Schulze, Matthias

Research Report

Überschätzte Cyber-Abschreckung: Analyse der in der neuen US Cyber-Doktrin vorgesehenen Abschreckungspotenziale und Lehren für Deutschlands "aktive Cyberabwehr"

SWP-Aktuell, No. 39/2019

Provided in Cooperation with:
Stiftung Wissenschaft und Politik (SWP), German Institute for International and Security Affairs, Berlin

Suggested Citation: Schulze, Matthias (2019) : Überschätzte Cyber-Abschreckung: Analyse der in der neuen US Cyber-Doktrin vorgesehenen Abschreckungspotenziale und Lehren für Deutschlands "aktive Cyberabwehr", SWP-Aktuell, No. 39/2019, Stiftung Wissenschaft und Politik (SWP), Berlin, https://doi.org/10.18449/2019A39

This Version is available at:
https://hdl.handle.net/10419/255616

SWP-Aktuell
NR. 39 JULI 2019

Überschätzte Cyber-Abschreckung

Analyse der in der neuen US Cyber-Doktrin vorgesehenen Abschreckungspotenziale und Lehren für Deutschlands »aktive Cyberabwehr«

Matthias Schulze

Befürworter offensiver Cyber-Operationen argumentieren, dass sie abschreckend auf etwaige Cyber-Angreifer wirken könnten, da die Angreifer mit einem digitalen Gegenschlag rechnen müssten. Diese Vorstellung, die für die neue US Cyber-Doktrin von 2018 bestimmend war, schwingt implizit auch in der Debatte über digitale Gegenangriffe in Deutschland mit. Diesem Kalkül liegt jedoch eine verkürzte Vorstellung von Abschreckung zugrunde. Abschreckung per Androhung von Vergeltung funktioniert im digitalen Raum nach anderen Prinzipien als etwa nukleare Abschreckung. Probleme der Attribution, Demonstration, Kontrollierbarkeit und Glaubwürdigkeit digitaler Fähigkeiten erhöhen die Gefahr, dass Abschreckung scheitert. Daher wäre die deutsche Cyber-Sicherheitspolitik gut beraten, die defensive Cyber-Sicherheit und die Robustheit (Resilienz) von Systemen zu steigern.

In Deutschland wird seit mehreren Jahren über aktive Cyber-Abwehr oder »hack backs« diskutiert, die darauf ausgelegt sind, offensiv zu wirken. Gegnerische Netzwerke sollen demnach penetriert werden, um Angriffe in Echtzeit zu stoppen, Daten zu löschen oder Rechner zu deaktivieren. Implizit steckt in der Forderung nach aktiver Abwehr eine weitere Überlegung: Ein Cyber-Angreifer könnte von einem Angriff gegen Deutschland abgeschreckt werden, wenn ihm digitale Vergeltung qua »hack back« drohe. Mit einem ähnlichen Argument wurde auch der Aufbau des Bundeswehr-Kommandos Cyber- und Informationsraum begründet. Bislang wurde aber für die deutsche Cyber-Sicherheitspolitik nicht analysiert, ob digitale Gegenangriffe überhaupt zur Abschreckung taugen.

Abschreckung

Abschreckung ist der potenzielle Gebrauch von Gewalt bzw. deren Androhung, um einen bestimmten Zweck zu erreichen. Abschreckung beruht auf dem Kalkül, dass das Angriffsverhalten (X) eines Angreifers (A) dadurch verändert werden kann, dass der Verteidiger (V) ihm negative Konsequenzen (Y) androht. Die logische Formel der Abschreckung lautet: Tue X nicht, weil sonst Konsequenzen Y drohen. Die Kosten von Y müssen schwerer wiegen als die Ge-

Stiftung Wissenschaft und Politik
Deutsches Institut für Internationale Politik und Sicherheit

winne, die bei einem Angriff X zu erwarten sind. Diese Form der Abschreckung enthält also immer ein Element des Zwangs und wird daher »deterrence by punishment« genannt. Sie unterscheidet sich von »deterrence by denial«, die darauf abzielt, durch bessere Härtung von Systemen und Resilienz die Kosten für Angriffe so in die Höhe zu treiben, dass diese nicht mehr lohnend erscheinen. Wenn nicht anders deklariert, ist im Folgenden immer Abschreckung durch Vergeltungsandrohung gemeint.

Damit Abschreckung funktionieren kann, müssen mindestens drei Bedingungen erfüllt sein:

1) die Konsequenzandrohung muss klar kommuniziert und für alle Parteien verständlich sein (»signaling«).
2) Beide Akteure müssen möglichst vollständige Informationen über die Fähigkeiten, Intentionen und am besten die Gedankenwelt des Gegenübers haben, um Kosten und Nutzen rational abschätzen zu können.
3) Die Konsequenzandrohung muss glaubhaft sein, also technisch durchführbar und im Dienste eines politischen Willens.

Erfolgreiche Abschreckung setzt also voraus, dass die Androhung eines Schadens vernehmlich und klar und vor allem glaubhaft kommuniziert wird.

Abschreckung gilt als erfolgreich, wenn A eine Handlung *nicht* ausführt. Die Kausalität eines Nicht-Ereignisses lässt sich logisch nicht überprüfen. Man kann nie genau sagen, ob es die Gewaltandrohung war, die zur Verhaltensänderung führte, oder ob es dafür andere Gründe gab. Einige halten Abschreckung daher für einen Mythos.

Abschreckung basiert auf der »Rational Choice«-Theorie. Dabei gilt die Annahme, dass Akteure Kosten und Nutzen ihrer Handlung abwägen und rational die weniger kostspielige Handlungsoption auswählen. Daran wird kritisiert, dass Akteure niemals sämtliche objektiven Informationen haben und die Konsequenzen ihrer Handlungen darum nie vollständig abschätzen können. Ferner handeln sie oft irrational, oder nach Normen oder Gewohnheiten. Abschreckung wirkt nur im Kopf des Angreifers, in den man nicht hineinsehen kann. Sie ist also letztlich ein Ratespiel: »Ich glaube, dass du glaubst, dass ich glaube« und so weiter. Das logische Problem aller Abschreckungstheorien ist, dass man nie wissen kann, ob Abschreckung tatsächlich wirkt. Das ändert sich erst in dem Moment, in dem sie versagt.

Cyber-Abschreckung

Die Übertragung der Abschreckungsstrategie auf den digitalen Raum wird von Cyber-Sicherheitsforschern als problematisch bewertet. Im Kalten Krieg galten andere Rahmenbedingungen, nukleare Abschreckung folgt zudem eigenen Prinzipien. In der bipolaren Welt des Kalten Krieges war Abschreckung symmetrisch und wurde von ungefähr gleich starken Akteuren praktiziert, die ihre Motive hinreichend gut einschätzen konnten. Cyber-Abschreckung ist multipolar und findet zwischen asymmetrischen Opponenten statt. Insofern kann Cyber-Abschreckung leichter versagen und ist somit keine verlässliche Politikoption.

Attributionsproblem

Erfolgreiche Attribution ist die wichtigste Vorbedingung für Abschreckung, da sie einer Schadensandrohung Legitimität und strategisches Gewicht verleiht. Oftmals ist aber nicht klar, wer hinter Cyber-Vorfällen steckt. Folglich lässt sich auch niemand identifizieren, dem Schaden angedroht werden kann. Das Attributionsproblem beschreibt die Schwierigkeit, Cyber-Angriffe einem Akteur zuzuordnen, der seine Absicht zuvor nicht kommuniziert hat und kein Bekennerschreiben hinterlässt.

Dabei betrifft das Attributionsproblem beide Seiten: Wenn A V digital angreift, weiß V nicht automatisch, dass es A war. Wenn V zu einem digitalen Gegenschlag ansetzt, weiß wiederum A nicht notwendigerweise, dass es V war. Es gibt im digitalen Raum kaum ein Ziel, das nur von einem Akteur angegriffen wird. Fehl-

wahrnehmungen sind daher an der Tagesordnung. Ferner besteht das Risiko, dass Angreifer unter falscher Flagge agieren oder behaupten, für Angriffe verantwortlich zu sein, die sie gar nicht ausgeführt haben. In sich zuspitzenden geopolitischen Konfliktsituationen wird die Rolle des Attributionsproblems jedoch überschätzt. Wenn zum Beispiel in Südkorea im Zuge einer Episode im Konflikt mit Nordkorea Server geflutet werden, fällt eine Antwort auf die Frage, wem das nutzt (»cui bono«), weniger schwer als bei verdeckten Spionageoperationen. Für effektive Abschreckung muss Attribution allerdings unanfechtbar, genau und unmittelbar erfolgen. Je mehr Zeit zwischen Vorfall und Attribution vergeht, desto weniger legitim ist eine Gegenreaktion des Angegriffenen.

Demonstrationsproblem

Damit A eine Schadensandrohung als glaubhaft bewerten kann, muss ihm das Schadenspotenzial eines zu erwartenden Gegenangriffs bekannt sein. Aus diesem Grund werden auf Militärparaden Waffen vor aller Welt zur Schau gestellt. Dieses Transparenzprinzip funktioniert aber bei Cyber-Fähigkeiten nicht ohne weiteres. Die Demonstration einer Cyber-Fähigkeit aus Gründen der Schadensandrohung führt oftmals zum Verlust dieser Wirkung. Offensive Cyber-Fähigkeiten folgen dem Gesetz des sinkenden Ertrags: Jede Verwendung einer Fähigkeit führt dazu, dass sie in Zukunft weniger wirksam ist.

Ein niedrigschwelliger »Distributed Denial of Service (DDoS)«-Angriff mag beim ersten Mal erfolgreich sein. Wenn der Angegriffene aber weiß, dass ein erneuter Gegenschlag droht, kann er vorsorglich kritische Systeme vom Netz nehmen oder den schädlichen Netzwerkverkehr umleiten. Daher taugen DDoS-Angriffe nur begrenzt zur Konsequenzandrohung. Bei 0-Day-Kapazitäten, Angriffen also, die auf unbekannten und daher nicht behobenen Sicherheitslücken basieren, existiert das gleiche Problem. Je häufiger sie eingesetzt werden, desto größer ist die Wahrscheinlichkeit, dass sie enttarnt und somit aller Welt zur Verfügung gestellt werden. Mit einem Patch der Sicherheitslücke verliert die Fähigkeit ihre Wirksamkeit.

Das hat zwei Implikationen: 0-Day-Fähigkeiten können nicht glaubhaft demonstriert werden, ohne ihre Wirksamkeit zu gefährden. Sie taugen also nur bedingt zur Gewaltandrohung. Die Ausnahme wäre, wenn ein Angreifer über mehrere verdeckte Punkte für einen Zugriff auf ein gegnerisches System verfügt. Dann ließen sich 0-Day-Angriffe zum »signaling« nutzen. Zweitens kann ein Verteidiger eine veröffentlichte 0-Day-Fähigkeit umbauen und gegen den Angreifer richten.

Proportionalität und Angemessenheit von Gegenschlägen

Abschreckung versagt, wenn die Gewaltandrohung als nicht glaubhaft bewertet wird und in der Folge Waffen eingesetzt werden. Dabei stellen sich Fragen nach der Proportionalität, Effektivität und Zielgenauigkeit offensiver Cyber-Gegenschlagskapazitäten. Wie viel objektiver Schaden muss zugefügt werden, damit A die Kosten eines weiteren offensiven Vorgehens als zu hoch einstuft? Woher weiß V, ob A die Bedrohung bestimmter Ziele als besonders schmerzhaft erachtet oder eben nicht. A und V haben dazu unterschiedliche Wahrnehmungen. Es herrscht kein internationaler Konsens darüber, wie eine proportionale Gegenreaktion aussehen könnte. Insofern besteht die Gefahr, dass das Eskalationsrisiko steigt.

Der Schaden, der durch einen Gegenschlag zugefügt wird, muss angemessen sein. Ist der von V angedrohte Schaden zu groß, steigt die Wahrscheinlichkeit eines erneuten Gegenschlags durch A. In der Politikwissenschaft ist gut erforscht, dass der Einsatz offensiver Mittel zur Vergeltung in der Regel Eskalationsspiralen in Gang setzt, wenn er als unangemessen wahrgenommen wird. Damit wäre Abschreckung gescheitert. Ist der angedrohte Schaden zu gering und somit nicht glaubhaft, wirkt Abschreckung ebenfalls nicht und schlägt wieder-

um fehl. Das genaue Maß zu bestimmen ist hochgradig komplex und auch eine Funktion des Attributionsproblems: Je geringer die Chance ist, erwischt zu werden, desto größer muss der von V angedrohte Schaden sein, wenn A davon überzeugt werden soll, dass ein Angriff die potenziellen Kosten nicht wert ist.

Fehlende Kontrollierbarkeit

Die Schadenswirkung von Cyber-Fähigkeiten ist sehr unzuverlässig und nur bedingt zu kontrollieren. Es ist schwierig, Cyber-Fähigkeiten auf ein Ziel zu beschränken und Kollateraleffekte — etwa in unbeteiligten Drittstaaten — zu vermeiden. Das gilt insbesondere in zeitkritischen Situationen. Die Effektivität und somit das genaue Schadenspotenzial von Cyber-Fähigkeiten lassen sich im Vorfeld oft nur schwer bestimmen. Die Schadenswirkung wird maßgeblich durch die Konfiguration des Zielsystems bestimmt. Insofern ist es häufig nicht möglich, zu antizipieren, wie lange etwa ein Cyber-Gegenangriff ein System lahmlegen kann.

Die große Ungewissheit über die Schadenswirkung von Cyber-Fähigkeiten erschwert deren proportionalen und kontrollierten Einsatz. Dadurch steigt das Risiko von Abschreckungsversagen. Auch Angriffe wie Stuxnet (2010), die mit hohem Aufwand für bestimmte Ziele maßgeschneidert wurden, schossen über das Ziel hinaus. Kollateraleffekte wie bei WannaCry oder NotPetya (beide 2017) sind in Cyber-Konflikten die Normalität. Denn niemand vermag realistisch abzuschätzen, wo bestimmte Systemkonfigurationen noch zum Einsatz kommen.

Andererseits können Schäden wiederum zu präzise kalkuliert werden. Wenn sich zum Beispiel V anschickt, einen Cyber-Angriff auf einen Staudamm durch A mit einem Vergeltungsschlag auf einen Damm von A zu beantworten, kann A diesen vorsorglich vom Netz nehmen. Es ist schwierig, das richtige Maß für eine Schadensandrohung zu finden, die weder zu präzise noch zu vage ist, zumal die Gefahr eines Abschreckungsversagens groß ist. Zudem steigt in asymmetrischen Kontexten und aufgrund fehlender Kontrollierbarkeit das Eskalationsrisiko. Das lässt Cyber-Fähigkeiten ungeeignet zur Abschreckung erscheinen.

Hoch- und niedrigschwellige Abschreckung

International gibt es keinen Konsens darüber, welche Cyber-Aktivitäten abschreckungswürdig sind (politische vs. wirtschaftliche Spionage vs. Sabotage). Je nach Intensität der Aktivitäten sind die Erfolgschancen für Abschreckung unterschiedlich groß. Bei hochschwelliger Abschreckung werden gravierende Aktionen unterlassen, etwa der physische Gewalteinsatz oder Cyber-Angriffe auf kritische Infrastrukturen, weil die Kosten als zu scherwiegend bewertet werden. Hierzu gehört das »worst-case«-Szenario eines digitalen Überraschungsangriffs auf strategische Infrastrukturen, bei dem Menschen sterben und hochgradige physische Zerstörung die Folge ist (»digitales Pearl Harbor«). Ein solches Ereignis hat es in der mehr als dreißigjährigen Geschichte von Cyber-Konflikten noch nie gegeben. Der Grund ist, dass dessen Folgen kaum zu bemessen wären und ein Angreifer mit Rückschlagseffekten zu rechnen hätte.

Erstens würde ein solcher Angriff als Gewaltakt nach internationalem Recht bewertet werden und zum Beispiel Akte der (kollektiven) Verteidigung legitimieren. Ein derartiger Cyber-Angriff würde also vermutlich in einen physischen Konflikt eskalieren, weshalb Staaten in Friedenszeiten davon absehen. Zweitens lässt sich aufgrund der interdependenten und hochgradig vernetzten Internetinfrastruktur nicht zuverlässig garantieren, dass eigene Systeme nicht ebenso betroffen wären. Angesichts dessen haben Staaten kein Interesse daran, solche strategischen Angriffe auszuführen, wenn damit nicht wirklich etwas politisch zu gewinnen wäre. Hier ist eine implizite Norm der Zurückhaltung wirksam, die in verschiedenen internationalen Gremien zu bemerken ist. Abschreckung kann denn auch durch Normen funktionieren, die unangemessenes Verhalten tabuisieren.

Diese Zurückhaltung existiert aber nicht bei niedrigschwelligen Vorfällen, bei denen es nicht zu einem bewaffneten Angriff kommt. Staaten gestalten ihre Cyber-Aktivitäten bewusst so, dass sie unterhalb dieser Schwelle bleiben und insofern nicht eskalierend wirken. In diese Kategorie gehören Cyber-Spionage, hybride Maßnahmen, Cyber-Kriminalität, Hacktivismus und Vandalismus, die einen Großteil aller Cyber-Aktivitäten ausmachen. Es gilt als unwahrscheinlich, dass Abschreckung bei niedrigschwelligen Vorfällen wirkt, etwa bei Spionage. Die Chance, ungeschoren davonzukommen, ist groß, zumal Staaten an einer Sanktionierung nicht interessiert sind, weil sie selber spionieren.

Nichtstaatliche Akteure

Niedrigschwellige Handlungen begehen auch nichtstaatliche Akteure. Anders als im nuklearen Zeitalter besitzen auch sie offensive Cyber-Fähigkeiten. Das Spektrum der Akteure reicht von Script-Kiddies mit geringen Fähigkeiten über Cyber-Kriminelle mit mittleren Fähigkeiten bis hin zu Cyber-Söldnern mit erheblichen Fähigkeiten. Zudem gibt es sogenannte Proxy-Akteure, die zum Teil unabhängig, zum Teil im Staatsauftrag Ziele angreifen.

Abschreckung funktioniert nur, wenn Motivation, Interessen, Fähigkeiten und die Kontaktadresse der Opponenten bekannt sind. Bei den zahlreichen nichtstaatlichen »fortgeschrittenen andauernden Bedrohungen« (Advanced Persistent Threats) fehlt ein Großteil dieser Informationen. Darum lassen sie sich nicht effektiv abschrecken. Theoretisch müsste eine wirkungsvolle Abschreckungspolitik für jeden Einzelnen unter den Tausenden Cyber-Akteuren maßgeschneidert werden. Das ist selbst großen Cyber-Mächten unmöglich.

Aus der Terrorismusforschung ist bekannt, dass Abschreckung durch Vergeltung wenn überhaupt nur gegen Staaten funktioniert, nicht aber gegen nichtstaatliche Akteure. Bei ihnen ist der gegenteilige Effekt zu beobachten: Die Anwendung repressiver Gewalt mit dem Ziel, Terror zu bekämpfen, führt aufgrund der wahrgenommenen Ungerechtigkeiten oft zu mehr Terrorismus. Gleiches lässt sich im digitalen Raum beobachten. Nicht einmal offensiv-dominante Staaten wie die USA sind in der Lage, Cyber-Angriffe nichtstaatlicher bzw. staatlicher Akteure wie Russland oder China abzuschrecken. Abschreckung nichtstaatlicher Akteure folgt eher der Logik kriminologischer Abschreckung, bei der es darum geht, die Frequenz und Intensität von Vorfällen zu reduzieren, ohne sie jedoch gänzlich verhindern zu können. Angesichts der Vielzahl nichtstaatlicher Akteure ist die Gefahr groß, dass sie nicht nach rationalen Prinzipien handeln, nach denen Staaten agieren würden. Bei Hackern etwa dominieren nicht notwendigerweise rationale Handlungsmotive, sondern auch kognitive und normative, etwa der Wunsch, Ruhm zu erlangen und Spaß zu haben (»Lulz«).

Glaubwürdigkeit und Eskalation

Eine Vergeltungsandrohung muss nicht nur eine möglichst genaue Schätzung der zu erwartenden Kosten bei A induzieren, sie muss auch glaubhaft sein. Wenn A nicht glaubt, dass V, erstens, technisch in der Lage ist, mit digitalen Mitteln genau bemessene Kosten zu verursachen, oder, zweitens, politisch nicht willens ist, die Gefahr einer Eskalation einzugehen, versagt Abschreckung.

Das Glaubwürdigkeitsproblem ist bei Cyber-Konflikten noch größer. Intentionen und politischer Wille sind oftmals unklar, da ein Großteil staatlicher Cyber-Aktivität von Nachrichtendiensten betrieben wird und unter Cyber-Spionage fällt, mit anderen Worten verborgen ist. Das Eindringen in Systeme zu Zwecken der Spionage oder Sabotage kann nicht eindeutig unterschieden werden, so dass hier die Gefahr der Fehlwahrnehmung steigt. Staaten sind außerstande, ihre relative Cyber-Macht objektiv einzuschätzen. Für Abschreckung im Sinne des »Rational Choice«-Ansatzes sind möglichst vollständige Informationen nötig, zu denen auch die Einschätzung relativer Stärke gehört. Dies scheitert an

dem Umstand der Geheimhaltung sowie an der »dual-use«-Natur von Cyber-Fähigkeiten, die sich für offensive und für defensive Zwecke nutzen lassen.

Auch sind nicht alle Staaten politisch dazu bereit, sich auf eine »tit for tat«-Eskalationsdynamik gegenseitiger Vergeltungsschläge einzulassen. Solche Auseinandersetzungen werden in der Spieltheorie als »chicken game« bezeichnet: Im klassischen Szenario rasen zwei Akteure direkt mit dem Auto aufeinander zu; derjenige, der zuerst ausweicht, ist das »chicken«, der Feigling. In Demokratien unterstützt die Wahlbevölkerung aggressive Außenpolitik in der Regel nicht. Daher hat die Exekutive oft weniger Spielraum, glaubhaft Schaden anzudrohen. Glaubhaftigkeit hängt allerdings auch von vergangenen Entscheidungen und der Reputation einer Regierung ab. Wenn diese in der Vergangenheit zögerlich auf Aggressionen reagiert hat, sind künftige Schadensandrohungen weniger glaubhaft.

Das Problem bei der schrittweisen Eskalation im Cyberspace ist, dass der Schaden des Vergeltungsangriffs etwas höher sein muss als der des vorausgegangenen Angriffs. Da es schwierig ist, die Proportionalität zu bestimmen, drohen Kollateraleffekte. Unklar ist, wie Eskalationsdynamiken im Cyberspace funktionieren, ob beispielsweise mit digitalen Mitteln eine ähnliche Eskalationsstufe erreicht werden kann wie mit physischen Waffen. Einige Kommentatoren argumentieren, dass digitale Mittel eher eskalationsbegrenzend wirken, weil physische Effekte schwer zu erzeugen sind und das Schadenspotenzial insofern begrenzter ist. Empirisch betrachtet ist Eskalation das wahrscheinlichste Ergebnis einer Abschreckungspolitik, die auf den Einsatz offensiver Cyber-Mittel setzt.

Abschreckung und »persistent engagement« in den USA

Der Mechanismus der Abschreckung lässt sich also nicht ohne weiteres auf den digitalen Raum übertragen. Falken und Akteure nationaler Sicherheitspolitik sind jedoch anderer Meinung und glauben daran, dass die Aufbietung starker offensiver Mittel im Zweifelsfall auch viel hilft. Sie plädieren für eine verstärkte Offensive. Obwohl die USA eine formidable Cyber-Macht sind, konnten sie Russland nicht davon abschrecken, mit Cyber-Fähigkeiten Einfluss auf die US-Präsidentschaftswahl 2016 zu nehmen. Als Reaktion auf dieses Versagen stellte das Pentagon 2018 eine neue Cyber-Doktrin vor. Diese enthält neuartige Konzepte wie »defending forward«, »persistent engagement« und »preparation of the battlefield«. Die Doktrin gibt dem US Cybercommand einen größeren Spielraum für offensives Handeln, für das keine Autorisierung des Präsidenten mehr erforderlich ist.

Vorwärtsverteidigung (»defending forward«) bedeutet, dass Netzwerke nicht mehr im eigenen Umfeld oder Territorium verteidigt werden, sondern auf Systemen potenzieller Angreifer, und das weltweit. Auf diesen Systemen sollen in erster Linie nachrichtendienstliche Erkenntnisse gewonnen werden, um Angriffe frühzeitig zu detektieren.

»Persistent engagement« meint, gegnerische Cyber-Angreifer dadurch zu binden und zu beschäftigen, dass sie permanent Angriffen amerikanischer Hacker ausgesetzt werden. Gegner sollen ständig amerikanische Eindringversuche abwehren müssen, damit ihnen — so die Theorie — keine Ressourcen mehr für eigene Offensiven bleiben. Da kein anderer Staat über ähnlich große personelle Ressourcen verfüge wie die USA, sollen auf diese Weise die Kosten für Angreifer steigen. In der Doktrin werden eindeutig China und Russland als potenzielle Ziele dieser Maßnahmen genannt.

Die dritte Maßnahme, die in der Doktrin vorgesehen ist, wird mit konkreten Abschreckungseffekten begründet: »die Vorbereitung des Schachtfelds« (»preparation of the battlefield«). Gegnerische Netzwerke sollen penetriert werden, um darin sogenannte Hintertüren oder Logikbomben zu implantieren, die sich in künftigen Konflikten ausnutzen lassen. Eine Logikbombe ist eine Schadsoftware, die unerkannt in einem Netzwerk lauert, bis sie

zu einem späteren Zeitpunkt aktiviert wird. Damit wäre ein konkreter Schaden angedroht. Ein Gegner müsste sich dann stets fragen, ob er alle Angriffsvektoren der Amerikaner enttarnt und eine verborgene Hintertür im eigenen Netzwerk übersehen hat. Die Verfasser der Doktrin hegen die Hoffnung, dass Angreifer in Anbetracht dieser Unsicherheit von schwerwiegenden Offensiven absehen, etwa gegen kritische Infrastrukturen. Russland reagierte jüngst ungehalten auf die Versuche amerikanischer Hacker, in russische Stromkraftwerke einzudringen, um dort Hintertüren zu platzieren. Der Kreml warnte zudem vor einer Eskalation im Cyber-Bereich. Dies ist ein Indiz dafür, dass die neue Cyber-Doktrin der USA, die noch offensiver ausgerichtet ist als ihre Vorgängerin, Eskalationen befeuert.

»Persistent engagement« fand im Zuge der Midterm Elections 2018 statt: Ein zentraler Hub niedrigschwelliger russischer Cyber-Aktivität, die Trollfabrik Internet Research Agency in St. Petersburg, wurde temporär lahmgelegt. Allerdings nahm diese kurz danach wieder ihre Tätigkeit auf. Taktisch mag die Operation ein Erfolg gewesen sein. Ob diese Form der Abschreckung aber strategisch, also langfristig wirkt, kann bezweifelt werden. Es steht zu befürchten, dass andere Cyber-Mächte nun ebenfalls in größerem Maße in die Offensive investieren und mehr Personal ausbilden, um dem »persistent engagement« standzuhalten.

Das Resultat wäre ein verschärfter Rüstungswettlauf mit dem Ziel, stets mehr Cyber-Kräfte mobilisieren zu können als der Rivale. Die in der Doktrin vorgesehenen Mittel wirken vermutlich kaum gegen mehr als eine Handvoll Opponenten gleichzeitig. Niedrigschwellig agierende Angreifer lassen sich damit auch nicht stoppen.

Wenn alle Cyber-Mächte eine solche Doktrin verfolgen würden und damit anfingen, überall Hintertüren zu platzieren, wäre der globale Cyber-Space hochgradig volatil. Hintertüren sind nicht exklusiv und können potenziell von jedem kundigen Angreifer ausgenutzt werden. Die Kosten einer offensiven Politik wären vermutlich höher als der theoretische Zugewinn an Sicherheit. Die neue Doktrin geht somit weit über das Konzept der »aktiven Cyber-Abwehr« der Obama-Ära hinaus. Dieses sah vor, auf Cyber-Angriffe offensiv zu reagieren, aber eben nur, um diese an der Quelle zu stoppen. Das ist auch das Konzept, über das die deutsche Bundesregierung gegenwärtig in einer modifizierten Form nachdenkt.

Abschreckung durch deutsche Cyber-Fähigkeiten?

Ob der bloße Besitz deutscher Cyber-Offensivfähigkeiten abschreckende Wirkung hätte, ist zu bezweifeln. Neben all den zuvor geschilderten Problemen der Attribution, der Demonstration, der Proportionalität und Kontrollierbarkeit digitaler Gegenreaktionen fällt es schwer zu glauben, dass Deutschland bereit wäre, in eine Eskalationsdynamik im Cyber-Raum einzutreten. Die Kultur der Zurückhaltung in der Außen- und Sicherheitspolitik ist nach wie vor stark ausgeprägt. Die Bevölkerung steht einer aktiveren Außenpolitik bzw. der Übernahme größerer Verantwortung kritisch gegenüber. Das gilt insbesondere, wenn es dabei zum Gewalteinsatz kommt, ob nun digital oder physisch.

Deutschland hätte hier also vermutlich ein Glaubwürdigkeitsproblem. Ein starker Opponent würde testen wollen, ob Deutschland politisch bereit ist, zur Abschreckung aktive Cyber-Abwehrmittel einzusetzen und die Konsequenzen einer Eskalation zu ertragen. Bisher fehlt in Deutschland eine politische Strategie, wie mit einer solchen Situation umgegangen werden soll. Sie müsste für alle relevanten Cyber-Bedrohungen maßgeschneidert werden und die zuvor erwähnten Elemente von Bedrohungskommunikation ebenso enthalten wie Maßnahmen zur Bereitstellung proportionaler und wirkungsvoller Cyber-Reaktionsmittel. Außerdem müsste der politische Wille gegeben sein, diese Mittel trotz Gefahr der Eskalation einzusetzen. Ob dies dann auch wirken würde, lässt sich in Anbetracht der zahlreichen Probleme anzweifeln.

Solange diese Strategie aber nicht existiert, ist »deterrence by denial« für Deutschland die bessere Strategie. Diese Schlussfolgerung lässt sich aus den Defiziten der Abschreckung durch Vergeltung herleiten: Diese versagt auch deswegen, weil Ziele zu leicht angreifbar sind. Im Endeffekt ist es für den Angreifer daher immer kostengünstiger, Schwachstellen auszunutzen, als dies nicht zu tun.

Der erste Schritt in Richtung eines wirksamen Abschreckungssystems sollte also sein, die Cyber-Sicherheit und die Resilienz zu steigern, um Cyber-Angriffe kostspieliger zu machen.

Im zweiten Schritt sollten begleitende Maßnahmen der Außenpolitik ausgebaut werden. Es spricht vieles dafür, dass Abschreckung, wenn überhaupt, nur im Konzert mit anderen Maßnahmen funktioniert — im besten Fall im Rahmen eines internationalen Cyber-Regimes, das es aber noch nicht gibt. Dazu würden internationale Diplomatie, Abschreckung durch Normen oder durch internationale Verflechtung, aber auch durch Regime und Organisationen gehören, die staatliches Verhalten Regeln unterwerfen. Die Bemühungen der Cyber-Außenpolitik sollten in diese Richtung intensiviert werden.

Cyber-Konflikte sind weitgehend unreguliert, etablierte Normen für angemessenes Verhalten und rote Linien gibt es noch nicht. Auch deshalb ist das Risiko groß, dass Abschreckung versagt und eine Eskalationsdynamik auslöst. Deutschland sollte sich also überlegen, ob es sich an diesem Spiel beteiligen will und ob es bereit ist, etwaige negative Konsequenzen zu erdulden. Cyber-Sicherheit durch Resilienz ist jedenfalls die nachhaltigere Strategie, da sie gegen alle Akteure in gleicher Weise wirkt und nicht maßgeschneidert werden muss.

Fazit

Die Existenz offensiver Cyber-Fähigkeiten allein wirkt nicht abschreckend, insbesondere wenn nicht glaubhaft vermittelt wird, dass die Bereitschaft besteht, sie auch zu nutzen. Aber selbst dann gibt es genügend Fallstricke, die Abschreckung als ineffektives Politikkonzept erscheinen lassen, dem zu viele Risiken anhaften. Die Risiken des Abschreckungsversagens sind mannigfaltiger als in der analogen Welt. Abschreckung durch Gewaltandrohung ist mit hoher Wahrscheinlichkeit eine zum Scheitern verurteilte Strategie.

Wenn schon die risikofreudigeren Cyber-Nationen mit ihrer Cyber-Abschreckung scheitern, ist von einer deutschen Cyber-Abschreckungspolitik — aufgrund der traditionellen Zurückhaltung in der Außen- und Sicherheitspolitik — erst recht kein Erfolg zu erwarten. Solange Deutschland keine Eskalationsstrategie hat und nicht bereit ist, mögliche Konsequenzen einer offensiven Cyber-Abschreckungspolitik zu erdulden und die Bevölkerung darüber zu informieren, sollte davon abgesehen werden. Stattdessen sollte die deutsche Politik den Fokus weiterhin auf »deterrence by denial« legen: die Härtung von Systemen und den Aufbau von Resilienz.

Dr. Matthias Schulze ist Wissenschaftler in der Forschungsgruppe Sicherheitspolitik.

SWP
Stiftung Wissenschaft und Politik
Deutsches Institut für Internationale Politik und Sicherheit

Ludwigkirchplatz 3—4
10719 Berlin
Telefon +49 30 880 07-0
Fax +49 30 880 07-100
www.swp-berlin.org
swp@swp-berlin.org

ISSN 1611-6364
doi: 10.18449/2019A39