Schulze, Matthias

Research Report

Hacking back? Technische und politische Implikationen digitaler Gegenschläge

SWP-Aktuell, No. 59/2017

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

Suggested Citation: Schulze, Matthias (2017) : Hacking back? Technische und politische Implikationen digitaler Gegenschläge, SWP-Aktuell, No. 59/2017, Stiftung Wissenschaft und Politik (SWP), Berlin

This Version is available at:
https://hdl.handle.net/10419/255484

SWP-Aktuell

Stiftung
Wissenschaft und
Politik

Deutsches Institut
für Internationale
Politik und Sicherheit

Hacking back? Technische und politische Implikationen digitaler Gegenschläge

Matthias Schulze

Die Bundesregierung diskutiert derzeit die Frage, inwiefern von staatlicher Seite auf Cyber-Angriffe mit digitalen Gegenschlägen reagiert werden kann und soll. Befürworter solcher Maßnahmen argumentieren, der Staat müsse in der Lage sein, eine Cyber-Attacke durch Zerstörung des Ursprungsrechners zu beenden – vor allem in Krisensituationen, etwa wenn wichtige Infrastrukturen bedroht sind. Bei genauerer Betrachtung zeigt sich indes, dass Gegenangriffe problematisch sind. Erstens lässt sich in der Praxis nicht schnell genug ermitteln, wer der Verursacher einer Attacke ist. In zeitkritischen Situationen sind Gegenschläge mit großer Wahrscheinlichkeit wirkungslos. Zweitens ist unklar, zu welchen Ergebnissen schnelle Gegenangriffe führen. Und drittens stellen sich Fragen nach den globalen politischen Implikationen eines solchen Vorgehens.

An 23. Dezember 2015 gingen im ukrainischen Kyivoblenergo-Elektrizitätswerk für drei Stunden die Lichter aus. Der Stromausfall traf 225 000 Menschen; für den Vorfall wurde weithin Russland verantwortlich gemacht. Zum ersten Mal in der Geschichte hatte ein Cyber-Angriff so umfassende Folgen. Zwar sind großflächige Digital-Attacken auf kritische Infrastrukturen sehr selten, trotzdem dienen sie immer wieder als Argument dafür, staatliche Organe mit neuen Cyber-Fähigkeiten auszustatten. Vor allem Nachrichtendienste fordern entsprechende Angriffsmittel für sich, um Bedrohungen an der Quelle neutralisieren zu können. Dahinter steht die Annahme, passive Verteidigungssysteme wie Firewalls und Anti-Viren-Software seien wirkungslos gegen hochqualifizierte Angreifer (Advanced Persistent Threats). Lege etwa ein Rechner im Ausland deutsche Stromnetze lahm, müsse man ihn im Sinne eines »finalen Rettungsschusses« zerstören können. Staatliche Akteure wollen notfalls also zur Selbstverteidigung auf Cyber-Sabotage mit Gegenangriffen reagieren. So einleuchtend das Anliegen klingen mag, so schwierig wäre es in der Praxis umzusetzen. Nicht nur ist es gemäß Cybercrime-Konvention des Europarats (2001) illegal, unbefugt in digitale Systeme einzudringen; es ist als Krisenreaktionsmaßnahme auch technisch und politisch heikel.

Wie erkennt man einen Angriff?

Wer zurückschlagen will, muss wissen, dass er angegriffen wird. Anders als bei physischen Waffen gibt es bei Schadsoftware

Matthias Schulze ist Wissenschaftler in der Forschungsgruppe Sicherheitspolitik.

keinen direkten Zusammenhang zwischen Einsatz und Wirkung. Nicht jeder Cyber-Angriff produziert unmittelbar sichtbare Effekte; daher bleiben viele unerkannt. Manche *sollen* auch gar nicht erkannt werden. Dies gilt vor allem für komplexe Operationen von Nachrichtendiensten. 2010 etwa ließ »Stuxnet«, die bis dato destruktivste dokumentierte Schadsoftware, iranische Atomzentrifugen durchdrehen – und zunächst war unklar, ob es sich um technisches Versagen oder eine gezielte Störung handelte. Komplexe Cyber-Angriffe verfügen über Täuschungsmechanismen, so dass sie im technischen Idealfall gar nicht erkannt werden.

Die durchschnittliche Erkennungszeit für Netzwerk-Penetrationen liegt industrieweit zwischen 150 und 200 Tagen. Dieses große Zeitfenster macht digitale Gegenangriffe völkerrechtlich problematisch. Nach dem »Tallinn Manual«, das zwischenstaatliche Cyber-Operationen verrechtlicht, sind Gegenschläge zur Selbstverteidigung nach Artikel 51 der UN-Charta zulässig, sofern sie *unverzüglich* nach einem Angriff mit destruktiven physischen Effekten stattfinden. Ob ein Gegenschlag erlaubt ist, wenn er erst Monate später erfolgt, ist strittig und hängt vom Einzelfall ab. »Laute« Vorfälle, wie einfache »Distributed Denial of Service«-Attacken, produzieren zwar sofort sichtbare Effekte. Sie sind aber in der Regel besser durch passive Verteidigungsmaßnahmen zu stoppen – etwa sogenannte DNS-Umleitungen, das Aufstocken von Bandbreite oder das Blocken von IP-Adressen.

Wer ist der Urheber?

Das Erkennen eines Vorfalls reicht noch nicht aus, um einen Gegenschlag zu starten. Zunächst gilt es, den Urheber zu ermitteln. Dieser Prozess wird als Attribution bezeichnet; er ist aufgrund technischer Funktionen des Internets schwierig und oft langwierig, wenn auch nicht unmöglich. Attribution gleicht Detektivarbeit. Es bedarf dazu technischer Forensik und einer Analyse der betroffenen Systeme und des Schadcodes, sofern er gefunden werden kann. Handwerklich gute Cyber-Angriffe hinterlassen kaum Spuren. Sie erfolgen in der Regel über mehrere kompromittierte Rechner (oder Bots), die hintereinander geschaltet sind und oft in verschiedenen Ländern stehen. Betroffen sind dabei nicht selten die Rechner unbeteiligter Dritter, wie Krankenhaus-Computer oder Fahrkartenautomaten. Dadurch lässt sich der eigentliche Urheber eines Angriffs nur schwer identifizieren.

Allgemein gilt die Faustregel: Je mehr Zeit und Ressourcen für die Attribution zur Verfügung stehen, desto wahrscheinlicher kann man einen Urheber bestimmen. Umgekehrt gilt, je hastiger die Attribution erfolgt, desto mehr Fehler stellen sich ein und desto wahrscheinlicher ist, dass kein oder gar das falsche Ziel identifiziert wird. Cyber-Attacken unter falscher Flagge sind keine Seltenheit, wie ein Hacker-Angriff auf den französischen Fernsehsender TV5 Monde im April 2015 zeigte. Angesichts der Serie von Terroranschlägen im Land ging man zunächst von einem »Cyber-Kalifat« als Täter aus, bis sich Monate später eine Spur nach Russland fand. Viele Cyber-Operationen sind bis heute nicht eindeutig attribuiert, darunter etwa »Moonlight Maze«, eine mutmaßlich russische Spionagekampagne in den USA von 1998. Das bedeutet, dass sich in zeitkritischen Situationen, wie während eines laufenden Cyber-Angriffs, oft nicht rechtzeitig das richtige Ziel für einen Gegenangriff ermitteln lässt. Die Gefahr ist groß, dass man das falsche Ziel – womöglich einen Krankenhaus-Rechner – zerstört.

Sind Gegenangriffe effektiv?

Je kompetenter und vorsichtiger der Gegner, desto schwieriger ist die Attribution. Aber auch die besten Hacker machen Fehler, so dass es oft eine Indizienkette gibt, die auf eine bestimmte Gruppe deutet. Je qualifizierter der Gegner, desto schwieriger wird aber auch ein Gegenschlag, vor allem wenn dabei »aus der Hüfte geschossen« wird. Komplexe Cyber-Angriffe erfordern ein hohes Maß an Kenntnis des Zielsystems

und seines Einsatzkontexts. Solche Angriffe müssen in der Regel maßgeschneidert sein, um wirken zu können. Dazu muss man systemspezifische Schwachstellen kennen.

Stuxnet etwa war nur deshalb effektiv, weil seine Urheber genaue nachrichtendienstliche Informationen über die Steuerungssysteme der iranischen Zentrifugen hatten; daher konnten sie unbekannte Software-Schwachstellen (sogenannte Zero-Day-Sicherheitslücken) ausnutzen. Während der mehrjährigen und kostspieligen Entwicklung der Schadsoftware wurde sogar das Zielsystem simuliert, um die Wirkung von Stuxnet zu garantieren. Die ersten Versionen der Angriffssoftware wirkten nicht und führten zu Fehlschlägen. Hier zeigt sich ein grundsätzliches Problem von Cyber-Angriffen. Anders als dies etwa bei Artilleriebeschuss der Fall ist, lassen sich die destruktiven Effekte digitaler Attacken durch den Angreifer selbst nur schwer antizipieren. Der Störversuch kann wirkungslos sein, sobald auf Seiten des Angegriffenen auch nur eine einzige Schwachstelle behoben wurde. Vor allem für Schnellschüsse gilt: Je weniger Vorbereitungszeit es gibt, desto ungewisser ist das Ergebnis.

Kosten und Nutzen

Hinzu kommt ein weiteres Problem. Die Defensive ist der Offensive nicht so unterlegen, wie immer wieder behauptet wird. »Honey pots« (Honigtöpfe) etwa sind Systeme, die einem Angreifer vorgaukeln, attraktive Ziele zu sein. Wird dieser Honigtopf angegriffen, dokumentiert das System die Modalitäten des Vorgangs – so gewinnt es Kenntnisse über den Angriffsvektor, die verwendete Software und ausgenutzte Sicherheitslücken. Dieses Wissen wird dann genutzt, um die Verteidigung zu verbessern. Komplexe Cyber-Angriffe erfolgen nach dem Muster »use and lose«. Kennt der Verteidiger den Angriffsvektor und die genutzten Schwachstellen, kann er Letztere beheben, und der Angriff bleibt künftig wirkungslos. Bei schnellen Cyber-Gegenschlägen wiederum besteht die Gefahr, dass man dem Gegner ungewollt seine eigenen Angriffsfähigkeiten offenbart und so – oft kostspielige – Software verschwendet.

Gute Cyber-Verteidigung umfasst Resilienz und redundante Systeme. Aufschlussreich ist der Fall des 2016 ausgehobenen »Avalanche«-Botnetzes, das auch für Cyber-Angriffe verwendet wurde. Botnetze bestehen aus gehackten Computern, die koordiniert Befehle ausführen, etwa zur Verteilung von Spam. Avalanche war so programmiert, dass dynamisch ein anderer Steuerungsserver eingesprungen wäre, hätte ein Gegenschlag zum Ausfall des Kommandorechners geführt – der Angriff wäre also wirkungslos gewesen. Je schneller man reagiert, desto weniger weiß man um solche Eigenschaften des Gegners. Die Zerstörung von Zielcomputern kann überdies dazu führen, dass wichtige forensische Informationen auf diesen Systemen mitvernichtet werden. Aus Sicht der Strafverfolgung ist es daher sinnvoller, Steuerungsrechner von Cyber-Angriffen zu übernehmen, anstatt sie zu zerstören. Allerdings ist die Frage digitaler Evidenz angesichts einer steten Veränderbarkeit von Daten rechtlich ungeklärt.

Kollateralschäden und Eskalation

Es ist also nicht garantiert, dass Gegenschläge in Krisensituationen zum gewünschten Ergebnis führen. Aber selbst wenn sie wirken, kann es unintendierte Nebenfolgen geben. Zum einen besteht die Gefahr von Kaskaden-Effekten. Oft ist unklar, welche anderen Systeme vom Ziel des Gegenschlags abhängen, so dass sich hier Ausfälle potenzieren können. Militärische, öffentliche oder private Ziele lassen sich zudem kaum voneinander trennen.

Zum anderen kann es zu diplomatischen Verwerfungen kommen, wenn das Ziel des Gegenangriffs im Ausland liegt. Zwischenstaatliche Eskalationen sind aber kein Selbstläufer; es kommt auf die Art des Gegenschlags an. Je destruktiver er ist, desto wahrscheinlicher sind politische Konsequenzen. Es ist auch nicht unerheblich, ob ein Gegenangriff im Verborgenen oder

mit Ansage stattfindet. Gibt man einem politischen Antagonisten zu verstehen, dass man einen Cyber-Gegenschlag zur Selbstverteidigung plant, kann er sich darauf einstellen – was die Wirksamkeit der Reaktion zu mindern droht. Kündigt man den Gegenangriff nicht an, dürfte seine Wirkung größer ausfallen, vermutlich aber auch das diplomatische Störpotential, sofern die Attribution gelingt.

Problematische Lösungen

Generell zeigt sich folgendes Problem: Der Erfolg von Cyber-Gegenschlägen ist gerade dann besonders ungewiss, wenn diese politisch legitim erscheinen, nämlich im Fall von Selbstverteidigung während einer Krise. Welche Auswege gibt es? Vor allem Nachrichtendienste propagieren zwei problematische Lösungen.

Erstens kann die Zielgenauigkeit von Cyber-Gegenschlägen erhöht werden, wenn man Kenntnis über *alle* potentiellen Angreifer und deren Technologie hat. Daraus lässt sich ableiten, dass man Cyber-Arsenale anlegt, in denen maßgeschneiderte Angriffswerkzeuge für zuvor definierte Gegner, ob staatlich oder nichtstaatlich, auf Abruf lagern. Solche Instrumente basieren oft auf unbekannten Sicherheitslücken. Diese werden somit geheim gehalten und können nicht geschlossen werden. Da alle Akteure in einer vernetzten Welt ähnliche Hard- und Software nutzen, kann jede Sicherheitslücke – je nach Programm – Milliarden von Nutzern betreffen. Es macht also die globale IT-Infrastruktur unsicherer, wenn Angriffstools gehortet werden. Das gilt in umso stärkerem Maße, je mehr Akteure offensive Fähigkeiten entwickeln. Diese Gefahr ist keineswegs abstrakt. Wie jüngste Leaks zeigen, können solche Angriffswerkzeuge gestohlen und von Kriminellen umfunktioniert werden. Der Erpressungstrojaner »WannaCry« von Mai 2017 basierte auf einer Sicherheitslücke, welche die NSA jahrelang geheim gehalten hatte und die von einer Gruppe namens »Shadow Brokers« entwendet und veröffentlicht wurde.

Die zweite problematische Lösung besteht darin, gegnerische Netzwerke zu überwachen. So lassen sich potentielle Saboteure quasi an der Quelle beobachten. Nach unbestätigten Berichten gelang es der NSA, den Cyber-Angriff auf Sony Pictures von November 2014 zu attribuieren, weil man die Aktivitäten nordkoreanischer Hacker in Echtzeit verfolgte. Die Gefahr ist, dass es künftig mit defensiven Erfordernissen legitimiert wird, wenn Staaten offensiv in ausländische Regierungsnetzwerke eindringen – wie etwa beim digitalen Angriff auf den Bundestag von 2015, den vermutlich russische Hacker ausführten. Auch bei dieser Variante würde die globale IT-Infrastruktur insgesamt unsicherer werden.

Fazit

Das unbefugte Eindringen in fremde Rechner ist immer problematisch, weil darunter die Sicherheit des betroffenen Systems leidet. Je mehr Staaten digitale Gegenschläge ausführen, desto stärker ist die Cyber-Sicherheit aller betroffen. Da ein weltweites Verbot digitaler (Gegen-) Angriffe unrealistisch ist, sollte deren Einsatz zumindest reglementiert werden. Die Nutzung von »Hack back«-Fähigkeiten sollte als Ultima Ratio gelten und multilateral abgestimmt sein. Alleingänge und Schnellschüsse sind hier kontraproduktiv, denn es gibt viele Ungewissheiten. Allgemein sollte gelten, dass vor allem politisch heikle Gegenschläge von unabhängigen Stellen – parlamentarischen Kontrollgremien oder Richtern – legitimiert bzw. zumindest nachträglich mandatiert werden müssen. In den USA etwa muss der Präsident destruktive Cyber-Angriffe autorisieren, weil sie als kriegerischer Akt interpretiert werden können.

Für unmittelbare Gefahren gibt es alternative, defensive Möglichkeiten der Reaktion – so das Sperren der IP-Ranges, das Umleiten des Angreifers auf einen Honigtopf, das Abklemmen des eigenen Systems vom Netz oder die Nutzung redundanter Strukturen (Cyber-Resilienz). Langfristig sind diese Varianten zu bevorzugen.

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

Dieses Aktuell bietet die Zusammenfassung eines SWP-Arbeitspapiers von Thomas Reinhold (IFSH) und Matthias Schulze:

Digitale Gegenangriffe. Eine Analyse der technischen und politischen Implikationen von »hack backs«

Arbeitspapier der Forschungsgruppe Sicherheitspolitik, 2017/Nr. 1, August 2017