Cyberkrieg – eine vorhersehbare Überraschung?

Matthias Wolfram*

Abstract: While cyber attacks are subject of a wide range of publications, the question of whether a cyber war is going on or even possible at all remains hotly contested with the opponents seemingly gaining the upper hand lately. But the characterization as a mere hype or as threat inflation to augment own funding in times of shrinking budgets misses two points: not only are cyber wars theoretically possible, but we still miss coherent categories and definitions to grasp the full extent of possible attacks. The following essay is trying to weigh these aspects and offers two scenarios of plausible cyber wars as well as steps towards a better definition of the challenges.

Keywords: Cyberwar, cyberspace, threat, disruption
Cyberkrieg, Cyberraum, Bedrohung, Unterbrechung

Sind Cyberkriege ein Hirngespinst oder besteht tatsächlich die Möglichkeit einer kriegerischen Auseinandersetzung, die sich ausschließlich im Cyberraum[1] abspielt? Spätestens seit der Entdeckung des Schadprogrammes Stuxnet hat die Diskussion um Cyberangriffe und ihr Schadpotenzial Fahrt aufgenommen. Dabei sind sich die Teilnehmer bis heute uneinig, wie diese Angriffe einzustufen sind und welche Bedeutung dies für die zukünftige Konfliktaustragung hat. Findet der Begriff „Cyberwar" auch oft effektheischend Verwendung in den Medien, so sind sich Fachleute in der Einschätzung einig, dass ein Cyberkrieg, der diesen Namen verdient hätte, bisher nicht stattgefunden hat. Einige Experten gehen so weit zu bestreiten, dass es Cyberkrieg überhaupt geben könnte.[2] Auch der ehemalige „Cybersecurity Coordinator" des Weißen Hauses, Howard Schmidt, zog gegen den Begriff „Cyberwar" zu Felde.[3] Der Begriff wird allerdings vielfach genutzt, darunter auch im Deutschen Bundestag sowie durch das Verteidigungsministerium, wie in Anhörungen des Verteidigungsausschusses im Jahr 2012 deutlich wurde.[4] Die Bewertung bisheriger Vorkommnisse und potenzieller zukünftiger Entwicklungen ist damit äußerst heterogen und deckt nahezu die gesamte Bandbreite möglicher Meinungen zu der Frage ab. Dies spiegelt vor allem die Tatsache wieder, dass Auseinandersetzungen im Cyberraum erst langsam beginnen und ein bisher noch nicht in seiner vollen Tragweite zu erkennendes Phänomen sind, zu dem noch keine ausreichenden empirischen Daten vorliegen. Es in Gänze zu erfassen und zu bewerten, ist daher noch gar nicht möglich, sodass sich die Debatte in Teilen mit bisher noch hypothetischen Fragen auseinandersetzt. Die Gefahr weitreichender Konsequenzen macht allerdings eine vorausschauende und antizipierende Diskussion des Potenzials von Cyberangriffen sowie die Analyse ihrer maximalen Auswirkungen notwendig, auch wenn die Faktenlage noch keine abschließende Bewertung erlaubt.

1. Cyberkrieg und Computernetzwerkoperationen

Bei der Betrachtung des Themenkomplexes Cyberkrieg stellt sich zunächst die grundsätzliche Frage, ob ein Cyberkrieg notwendigerweise ausschließlich im Cyberraum ausgetragen werden muss, um diesen Namen zu rechtfertigen, oder ob eine teilweise Auseinandersetzung in mehreren Domänen, die auch den Cyberraum mit einbezieht, diese Bezeichnung verdient. Bei allen noch so kontrovers geführten Debatten zu dem Thema gestehen selbst Zweifler ein, dass zukünftige Kriege unter Beteiligung hochtechnisierter Streitkräfte mit höchster Wahrscheinlichkeit immer über eine Cyberkomponente, die Computernetzwerkoperationen (CNO), verfügen werden. Die in den Medien kolportierte Ausschaltung syrischer Radarstellungen, um einen israelischen Luftangriff auf die Nuklearanlage Dayr ez-Zor in Nordsyrien im Jahr 2007 zu ermöglichen, zeigt eindrucksvoll das Potenzial solcher Operationen. Sie sind zukünftig als Bestandteil jeglicher Kriegführung moderner Streitkräfte zu erwarten, eingebunden in den Rahmen der allgemeinen militärischen Operationsführung. In ihrer Rolle als Unterstützungsfunktion klassischer konventioneller Militäroperationen erfolgen sie gleichzeitig mit diesen oder zu ihrer direkten Vorbereitung. Daher sind sie logisch nicht als Cyberkrieg und damit eigenständige, in sich geschlossene Maßnahmen zu bewerten, sondern als Teilaspekt einer Gesamtkonzeption moderner Kriegführung. Ihre Bezeichnung als CNO, analog zu Luft-, Land- oder Seeoperationen, macht diesen unterstützenden Charakter deutlich. Ein Luft-, Land- oder Seekrieg hingegen impliziert streng genommen, dass die kriegerische Auseinandersetzung ausschließlich in dem jeweiligen Medium stattfindet oder die einzelnen Komponenten getrennt zu betrachten sind, da sie nicht streitkräftegemeinsam und zusammenhängend angelegt sind. Demnach wäre ein Cyberkrieg konsequenterweise als eine nur im Cyberraum ausgetragene Auseinandersetzung einzustufen. Betrachtet man speziell eine solche potenzielle Konfrontation, stellen

* Major i.G. Dr. phil. Wolfram ist Austauschoffizier im französischen Verteidigungsministerium in Paris. Der Autor gibt ausschließlich seine persönliche Meinung wieder. Dieser Beitrag ist double-blind peer-reviewed.

1 Als Cyberraum wird der virtuelle Raum verstanden, der sich aus der Gesamtheit der Informations- und Telekommunikationsinfrastruktur ergibt. Er geht damit weit über die technische Dimension des Internet als einzelnem globalem Netzwerk hinaus und bezieht auch davon getrennte Netzwerke und Rechnersysteme mit ein.

2 Rid, Thomas: Cyber War Will Not Take Place, in: Journal of Strategic Studies, Vol. 35, Nr. 1, Oktober 2011; Baud, Michel: La cyberguerre n'aura pas lieu, mais il faut s'y préparer in: Politique étrangère, Vol. 77, Nr. 2, Sommer 2012, S. 305-316.

3 Chabrow, Eric : Howard Schmidt Dismisses Cyberwar Fears, 06.03.2010, URL : http://www.govinfosecurity.com/howard-schmidt-dismisses-cyber-war-fears-a-2267, letzter Zugriff 08.08.2012.

4 Vgl. Tagesordnung der 120. Sitzung des Verteidigungsausschusses in der 17. Wahlperiode am 13.06.2012, Berlin 07.06.2012, S. 7: Beratung des Berichts des Bundesministeriums der Verteidigung zum Themenkomplex „Cyber Warfare". « Cyber War » stand u.a. bereits für die Sitzungen 105-108 auf den Tagesordnungen.

https://doi.org/10.5771/0175-274x-2013-3-170 - Generiert durch IP 216.73.216.36, am 22.01.2026, 23:11:18. © Urheberrechtlich geschützter Inhalt. Ohne gesonderte Erlaubnis ist jede urheberrechtliche Nutzung untersagt, insbesondere die Nutzung des Inhalts im Zusammenhang mit, für oder in KI-Systemen, KI-Modellen oder Generativen Sprachmodellen.

sich drängende Fragen für moderne Sicherheits- und Verteidigungspolitik, die bisher noch einer Antwort harren: Kann hier von einem Krieg gesprochen werden, was erhebliche rechtliche Folgen hätte, und wenn ja, ab welcher Schwelle? Welchen Schaden könnte ein solcher Krieg verursachen und als wie bedrohlich ist sein Eintreten folglich einzustufen? Eröffnet eine solche Auseinandersetzung auch nichtstaatlichen Akteuren, die bislang nur mit äußerstem Aufwand mittels punktueller Terrorakte zu einem Angriff auf Staaten in der Lage waren, den Zugang zu einem Krieg?

Die folgenden Ausführungen werden sich aufgrund seiner Bedeutung auf den Fall des reinen Cyberkrieges konzentrieren. Naturgemäß können nicht alle aufgeworfenen Fragen im Detail im Rahmen dieses Artikels diskutiert werden. Daher sollen zunächst die grundlegenden Fragen der Möglichkeit der Existenz und der potenziellen Form eines Cyberkrieges im Fokus der folgenden Ausführungen stehen.

2. Das Wesen des Krieges

Will man die Frage der Existenz und die Grenzen des bisher nicht empirisch zu fassenden reinen Cyberkrieges ausloten, bietet sich eine Annäherung über das Verständnis des Wesens von Krieg an. Seine grundlegenden Wesenszüge haben sich über die letzten Jahrhunderte trotz aller technischen und gesellschaftlichen sowie organisatorischen Neuerungen nicht geändert und können auch für mögliche zukünftige Kriege zugrunde gelegt werden. Krieg mag ein Chamäleon sein, das unter den jeweils aktuellen Rahmenbedingungen immer wieder sein Aussehen ändert; seine Natur jedoch kann er nicht verleugnen.[5] Somit besitzen die grundsätzlichen Ausführungen von Carl von Clausewitz auch nach über zweihundert Jahren noch ihre Aktualität mit der Feststellung, Krieg sei „ein Akt der Gewalt […], um den Gegner zur Erfüllung unseres Willens zu zwingen."[6] Um den hier nur unpräzisen Begriff der Gewalt unterhalb der von Clausewitz betrachteten militärischen Auseinandersetzung ausreichend zu qualifizieren, ist aber eine Ergänzung notwendig: Gewalttätige Auseinandersetzungen müssen erst eine gewisse Schwelle überschreiten, um als Krieg zu gelten. Somit ist Krieg vom Begriff her ein Akt beträchtlicher, organisierter Gewalt, um eigene Ziele durchzusetzen.[7] Genauer ist diese Gewalt allerdings kaum zu fassen: Eine Quantifizierung ihrer Konsequenzen durch Opferzahlen ist mit erheblichen Schwierigkeiten behaftet, zöge sie doch eine weitgehend willkürliche Grenze und schlösse damit gegebenenfalls Vorfälle aus, die nach allgemeinem Verständnis als Krieg angesehen werden. Der von der Arbeitsgemeinschaft Kriegsursachenforschung (AKUF) zusätzlich angeführte Aspekt der zeitlichen Dauer, der „eine gewisse Kontinuierlichkeit der Feindseligkeiten"[8] voraussetzt, ist ebenfalls fragwürdig. Zwar schließt dies zu Recht Ereignisse wie beispielsweise die Schusswechsel an der „Line of Control" in Kaschmir oder ähnliche Scharmützel geringeren Umfangs auch zwischen staatlichen Streitkräften aus. Erhebliche, wenngleich kurze Angriffe, wie es konventionelle oder gar nukleare Militärschläge wären, würden bei dieser Beschreibung aber nicht als Krieg gewertet, was ebenfalls zu kurz greift. Die „Mutual Assured Destruction" eines befürchteten dritten Weltkriegs zwischen NATO und Warschauer Pakt hätte wohl keinen ganzen Tag in Anspruch genommen und wäre dennoch verheerend gewesen. Grundsätzlich eine zeitliche Mindestdauer von Auseinandersetzungen festlegen zu wollen, erscheint daher vor allem für die aktuelle Fragestellung ebenfalls als wenig zweckmäßig.

Die zugrunde gelegte „beträchtliche organisierte Gewalt" wird in vielen Betrachtungen auf Staaten fokussiert, was sich häufig in der Charakterisierung als „*militärisch* organisiert" manifestiert. Dies trifft allerdings auch auf andere Akteure zu: Als klarstes Beispiel steht für eine solche militärisch organisierte, aber nichtstaatliche Gruppe die Hisbollah, die es 2006 schaffte, den Südlibanon ohne Hilfe der staatlichen Streitkräfte des Landes gegen die israelische Armee zu halten. Sie erreichte dies nicht mit nadelstichartiger Guerillataktik, sondern durch die oft starre Verteidigung befestigter Ortschaften im Stile konventioneller Streitkräfte. Auch wenn dies nur durch die besonderen Rahmenbedingungen möglich war, so macht dies dennoch deutlich, dass „militärisch" nicht in jedem Fall „staatlich" bedeutet. Grundsätzlich spricht daher mit Blick auf die Realitäten nichts dagegen, den Krieg als militärischen Gewalteinsatz von seiner Staatenzentriertheit zu befreien: Die Realität zeigt, dass nichtstaatliche Akteure willens und in der Lage sind, Staaten organisiert und anhaltend mit erheblicher Waffengewalt herauszufordern. Dies spricht dafür, den Begriff nicht auf Staaten zu begrenzen und entsprechend zu öffnen, wie es auch Ruloff/Schubiger tun.

Zentraler Aspekt einer Einstufung von Auseinandersetzungen als Cyberkrieg ist damit die Einstufung von Attacken als Gewalt. Diese lässt sich schlüssig über den bewirkten Schaden bemessen: Um als beträchtliche Gewalt im Sinne der Kriegsdefinition zu gelten, müssten die Angriffe erhebliche gewaltgleiche Auswirkungen nach sich ziehen und damit nachweisbare physische Konsequenzen haben. Die bloße Zerstörung einer einzelnen Maschine oder Anlage durch computergestützte Angriffe würde eine solche Bewertung allerdings kaum rechtfertigten. Sie ließe sich je nach ihren Rahmenbedingungen unter Sabotage oder Terrorismus subsummieren, nicht aber unter den Begriff des Krieges. Basierend auf diesen theoretischen Erwägungen lässt sich festhalten: Die für einen Cyberkrieg zu überschreitende Schwelle ist erheblich und schließt die bis heute erfolgten Attacken im Cyberraum klar aus. Im nächsten Abschnitt soll daher der Frage nachgegangen werden, ob ein Cyberkrieg nach diesen Bedingungen überhaupt plausibel erscheint und welche Szenarien diesbezüglich vorstellbar sind.

3. Plausibilität eines Cyberkrieges

Experten sind sich einig, dass heute Angriffe mit erheblichen Folgen in der „realen Welt" durch Schadprogramme möglich

5 Vgl. Hahlweg, Werner (Hrsg.): Vom Kriege: hinterlassenes Werk des Generals Carl von Clausewitz, 19. Auflage, Dümmler Verlag, Bonn 1980, S. 214.
6 Ebenda, S. 212.
7 Vgl. Ruloff, Dieter/Schubiger, Livia: Kriegerische Konflikte: Eine Übersicht, in: APuZ 16-17/2007, Bundeszentrale für politische Bildung, Bonn, 2007, S. 10-17, hier S. 11.
8 Vgl. Schreiber, Wolfgang: Kriege und bewaffnete Konflikte 2012, AKUF Analysen Nr. 11, Hamburg 2012, S. 7.

https://doi.org/10.5771/0175-274x-2013-3-170 - Generiert durch IP 216.73.216.36, am 22.01.2026, 23:11:16. © Urheberrechtlich geschützter Inhalt. Ohne gesonderte Erlaubnis ist jede urheberrechtliche Nutzung untersagt, insbesondere die Nutzung des Inhalts im Zusammenhang mit, für oder in KI-Systemen, KI-Modellen oder Generativen Sprachmodellen.

sind.[9] Diese können stark unterschiedlicher Natur sein: Sie reichen von der Manipulation medizinischer Geräte mit direkt lebensbedrohlichen Folgen für einzelne Individuen bis hin zur (Zer-)Störung komplizierter Anlagen und Netzwerke, die durch eine Veränderung von Umweltbedingungen indirekt schwerwiegende Konsequenzen für Verkehrsströme und Fertigungsprozesse sowie allgemeine Lebensbedingungen bewirken.[10] Wie oben ausgeführt erfüllen jedoch geringfügige Attacken mit begrenzten Schäden und einzelnen direkten oder indirekten Opfern die Definition eines Krieges noch nicht. Einzig umfangreiche Angriffe mit beträchtlicher, organisierter Gewalt und weitreichenden Folgen erfüllen diese Kriterien. Etwas Entsprechendes ist aber nur durch umfangreiche zielgerichtete, jeweils individuelle Schadprogrammierung für viele einzelne Systeme zu erreichen, wie auch die Analyse von Stuxnet gezeigt hat.[11] Als unstrittig ist daher zwar anzusehen, dass großflächige, gezielte Cyberattacken erhebliche Störungen im Alltag sowie dem gesellschaftlichen und wirtschaftlichen Leben hervorrufen und auch substanzielle Auswirkungen auf die Handlungsfähigkeit von Staaten haben können.[12] Sie setzen jedoch einen erheblichen Zeit- und Ressourcenaufwand und damit eine hohe Akteursqualität voraus.

3.1 Denkbare Szenarien eines Cyberkrieges

Um die theoretischen Ausführungen zu der Frage der Möglichkeit eines reinen Cyberkrieges plastischer zu gestalten, bietet es sich an, denkbare Szenarien zu skizzieren. Für einen Krieg, der nur im Cyberspace ausgetragen würde, aber dennoch schwerwiegende Auswirkungen auf die angegriffene Gesellschaft hätte, ließen sich auf der Grundlage der heute öffentlich zugänglichen Erkenntnisse zwei plausible Szenarien bilden. Beiden lägen die Schwierigkeit der eindeutigen Zuschreibung von Attacken sowie der Wille des Angreifers, keine weitere Eskalation zu verfolgen und einen militärischen Schlagabtausch zu vermeiden, zugrunde. Die Problematik den Angreifer zu ermitteln bei gleichzeitig zu erwartendem öffentlichen Druck zur Reaktion würde für das Opfer eher einen „Cybergegenschlag" denn einen konventionellen Gegenangriff nahelegen.

1) Konfliktaustragung durch disruptive Attacken

Die Unterbrechung wichtiger Prozesse und Abläufe in hochgradig vernetzten Gesellschaften, die Disruption, kann in den betroffenen Gesellschaften schwerwiegende Folgen und je nach betroffenen Teilsystemen Auswirkungen auf Leib, Leben und Wohlergehen der Bevölkerung haben. Vorstellbar sind gezielte Disruptionen für alle Systeme, die computergesteuert werden, selbst wenn sie nicht an das Internet angebunden sind: Die Möglichkeit des Einschleusens von Schadsoftware in geschlossene Netze ist spätestens seit Stuxnet bekannt. Damit ist eine Störung oder Unterbrechung von allen rechnergesteuerten Systemen wie Stromnetzen und Informations- und Telekommunikationsnetzen grundsätzlich denkbar.[13] In der Konsequenz betrifft die Gefahr alle durch Rechner gesteuerte und vernetzte Infrastrukturen wie – je nach Organisation und Steuerung – die Verkehrsinfrastruktur, Wasserversorgung, Lebensmittelproduktion oder die logistischen Ketten ihrer Verteilung. Zwar sind nicht alle diese Systeme überall gleich gefährdet, die Möglichkeit einer auch längeren Unterbrechung oder Störung von wichtigen Steuerungssystemen ist allerdings an vielen Stellen existent. Eine solche Disruption ließe sich zur Ablenkung oder politischen und wirtschaftlichen Schwächung eines Kontrahenten mit dem Ziel der eigenen Interessendurchsetzung nutzen und wäre sowohl punktuell anlassbezogen als auch strategisch langfristig vorstellbar. Ein plausibles Beispiel für ein solches Szenario, wenngleich ohne Erläuterung einer möglichen Motivation des Angreifers, findet sich bereits in der Übung „Eligible Receiver" der U.S.-Streitkräfte von 1997. Dabei wurde von einem Staat ausgegangen, der eine direkte militärische Konfrontation vermeiden, aber verwundbare amerikanische Informationssysteme angreifen wollte. Zu den Zielen der Angreifer gehörte die Verschleierung ihrer Identität und die Verzögerung oder Verhinderung einer militärischen Reaktion der USA.[14] Erst kürzlich bezog sich auch der kaum des Bellizismus verdächtige US-amerikanische Präsident Barack Obama mehrfach auf ein solches Szenario.[15] Der deutschen „Länderübergreifenden Krisenmanagementübung" LÜKEX lag 2011 ebenfalls ein Szenario zugrunde, in dem zielgerichtete massive Cyberattacken zu erheblichen Beeinträchtigungen kritischer Infrastrukturen und Versorgungsengpässen in der Bevölkerung führten.

2) Verhinderung militärischer Machtprojektion

Eine weitere plausible Anwendung eines Cyberkrieges in der Praxis ist die Vermeidung einer konventionellen Auseinandersetzung durch Störung und Verhinderung von Verlegung und Aufmarsch militärischer Kräfte durch gezielte Cyberangriffe. Besonders eng getaktete logistische Abläufe, die vielfach auf einer computergestützten Planung und Steuerung beruhen, sind durch eine Attacke auf neuralgische Punkte und Prozesse potenziell leicht zu stören. Unterhalb der Schwelle offener militärischer Gewaltanwendung erlaubt auch dieses Szenario unter Inkaufnahme von vorrangig materiellen und finanziellen Folgen die Durchsetzung eigener Ziele unter Absicherung gegen militärische Gegenmaßnahmen. Hier ergibt sich

9 Vgl. u.a. Lewis, James: America is under attack: why urgent action is needed, Testimony before the House Committee on Homeland Security, 24.04.2012, CSIS, S. 5f; Direction de l'information légale et administrative: Livre Blanc de défense et sécurité nationale, Paris, 2013, S. 45.

10 Vgl. bspw. Finkle, Jim: Exclusive: Medtronic probes insulin pump risks, in: Reuters online, 25.10.2011, Reichenbach, Gerold/Göbel, Ralf/Wolff, Hartfrid/Stokar von Neuforn, Silke (Hrsg.): Risiken und Herausforderungen für die Öffentliche Sicherheit in Deutschland. Grünbuch des Zukunftsforums Öffentliche Sicherheit. Szenarien und Leitfragen, Berlin 2008, S. 16ff.

11 Vgl. Falliere, Nicolas/O'Murchu, Liam/Chien, Eric: W32. Stuxnet Dossier, Symantec White Paper Version 1.4, Cupertino 2011, S. 3.

12 Vgl. Billo, Charles/Chang, Welton: Cyber Warfare. An Analysis of the Means and Motivations of selected Nation States, Dartmouth College, Hanover/USA, November 2004, S. 14; Bundesministerium der Verteidigung (BMVg): Bericht zum Themenkomplex „Cyber-Warfare", Ausschussdrucksache 17(12)896, 13.04.2012, S. 2.

13 Vgl. Reichenbach/Göbel/Wolff/Stokar von Neuforn, Berlin 2008, a.a.O., S. 16ff; Rustici, Ross: Cyberweapons: Leveling the International Playing Field, in: Parameters, Herbst 2011, S. 32-42, hier S. 34. Rustici skizziert einen solchen umfassenden Cyberangriff wie folgt: « A hypothetical cyber campaign could unfold in the following manner: 1) mid-air collisions of civilian airlines coupled with derailments of AMTRAC and commuter or subway trains; 2) cell phone blackouts; 3) gas line ruptures, oil refinery shut downs, and the breaching of dams though utilizing the emergency release valves; 4) the state launching the cyberattack announcing responsibility; 5) cutting the national power grid. » Ebenda, S. 41.

14 Vgl. Hildreth, Steven: Cyberwarfare, Congressional Research Service, RL30735, 19.06.2011, S. CRS-4.

15 Vgl. Obama, Barack: Taking the Cyberattack Threat Seriously, in: Wall Street Journal, 20.07.2012, S. A11; ebenso die "State of the Union Adress" des 12.02.2013.

https://doi.org/10.5771/0175-274x-2013-3-170 - Generiert durch IP 216.73.216.36, am 22.01.2026, 23:11:18. © Urheberrechtlich geschützter Inhalt. Ohne gesonderte Erlaubnis ist jede urheberrechtliche Nutzung untersagt, insbesondere die Nutzung des Inhalts im Zusammenhang mit, für oder in KI-Systemen, KI-Modellen oder Generativen Sprachmodellen.

mit Blick auf aktuelle Area-Denial-/Anti-Access-Konzepte und noch immer existierende Territorialkonflikte ein konsistentes Szenario: Nach der Besetzung umstrittener Inseln durch einen Staat entscheidet sich ein Verbündeter des Aggressionsopfers zu einem Militäreinsatz, um den betroffenen Partner zu unterstützen. Dabei soll die Besetzung vorrangig mit einer Demonstration militärischer Stärke rückgängig gemacht werden, eine militärische Befreiung des Territoriums wird jedoch im Notfall nicht ausgeschlossen. Um dieses Eingreifen und eine entsprechende militärische Eskalation der Lage zu verhindern, sabotieren die gegnerischen Spezialisten logistische Einrichtungen, vor allem Häfen und Flughäfen, aber auch Kraftwerke, Straßen- und Schienenverbindungen mit Hilfe von Cyberangriffen, die sich bis hin zur physischen Zerstörung von computergesteuerten Verkehrsregelungs- und Steuerungssystemen auswirken.[16] Ohne dass klassische militärische Mittel wie Raketen oder Flugzeuge zum Einsatz gekommen wären, würde das Drittland in diesem Fall durch einen Präventivschlag mit physischen Schäden möglicherweise von dem Eintritt in den bewaffneten Konflikt abgehalten werden. Betrachtet man das von Clausewitz zugrunde gelegte Verständnis von Krieg als „erweitertem Zweikampf", so lässt sich vor dem Hintergrund der obigen Szenarien auch ein solches Ringen im Cyberraum als Folge eines Angriffs vorstellen. Durch die Schwierigkeit der Attribution der Möglichkeit einer konventionellen militärischen Reaktion beraubt, könnte ein angegriffener Staat im Cyberraum versuchen, den gegnerischen Akteur niederzuringen, was durchaus plausibel zu gewaltgleichen Schäden außerhalb des Cyberraumes und an den Netzinfrastrukturen führen könnte.

In beiden Szenarien ist die Eskalation von virtuellen zu realen physischen Schäden eine entscheidende Stufe. Zwar ist bei einer reinen Lähmung und Verlangsamung von Logistik noch vorstellbar, dass kein Sachschaden entsteht und es bei rein monetären Verlusten durch Unterbrechung logistischer Ketten bleibt. Kommt es aber tatsächlich zu beträchtlichen Sach- und Personenschäden, erscheint eine Einstufung der Situation als Krieg auch aus politischer Sicht sehr viel eher wahrscheinlich und nur schwer zu umgehen. Diese weitreichende Folge ist allerdings schwer vorherzusehen, ist doch die offizielle Einstufung als Krieg eine nahezu rein politische Entscheidung. Sie hängt daher stark von verschiedenen Einflussfaktoren ab, wie der Position der jeweiligen Regierung und der Notwendigkeit, für eigene und fremde Adressaten Stärke zu demonstrieren sowie der Möglichkeit, selbst abgestuft auf eine solche Attacke zu reagieren. Die Beantwortung der Frage, ob solche Angriffe grundsätzlich einen kriegerischen Akt darstellen, wäre jedoch unabhängig von ihrer offiziellen Benennung als solcher, wenn eine schlüssige, anerkannte Definition vorläge.

Ein wie hier angenommen breit angelegter, andauernder und gezielter Cyberangriff auf essentielle Systeme und Dienste mit substanziellen Sach- und Personenschäden ist selbstverständlich kein simpler Akt einzelner Hacker, die damit Staaten mit geringem Aufwand in die Knie zwingen können. Ein entsprechender Angriff bedürfte umfassender Erkundung der jeweils genutzten Systeme und Konfigurationen und eine darauf abgestimmte Schadprogrammierung, die im besten Falle – aber nicht notwendigerweise – unter Laborbedingungen hinsichtlich ihrer Wirkung erprobt werden müsste. Dies erfordert erhebliche personelle und zeitliche Ressourcen, ist aber damit letztlich nicht unmöglich für nichtstaatliche Akteure. Ein Cyberkrieg wäre daher nicht mehr nur auf Staaten und quasistaatliche Gebilde wie beispielsweise die Hisbollah als Akteure beschränkt, sondern könnte vor allem im Fall langfristig planender und finanziell sowie materiell gut ausgestatteter Organisationen und Gruppierungen auch von nichtstaatlichen Konfliktparteien geführt werden.

3.2 Wahrscheinlichkeitsabschätzung

Häufig wird zu Recht darauf hingewiesen, dass es bisher keine Fälle eines Cyberkrieges oder von bewiesenen schwerwiegenden Cyberangriffen gegeben hat. Hier gilt jedoch nach wie vor die Feststellung, dass der bisher fehlende empirische Beweis nicht mit der Unmöglichkeit einer solchen Entwicklung gleichbedeutend ist.[17] Der Direktor der NATO-Agentur NCSA, General Kurt Hermann, unterstrich z.B., dass Cyberangriffe bisher nicht militärisch relevant gewesen sind, „betonte aber gleichzeitig die exponentiell wachsende, reale Gefahr von Cyber-Militärschlägen."[18] Diese erscheinen als Präventivschläge zur Vermeidung oder Substituierung von realen militärischen Angriffen wie oben beschrieben durchaus plausibel und müssen nicht in einem Jahre andauernden, existenzielle Schäden hervorrufenden Konflikt gipfeln, um als Cyberkrieg eingestuft werden zu können. Grundsätzlich decken sich allerdings die Einschätzungen der meisten Experten bisher darin, dass ein reiner Cyberkrieg theoretisch möglich, aber unwahrscheinlich ist.[19] Beobachter und Analysten täten daher gut daran, den Begriff nicht zu sehr zu strapazieren und mit Vorsicht zu gebrauchen – und vor allem nicht für eindeutige Fälle von Spionage oder Kriminalität –, aber die potenzielle Existenz des Phänomens in bestimmten, engen Grenzen auch nicht rundweg auszuschließen.

Insgesamt ist eine detaillierte, fundierte Einschätzung der Bedrohung aufgrund der wenigen öffentlich zugänglichen Beweise und erheblicher Geheimhaltung noch immer sehr schwierig. Selbst der ehemalige NSA- und CIA-Chef General Michael Hayden als eingeweihter ehemaliger Entscheidungsträger gab öffentlich zu: „Let me be clear: This stuff is overprotected. It is far easier to learn about physical threats from US government agencies than to learn about cyber threats. […]

16 Angelehnt an Schilderung von Roger Cliff: Anti-Access Measures in Chinese Defense Strategy, Testimony before the U.S. China Economic and Security Review Commission, 27.01.2011, The RAND Corporation CT-354, S. 6f. Ähnlich auch Lewis, James: Tresholds for Cyberwar, CSIS, September 2010, S. 3.

17 Analog stellte Manach für den Cyberterrorismus fest: „Que les cyberterroristes n'aient encore pas frappé ne prouve en effet nullement qu'ils ne le feront jamais." Manach, Jean Marc: Cyberterrorisme, la guerre de l'information, in : L'Atlas du Monde diplomatique 2009, S. 46f, hier S. 47.

18 Grunert, Florian: Ein Bericht über die Handelsblatt-Konferenz „Cybersecurity 2011" in Berlin, in : ZFAS (2012) Nr. 5, S. 137-143, hier S. 139.

19 Lewis, James: Testimony, House Committee on Homeland Security, Subcommittee on Cybersecurity, Infrastructure protection and Security Technologies: Examining the Cyber Threat to Critical Infrastructure and the American Economy, 16.03.2011, S. 3. Ähnlich Sommer/Brown 2011, a.a.O., S. 81: "A pure cyberwar, that is one fought solely with cyber-weapons, is unlikely." und Dunn Cavelty, Myriam: Unraveling the Stuxnet Effect, in: Military and Strategic Affairs, Vol. 3, Nr. 3, Dezember 2011, S. 11-19, hier S. 15: "In fact, it has been convincingly shown that a „pure (or strategic) cyberwar is very unlikely to ever occur […]."

https://doi.org/10.5771/0175-274x-2013-3-170 - Generiert durch IP 216.73.216.36, am 22.01.2026, 23:11:18. © Urheberrechtlich geschützter Inhalt. Ohne gesonderte Erlaubnis ist jede urheberrechtliche Nutzung untersagt, insbesondere die Nutzung des Inhalts im Zusammenhang mit, für oder in KI-Systemen, KI-Modellen oder Generativen Sprachmodellen.

we need to recalibrate what is truly secret."[20] Bis dies erreicht wird, darf eine differenzierte, informierte Diskussion der Frage aber nicht ausgeschlossen sein. Vor allem analytisch-konzeptionelle Fragen können und müssen bereits vorher erörtert werden, um im Falle einer entsprechenden Entwicklung nicht vollkommen überrascht zu werden. Eine Debatte scheint daher durchaus weiterhin sinnvoll und sollte nicht als überzogene Panikmache abgetan werden, auch wenn eine konkrete Gefährdung derzeit noch nicht zu erkennen ist.

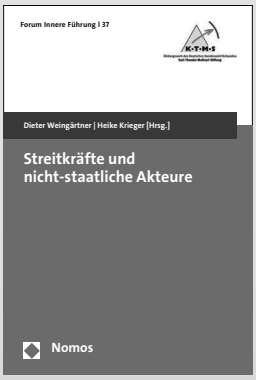
Die mitunter in diese Diskussion geäußerte Vermutung, dass eine Austragung von Auseinandersetzungen im schadensfreien oder schadensarmen Cyberraum als positives Ventil zur Reduzierung von Eskalationsrisiken dienen kann, erscheint dabei weit hergeholt. Zum einen setzt dies voraus, dass der Konflikt auf die nicht alltagsnotwendigen Netze beschränkt bleibt oder keine gravierenden Schäden außerhalb dieser anrichtet, zum anderen wird die psychologische Wirkung eines als Angriffs perzipierten und eingestuften Ereignisses als erstaunlich gering bewertet. Gerade Letzteres kann jedoch leicht auch als Einschränkung der Handlungsfähigkeit und damit als Angriff auf die Souveränität eines Staates verstanden werden und somit erst recht eine Eskalation heraufbeschwören, vor allem, wenn der angegriffene Staat nicht mit gleicher Münze zurückzahlen kann.

4. Bewertung

Grundsätzlich gilt für alle Cyberattacken mit gewaltgleichen Konsequenzen die Feststellung des ehemaligen Direktors des "U.S. National Economic Council", Stephen Friedman, der anlässlich der Übung "Cyber Shockwave" 2010 feststellte: "[…] this is a predictable surprise and we need to get our act together."[21] Für einen reinen Cyberkrieg als eine auf den Cyberspace beschränkte, gewalttätige Konfliktaustragung, die das Niveau eines Krieges erreicht, ergibt sich insgesamt das Bild eines langfristig möglichen, aber wenig wahrscheinlichen Ereignisses: ein klassisches „high impact, low probability event". Dies darf jedoch nicht darüber hinwegtäuschen, dass es nicht unmöglich ist und für eine zukünftig noch stärker vernetzte Gesellschaft erhebliche Schäden und Folgewirkungen entstehen könnten. Wie oben beschrieben, werden die Unterbrechung, Störung oder Lähmung von rechnergesteuerten Systemen wie Kommunikations- und Stromnetzen von Experten als schwierige, aber reale Möglichkeit eingeschätzt. Ein entsprechender längerer Ausfall von im Alltag essentiellen und häufig nicht redundanten Diensten würde mit hoher Wahrscheinlichkeit erhebliche wirtschaftliche und finanzielle Verluste, aber auch Personenschäden nach sich ziehen. Zahlreiche Staaten streben schon heute nach der Fähigkeit zu solchen Angriffen, auch unter Einbeziehung ziviler Firmen, sodass eine Verbreitung entsprechenden Wissens auch außerhalb der eher kleinen militärischen Zirkel zu erwarten ist. Der Rückgriff auf relativ kurze, begrenzte Cyberangriffe mit signifikanten Schäden in der realen Welt als Präventivschläge oder Kontrahenten lähmende „limited wars" sollte daher vor allem als zukünftig mögliche Bedrohung durchaus ernst genommen werden. Der Begriff Krieg muss dabei losgelöst von seiner rein militärischen Seite der Kriegführung politisch gedacht werden – im Sinne von Clausewitz als gewaltsame Durchsetzung des Willens der Beteiligten.

Zwar ist es richtig, dass es bisher keinen Cyberkrieg gegeben hat und Alarmismus nicht hilfreich ist. Staatliche Sicherheitsvorsorge hat aber eine solche Möglichkeit trotzdem in Betracht zu ziehen und Vorkehrungen zu treffen. Diese könnten vielfältiger Natur sein und primär defensiven völkerrechtlichen, diplomatischen oder organisatorischen Charakter haben. Eine öffentlichkeitswirksame Verneinung der Möglichkeit eines Cyberkrieges ohne Prüfung aller theoretisch möglichen Szenarien ist aber wenig sinnvoll, gaukelt dies doch eine nicht gegebene vollkommene Sicherheit vor. Lässt man sich auf diesen kategorischen Ausschluss ein, wird der erste substanziell schädigende oder lähmende Cyberangriff tatsächlich eine Überraschung sein, die hätte vorhergesehen werden können.

Militärforschung



Streitkräfte und nicht-staatliche Akteure
Herausgegeben von Dieter Weingärtner und Heike Krieger
2013, 215 S., brosch., 44,– €
ISBN 978-3-8487-0377-7
(Forum Innere Führung, Bd. 37)

Nicht-staatliche Akteure spielen im militärischen Bereich eine immer größere Rolle. Dies gilt für den bewaffneten Konflikt ebenso wie für den rein innerstaatlichen Bereich. Sie stehen Streitkräften als Gegner oder als Partner gegenüber. Für die Bundeswehr ergeben sich daraus zahlreiche Fragen des internationalen und nationalen Rechts.

Bestellen Sie jetzt telefonisch unter 07221/2104-37.
Portofreie Buch-Bestellungen unter www.nomos-shop.de/20958
Nomos

20 Hayden, Michael: The Future of Things "Cyber", in: Strategic Studies Quarterly, Vol. 3 (2011), S. 5, URL: http://www.au.af.mil/au/ssq/2011/spring/hayden.pdf, letzter Zugriff 23.07.2012.

21 Bipartisan Policy Center: Cyber ShockWave Shows U.S. Unprepared For Cyber Threats, 17.02.2000, URL: http://bipartisanpolicy.org/news/press-releases/2010/02/cyber-shockwave-shows-us-unprepared-cyber-threats, letzter Zugriff 08.08.2012.

https://doi.org/10.5771/0175-274x-2013-3-170 - Generiert durch IP 216.73.216.36, am 22.01.2026, 23:11:18. © Urheberrechtlich geschützter Inhalt. Ohne gesonderte Erlaubnis ist jede urheberrechtliche Nutzung untersagt, insbesondere die Nutzung des Inhalts im Zusammenhang mit, für oder in KI-Systemen, KI-Modellen oder Generativen Sprachmodellen.