Thomas Rid
Mythos Cyberwar

THOMAS RID

MYTHOS CYBERWAR

Über digitale Spionage, Sabotage und andere Gefahren

Aus dem Englischen
von Bettina Engels und Michael Adrian

Edition Körber

Die englische Originalausgabe erschien 2013 unter dem Titel »Cyber War Will Not Take Place« bei Oxford University Press/Hurst, London sowie 2017 bei C. Hurst & Co. Publishers Ltd., London UK, 2017

Bibliografische Information der Deutschen Nationalbibliothek

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet unter http://dnb.d-nb.de abrufbar.

Umschlag: Groothuis. www.groothuis.de
Cover: iStockphoto.com/MATJAZ SLANIC
Herstellung: Das Herstellungsbüro, Hamburg|
www.buch-herstellungsbuero.de
Druck und Bindung: CPI – Clausen & Bosse, Leck
Printed in Germany

ISBN 978-3-89684-260-2

www.edition-koerber.de

Inhalt

Vorwort

Es ist zu einer beliebten Phantasie geworden, dass uns ein Cyberkrieg droht. Hollywood hat derlei Befürchtungen bereitwillig aufgegriffen und für uns bebildert. Filme wie *Kriegsspiele*[1] oder, etwas aktueller, *Stirb langsam 4.0*[2] wandeln dabei auf vorhersehbaren erzählerischen Pfaden: Finstere Mächte mobilisieren geheime und komplexe Computernetzwerke, um die Welt ins Chaos zu stürzen, ganze Nationen in Geiselhaft zu nehmen und durch einen Einbruch in die gewaltigen und mächtigen Computersysteme des Pentagons einen Atomkrieg auszulösen. Solche Ängste haben immer einen Nerv getroffen. So war auch HAL, Stanley Kubricks alles kontrollierende Maschine an Bord eines Raumschiffs in seinem Film *2001 – Odyssee im Weltraum*[3] aus dem Jahr 1968, eine eindringliche Verkörperung der tief sitzenden menschlichen Angst, die Kontrolle an die Technik zu verlieren. In Zeiten, in denen immer mehr Menschen und Dinge online gehen, greifen solche Befürchtungen stärker um sich denn je.

Die meisten Menschen, ob jung oder alt, arbeiten mit Computern, ohne das Zusammenspiel von Hardware und Software wirklich zu verstehen. Sehr viele tragen ihr Smartphone permanent bei sich. Und sehr viele sind geradezu süchtig nach Vernetzung und checken, wo sie gehen und stehen, ihre E-Mails oder Nachrichten-Feeds aus den Sozialen Netzwerken. Eine ganze Generation ist in dem Glauben aufgewachsen, ihr persönliches und berufliches Glück hänge von digitalen Geräten und permanenter Erreichbarkeit ab. Wer auf seinem Touchscreen herumfingert,

noch bevor der Frühstückskaffee fertig ist, wird intuitiv verstehen, dass praktisch alles, was der Tag noch bringen kann, computergesteuert ist: das Wasser aus der Leitung, die Kaffeemaschine, versorgt mit Strom aus dem Kraftwerk, die Ampelschaltung im Straßenverkehr und die S-Bahn, mit der er oder sie zur Arbeit fährt, der Geldautomat, an dem sie Geld holt, der Aufzug, der sie in ihr Büro transportiert, das Flugzeug, das sie nach Berlin oder Neu-Delhi oder New York bringt, das Navigationssystem, das ihr in einer unbekannteren Stadt den Weg weist, und vieles andere mehr. All diese Lebensbegleiter sind mittlerweile alltäglich und unscheinbar geworden – solange sie funktionieren. Genauso alltäglich und allgegenwärtig ist die perfide Angst, dass hinterhältige Bösewichter permanent darauf lauern, in diese Computer und ihre gesamte Software einzudringen und sie zu zerstören, um so ganze Gesellschaften in die Knie zu zwingen: Kein Wasser wird mehr fließen, die Lichter werden verlöschen, Züge entgleisen, Banken unsere Finanzdaten verlieren, Chaos wird auf den Straßen ausbrechen, und Flugzeuge werden vom Himmel fallen. Niemand, so die Devise, ist vor dem kommenden Cyberkrieg sicher, unser digitaler Untergang nur eine Frage der Zeit.

Diese Ängste führen uns in die Irre. Sie lenken uns von der wirklichen Bedeutung des Themas Cybersicherheit ab: Vieles spricht dafür, dass Cyberangriffe keine neuen Schneisen für gewaltsame Auseinandersetzungen schlagen, sondern vielmehr das Gewaltniveau ehemals gewaltsamer Konflikte absenken. Erst im 21. Jahrhundert wurde es Streitkräften möglich, Radarstationen und Raketenwerfer lahmzulegen, ohne das Luftabwehrsystem eines Gegners bombardieren und dabei Bedienmannschaften und womöglich Zivilisten töten zu müssen. Heute lässt sich das durch einen Cyberangriff bewerkstelligen. Erst im 21. Jahrhundert sahen sich Geheimdienste in der Lage, gewaltige Mengen an Geheiminformationen durch Computerhacks herauszufiltern und herunterzuladen, ohne Spione an gefährliche Orte zu entsenden,

wo diese erst einmal Informanten bestechen, erpressen und gegebenenfalls schädigen müssten. Erst seit dem 21. Jahrhundert können Rebellen und Widerstandskämpfer mit gewaltlosen Mitteln den staatlichen Machtanspruch untergraben, indem sie Anhänger und Sympathisanten online mobilisieren und zu Tausenden auf die Straße bringen.

Der weltweite Vormarsch vernetzter Computer verändert das Geschäft von Soldaten, Spionen und Subversiven. Der Cyberspace erzeugt neue – und oft nicht gewaltsame – Handlungsoptionen. Aber auch diese neuen Optionen stoßen auf je eigene Beschränkungen und Schwierigkeiten, die wiederum alle gleichermaßen betreffen, ob sie sich vor neuen Angriffsmöglichkeiten zu schützen versuchen oder die neuen Technologien offensiv für ihre Ziele nutzen wollen. Das vorliegende Buch lotet die Möglichkeiten und Grenzen politisch motivierter Gewalt im Cyberspace aus, mag diese im Namen eines Staates erfolgen oder nicht.

Die zunehmende Häufigkeit technisch raffinierter Computerhacks birgt zweifellos erhebliche Risiken und Gefahren, und so ist es ganz entscheidend, diese Risiken und Gefahren richtig zu verstehen und adäquat zu beantworten, damit sie sich entschärfen lassen. Aus diesem Grund sei hier ein kurzes Wort zur neueren Debatte über Cybersicherheit erlaubt: Denn sie ist unzulänglich und vielerorts von unterirdischer Qualität. Die allgemeine Diskussion findet in Technologie-Fachblättern, Zeitschriften und spezialisierten Netzforen, aber natürlich auch in den Massenmedien, der Wissenschaft, in Blogs und Mikroblogs statt. Sie wird auf unzähligen Workshops und Konferenzen geführt, zu denen Vertreter der Privatwirtschaft, des Staates, der Nachrichtendienste und des Militärs sowie Hacker und Wissenschaftler aus vielen wissenschaftlichen Disziplinen zusammenkommen. Sie erfolgt sowohl öffentlich als auch hinter verschlossenen Türen oder gar unter strengster Geheimhaltung. Zweifellos produziert eine Reihe ausgewiesener Experten regelmäßig hoch qualifizierte Forschungs-

ergebnisse zum Thema Cybersicherheit; ohne deren solide Arbeit hätte dieses Buch gar nicht geschrieben werden können. Doch je weiter man in politische oder militärische Kreise, in Denkfabriken, Parlamente, Ministerien und Militärakademien vordringt, desto rarer scheinen sich echte Spezialisten zu machen und desto schriller wird der Ton. Die Naivität der strategischen Debatte erweist sich am Aufkommen eines merkwürdigen Jargons, der sich nicht zuletzt in der von politischen Bescheidwissern und nicht wenigen Uniformträgern geradezu inflationär gebrauchten substantivierten Form des Wortes »cyber« ausdrückt und ungefähr so klingt: »Ich interessiere mich für Cyber« oder »Wie definiert man Cyber?« – eine Frage, die mir ein Beamter allen Ernstes stellte, unmittelbar nachdem ich bei einer Präsentation vor beiden Kammern des britischen Parlaments empfohlen hatte, dieses trendige, aber leere Schlagwort *nicht* substantivisch zu gebrauchen. Weder Informatiker, Programmierer oder Experten für Softwaresicherheit noch Technikjournalisten oder seriöse Wissenschaftler verwenden »Cyber« normalerweise als Substantiv. Überhaupt habe ich im Lauf der Jahre ein extremes Misstrauen gegenüber »Substantivierern« entwickelt, die oft kaum einen Gedanken an die erforderlichen technischen Details zu verschwenden scheinen – ein Phänomen, das sich in Washington ebenso beobachten lässt wie in London, Paris, Berlin und anderswo. Umso wichtiger ist es, die Qualität der Debatte zu beflügeln. Die Öffentlichkeit hat eine informiertere, differenziertere und realistischere Diskussion verdient als die bisher geführte. Und sie verdient auch besser durchdachte und umgesetzte Richtlinien und Gesetze zur Cybersicherheit.

Mythos Cyberwar wurde in dem Bestreben geschrieben, der Leserschaft einen fundierten und dennoch verständlichen Beitrag zu dieser Debatte an die Hand zu geben, in dem Versuch, die Diskussion zu vertiefen, den Hype herunterzukochen und angemessen auf einige der drängendsten Sicherheitsfragen einzugehen.

Das Buch soll Studenten, Analysten und Journalisten als Quelle dienen. Die Diskussionen und Seminare über Cybersicherheit finden in verschiedenen akademischen Fachrichtungen statt, von denen Politikwissenschaft und Informatik an erster Stelle stehen, gefolgt von Rechtswissenschaft und Soziologie. Ich hoffe, dass all die unterschiedlichen Rezipienten dieses Buch aufschlussreich finden werden: Ingenieurinnen, Computercracks und Technikfreaks profitieren vielleicht von der strategischen Vogelperspektive, Politexpertinnen und Soziologen ziehen womöglich einen Nutzen aus den verständlich dargestellten technischen Details, und Studierende all dieser Disziplinen wissen vielleicht beides zu schätzen. Als einzelner Autor kann man sich allerdings nicht der Illusion hingeben, das gesamte Spektrum der Cybersicherheit abzudecken, wie die lange Liste von Danksagungen deutlich macht. Um der besseren Zugänglichkeit willen sind die neun Kapitel dieses Buches als eigenständige Essays angelegt, von denen jeder mit je eigenen Fragen, Argumenten und Mikro-Fallstudien aufwartet.

Eine Bemerkung noch zu den hier verwendeten Quellen. Die anregendsten Debatten um die jüngsten Entwicklungen im Bereich der Cybersicherheit spielen sich nicht in wissenschaftlichen Zeitschriften ab, sondern in zahlreichen Technologie-Blogs und auf Websites, die man nicht als Blog bezeichnen kann. Auch von den wichtigsten längeren Studien und Berichten sind viele nicht in Zeitschriften erschienen, die sich nach akademischen Konventionen zitieren lassen, sondern auf Websites von Unternehmen oder manchmal von Einzelpersonen. Andere Artikel, die womöglich schwieriger aufzutreiben sind, zitiere ich mit einer URL. Weil aber viele URLs so aufgebläht und oft kurzlebig sind, habe ich beschlossen, stattdessen einen bitly.com-Link mit Statistiken zur Verfügung zu stellen[4], der dem Leser den vollständigen Link, das Datum seiner ersten Verwendung und weitere Nutzerstatistiken bietet – selbst wenn dieser Link abgelaufen ist.

Das Argument

Über den tragischen Sommer 1914, in dem Europa seinen politischen Absturz in den Ersten Weltkrieg erlebte, schrieb der französische Dramatiker Jean Giraudoux Mitte der dreißiger Jahre sein berühmtes Theaterstück *La guerre de Troie n'aura pas lieu (Kein Krieg in Troja)*.[5] Die Handlung des Zweiakters spielt innerhalb der Stadtmauern Trojas. Hektor, ein enttäuschter trojanischer Feldherr, bemüht sich vergeblich, den Krieg mit den Griechen, wie ihn die Seherin Kassandra prophezeit hat, abzuwenden. Giraudoux, Veteran des Ersten Weltkriegs, war im französischen Außenministerium am Quai d'Orsay tätig. Seine Tragödie ist eine eloquente Kritik an den europäischen Politikern, Diplomaten und Intellektuellen, die damals gerade wieder dabei waren, die Höllenhunde des Krieges zu entfesseln. Im November 1935 hatte das Stück am Théâtre de l'Athénée in Paris Premiere, fast genau vier Jahre bevor sich die unheilvollen Ahnungen des Dramatikers bewahrheiten sollten.

Wenn man den jüngeren Einlassungen zum Thema Cyberkrieg Glauben schenken möchte, dann ist die Welt heute wieder an einem ähnlichen Punkt angelangt wie 1935. »Der Cyberkrieg wird kommen!«, erklärten John Arquilla und David Ronfeldt von der Denkfabrik RAND (»Research and Development«) Corporation im Jahr 1993.[6] Das Establishment brauchte eine Weile, um ihren Gedanken aufzugreifen. »Der Cyberspace ist ein Bereich, in dem die Air Force fliegt und kämpft«, verkündete Michael Wynne, Staatssekretär und ziviler Leiter des amerikanischen Luftwaffenamts, 2006. Vier Jahre später blies die Pentagon-Führung ins gleiche Horn. »Auch wenn der Cyberspace ein vom Menschen erschaffener Bereich ist«, schrieb der amerikanische Vize-Verteidigungsminister William Lynn 2010 in einem Artikel für *Foreign Affairs*, »ist er für militärische Operationen mittlerweile von ebenso großer Bedeutung wie Land, Meer, Luft und Weltraum.«[7] Richard Clarke, der ehemalige Cybersicherheitspapst im Weißen Haus, malte Ka-

tastrophen an die Wand, die »9/11« wie ein Kinderspiel aussehen lassen würden, und forderte »sechs einfache Maßnahmen, die wir jetzt ergreifen müssen, um eine Katastrophe im Cyberkrieg zu verhindern«.[8] Im Februar 2011 warnte der damalige CIA-Direktor Leon Panetta den für die Aufsicht der Geheimdienste zuständigen Ausschuss des Repräsentantenhauses, das United States House Permanent Select Committee on Intelligence: »Das nächste Pearl Harbor könnte durchaus ein Cyberangriff sein.«[9] Als Pentagon-Chef wiederholte Panetta später seine düstere Warnung. Ende des Jahres 2012 orakelte Mike McConnell, bis 2009 George W. Bushs Direktor der nationalen Nachrichtendienste, Amerika könne es sich nicht leisten, »auf die Cyber-Parallele zum Einsturz des World Trade Centers zu warten«.[10] Doch während amerikanische Politiker laut vor dem digitalen Untergang warnten, waren Amerikas Geheimagenten gerade damit beschäftigt, einen hochraffinierten, später als »Stuxnet« bekannt gewordenen Computerwurm freizusetzen, der das iranische Programm zur Atomanreicherung in Natanz zerstören sollte. Ein weithin beachteter investigativer Artikel in *Vanity Fair* kam zu dem Schluss, das Ereignis sei ein Vorgeschmack auf die destruktive neue Gestalt der Kriegsführung im 21. Jahrhundert: »Stuxnet ist das Hiroshima des Cyberkriegs.«[11]

Aber stimmt das eigentlich? Stehen die Kassandras auf der richtigen Seite der Geschichte? Konfrontieren uns Cyberkonflikte tatsächlich mit einem »fünften Bereich« der Kriegsführung? Steht uns wirklich ein Cyberkrieg bevor?

Dieses Buch vertritt die Position, dass mitnichten ein Cyberkrieg stattfinden wird – und beabsichtigt damit auch keine Anspielung auf den ironischen Beiklang Giraudoux'. *Mythos Cyberwar* ist vielmehr als Kommentar über die Vergangenheit, die Gegenwart und die absehbare Zukunft zu lesen: Es hat in der Vergangenheit keinen Cyberkrieg gegeben, es findet gegenwärtig keiner statt, und es ist überaus wahrscheinlich, dass auch in Zukunft keiner über uns hereinbrechen wird. Vielmehr geschieht das genaue Gegen-

teil: eine durch Computer ermöglichte Offensive gegen die Gewalt an sich. Denn alle bisherigen und aktuellen politischen Cyberattacken sind – im Gegensatz zur Computerkriminalität – raffinierte Versionen dreier Tätigkeiten, die so alt sind wie die menschlichen Konflikte selbst: Sabotage, Spionage und Subversion. Bei näherer Betrachtung sind Cyberangriffe sogar eher ein Mittel zur Eindämmung als zur Eskalation politischer Gewalt, und zwar aus dreierlei Gründen. Zum einen ermöglichen auf der hoch entwickelten technischen Seite ein als Waffe eingesetzter Programmcode sowie komplexe *Sabotage*operationen extrem präzise Angriffe auf die Funktionsfähigkeit technischer Systeme des Gegners, ohne dass die diese Systeme bedienenden und kontrollierenden Menschen dabei *unmittelbar* körperlich zu Schaden kämen. Noch wahrscheinlicher aber sind Szenarien einer codebasierten Sabotage, die mit hohen finanziellen Verlusten einhergehen und extrem imageschädigend sind, auch wenn dabei keinerlei Hardware zu Schaden kommt. Zum anderen wandelt sich die *Spionage*: Durch Computerangriffe lassen sich Daten herausschleusen, ohne zuvor Menschen einschleusen, also durch hochriskante Operationen in Gefahr bringen zu müssen. Paradoxerweise verhält es sich aber so, dass die Geheimdienste umso weniger Cyberspionage im engeren Sinne betreiben, je fähiger sie in diesem Bereich werden. Und schließlich die *Subversion*: Vernetzte Computer und Smartphones machen es möglich, Anhänger friedlich für politische Ziele zu mobilisieren. Die Untergrabung der Legitimität einer herrschenden Ordnung, mithin des kollektiven Vertrauens in diese Ordnung, bedarf also unter Umständen vor allem dann weniger gewaltsamer Mittel als zu früheren Zeiten, wenn der Staat kein Monopol über die Kommunikationsmittel mehr besitzt. Dies gilt insbesondere für die Frühphasen von Unruhen.

Doch angriffslustige Technikenthusiasten sollten sich nicht zu früh freuen. Denn dieser Wandel im Charakter der politischen Gewalt schränkt nämlich seinerseits die Möglichkeiten ein. Und

diese begrenzten Möglichkeiten vermindern die Nützlichkeit von Cyberattacken in hohem Maße. Der klassische Einsatz organisierter Gewalt und die Gefährdung eines speziell für diesen Zweck ausgebildeten Personals bringen einzigartige Vorteile mit sich, die sich im Cyberspace, wenn überhaupt, nur schwerlich replizieren lassen. Diese Beschränkungen gelten wiederum für alle drei Formen der politischen Gewalt auf unterschiedliche Weise. Für die Aktivisten der Subversion bedeuten die neuen Formen der Online-Organisation und -Mobilisierung zunächst einmal auch eine größere Mobilität der Mitglieder, eine stärkere Abhängigkeit von Zielen und einen geringeren Einfluss der Anführer, die einst vielleicht noch persönlich inneren Zusammenhalt und Disziplin erzwingen konnten. Eine Bewegung in Gang zu setzen, ist heutzutage weit einfacher geworden, mit ihr Erfolge einzufahren hingegen schwieriger. Reine Cyberspionage ohne menschliche Informanten stellt zudem diejenigen, die anschließend die Daten in einen Zusammenhang bringen, also geheimdienstliche Erkenntnisse interpretieren, bewerten und in politische (oder kommerzielle) Vorteile ummünzen sollen, vor völlig neue Probleme. Es ist mit anderen Worten zwar einfacher geworden, an bestimmte Daten heranzukommen, nicht aber, diese Daten auch zu nutzen. Und schließlich ist auf technischer Seite die Herausforderung immens, Cyberwaffen für übergeordnete politische Ziele und nicht nur für einmalige, nicht wiederholbare Sabotageakte einzusetzen, die eher etwas für Computernerds mit Tunnelblick sind als für Staatenlenker mit politischer Weitsicht.

Die Argumentation des Buches wird in den ersten sieben Kapiteln entfaltet. Das erste Kapitel umreißt, was ein Cyberkrieg ist – oder vielmehr, was ein Cyberkrieg wäre, wenn er denn tatsächlich stattfände. Jede Erörterung dieser Frage muss an der Begrifflichkeit ansetzen. Ein Akt des Angriffs muss bestimmten Kriterien genügen, um als kriegerische Handlung gelten zu können: Er muss instrumentell, also ein Mittel zum Zweck sein; er muss

politisch und vor allem potentiell gewaltsam sein. Im zweiten Kapitel wird untersucht, wie sich im Zusammenhang mit Cyberattacken das Verständnis von Gewalt verändert. Das dritte Kapitel ist der zunehmend beliebten Idee der »Cyberwaffen« gewidmet und reflektiert das Potential und die Grenzen von Schadsoftware. Anschließend widmet sich das Buch einzelnen häufig zitierten Beispielen für politische Offensiv- oder Gewaltakte im Cyberspace. Das vierte Kapitel thematisiert die *Sabotage*. Bis heute hat es auf der ganzen Welt noch keinen einzigen nennenswerten physisch zerstörerischen Angriff auf hochsensible und schlecht gesicherte industrielle Kontrollsysteme – etwa von Kraftwerken, des Stromnetzes oder anderer elementarer Bestandteile der Infrastruktur – gegeben; hier wird eine mögliche Erklärung für dieses auffällige (und vielleicht ja nur vorübergehende) Ausbleiben vorgeschlagen und das wahre Risiko eines zukünftigen (alles lahmlegenden) Großangriffs auf die Infrastruktur einer Industriegesellschaft abgeschätzt. Das fünfte Kapitel nimmt *Spionage* im Sinne von Attacken auf Computernetzwerke unter die Lupe. Die Cyberspionage stellt in vielerlei Hinsicht eine Paradoxie dar: Sie findet fast immer in Form eines – natürlich unblutigen – Einbruchs in ein Netzwerk statt, der für entwickelte Nationen zugleich die grundsätzlichste und potentiell umwälzendste Bedrohung darstellt, allerdings zumeist aus ökonomischen Gründen und nicht im engeren Sinne aus Gründen der nationalen Sicherheit. Im sechsten Kapitel geht es um die vielleicht am weitesten verbreitete Form von politischer Gewalt im Cyberspace, die *Subversion*. Eines seiner Zwischenergebnisse lautet, dass die Einstiegskosten für subversive Aktivitäten zwar durch Technologie gesunken, die Hürden für ihren nachhaltigen Erfolg dagegen aber höher geworden sind. Das siebte Kapitel bewertet das Problem der *Attribution*, also der Rückverfolgung oder Zuordnung eines Angriffs als dem Dreh- und Angelpunkt der Cybersicherheit. Wenn man die Attribution endlich als ein politisches und nicht so sehr als ein technisches Problem

begreift, dann versteht man auch, dass dieses Problem selbst eine Funktion der Schwere des Angriffs ist. Das Schlusskapitel bietet eine Zusammenfassung und eröffnet die Aussicht auf eine Fortsetzung der Debatte jenseits der allzu strapazierten Metapher des »Cyberkriegs«.[12]

1. Was ist ein Cyberkrieg?

Der prägnanteste und grundlegendste Begriff vom Krieg findet sich immer noch bei Carl von Clausewitz. Sunzi aber, der wesentlich ältere Strategietheoretiker, geisterte in den 1990er Jahren dennoch häufiger durch die Debatten um Informationskriege, obwohl der chinesische General und Philosoph eher mit griffigen Aphorismen als mit systematischen Theorien aufwartet – weite Teile seines Buchs *Die Kunst des Krieges* aus dem Jahr 500 v. Chr. lesen sich wie ein abgehackter Twitter-Feed. Sunzis moderne preußische Nemesis hat ein wesentlich präziseres und in sich konsistenteres Instrumentarium für eine gründliche Analyse anzubieten. Selbst wenn Clausewitz' Begriffe und Vorstellungen natürlich in vielerlei Hinsicht ebenso an ihre Grenzen stoßen, stellen sie doch für Fachleute und Verantwortliche des Militärs immer noch eine Art von Grundwortschatz dar. Clausewitz nennt drei Hauptkriterien, die jeder aggressive oder defensive Akt erfüllen muss, um als eigenständige Kriegshandlung zu gelten. Die bislang bekannt gewordenen Cyberattacken genügen diesen Kriterien nicht.

Das erste Element ist die gewaltsame Natur des Krieges. »Der Krieg ist also ein Akt der Gewalt, um den Gegner zur Erfüllung unseres Willens zu zwingen«, schreibt Clausewitz auf der ersten Seite seines Buches *Vom Kriege*.[1] Jeder Krieg impliziert den Einsatz von Gewalt. Birgt eine Handlung nicht wenigstens ein Gewaltpotential, ist sie auch keine Kriegshandlung und kein bewaffneter Angriff – und der Gebrauch des Wortes wird eine metaphorische Dimension annehmen, so wie beim »Krieg« gegen die Fettleibig-

keit oder dem »Krieg« gegen den Krebs. Eine echte Kriegshandlung bzw. ein bewaffneter Angriff ist prinzipiell immer und manchmal de facto tödlich, mindestens für einige Beteiligte auf mindestens einer Seite. Lässt man den Aspekt der körperlichen Gewalt vollkommen unter den Tisch fallen, dann ist »Krieg«, um mit Jack Gibbs zu sprechen, ein Larifari-Begriff.[2] Dasselbe gilt für die Idee einer Waffe. In Clausewitz' Denken ist Gewalt bei allen Kriegen die entscheidende Größe. Die beiden Feinde – denn er betrachtet normalerweise zwei Parteien – versuchten, die Gewalt eskalieren zu lassen, es sei denn, »Friktionen«, Unwägbarkeiten oder die Politik hinderten sie daran.[3]

Das zweite Element, das Clausewitz am Krieg hervorhebt, ist sein instrumenteller Charakter. Eine Kriegshandlung ist immer instrumentell, sie folgt also unter Einsatz eines bestimmten Mittels einem bestimmten Zweck: Physische Gewalt bzw. die Androhung physischer Gewalt ist das *Mittel*, dem Feind den Willen des Angreifers aufzuzwingen das *Ziel*. Eine solche Definition ist »wenigstens in der theoretischen Vorstellung notwendig«, argumentiert Clausewitz.[4] Um das Kriegsziel zu erreichen, muss ein Feind wehrlos gemacht werden oder, genauer gesagt, gegen seinen Willen in eine Lage versetzt werden, in der jeder Versuch einer Veränderung dieser Lage durch weiteren Einsatz von Waffengewalt mindestens in den Augen dieses Feindes nur weitere Nachteile mit sich bringen würde. Gänzliche Wehrlosigkeit ist lediglich die extreme Form dieser Situation. Beide Kriegsparteien bedienen sich der Gewalt auf diese instrumentelle Art und Weise, sie formen das Verhalten des jeweils anderen, sie geben einander, wie es der preußische Philosoph ausdrückt, das Gesetz.[5] Der instrumentelle Gebrauch von Mitteln findet auf technischer, operativer, strategischer und politischer Ebene statt. Je höher das erwünschte Ziel gesteckt ist, desto schwieriger ist es zu erreichen. Entgegen der etwas gestelzten Sprache seiner Zeit formuliert Clausewitz hier hier ohne Umschweife: »[D]ie politische Absicht ist der Zweck, der

Krieg ist das Mittel, und niemals kann das Mittel ohne Zweck gedacht werden.«[6]

Damit sind wir beim dritten und wichtigsten Merkmal des Krieges – seinem politischen Charakter. Eine Kriegshandlung ist immer politisch. Über das unmittelbare Ziel einer Schlacht, den Feind »niederzuwerfen« und wehrlos zu machen, mögen Kommandeure wie Strategen vorübergehend den eigentlichen Zweck des Krieges aus den Augen verlieren. Der Krieg ist niemals ein einzelner Akt oder eine einzelne Entscheidung. In der wirklichen Welt ist der eigentliche Zweck des Krieges immer ein politischer. Er geht über die Anwendung von Gewalt hinaus. Diese Einsicht ist es, die Clausewitz' berühmter Satz ausdrückt: »Der Krieg ist eine bloße Fortsetzung der Politik mit anderen Mitteln.«[7] Um politisch zu sein, muss ein politisches Gebilde oder der Repräsentant eines politischen Gebildes, egal, wie es verfasst ist, eine Absicht, einen Willen besitzen. Diese Absicht muss zum Ausdruck gebracht werden. Und der Wille der einen Seite muss dem Gegner zu irgendeinem Zeitpunkt der Auseinandersetzung übermittelt werden (was nicht heißt, dass er öffentlich gemacht werden müsste). Ein Akt der Gewalt und seine eigentliche politische Absicht müssen sich zu irgendeinem Zeitpunkt der Konfrontation auch einer Seite zurechnen lassen. Die Geschichte kennt keine Kriegshandlungen, die sich nicht früher oder später zurechnen ließen.[8]

Um diese Kriterien auf Cyberattacken anwenden zu können, muss zunächst einmal eine wesentliche Modifikation vorgenommen werden. Das alles entscheidende Element jeder kriegsähnlichen Handlung bleibt der »Einsatz von Gewalt«. Ein solcher Einsatz von Gewalt ist üblicherweise ziemlich massiv und kompakt, auch wenn man ihn in seine einzelnen Bestandteile zerlegen kann. In den meisten bewaffneten Konflikten – konventioneller oder nicht konventioneller Art – erfolgt der Einsatz von Gewalt mehr oder weniger unvermittelt: sei es ein F-16-Bomber, der Ziele aus der Luft beschießt, Artillerie-Trommelfeuer oder ein Droh-

nenangriff, selbst gebaute Sprengkörper, die am Straßenrand platziert werden, oder gar ein Selbstmordattentäter auf einem öffentlichen Platz. In all diesen Fällen wird die auslösende Tat eines Kämpfers oder Aufständischen – etwa das Drücken eines Knopfes oder Betätigen eines Abzugs – unverzüglich und unmittelbar zu Todesopfern führen, selbst wenn ein Zeitzünder oder eine Fernbedienung zwischengeschaltet ist wie bei Drohnen oder Cruise Missiles, und auch dann noch, wenn ein programmiertes Waffensystem halb autonom darüber zu entscheiden vermag, welches Ziel es anpeilt und welches nicht.[9] Eine Cyberkriegshandlung würde ganz anderen Spielregeln gehorchen.

Im Rahmen einer Cyberkriegshandlung wird der eigentliche Einsatz von Gewalt wahrscheinlich in einer wesentlich komplexeren und vermittelteren Abfolge von Ursachen und Wirkungen bestehen, die letztlich zu Zerstörung und Verlusten führt.[10] Ein Szenario, das man sich in diesem Zusammenhang gerne ausmalt, ist ein chinesischer Cyberangriff auf das amerikanische Festland, sollte etwa die Taiwan-Frage eine schwere politische Krise auslösen. Mittels sogenannter Logikbomben, die zuvor in das amerikanische Elektrizitätsnetz eingeschleust wurden, könnten die Chinesen mit einem flächendeckenden Stromausfall eine gesamte Großstadt lahmlegen. Dies könnte einen immensen Verlust an Finanzdaten zur Folge haben. Züge könnten entgleisen und verunglücken. Luftverkehrssysteme und ihre Back-ups könnten zusammenbrechen, wodurch Hunderten von Flugzeugen in der Luft die Kommunikationsverbindung abgeschnitten wäre. Die industriellen Kontrollsysteme hochsensibler Kraftwerke, etwa von Atommeilern, könnten beschädigt werden, was in letzter Konsequenz den Ausfall des Kühlkreislaufs, eine Kernschmelze und die Verseuchung der Umwelt bedeuten könnte[11] – dabei würden Menschen schwer verletzt oder sogar getötet werden. Militäreinheiten könnten außer Gefecht gesetzt werden. In einem solchen Szenario ist die Kausalkette, durch die der Umstand, dass jemand

auf einen Knopf drückt, mit dem Umstand verbunden ist, dass ein anderer verletzt wird, vermittelt und von Zufällen und Friktionen durchsetzt. Doch auch eine derart vermittelte, durch einen Cyberangriff verursachte Zerstörung *könnte* zweifellos eine Kriegshandlung darstellen, auch wenn nicht die Mittel, sondern nur die Folgen mit Gewalt verbunden wären.[12] Außerdem *könnten* nicht gewaltsame Cyberattacken in hoch vernetzten Gesellschaften auch ohne gewaltsame Effekte ökonomische Auswirkungen haben, die über den Schaden eines vergleichsweise kleineren physischen Angriffs hinausgehen.[13] Derartige Szenarien haben zum einen weithin große Verwirrung gestiftet: »Selten hat man über etwas so Wichtiges mit so wenig Klarheit und offenbar so wenig Verständnis gesprochen wie über dieses Phänomen«, kommentierte Michael Hayden, der ehemalige Direktor sowohl der Central Intelligence Agency (CIA) als auch der National Security Agency (NSA).[14] Und zum anderen weisen all diese Szenarien bislang ein entscheidendes Manko auf: Sie gehören ins Reich der Fiktion, um nicht zu sagen: der Science-Fiction.

Wenn wir den Einsatz von Gewalt im Krieg als physisch gewaltsam, instrumentell und politisch verstehen, dann gibt es keinen Cyberangriff, der diesen drei Kriterien gleichermaßen genügt. Doch nicht nur das: Es hat bislang überhaupt nur wenige Cyberangriffe gegeben, die auch nur *einem* der Kriterien genügen. Um diese These zu belegen, wollen wir die am häufigsten zitierten Angriffe Fall für Fall und Kriterium für Kriterium durchgehen.

Der physisch zerstörerischste Cyberanschlag war bislang wahrscheinlich die Explosion einer sibirischen Pipeline – so er denn wirklich stattgefunden hat. Im Rahmen einer verdeckten Operation bedienten sich die Amerikaner 1982 angeblich manipulierter Software, um an der russischen Urengoi-Surgut-Tscheljabinsk-Pipeline, die die Gasfelder von Urengoi in Sibirien über Kasachstan mit den europäischen Märkten verbindet, eine große Explosion herbeizuführen. Da für das gigantische Pipeline-Projekt ein

hoch kompliziertes Steuerungssystem benötigt wurde, waren die sowjetischen Betreiber gezwungen, die dafür notwendigen Computer auf dem freien Markt zu beschaffen. Die zuständigen russischen Behörden wollten die für die Überwachung und Steuerung des Systems erforderliche Software (Supervisory Control and Data Acquisition, SCADA) von den Vereinigten Staaten erwerben, bekamen aber eine Abfuhr. Daraufhin bezogen die Russen die Software von einer kanadischen Firma. Angeblich gelang es der CIA, einen Schadcode in das in Sibirien installierte Steuerungssystem einzuschleusen. Die Software, die die Pumpen, Turbinen und Ventile steuerte, war so programmiert, dass sie eine Weile störungsfrei funktionierte, irgendwann aber »die Pumpengeschwindigkeit und Ventileinstellungen derart veränderte, dass sie einen Druck erzeugten, dem die Verbindungen und Nähte der Rohrleitungen unmöglich standhalten konnten«, wie Thomas Reed, damals in Diensten der NSA, berichtete.[15] Im Juni 1982 verursachten die manipulierten Ventile mutmaßlich eine Explosion und ein Feuer »gigantischen« Ausmaßes, das noch vom Weltall aus zu sehen war. Die US Air Force soll die Detonation auf drei Kilotonnen beziffert haben, was der Explosion eines kleinen atomaren Sprengkopfs entspräche.[16]

Doch diese Geschichte hat gleich drei Haken. Der erste betrifft die russischen Quellen. Als Reeds Buch 2004 erschien, bestritt Wassilij Ptschelintsew, ein ehemaliger KGB-Führungsoffizier der Region Tjumen, in der die Explosion angeblich stattfand, die Geschichte. Er mutmaßte, Reed habe wohl von einer Explosion gesprochen, die sich nicht im Juni, sondern an einem warmen Apriltag desselben Jahres 50 Kilometer von der Stadt Tobolsk entfernt ereignet hatte und dadurch verursacht worden war, dass sich im tauenden Tundraboden Leitungen verschoben hatten. Bei dieser Explosion war offenbar niemand verletzt worden.[17] Obwohl die Medien in den frühen achtziger Jahren sehr wohl über gewöhnliche Unfälle und Pipeline-Explosionen in der UdSSR be-

richteten, findet man keine Pressemeldungen aus dem Jahr 1982, die Reeds angebliche Explosion bestätigen. Auch spätere russische Quellen erwähnen den Vorfall mit keinem Wort. 1990, als die Sowjetunion noch existierte, veröffentlichte Generalleutnant Nikolaj Brusnizyn ein bemerkenswertes, überaus detailreiches kleines Buch, das unter dem Titel *Openness and Espionage* (Offenheit und Spionage) auch ins Englische übersetzt wurde. Brusnizyn war zum damaligen Zeitpunkt stellvertretender Vorsitzender des Gossnab, des Staatlichen Komitees für die materiell-technische Versorgung. Sein Buch enthält ein kurzes Kapitel über »Computerspionage«, in dem er diverse Gerätschaften vorstellt, die der sowjetische Geheimdienst in den vorangegangenen Jahren gefunden habe. Er listet drei Arten von Entdeckungen auf: in Gehäuse eingebaute »Signalgeber«, die überwachen sollen, wo importierte Geräte installiert würden; »zusätzliche elektronische ›Einheiten‹, die nichts mit der Maschine selbst zu tun haben«, durch die sich Daten abgreifen und übertragen lassen; und »technische Vorrichtungen, die einen Computer vollkommen funktionsuntüchtig machen«, indem sie »sowohl die Computersoftware als auch den Speicher zerstören«.[18] Brusnizyn konnte sogar mit Beispielen aufwarten. Das drastischste von ihnen war dem General zufolge ein »Virus« auf einem Computer, den eine westdeutsche Firma an eine sowjetische Schuhfabrik verkauft hatte. Man sollte doch meinen, dass Brusnizyn von dem Überraschungsangriff auf die Pipeline, so er denn stattgefunden hätte, auch gewusst und höchstwahrscheinlich über ihn geschrieben hätte, und wenn nicht über das Ereignis selbst, dann doch mindestens über die Möglichkeit einer Hardwaresabotage. Das tat er aber nicht.

Der zweite Haken betrifft die zur damaligen Zeit verfügbare Technologie. Es ist ungewiss, ob man 1982 schon ohne Weiteres eine »Logikbombe« hätte verstecken können. Drei Jahrzehnte nach einem vermeintlichen Vorfall aber die insgeheim modifizierte Software eines industriellen Steuerungssystems zu ana-

lysieren, ist schwierig bis unmöglich. Doch ein paar allgemeine Feststellungen lassen sich durchaus treffen: Die Technologie war seinerzeit viel primitiver. Ein System zur Steuerung von Gasleitungen wäre Anfang der 1980er Jahre vermutlich eine relativ einfache »Zustandsmaschine« mit einem 8-Bit-Mikrocontroller gewesen. Höchstwahrscheinlich war es im Jahr 1982 immer noch machbar, alle möglichen Ergebnisse aller möglichen Dateneingaben zu testen. (Bei den späteren Mikroprozessoren ist das nicht mehr der Fall.) Durch einen solchen Test können alle versteckten Ergebnisse entdeckt werden – eine Eingabe »X« führt zur gefährlichen Ausgabe »Y«.[19] Die Software auf Mängel zu testen, wäre mit anderen Worten relativ einfach gewesen. Selbst mit der damals erhältlichen Technologie hätte ein Regressionstest nicht länger als einen Tag gedauert, schätzt der langjährige Technikjournalist Richard Chirgwin.[20] Kurz gesagt war es im Jahre 1982 noch wesentlich schwieriger, Schadsoftware zu verstecken.

Und schließlich der dritte Haken: Selbst nachdem die CIA das sogenannte Farewell-Dossier freigegeben hatte, in dem man nachlesen konnte, wie die Sowjetunion mit schadhafter Technologie versorgt werden sollte, bestätigte der Dienst die vermeintliche Explosion nicht. Und falls sie stattgefunden haben sollte, ist nicht klar, ob sie Menschenleben gekostet hat. Die Faktenlage ist in diesem Fall so dünn und fragwürdig, dass er nicht als Beweis für eine erfolgreiche Logikbombe herhalten kann.

Ein anderes viel zitiertes Beispiel für einen Cyberkrieg ist die koordinierte Überflutung estnischer Websites mit Anfragen, die Ende April 2007 begann. Seinerzeit war Estland eines der Länder mit der besten Netz-Infrastruktur; zwei Drittel aller Esten nutzten bereits das Internet, und 95 Prozent aller Bankgeschäfte fanden auf elektronischem Wege statt.[21] Das kleine, gut vernetzte baltische Land bot Cyberattacken eine breite Angriffsfläche. Die Geschichte hinter dem oft zitierten Ereignis nahm etwa zwei Wochen vor dem 9. Mai ihren Ausgang – jenem in Russland emo-

tional hoch aufgeladenen Tag, an dem die Russen des Sieges über Nazi-Deutschland gedenken. Mit einem äußerst unsensiblen Timing hatten die Behörden von Tallinn beschlossen, das russische Denkmal für den unbekannten Soldaten des Zweiten Weltkriegs, einen zwei Meter großen Bronzesoldaten, vom Zentrum der Hauptstadt an den Stadtrand zu versetzen. Die russischsprachige Bevölkerung Estlands war darüber ebenso schockiert wie das russische Nachbarland. Am 26. und 27. April kam es in Tallinn zu gewaltsamen Ausschreitungen, im Zuge deren ein Mensch starb, 1300 Menschen verhaftet und 100 verletzt wurden.

Während der Straßenschlachten erreichte der Aufruhr auch das Internet. Die Cyberangriffe begannen in den späten Abendstunden des 27. April. Zunächst bedienten sich die Angreifer unbeholfener, technisch einfacher Methoden wie etwa einer Flut von Ping-Befehlen oder DoS-, d. h. Denial-of-Service- oder Dienstverweigerungsattacken – massenhafte schlichte Informationsanfragen an einen Server, wie die Aufrufe einer Website beispielsweise. Dann gestalteten sich die Anschläge etwas raffinierter. Am 30. April wurden erstmals einfache Botnetze eingesetzt, um den Umfang der DDoS-Attacken (der Distributed-Denial-of-Service oder dem durch Vielanfragen von zahlreichen verschiedenen Quellen herbeigeführten Zusammenbruch des Dienstes) auszuweiten, und auch zeitlich wurden diese kollektiven Aktionen immer koordinierter. Zu den Beeinträchtigungen zählten zudem E-Mail- und Kommentar-Spams sowie die Verunstaltung der Website der Estnischen Reformpartei. Estland erlebte damals die schlimmste DDoS-Attacke, die es je gegeben hatte. Die Angriffe wurden von einer extrem großen Menge gekaperter Computer – bis zu 85 000 – ausgeführt, und sie dauerten mit drei Wochen ungewöhnlich lange, nämlich bis zum 19. Mai. Ihren Höhepunkt erreichten sie am 9. Mai, an dem man in Moskau den Tag des Sieges feiert. 58 estnische Websites wurden gleichzeitig lahmgelegt. Die Online-Dienste der größten estnischen Bank, der Hansapank, fielen für 90 Minu-

ten und am darauffolgenden Tag für weitere zwei Stunden aus.[22] Zwar bekamen Handel und Banken, Staat und estnische Gesellschaft diese koordinierten Internetproteste zu spüren, deren Auswirkungen aber blieben letztlich gering. Die einzige langfristige Folge des Vorfalls war, dass die estnische Regierung die NATO dazu bewegen konnte, in Tallinn ein Kompetenzzentrum zur Cyberabwehr einzurichten, nämlich das Cooperative Cyber Defence Centre of Excellence.

An dieser Geschichte ist einiges bemerkenswert. Es wurde nicht aufgeklärt, wer hinter den Angriffen steckte. Estlands Verteidigungsminister genau wie der oberste Diplomat des Landes machten den Kreml verantwortlich, konnten jedoch keine Beweise vorlegen. Am Ende musste die Behauptung, Estland habe die IP-Adressen einiger der an den Angriffen beteiligten Computer zur russischen Regierung zurückverfolgen können, dementiert werden. Weder die Experten des Atlantischen Bündnisses noch die der Europäischen Kommission waren in der Lage, digitale russische Fingerabdrücke bei der Operation nachzuweisen. Die russischen Vertreter nannten die Vorwürfe einer Beteiligung ihres Landes »unbegründet«.[23]

Es ist wichtig, die damals neuartige Erfahrung, die Estland machte, richtig einzuordnen. Mihkel Tammet, im estnischen Verteidigungsministerium für die Informations- und Kommunikationstechnologie zuständig, beschrieb das, was im Vorfeld der Angriffe geschah, als »ein dem Zusammenziehen von Armeen vergleichbares Zusammenziehen von Botnetzen«.[24] Andrus Ansip, der damalige Premierminister Estlands, fragte: »Wodurch unterscheidet sich eine Blockade der Häfen oder Flughäfen eines souveränen Staates von der Blockade staatlicher Institutionen und von Nachrichten-Websites?«[25] Das war natürlich als rhetorische Frage gemeint. Die Antwort ist ganz einfach: Im Gegensatz zu einer Seeblockade ist die »Blockade« von Websites nicht einmal potentiell gewaltsam; im Gegensatz zu einer Seeblockade war die

DDoS-Attacke nicht instrumentell an ein taktisches Ziel geknüpft, sondern ein Akt des ungerichteten Protests; und im Gegensatz zu Schiffen, die die Ausfahrt versperren, blieben die Pings ohne politische Rückendeckung anonym. Ansip hätte fragen können, wodurch sich eine Großdemonstration, die den Zugang zu einem Gebäude versperrt, von einer Website-Blockade unterscheidet. Der Vergleich wäre etwas passender, wenn auch aus einem weiteren Grund immer noch schief: Für eine Demonstration alter Schule müssen viel mehr reale Menschen auftauchen.

Vor dem Hintergrund eines Bodenkriegs zwischen der Russischen Föderation und Georgien ereignete sich ein Jahr später, im August 2008, ein weiterer großer Vorfall, der die Kassandra-Rufe vor einem Cyberkrieg befeuerte. Dieser kurze bewaffnete Konflikt entzündete sich an einer Gebietsstreitigkeit um Südossetien. Am 7. August beantwortete die georgische Armee Provokationen mit einem Angriff auf die separatistischen Kräfte Südossetiens. Einen Tag später folgte die militärische Reaktion Russlands. Doch schon am 29. Juli, also etwas über eine Woche vor dem bewaffneten Konflikt und der Hauptwelle des Cyberangriffs, die beide am 8. August begannen, kam es zu ersten Computerattacken auf georgische Websites. Es war möglicherweise das erste Mal, dass ein unabhängiger Cyberangriff synchron mit einer konventionellen militärischen Operation erfolgte.[26]

Bei den Cyberattacken gegen Georgien lassen sich drei Arten unterscheiden. Einige symbolisch wichtige Websites des Landes wurden verunstaltet, so zum Beispiel die Seiten der Zentralbank und des Außenministeriums. Am prominentesten stach eine Collage aus den Porträts von Adolf Hitler und dem georgischen Präsidenten Micheil Saakaschwili hervor. Die zweite Angriffsart bestand in DoS-Attacken gegen öffentliche und privatwirtschaftliche Websites des Landes. Sie trafen unter anderem verschiedene Internetauftritte der georgischen Regierung sowie den des georgischen Parlaments, richteten sich aber auch gegen Presse-

organe, die größte georgische Geschäftsbank und andere mit weniger wichtigen Webpräsenzen. Der digitale Ansturm dauerte im Durchschnitt rund zwei Stunden und fünfzehn Minuten, der längste bis zu sechs Stunden.[27] Eine dritte Methode bestand darin, Schadsoftware in Umlauf zu bringen, um die Reihen der Angreifer und das Angriffsvolumen zu vergrößern. Diverse russischsprachige Foren halfen durch eine Verbreitung von Skripten, die es Nutzern ermöglichten, sich an der Aktion zu beteiligen; das Angriffsskript wurde sogar in einer archivierten Version – war.rar – gepostet, die sich primär gegen Websites der georgischen Regierung richtete. In ähnlicher Weise wurden E-Mail-Accounts georgischer Politiker gespammt.

Auch diese Episode hatte relativ geringe Auswirkungen. Ungeachtet der Kriegsrhetorik, deren sich die internationale Presse, die georgische Regierung und anonyme Hacker befleißigten, waren die Angriffe nicht gewaltsam. Zudem bot Georgien mit seinen 4,6 Millionen Einwohnern weit weniger Angriffsfläche für Attacken als Estland, weil es nicht sehr stark vernetzt war und nur wenige wichtige Dienstleistungen, wie Energie, Transport oder Bankwesen, überhaupt am Internet hingen. Abgesehen davon, dass eine Reihe georgischer Regierungs-Websites eine Zeit lang nicht aufrufbar war, hatte die ganze Angelegenheit kaum Folgen. Der Angriff war auch nur in sehr begrenztem Maße Mittel zu einem Zweck. Georgiens Zentralbank wies ihre Abteilungen an, alle elektronischen Dienste zehn Tage lang auszusetzen. Der wesentliche Schaden, den die Angriffe verursachten, bestand darin, dass sie die Möglichkeiten der Regierung zu internationaler Kommunikation beschnitten und auf diese Weise verhinderten, dass die Stimme des kleinen Landes in einem kritischen Moment gehört werden konnte. Sollten es die Angreifer auf diesen Effekt abgesehen haben, war seine Nützlichkeit allerdings begrenzt: Mit Googles Einwilligung unternahm das Außenministerium einen ungewöhnlichen Schritt und richtete einen Blog auf Googles

Blog-Plattform Blogger ein, sodass ein Kanal für Journalisten offen gehalten wurde. Vor allem aber war der Angriff seinem Wesen nach nicht wirklich politisch. Genau wie die Esten machte auch die georgische Regierung den Kreml verantwortlich. Doch auch in diesem Fall stritt der russische Staat seine Beteiligung an den Angriffen ab. Das Cyber-Security-Zentrum der NATO in Tallinn veröffentlichte bald darauf einen Bericht über die Angriffe. Obwohl es so aussah, als habe die digitale Überflutung auf koordinierte und gesteuerte Weise stattgefunden, und obwohl die Medien Russland in Verdacht hatten, »gibt es«, so schloss die NATO, »wie im Falle Estlands keinen schlüssigen Beweis«, wer hinter den DDoS-Angriffen steckt.[28]

Die Cyberangriffe, die mit den Straßenprotesten in Estland und dem kurzen Feldzug in Georgien einhergingen, waren Präzedenzfälle. Vielleicht lag es vor allem an der Neuartigkeit dieser Art von Attacken, dass sie derart viel öffentliche Aufmerksamkeit erregten und eine solche Kriegsrhetorik provozierten. Eine vergleichbare Beobachtung ließe sich für einen anderen Typus von »Cyberkrieg« machen, nämlich für hochkarätige Spionageoperationen wie die sogenannte Operation Moonlight Maze. Diesen etwas geisterhaften Namen erhielt ein hochgeheimer Fall von Cyberspionage, der 1999 aufgedeckt wurde. Die US Air Force stellte zufällig fest, dass jemand in ihre Netzwerke eingedrungen war, und alarmierte das FBI. Die Bundesermittler riefen die NSA zu Hilfe. Ihre gemeinsame Untersuchung förderte ein gewisses Muster zutage, nach dem jemand seit März 1998 in die Computer der NASA (National Aeronautics and Space Administration), des Energieministeriums und zahlreicher Universitäten und Forschungslabors eindrang. Dabei wurden Lagepläne militärischer Anlagen ebenso kopiert wie Konstruktionspläne und andere sensible Informationen. Die Störmanöver wurden fast zwei Jahre lang fortgesetzt. Dem Verteidigungsministerium gelang es, die Angriffe bis zu einem – damals so bezeichneten – Mainframe (Großrechner) in Russland zurück-

zuverfolgen. Doch auch in diesem Fall: keine Gewalt, unklare Ziele, keine politische Zuordnung.

Dennoch ist der empirische Trend nicht von der Hand zu weisen: In den vergangenen 15 Jahren haben Cyberattacken stetig zugenommen. Immer häufiger kommt es zu Großeinbrüchen in die Sicherheitsarchitektur staatlicher und privatwirtschaftlicher Ziele. Das Ausmaß der Angriffe wächst, ebenso wie die Zahl der an solchen Vorfällen beteiligten Personen, von Kriminellen über Aktivisten bis hin zur NSA. Die Bandbreite aggressiven Online-Verhaltens ist größer geworden. Zur gleichen Zeit hat die Raffinesse einiger Angriffe ein neues Niveau erreicht, und in dieser Hinsicht schlug der Computervirus Stuxnet, der Irans Atomprogramm stören sollte und 2010 entdeckt wurde, sicherlich ein neues Kapitel auf. Doch trotz all dieser Entwicklungen hat der im »Cyberkrieg« enthaltene Kriegsbegriff mehr mit dem »Krieg« gegen die Fettleibigkeit als mit dem Zweiten Weltkrieg zu tun – er hat eher eine metaphorische als eine strikt deskriptive Bedeutung. Es ist höchste Zeit, sich wieder auf traditionelle Begrifflichkeiten zu besinnen und Cyberangriffe als das zu verstehen, was sie in Wirklichkeit sind.

Um den Charakter einer Aggression zu bestimmen, ihre eher politische oder rein kriminelle Natur, empfiehlt es sich, Angriffe nach einer Skala zu sortieren, die von gewöhnlichen Verbrechen bis zum Extrem eines konventionellen Krieges reicht. Dann werden einige Unterscheidungsmerkmale sichtbar: Verbrechen sind in der Regel unpolitisch, Kriege sind immer politisch; Verbrecher verschleiern ihre Identität, uniformierte Soldaten stellen die ihre offen zur Schau. Politische Gewalt ist (genau wie die »politischen Verbrechen« der Kriminologie und der Rechtstheorie) auf dieser Skala in einer unklaren Mitte angesiedelt, sofern sie weder ein normales Verbrechen ist noch ein normaler Krieg. Der Einfachheit halber wollen wir diesen mittleren Bereich der Skala in drei Abschnitte unterteilen: Subversion, Spionage und Sabotage.

An allen drei Aktivitäten können sowohl Staaten als auch private Akteure beteiligt sein. Man neigt dazu, Cyberangriffe eher dem kriminellen Ende des Spektrums zuzuordnen. Am Maßstab einer sachgerechten Kriegsdefinition gemessen, hat es bis jetzt noch keinen bekannt gewordenen Cyber-»Kriegsakt« gegeben, sehr wohl aber politische Cyberattacken. Doch alle bekannt gewordenen politischen Cyberattacken – mögen sie kriminell sein oder nicht – lassen sich weder als gewöhnliche Verbrechen noch als konventionelle Kriege verbuchen. Ihre Absicht ist Subversion, Spionage oder Sabotage.

In allen drei Fällen geraten die Clausewitz'schen Kriterien durcheinander. Diese Handlungen müssen nicht mit Gewalt verbunden sein, um ihre Wirkung zu entfalten. Um zu funktionieren, müssen sie nicht instrumentell sein, da die Subversion Ausdruck kollektiver Leidenschaft und Spionage eher das Resultat einer Gelegenheit als einer Strategie sein kann. Und schließlich: Angreifer, die mit dem Ziel der Subversion, Spionage oder Sabotage tätig werden, handeln sehr wohl politisch; doch im scharfen Gegensatz zum Krieg haben sie wahrscheinlich dauerhaft oder mindestens zeitweise ein Interesse daran, nicht mit ihren Taten in Verbindung gebracht zu werden. Dies ist einer der Hauptgründe dafür, dass politische Verbrechen im Cyberspace, in dem es leichter ist, Spuren zu verwischen, als sie mit Gewissheit zuzuschreiben, stärker um sich greifen als Kriegshandlungen. Selbstverständlich können Subversion, Spionage und Sabotage – ob sie sich digitaler Mittel bedienen oder nicht – militärische Operationen flankieren. Beide Seiten können sich an derartigen Aktivitäten beteiligen und haben dies in der Tat schon seit Menschengedenken getan. Doch die Entwicklung digitaler Netzwerke zeigt ungleiche Auswirkungen. Um diese zu verstehen, müssen wir uns auf den Begriff der Gewalt zurückbesinnen.