen werden würden«[20], auch wenn das nicht immer zum wirtschaftlichen Vorteil der Vereinigten Staaten gereichte.

Die Vorstellung, dass Kriegszustände enden und dem Frieden weichen, beseelt die meisten Menschen noch heute. Wenn die Gewalt endet und Frieden herrscht, so die Hoffnung, kann sich politische Macht entfalten. Nur hat schon Hannah Arendt richtig festgestellt: Auf den Zweiten Weltkrieg folgten der Kalte Krieg mit seiner Politik von Wettrüsten und Abschreckung und die Schaffung des militärisch-industriellen Komplexes in den Vereinigten Staaten.[21] Wer von Arendt inspiriert weiterdenkt, muss konstatieren: Auf den Kalten Krieg, in dem die atomaren Waffen schwiegen, folgte der Krieg gegen den Terror und jetzt der »Cyberkrieg«. Dann wäre der Zustand, mit dem wir täglich leben, kein vollkommener Frieden, sondern ein täglich bedrohtes Stillhalten, das sich nie ganz sicher sein kann vor einer Eskalation. Dann sind wir zwar nicht unmittelbar physischer Gewalt ausgesetzt, aber leben mit dem ständigen Gefühl einer diffusen Bedrohung und der Möglichkeit, die Gewalt könnte sich eines Tages unerwartet körperlich manifestieren und jeden von uns treffen. Dann wären Macht und Gewalt, Frieden und Krieg doch nicht trennscharf gegeneinander abgrenzbar. Stattdessen lebten wir in einem diffusen Dauerzustand zwischen beiden Situationen – eben im Kontinuum einer hybriden Lage.

Der Gedanke, dass an die Stelle eines Dualismus von Krieg und Frieden ein kontinuierlicher Vorgang ohne klare Abgrenzung zwischen verschiedenen Zuständen, zwischen Beginn und Ende, Freund und Feind, Kombattant und Nichtkombattant, getreten sein könnte,

ist besonders für die Deutschen und ihre europäischen Nachbarn nicht leicht fassbar. Sie haben die bittere Erfahrung gemacht, dass Krieg in keinem Fall zum Ziel führt. Gewalt erzeugt Gegengewalt; und Krieg produziert unermessliche Kosten und unsagbares Leid. Vor allem die Generation der 1968er lehnte sich gegen den Krieg auf. Für die Folgen der Rebellion dürfen wir noch heute dankbar sein: Die Bürgerrechte, die Demokratie und der Rechtsstaat blühten auf, genauso wie die Wirtschaft und die Innovationskraft in der westlichen Welt.

Tiefere globale Verbundenheit, Technologien ganz zum Wohle der Menschheit, eine bessere Gesundheit, ein längeres Leben und vor allem mehr Demokratie und Frieden, der Kriege durch einträchtigen Welthandel zwischen den Nationen vollends ersetzen werde, lauteten auch die Versprechen von Kaliforniens Technologieelite.[22] Heute würde ihr wohl niemand mehr glauben. Tatsächlich leitet jede technologische Ära ihre ganz eigene waffentechnische Entwicklung und damit auch Form der Kriegsführung ein.[23] Der Erste Weltkrieg wurde industriell geführt, im Zweiten Weltkrieg jubelte Deutschland über den Propagandakrieg des Josef Goebbels in den ersten Radios, und seit der Aufrüstung mit Nuklearwaffen im Kalten Krieg droht der Untergang der ganzen Menschheit, kämen sie zum Einsatz.

Dass die Digitalisierung Angriffe auf demokratische Staaten erst zulässt, ist inzwischen eindrucksvoll bewiesen. Noch stehen wir am Anfang der digitalen Ära und verstehen nicht vollständig, welche Formen der sozialen Organisation sie noch für uns bereithält, wenn unbestimmte Gegner, heimlich oder offen, anonym oder erkennbar, unser Leben, unsere Wirtschaft oder Regierungen infizieren, manipulieren oder beschädigen. Auch wenn wir die Chancen der Digitalisierung nicht vertun möchten: Ein Unbehagen bleibt.