Arbeitspapier

Forschungsgruppe Sicherheitspolitik
Stiftung Wissenschaft und Politik
Deutsches Institut für Internationale
Politik und Sicherheit

Interdisziplinäre Forschungsgruppe Abrüstung,
Rüstungskontrolle und Risikotechnologien (IFAR)
Institut für Friedensforschung und Sicherheitspolitik
Universität Hamburg

Thomas Reinhold/Matthias Schulze

Digitale Gegenangriffe

Eine Analyse der technischen und politischen Implikationen von „hack backs“

FG03-AP Nr. 1
August 2017
Berlin

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

SWP-Arbeitspapiere sind Online-Veröffentlichungen der Forschungsgruppen. Sie durchlaufen kein förmliches Gutachterverfahren wie SWP-Studie, SWP-Aktuell und SWP-Zeitschriftenschau.

Matthias Schulze ist Wissenschaftler in der Forschungsgruppe Sicherheitspolitik an der SWP.

Thomas Reinhold ist non-resident fellow am Institut für Friedensforschung und Sicherheitspolitik an der Universität Hamburg.

Eine kürzere Form des Forschungspapiers ist unter dem Titel „Hacking back? Technische und politische Implikationen von digitalen Gegenschlägen“ als SWP-Aktuell erschienen.

Inhalt

Einleitung

Einer der zentralen Mythen des Cyberspace lautet, die Offensive habe gegenüber der Defensive die Oberhand.[1] Dieser Annahme zufolge muss ein Angreifer nur eine einzige Schwachstelle im IT-System seines Opfers finden, um auf das ganze System Zugriff zu haben, während letzterer sämtliche Schwachstellen kennen müsste, um seine Systeme ausreichend schützen zu können. Ein unachtsamer Mitarbeiter, der den fragwürdigen Anhang einer „phishing" Mail öffnet, reicht oftmals schon aus, um ein System lahmzulegen. Als Folge dessen wird argumentiert, dass passive Cybersicherheit, die vor allem auf Firewalls, Anti-Virensoftware und Intrusion Detection Systems basiert, offensiven Cyberoperationen von kenntnisreichen Akteuren, wie Advanced Persistent Threats (APT), unterlegen sei. APT-Gruppen betreiben enormen finanziellen und technischen Aufwand über größere Zeiträume hinweg, um in besonders attraktive Ziele, wie etwa Regierungssysteme, einzudringen und dabei passive Verteidigungsmechanismen zu umgehen. Angesichts der postulierten unzureichenden passiven Verteidigungsmöglichkeiten fordern immer mehr Stimmen, darunter insbesondere Militärs, Nachrichtendienste und private Sicherheitsfirmen, eine aktivere Verteidigung und beziehen sich dabei auf Maßnahmen, die Cyber-Angriffe auf eigene Netze direkt an der Quelle neutralisieren sollen. Der ehemalige Direktor der National Security Agency (NSA), General Keith Alexander, forderte bereits 2012 neue Kompetenzen für eine „aktive Verteidigung", die das Ausspähen gegnerischer Netze aus Gründen der Verteidigung beinhaltete.[2] Ähnlich argumentiert auch der Präsident des Bundesamtes für Verfassungsschutz, Hans-Georg Maaßen. Er will neue Befugnisse für digitale Gegenschläge als Reaktion auf Cyber-Angriffe: „Wir müssen auch in der Lage sein, den Gegner anzugreifen, damit er aufhört, uns weiter zu attackieren."[3] Innenminister Thomas de Maizière unterstützte diese Forderung im April 2017. Er bestand darauf, dass man im Falle eines Cyber-Angriffs auch imstande sein müsse, „notfalls feindliche Server zu zerstören".[4] Der Innenminister verglich destruktive Cyber-Gegenangriffe mit dem „digitalen finalen Rettungsschuss", den Polizeibehörden in Notsituationen, d.h. bei Gefahr für Leib und Leben, einsetzen dürfen. Aus Sicht des deutschen Verteidigungsministeriums (BMVg) wurde die Planung solcher Vorhaben in einer Anhörung im Verteidigungsausschuss über die Rolle der Bundeswehr im Cyberspace 2016 durch Staatssekretärin Suder mit folgenden Worten verneint: „[es gäbe] zur Zeit keine Planung aber [es gibt] immer wieder Gedanken dazu was ist zulässig und was ist technisch möglich".[5] In der Anhörung verwies Frau Suder darauf, das BMVg habe zur Analyse dieses Verteidigungskonzeptes bereits eine Studie herausgegeben. Nun soll der deutsche Bundessicherheitsrat bis zum Herbst 2017 eine erneute Machbarkeitsstudie erstellen, in der geprüft werden soll, unter welchen Bedingungen ein Gegenangriff zur digitalen Selbstverteidigung sinnvoll und legal ist.

In fachlichen Debatten werden Cyber-Gegenangriffe unter verschiedenen Termini wie „hacking back", „digital self defense", „responsive cyber defense" oder „active defense" seit geraumer Zeit teils kontrovers diskutiert. Meist beschreiben diese Begriffe den Vorgang des Eindringens in fremde Computernetzwerke, um Angriffe durch Hacker direkt an der Quelle, d.h. auf ihren eigenen Systemen zu unterbinden, indem etwa die angreifende Hard- und Software lahmgelegt oder gar zerstört werden. Befürworter argumentieren, dass so im Idealfall präemptiv Schaden abgewendet werden könnte, noch bevor oder während ein Cyber-Angriff stattfindet. Der Staat will also bei Hackerangriffen „zurückhacken" dürfen, während Kritiker darauf verweisen, dass dieser Vorstoß das aktuell noch

1 Lynn III, William J., "Defending a New Domain", in: *Foreign Affairs*, September/October 2010. https://www.foreignaffairs.com/articles/united-states/2010-09-01/defending-new-domain.

2 Nakashima, Ellen, "When Is a Cyberattack a Matter of Defense?" In: *Washington Post*, 27.02.2012. https://www.washingtonpost.com/blogs/checkpoint-washington/post/active-defense-at-center-of-debate-on-cyberattacks/2012/02/27/gIQACFoKeR_blog.html?-utm_term=.f299848fff64.

3 „Als Reaktion auf Attacken – Verfassungsschutz will Cybergegenangriffe starten", in: *Spiegel-Online*, 10.01.2017. http://www.spiegel.de/netzwelt/netzpolitik/bundesamt-fuer-verfassungsschutz-plant-cyber-gegenangriffe-a-1129273.html.

4 Greis, Friedhelm, „Digitaler Finaler Rettungsschuss: Regierung will bei IT-Angriffen zurückschlagen", in: *Golem.de*, 24.04.2012. https://www.golem.de/news/digitaler-finaler-rettungsschuss-regierung-will-bei-it-angriffen-zurueckschlagen-1704-127403.html.

5 Deutscher Bundestag (Hg.), Die Rolle der Bundeswehr im Cyberraum. Verfassungs-, Völker- und sonstige Nationale und Internationale rechtliche Fragen sowie ethische Aspekte im Zusammenhang mit Cyberwarfare und die hieraus erwachsenden Herausforderungen und Aufgaben für die Bundeswehr, Berlin, 22.02.2016. http://www.bundestag.de/ausschuesse18/a12/oeffentliche_anhoerung/cyber1/405094.

ungelöste „Attributions-Problem“ vollkommen außer Acht lasse.[6] Im schlimmsten Fall würde ein Cyber-Gegenangriff, sofern überhaupt ein Verursacher identifiziert werden kann, nicht nur dessen Angriffssysteme ausschalten, sondern wahrscheinlich zusätzlich auch zivile Infrastruktur unbeteiligter Drittparteien.[7] Dieses Arbeitspapier soll einige der weniger beleuchteten technischen, politischen, operativen und legalen Schwierigkeiten von „hack backs“ diskutieren. Die Diskussion um die Vor- und Nachteile von Cyber-Gegenangriffen entspannt sich anhand der folgenden Dimensionen: Sollte man offensiv gegen Cyber-Angriffe vorgehen (normative Dimension)? Wie würde solch ein Gegenschlag technisch und operativ aussehen (operative Dimension)? Was wären denkbare Folgen solcher Gegenschläge, etwa im Hinblick auf Konflikteskalation? Welche Akteure kommen überhaupt für solche Gegenschläge in Frage?

Passive vs. aktive Verteidigung

Bevor diese Fragen adressiert werden können, ist es zunächst sinnvoll, die verschiedenen Termini zu bestimmen, die in der Debatte häufig vermischt werden. Ein Arbeitspapier des US Department of Homeland Security weist darauf hin, dass Cyber-Angriff und Cyber-Verteidigung nicht in einem dualistischen Verhältnis zueinander stehen, sondern Praktiken umfassen, die sich auf einem Spektrum bewegen und nicht nur technischer Natur sind.[8] Am äußersten Ende des Spektrums umfasst Cyber-Verteidigung die *passive Verteidigung*, d.h. traditionelle Cyber-Security-Tools wie den Einsatz von Firewalls, Anti-Viren-Systemen, Intrusion Detection Systems, Rechtemanagement und Zugriffskontrollen. Auch das kurzfristige Sperren von bestimmten IP-Adressbereichen, von denen eine Distributed Denial of Service (DDoS)-Attacke kommt, oder die automatische, dynamische Aufstockung verfügbarer Netzwerk-Bandbreiten sind insofern passiv, als sie sich auf den eigenen Perimeter, also das eigene Netzwerk beschränken. Aber auch „awareness raising“, „Cyber-Resilienz“[9], ein zentrales Software- und Patch-Management und Personalschulungen gehören zu den passiven Verteidigungswerkzeugen, welche die Sicherheit von IT-Systemen erhöhen sollen.

Am anderen Ende des Spektrums finden sich Praktiken, die sich klar als *offensive Cyber-Angriffe* definieren lassen. Diesen Praktiken ist gemein, dass sie darauf abzielen, unberechtigt in ein fremdes Zielsystem einzudringen („penetration“) und dort bestimmte Effekte („payload“) auszulösen, die je nach Motivation der Angreifer und Komplexität der Operation divergieren. Gängige Motive sind Sabotage von Hard- oder Software des Zielsystems mittels Malware (wie beispielsweise beim sogenannten Stuxnet-Angriff[10]), das Exfiltrieren von sensitiven Informationen aus wirtschaftlichen (Cyber-Kriminalität) oder politischen Gründen (staatliche Spionage) und schließlich die Manipulation von Informationen (Informationskrieg und Täuschung). Statistisch betrachtet, fallen die meisten Cyber-Angriffe in die Kategorien Cyber-Kriminalität und Wirtschaftsspionage.[11] „Hacktivismus“, d.h. das Lahmlegen oder Beschmieren („defacement“) politischer Websites oder DDoS-Angriffe (wie bspw. 2007 in Estland[12]) sind ebenso weit verbreitet. Die Komplexität dieser Operationen ist in aller Regel eher gering, da sie kaum domänenspezifisches Wissen über das Zielsystem benötigen oder sich im Sinne von „digitalem

6 Attribution beschreibt den Vorgang, einem Akteur eine Handlung zuweisen zu können. Aufgrund technischer Gegebenheiten ist dies im Internet besonders schwierig, da Identitäten einfach gefälscht werden können. Mehr dazu: Clark, David D.; Landau, Susan, “Untangling Attribution”, in: *Harvard National Security Journal*, 2, 2011.

7 Herpig, Sven, „Cyberangriffe. Zurückhacken ist keine Lösung“, in: *Zeit Online*, 21.04.2017. http://www.zeit.de/digital/internet/2017-04/cyberangriffe-bundesregierung-hackback-gegenangriff.

8 Ferner weisen mehrere Autoren darauf hin, dass die Offensive keinesfalls immer die Oberhand im Cyberspace habe: Singer, P. W.; Friedman, A., “Cult of the Cyber Offensive. Why Belief in First Strake Ad-vantage Is Misguided Today as It Was in 1914”, in: *Foreign Policy*, 15.01.2014. http://foreignpolicy.com/2014/01/15/cult-of-the-cyber-offensive/.

9 Im Gegensatz zum militärischen Begriff der Verteidigung orientiert sich Cyber-Resilienz an der Biologie, konkret dem Verhalten des Immunsystems bei Virus-Erkrankungen. Gemeint sind Maßnahmen, die ergriffen werden können, wenn ein Angreifer bereits im System ist und Schaden anrichtet. Dazu gehören redundante Systeme, die bei Ausfall sofort einspringen und den Schaden begrenzen, wie zum Beispiel das Einspielen von Backups, um Erpressungstrojaner nutzlos zu machen. Mehr dazu: Singer, P. W.; Friedman, A., *Cybersecurity and Cyberwar: What Everyone Needs to Know* (1st ed.), New York: Oxford University Press, 2014, S. 169-173.

10 „Faktensammlung Stuxnet”, in: *Cyberpeace.org*, 2017. https://cyber-peace.org/cyberpeace-cyberwar/relevante-cybervorfalle/stuxnet/.

11 Passeri, Paolo, “February 2017 Cyber Attack Statistics”, in: *Hackmageddon*, February 2017. http://www.hackmageddon.com/2017/03/20/february-2017-cyber-attacks-statistics/.

12 „Faktensammlung Estland”, in: *Cyberpeace.org*, 2017. https://cyber-peace.org/cyberpeace-cyberwar/relevante-cybervorfalle/cyberattacke-auf-estland/.

Vandalismus" gegen ein beliebiges, mit Sicherheitslücken behaftetes IT-System richten. Destruktive Angriffe eines staatlichen Akteurs („Cyber-Warfare") passieren hingegen – soweit dies öffentlich bekannt wird – sehr selten. Das liegt daran, dass die Komplexität dieser Vorgehensweise im Gegensatz zum eben genannten „Hacktivismus" in aller Regel enorm hoch ist, weil sie sich gegen spezifische Ziele richtet, deren Schwächen und Zugriffspunkte analysiert werden müssen, um einen verdeckten Zugriff aufzubauen und diesen über längere Zeit hinweg aufrechtzuerhalten. Derartige Operationen sind gemeinhin nur mit nachrichtendienstlicher Unterstützung von staatlichen oder staatsnahen Akteuren und mit hohen finanziellen Ressourcen durchführbar.[13] Von „hack back" spricht man, wenn solche offensiven Cyber-Angriffe zur Bekämpfung von vorausgegangenen Cyber-Angriffen eingesetzt werden. Das NATO Cooperative Cyber Defence Centre of Excellence in Tallinn definiert in einer Studie diese responsiven Formen von Verteidigung „as the protection of a designated Communications and Information System (CIS) against an ongoing cyberattack by employing measures directed against the CIS from which the cyberattack originates, or against third-party CIS which are involved."[14]

Bevor man aber zu diesen Mitteln greift, gibt es noch eine ganze Reihe von Maßnahmen, die sich außerhalb des eigenen Perimeters und somit abseits von passiver Verteidigung bewegen, aber nicht notwendigerweise als offensiver Cyber-Gegenangriff zu werten sind. Diese Maßnahmen werden *aktive Verteidigung* genannt. Das SANS-Institut für Cyber-Sicherheit beschreibt aktive Verteidigung als: „the process of analysts monitoring for, responding to, learning from, and applying their knowledge to threats internal to the network."[15] Einige dieser Operationen sind rechtlich, politisch und technisch unproblematisch („low risk"), während andere Maßnahmen als „high risk" eingestuft werden, da sie im legalen Graubereich operieren.[16]

Zu den weniger problematischen Maßnahmen gehört z.B. der Informationsaustausch zwischen „Computer Incident/Emergency Response Teams" (CERT) und betroffenen Akteuren über gängige Schwachstellen und Angriffsvektoren. Verteidiger können aber auch sogenannte „honey pots" oder „sandboxes" einsetzen, die einem Angreifer vorgaukeln, ein Zielsystem von Interesse zu sein. Diese Maßnahmen dienen dazu, einen Angreifer *in situ,* also während er bereits im eigenen Netzwerk ist, dabei zu beobachten, wie er in ein simuliertes System eindringt, um dabei Informationen über sein/ihr Vorgehen zu erlangen. Dabei können oft wichtige Informationen über eingesetzte Malware, technische Infrastruktur und das Know-how des Angreifers gewonnen werden. Sogenannte „hunter teams" können diese Informationen nutzen, um den Angreifer zurückzuverfolgen und um mehr über seine Infrastruktur für Cyber-Angriffe (etwa Command & Control oder C2-Server für Botnets oder Malware) zu lernen. „Hunter teams" können z.B. „beacons" in für den Angreifer interessante Dokumente implantieren, die nach gelungener Exfiltration ihren Standort an die Teams senden, die IP-Adresse des Angriffs-Servers verraten und somit einen gewissen Grad an Attribution erlauben. In ihrer aggressiveren Form können „beacons" selbst als „spyware" fungieren, um Telemetrie-Daten über das System des Angreifers zu sammeln. Das Ausspähen gegnerischer Netzwerke durch „spyware" erfordert dabei häufig selbst die weitere „penetration", also das Hacken des Zielsystems. Oftmals muss dafür speziell entwickelte Schadsoftware eingesetzt werden, die Sicherheitslücken im Zielsystem ausnutzt. Diese Form von aktiver Verteidigung bedeutet, dass man heimlich IT-Systeme der Angreifer infiziert, den Netzwerkverkehr gegnerischer Netze mitliest und anschließend analysiert, was der Gegner vor Ort tut. Die Grenze zwischen Selbstverteidigung und aktiver Spionage ist hier sehr dünn und die Akteure bewegen sich rechtlich in einem Graubereich, da in jedem Fall fremde IT-Systeme manipuliert (d.h. die Integrität dieser Systeme verletzt) und unter Umständen die territoriale Integrität von Nationen verletzt werden können.

13 Lindsay, J. R., "Stuxnet and the Limits of Cyber Warfare", in: *Security Studies* 22, 2013, S. 389.

14 Minárik, T.; Stinissen, J.; Brangetto, P., "From Active Cyber Defence to Responsive Cyber Defence: A Way for States to Defend Themselves – Legal Implications", in: *NATO Legal Gazette* 35, 2014.

15 Copper, P., "Cognitive Active Cyber Defense: Finding Value Through Hacking Human Nature", in: *JLCW,* Volume 5, Winter 2017, Issue 2, S. 79.

16. "Into the Gray Zone. The Private Sector and Active Defense Against Cyber Threats", in: *Center for Cyber & Homeland Security*, Prpject Report, The George Washington University, October 2016, S. 10.

Passive Verteidigung (low risk)
• Awareness & Personalschulungen • Firewalls, Intrusion Detection, Patch-Management • Informationsaustausch • Sandboxen und Hönigtöpfe • Täuschung und falsche Ziele • Hunter Teams • Beacons
Perimetergrenze
• Spyware Beacons • Nachrichtendienstliche Ermittlungen (intelligence) • Botnetz Takedowns • Politische Sanktionen • Hack-Back (Eindringen in fremde Systeme) ▪ Rettungsmissionen & Datenlöschung ▪ Computer-Netzwerk-Exploitation und Überwachung fremder Netze ▪ Denial of Service
Offensive Cyber-Angriffe (high risk)[17]

Es gibt aber noch weitere Formen aktiver Verteidigung, die nicht notwendigerweise einem Cyber-Gegengangriff gleichkommen, aber nicht minder umstritten sind.[18] Dazu gehört die Praxis der „botnet takedowns". Botnetze sind Netzwerke von mit Schadsoftware infizierten Computern oder sogenannten Embedded Systems wie DSL-Routern sowie Geräten des „Internet of Things" (IoT), die durch Steuerungsserver dazu gezwungen werden *en masse* bestimmte Aktionen auszuführen. Oftmals handelt es sich dabei um private IT-Geräte deren Besitzer gar nicht wissen, dass sie Teil eines Botnetzes sind.[19] Botnet-Infrastrukturen werden für eine ganze Reihe von Cyber-Operationen genutzt, für einfache, aber massive DDoS-Angriffe auf Websites, für das automatisierte Verteilen von Spam, Malware oder „phishing mails", aber auch von Nachrichtendiensten, die ihre Aktivitäten verschleiern wollen.[20] Das Herunterfahren von Botnetzen ist technisch und rechtlich enorm kompliziert, da die Steuerungsserver oftmals über verschiedene Ländergrenzen hinweg verteilt sind und bisweilen komplett dezentral operieren, sodass die Attribution der Urheber ebenso kostspielig wie zeitintensiv ist. Das 2016 von Europol und verschiedenen internationalen Behörden abgeschaltete Avalanche-Botnetz operierte bereits seit 2009, konnte aber erst 2014 identifiziert werden, da die C2-Server über komplexe Tarnmechanismen verfügten. Aus diesem Grund mussten in einer groß angelegten internationalen Kooperation die Server in verschiedenen Ländern von deren Hosting-Anbietern simultan per richterlicher Anordnung abgeschaltet werden. Ein Hacking der Server war dazu nicht erforderlich. Der Fall Avalanche zeigt, dass dieser Prozess langwierig, diffizil und von ungewissem Erfolg ist.[21] Oftmals verweigern Länder zudem die Kooperation beim Abschalten von Botnetzen auf ihrem Territorium, sodass von diesen weiterhin ungehindert Cyber-Angriffe ausgehen können. Aufgrund dieser Problematik fordern Nachrichtendienste die Befugnis zum „hacking back", um etwa Botnetze aus der Ferne zu neutralisieren. Im Folgenden sollen dementsprechend um Argumente dargelegt werden, die für das „hacking back" sprechen.

Argumente für Cyber-Gegenangriffe

Cyber-Angriffe werden immer komplexer und vielschichtiger und insbesondere das „social engineering", also das Identifizieren menschlicher Angriffspunkte wird für umfangreiche Cyber-Operationen immer zentraler.[22] Dabei werden Ziele teils nachrichten-

17 Eigene Darstellung basierend auf: "Into the Gray Zone. The Private Sector and Active Defense Against Cyber Threats", wie FN 16.

18 Ebenfalls sei hier erwähnt, dass es auch nicht-technische Mittel der Cyber-Verteidigung gibt. Dazu können diplomatische Maßnahmen zählen, Wirtschaftssanktionen, Mechanismen internationaler Strafverfolgung (Interpol), Handelsbarrieren für Unternehmen, die Cyber-Kriminelle unterstützen oder bilaterale Verträge wie z.B. zwischen den USA und China.

19 2005 wurde ein Fall bekannt, in dem das Computer-System eines Krankenhauses in Seattle Teil eines Botnetzes war. Zu dem Botnetz gehörten aber auch Schulen, Universitäten und Firmen: "Man Gets 3 Years for 'Botnet' Attack on Hospital, School District, Military Installations", *The Sidney Morning Herald*, August 26, 2006.
http://www.smh.com.au/news/Technology/Man-gets-3-years-for-botnet-attack-on-hospital-school-districtmilitary-installations/2006/08/26/1156012780632.html.

20 Reid, Kevin, "Get Botnets Before They Get Us", in: *The Cipher Brief*, April 30, 2017.
https://www.thecipherbrief.com/article/tech/get-botnets-they-get-us-1092.

21 Jolmes, Johannes; Mundt, Anna, „Raubzug im Netz – Wie Verbraucher geplündert werden", in: *ARD, Das Erste, Panorama*, Sendung vom 20.04.2017.
http://daserste.ndr.de/panorama/archiv/2017/Raubzug-im-Netz-wie-Verbraucher-gepluendert-werden,botnetz112.html.

22 Exemplarisch sei auf den aktuellen „2017 Verizon Data Breach Investigations Report" verwiesen, der attestiert, dass von allen im Vorjahr gemeldeten und von Verizon analysierten Hacking-Vorfällen "81% of hacking-related breaches le-

dienstlich ausgespäht, um interne Informationen über Organisationsstrukturen, Kommunikationsabläufe und Mitarbeiter zu erlangen. Diese Informationen werden genutzt, um in professionellen, personalisierten E-Mails eine genau auf das Ziel maßgeschneiderte Schadsoftware zu verteilen oder die Passwörter von Mitarbeitern zu stehlen. Befürworter des „hacking back" argumentieren, dass sich solche Advanced Persistent Threats (APT) in der Regel nicht von rein passiven Systemen aufhalten lassen, da diese auch oftmals unbekannte Schwachstellen („Zero day" bzw. „0-day") in der Perimeter-Verteidigung ausnutzen um ein System lahmzulegen. Bei persistenten Angriffen sei es nur eine Frage der Zeit, bis der Gegner ins eigene Netzwerk eindringt und mit der Daten-Exfiltration auf fremde Server beginnt. Die jüngsten Hacking-Angriffe auf das US Democratic National Committee 2016 und den Bundestag 2015, die vermutlich beide auf dieselbe russische APT-28 Hackergruppe zurückzuführen sind, zeigen eindrucksvoll die Schwachstellen passiver Verteidigung.[23] Aus diesem Grund scheint es zunächst sinnvoll, sich des Problems von Cyber-Angriffen per „hacking back" entledigen zu wollen. Die Überlegung ist, dass Cyber-Angriffe aufhören, wenn der Ursprungsrechner des Hackers bzw. die C2-Infrastruktur, die für die Hacks benutzt wird, lahmgelegt wird. Innenminister Thomas de Maizière scheint dieses Szenario im Kopf zu haben, wenn er „die Rückverfolgung und gegebenenfalls das Unschädlichmachen eines Servers aus dem Ausland" fordert.[24]

Rettungsmissionen

Ein weiterer Grund für „hacking back" wird in der Literatur als „rescue missions", also Rettungsmissionen, bezeichnet. Hans-Georg Maaßen argumentiert: „Wir haben ein Interesse daran, dass Angreifer die Daten verlieren, die sie gestohlen haben. Man muss solche Daten eventuell zum Schutz des Opfers zerstören."[25] In der Theorie soll also der Angreifer zurückverfolgt werden und im Anschluss die gestohlenen Informationen per eingeschleuster Malware gelöscht und das Dateisystem des Ursprungsrechners zerstört werden.

„Hack backs" zur Beweissicherung

Insbesondere amerikanische Strafverfolgungsbehörden und Nachrichtendienste führen ein weiteres Argument für „hack backs" ins Feld, welches in der deutschen Debatte bisher nicht aufgetaucht ist. Das FBI machte 2015 Schlagzeilen als es zentrale Server des Kinderpornografie-Rings „Playpen" hackte.[26] Statt die Server zu zerstören und somit den Ring unschädlich zu machen, manipulierten FBI-Hacker den Server so, dass dieser eingehende Verbindungen protokollierte – eine Technik, die sich „watering hole" nennt. Computern, die sich mit dem „Playpen"-Server verbinden wollten, wurde eine Malware eingeschleust, die eine bis dato unbekannte Sicherheitslücke im Tor-Browser ausnutzte und somit das Dechiffrieren von anonymisierten Verbindungen erlaubte. Das FBI kontrollierte den Server 13 Tage lang und dechiffrierte über 8000 IP- und MAC-Adressen in 120 Ländern.[27] Es folgten zahlreiche Hausdurchsuchungen und teils internationale Strafprozesse. Der Fall war deswegen kontrovers, weil das FBI tausende, teils internationale Rechner mit einem einzelnen Durchsuchungsbefehl hackte und den Server nicht sofort abschaltete, somit also die Distribution illegaler Materialien tolerierte. Rechtlich operierte das FBI in einem Graubereich, bis die sogenannte „Rule 41" im Dezember 2016 angepasst und dem FBI das Hacken außerhalb der US-Jurisdiktion per Richterbeschluss erlaubt wurde.[28] Das Beispiel illustriert, dass es ein berechtigtes Interesse an „hack backs" zur Informationsgewinnung gibt. Ebenso ist vorstellbar, dass Behörden die C2-Infrastruktur von Cyber-Angreifern hacken, um wichtige Informationen

veraged either stolen and/or weak passwords [and] 43% were social attacks", *Verizon, 2017 Data Breach Investigations Report*, 2017, S. 3.

23 Beuth, Patrick; Biermann, Kai; Klingst; Martin; Stark, Holger, „Bundestags-Hack: Merkel und der schicke Bär", in: *Zeit Online*, 2017, http://www.zeit.de/2017/20/cyberangriff-bundestag-fancy-bear-angela-merkel-hacker-russland.

24 Greis, Friedhelm, „Digitaler Finaler Rettungsschuss: Regierung will bei IT-Angriffen zurückschlagen", in: *Golem.de*, 20.04.2017. https://www.golem.de/news/digitaler-finaler-rettungsschuss-regierung-will-bei-it-angriffen-zurueckschlagen-1704-127403.html.

25 Balser, Markus, „Kampf gegen Hacker. Verfassungsschutz will angreifen", in: *Süddeutsche online*, 27.04.2017. http://www.sueddeutsche.de/wirtschaft/kampf-gegen-hacker-verfassungsschutz-will-angreifen-1.3481446.

26 Cox, Joseph, "The FBI Hacked Over 8,000 Computers In 120 Countries Based on One Warrant", in: *Motherboard*, November 23, 2016. https://motherboard.vice.com/en_us/article/fbi-hacked-over-8000-computers-in-120-countries-based-on-one-warrant.

27 MAC-Adressen sind Identifikationsnummern für Netzwerk-Hardware.

28 Hennessy, Susan, "Rule 41: Resolving Procedural Debates to Face the Tough Questions on Government Hacking", in: *Lawfare*, January 12, 2016. https://www.lawfareblog.com/rule-41-resolving-procedural-debates-face-tough-questions-government-hacking.

zu gewinnen und die im Cyberspace außerordentlich schwierige Attribution von Urhebern zu erlauben.[29] Ein Fallbeispiel hierfür wäre die Attribution des Cyber-Angriffs auf Sony Pictures im Jahr 2014, die angeblich nur deswegen gelang, weil die NSA die Operation in Nordkoreas Netzwerken *in situ* beobachtete.[30] Im Sinne der NSA bedeutet aktive Verteidigung Spionage in fremden Computernetzen. Die Beispiele zeigen aber auch, dass das Zerstören dieser Server und der darauf gespeicherten Evidenz je nach Fall unsinnig wäre, da unter Umständen potenziell wichtige „intelligence" vernichtet werden könnte. Aus nachrichtendienstlicher Sicht ist deswegen die „computer network exploitation", also das Ausspähen fremder Netze, gegenüber der destruktiven „computer network attack" fast immer zu bevorzugen.

Cyber-Hygiene

Private Firmen, die insbesondere im Bereich „botnet takedowns" tätig sind, argumentieren zudem mit der „globalen Cyber-Hygiene". Statt einer militärischen Sichtweise werden hier das Ausschalten von Botnetzen und das Reinigen befallener Bots mit Maßnahmen zur öffentlichen Gesundheit im Cyberspace verglichen. Ähnlich wie eine Pandemie durch Zwangsimpfungen bekämpft werden kann, sollen Sicherheitsaktualisierungen von Software (sogenannten „bugfixes" und „patches") notfalls per Zwang auf Bot-Rechner gebracht werden.[31] Im Klartext würde das bedeuten, einen Rechner per Sicherheitslücke zu hacken um einen Patch einzuspielen, der diese oder anderen Sicherheitslücken schließt. Da Botnetze mannigfaltig und für eine Vielzahl von Cyber-Security-Problemen verantwortlich sind, überwiege hier das höhere Gut der öffentlichen „Gesundheit" gegenüber den Privatsphäre-Interessen der Computerbesitzer befallener Systeme. Ein ähnliches Phänomen konnte jüngst beobachtete werden, als eine bisher nicht näher identifizierte Malware mit Namen „Brickerbot" unsichere Internet of Things-Geräte hackte und anschließend lahmlegte. Viele dieser IoT-Geräte waren im Jahr 2016 Teil des „Mirai"-Botnetzes, welches verschiedene Ziele mit massiven DDoS-Anfragen überhäuft hatte.[32]

„Hack backs" als ultima ratio

Häufig argumentieren Befürworter von „hack backs" mit deren Notwendigkeit in Krisensituationen. Wenn also eine groß angelegte Cyber-Operation kritische Infrastrukturen wie Elektrizitätswerke lahmlege, müsse man als *ultima ratio*, wenn alle anderen passiven und aktiven Mittel versagen, oder aufgrund von Zeitdruck nicht durchführbar sind, im Notfall „den Stecker beim Angreifer ziehen" können. Innenminister de Maizière argumentiert mit der Analogie, dass auch Polizisten bei Gefahr im Verzug ihre Dienstwaffe benutzen dürfen um Angreifer zu verwunden.[33]

Auch aus Sicht militärischer Entscheidungsträger spricht einiges für digitale Selbstverteidigung. Statt im Verteidigungsfall bei einem konventionellen Angriff mit gleichen Mitteln zu reagieren, könne ein Cyber-Gegenangriff in der Theorie z.B. die Steuerungssysteme von Langstreckenraketen lahmlegen oder die Kommunikation des Gegners stören.[34] Ebenso müsse man bei Angriffen über den Cyberspace, von denen eine unmittelbare Gefährdung der Sicherheit Deutschlands ausgeht, mit adäquaten Mitteln reagieren und den Angriff abwenden können. Solch ein digitaler Gegenschlag hätte den Vorteil, dass er vermutlich völkerrechtlich gedeckt wäre (UN Charta Art. 51) und im besten Fall der Angreifer unschädlich gemacht wird, ohne dass das Leben eigener Soldaten unnötig gefährdet wird. Während ein „hack back" als Reaktion auf konventionelle Angriffe vermutlich rechtlich legitim ist, ist die Reaktion auf einen digitalen Angriff weniger eindeutig. Gemäß dem Tallinn-Manual kommt es hier in erster Linie auf die Art der Schadenswirkung des ersten Angriffes an. Ob man auf konventionelle Angriffe digital reagiert oder auf digitale Angriffe mit physischen Gegenschlägen reagieren sollte, ist in der Literatur umstritten.

29 Rid, T.; Buchanan, B., "Attributing Cyber Attacks", in: *Journal of Strategic Studies*, 2014, 38(1-2), 4-37, S. 5.
30 Die Evidenz für diese Hypothese ist allerdings nicht eindeutig: Sanger, David; Fackler, Martin, "N.S.A. Breached North Korean Networks Before Sony Attack, Officials Say", January 18, 2015. https://www.nytimes.com/2015/01/19/world/asia/nsa-tapped-into-north-korean-networks-before-sony-attack-officials-say.html?_r=0.https://www.nytimes.com/2015/01/19/world/asia/nsa-tapped-into-north-korean-networks-before-sony-attack-officials-say.html?_r=0.
31 Lin, Patrick, "Ethics of Hacking Back. Six Arguments from Armed Conflict to Zombies", *Ethics + Emerging Sciences Group*, 2016, S. 19.
32 Thomson, Iain, "Forget Mirai – Brickerbot Malware Will Kill Your Crap IoT Devices", in: *theRegister*, August 4, 2017. https://www.theregister.co.uk/2017/04/08/brickerbot_malware_kills_iot_devices/.
33 Greis, Friedhelm, „Digitaler Finaler Rettungsschuss: Regierung will bei IT-Angriffen zurückschlagen", wie FN 4.
34 Dieses Argument findet sich bereits beim Vordenker des Cyber-War: Rona, Thomas P., "Weapon Systems and Information War", *Boeing Aerospace Company*, July 1976.

Diese Beispiele zeigen, dass aktive Verteidigung je nach Auslegung verschiedene Tätigkeiten umfasst, die nicht mit „hack back“ synonym sein müssen. Ferner zeigt sich, dass hier je nach Fall, Akteur und eingesetzten Mitteln unterschieden werden muss und dass es offenbar legitime Einsatzzwecke von „hack backs“ gibt. Wie kann man diese Argumente einordnen und bewerten?

Gegenargumente

Aus technischer Sicht berührt *jeder* unbefugte Zugriff auf ein IT-System die Integrität, Authentizität und unter Umständen auch die Verfügbarkeit dieses Systems. Dies gilt umso mehr, wenn der Zugriff verdeckt erfolgen muss und zu diesem Zweck Sicherungsmaßnahmen sowie das protokollieren von Zugriffen unterbunden oder Spuren in Log-Daten entfernt werden müssen. Vor diesem Hintergrund wäre bereits der geheime Zugriff für die notwendige IT-Forensik, um bei Gegenangriffen über die beteiligten, zwischengeschaltenen IT-Systeme hindurch das System des Angreifers zu identifizieren, eine Gefährdung dieser Systeme. „Hack backs“ gefährden also die Sicherheit der Zielsysteme, was je nach Einsatzzweck des Geräts unterschiedliche Implikationen haben kann. Das Problem wird insbesondere dadurch erschwert, dass man häufig gar nicht so genau weiß, wer der Angreifer ist (und ob man das richtige Zielsystem erwischt hat oder nur einen weiteren Hub unbeteiligter Dritter).

Das Problem der Attribution

Ein zentrales Argument der Kritiker von digitalen Gegenangriffen beruht auf dem Attributions-Problem, welches besagt, dass es aufgrund struktureller Merkmale des Internets schwierig ist, Cyber-Angriffe einem Urheber zuzuschreiben.[35] IP-Adressen sind einfach zu fälschen, Identitäten einfach zur anonymisieren (etwa durch besagtes TOR-Netzwerk) und Operationen unter falscher Flagge sind denkbar. Aus Gründen der Verschleierung finden Cyber-Angriffe in der Regel über oft vielfach hintereinander gereihte gekaperte Drittrechner/Bots statt.[36] Das Ziel des Angriffs sieht also nur die IP-Adresse des unbeteiligten Dritten, nicht aber die des Urhebers. Selbst wenn es gelingen sollte, die Urheber-IP-Adresse zu ermitteln (technische Attribution) ist damit nicht eindeutig zu klären, wer vor dem Computer saß (soziale Attribution), ob dieses IT-System gezielt und ausschließlich für die Cyber-Attacke verwendet wurde, oder ob das Gerät noch für andere, u.U. relevante Aufgaben, etwa in einem Krankenhaus, zuständig ist. Eine Analogie wäre die Bombardierung von zivilen Wohngebäuden, in denen sich auch militärische Kombattanten befinden. Die Wahrscheinlichkeit das falsche Ziel zu treffen erhöht sich insbesondere in den zuvor erwähnten Notstandssituationen, in denen nicht viel Zeit für den Attributionsprozess bleibt. Rid und Buchanan stellen folgende Faustregel auf: Je mehr Zeit man für Netzwerk-Forensik hat, desto genauer wird die Attribution, d.h. desto sicherer kann man sagen, wer der Urheber ist.[37] Dies ist aber keine Garantie. Viele Cyber-Angriffe sind auch bis heute nicht zweifelsfrei attribuiert. „Smoking gun“-Beweise fehlen oftmals, so dass lediglich Indizienketten für oder gegen bestimmte Angreifer sprechen.

Umgekehrt gilt: je weniger Zeit für die Attribution zur Verfügung steht, desto größer die Wahrscheinlichkeit, bei einem Gegenschlag das falsche Ziel zu treffen. D.h. dass gerade in zeitkritischen Krisenreaktionen wie einem großangelegten, strategischen Cyber-Angriff die zielgenaue Attribution wahrscheinlich nicht rechtzeitig gelingen wird.

Dazu kommt das Problem, dass nicht alle Cyber-Angriffe unmittelbar sichtbare Effekte produzieren. Einfache DDoS-Attacken sind relativ „laut“ und sichtbar, können aber mit einfachen Mitteln wie der Sperrung von IP-Addressen deflektiert werden. Destruktive Cyber-Angriffe gehen in der Regel eher „leise“ und unsichtbar vonstatten, werden also oftmals gar nicht als solche erkannt. Ob es ein Bug, ein Unfall oder ein Cyber-Angriff ist, der ein System lahmlegt, ist oft nicht unmittelbar ersichtlich. Stromausfälle durch Defekte oder Unfälle (umgestürzte Bäume) sind weitaus wahrscheinlicher als Cyber-Angriffe.[38] Die meisten Cyber-Angriffe werden deshalb erst nach durchschnittlich 150-200 Tagen als solche identifiziert. Erst dann beginnt der Prozess der Attribution zu einem Verursacher.[39] Bis also tatsächlich ein Ziel für einen Gegenan-

35 Rid, Thomas; Buchanan, Ben, “Attributing Cyber Attacks”, in: *Journal of Strategic Studies* 38 (2014): 4–37, S. 5.
36 Clark, David D.; Landau, Susan, “The Problem Isn’t Attribution: It’s Multi-Stage Attacks”, *Proceedings of the Re-Architecting the Internet Workshop*, Article No. 11, 2010.
37 Rid, Thomas; Ben Buchanan, wie FN 35, hier: S. 32.
38 Lewis, James A., “Assessing the Risk of Cyber Terrorism, Cyber War and Other Cyber Threats”, in: *Center for Strategic & International Studies*, 2002, S. 5.
39 Davis II, John S. et al., “Stateless Attribution: Toward International Accountability in Cyberspace”, *Rand Corporation,* 2017, S. 24.

griff bestimmt ist, können je nach Fall Tage, Monate oder gar Jahre vergehen.[40] Das Beispiel des bisher destruktivsten Cyber-Angriffs Stuxnet ist hier illustrativ. Iranische Atomwissenschaftler hielten den Ausfall der Zentrifugen zunächst für einen Unfall und nicht für einen Cyber-Angriff, da die Systeme nicht mit dem Internet verbunden waren. Erst nach Wochen verdichteten sich die Hinweise auf einen Angriff.[41] Die Attribution von Stuxnet ist auch bis heute nicht abschließend geklärt, auch wenn gemeinhin Israel und die USA dafür verantwortlich gemacht werden. Diese lange Zeitspanne ist im Sinne des Völkerrechts problematisch. Das Recht auf Selbstverteidigung bei destruktiven Angriffen nach UN Charta Art. 51 erfordert, dass die Reaktion unmittelbar zu erfolgen hat. Wenn ein Gegenschlag aber erst Monate später stattfindet, kann dieser selbst als eigenständiger aggressiver Akt und nicht als legitime Selbstverteidigung interpretiert werden.[42]

Politische Eskalation

Die Gefahr einer politischen Eskalation bei falscher Attribution wird als weiteres zentrales Gegenargument ins Feld geführt. Man stelle sich vor, Südkorea zerstöre fälschlich einen Computer in Nordkorea mit einer Cyber-Gegenattacke obwohl z.B. Russland der erste Urheber war um die politischen Spannungen auf der koreanischen Halbinsel weiter zu verschärfen. Im schlimmsten Fall könnte Nordkorea mit konventionellen Waffen reagieren. Immer mehr Cyber-Sicherheitsstrategien argumentieren, dass auf Cyber-Angriffe auch mit physischen Waffen reagiert werden kann, so dass dieses Szenario zumindest denkbar ist.[43] Sogenannte „false flag operations" sind im Cyberspace keine Seltenheit. Als im April 2015 im Rahmen der Terrorserie des sogenannten Islamischen Staates in Frankreich die TV-Programme des Senders TV5 Monde ausfielen, bekannte sich ein bis dato unbekanntes „Cyber-Kalifat" zu dem Angriff. Heute ist man sich relativ sicher, dass dieser Angriff eine „false flag"-Operation war, die vermutlich den russischen Hackern von APT-28 zuzuschreiben sind.[44] Wer aber die realen Akteure hinter APT-28 sind und ob diese wirklich vom Kreml instruiert wurden, konnte bis heute nicht eindeutig nachgewiesen werden. Dieses Beispiel zeigt, wie wichtig eine sorgfältige Forensik und Attribution ist. Schnellschüsse sind in der Regel kontraproduktiv.

Ob Cyber-Gegenangriffe aber zwangsläufig eine Eskalationsdynamik auslösen, ist in der Forschung umstritten. Valeriano und Manes weisen darauf hin, dass Eskalationsdynamiken (also „tit for tat"- Reaktionen) insbesondere zwischen Staaten auftreten, die sich bereits in physischen Konflikten befinden und in geografischer Nähe zueinander liegen.[45] Wenn Deutschland einen Server in Japan zerstört, ist eine Eskalation oder ein „hack back" seitens Japans unwahrscheinlicher als im Falle Ukraine-Russland. Lin weist darauf hin, dass sich Staaten schon seit Jahren gegenseitig hacken und dass Eskalationen in der Tat eher selten sind.[46] Es gibt also keinen deterministischen Zusammenhang zwischen „hack-backs" und politischen Krisen. Vielmehr kommt es auf den geopolitischen Kontext sowie die Intensität des „hack backs" an. Ob eine Gegenreaktion nach einem Hack ausgelöst wird, hängt vom vorgefallenen Schaden ab. Cyber-Forensik ist kostspielig, so dass es sich oftmals nicht lohnt, bei kleineren, d.h. nicht-destruktiven Vorfällen den Attributionsprozess zu starten. Zudem müssen Angriffe auch erst entdeckt werden, was insbesondere bei nachrichtendienstlichen Angriffen schwierig ist. Wie bereits dargestellt, bemühen sich die meisten Cyber-Angriffe darum verborgen zu bleiben und eben keinen sichtbaren Schaden anzurichten.

Ob eine politische Eskalation stattfindet, hängt auch von der Art des „hack backs" ab. Ein Staat wird anders auf eine Komplettüberwachung seiner Netze

https://www.rand.org/content/dam/rand/pubs/research_reports/RR2000/RR2081/RAND_RR2081.pdf.

40 Eindrucksvoll hier die Operation Moonlight Maze von 1998, die russischen Gruppierungen zugeschrieben wurde. Rid et al. konnten jüngst einen zentralen Beweis liefern, dass aktuelle APT-Gruppen aus Russland nach wie vor Code-Bausteine aus der Moonlight Maze-Attacke verwenden: Guerro-Saade, Juan Andres; Raiu, Costin; Moore, Daniel; Rid, Thomas, "Penquin's Moonlit Maze. The Dawn of Nation-State Digital Espionage", *Kaspersky Lab*, 2017.

41 Barzashka, Ivanka, "Are Cyber-Weapons Effective?" In: *The RUSI Journal,* 158 (2013): 48–56, S. 51-52.

42 Siehe dazu Tallinn-Manual, welches das Völkerrecht auf das Internet anwendet. Schmitt, Michael N., *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Tallinn: T, 2013, S. 60.

43 "The DOD Cyber Strategy", *Department of Defense*, 2015.

44 Schindler, John R., "False Flags: The Kremlin's Hidden Cyber Hand", in: *Observer*, 18.06.2016. http://observer.com/2016/06/false-flags-the-kremlins-hidden-cyber-hand/.

45 Maness, Ryan C.; Valeriano, Brandon, "The Impact of Cyber Conflict on International Interactions", in: *Armed Forces & Society* 42 (2016): 301–23.

46 Lin, Patrick, "Ethics of Hacking Back. Six Arguments from Armed Conflict to Zombies", wie FN 31, hier: S. 17-19.

reagieren („active defense“ im Sinne der NSA) als z.B. bei einem „botnet takedown“ auf seinem Territorium. Wenn ein „hack back“ durch eine zuvor gestohlene Datei mit einem „beacon“ ausgelöst wird, wird der so ertappte Dieb vermutlich kaum öffentlich protestieren. Es spielt außerdem eine Rolle, welche diplomatischen Prozesse dem „hack back“ vorausgehen. Wenn der deutsche Verfassungsschutz ohne vorherige diplomatische Konsultationen ein Botnetz in Russland zerstört, wird sich dies vermutlich negativer auf die bilateralen Beziehungen auswirken, als wenn zunächst in bilateralen Regierungskonsultationen darum gebeten wurde, im beiderseitigen Einvernehmen das Botnetz auf strafrechtlichem Wege auszuhebeln. Es kommt ebenfalls darauf an, ob ein Cyber-Gegenangriff offen, d.h. attribuierbar, oder im Verborgenen stattfindet.[47] Will man, um beim vorher genannten Beispiel zu bleiben, Russland zu verstehen geben, dass der Gegenangriff von Deutschland ausging und dass diese Maßnahme als Antwort auf ein zuvor stattgefundenes Ereignis zu verstehen ist, oder will man den Angriff verschleiern? Je nach Vorgehen ergeben sich daraus unterschiedliche Konsequenzen, insbesondere in Bezug auf die Abschreckung künftiger Angriffe. Im Sinne guter Diplomatie mag das Ankündigen eines Gegenschlages geboten sein, gleichzeitig reduziert sie jedoch die Wirksamkeit des „hack backs“. Martin Libicki beschreibt das Abschreckungsdilemma im Cyberspace folgendermaßen: Wenn ich dem Gegner meinen Cyber-Angriff ankündige, könnte dieser zunächst von einem Bluff ausgehen, so dass mein Gegenspieler einen Beweis der eigenen Cyber-Fähigkeiten sehen will. Offenbart man nun aber seine eigenen Cyber-Angriffsfähigkeiten durch einen Cyber-Angriff, kann sich der Gegner darauf einstellen, was die wiederholte Wirksamkeit dieser Tools mindert.[48] Verdeckte, d.h. nicht attribuierbare Gegenschläge erfordern ihrerseits viel Verschleierungsaufwand und nachrichtendienstliche Kenntnis des Zielsystems, sind daher kosten- und zeitintensiv, weshalb ein schnelles Zurückschlagen auch hier die Fehler- und Entdeckungsquote erhöht.

47 Perkoski, Evan; Poznansky, Michael, “An Eye for an Eye: Deterring Russian Cyber Intrusions”, *War on the Rocks, Texas National Security Network*, December 19, 2016. https://warontherocks.com/2016/12/an-eye-for-an-eye-deterring-russian-cyber-intrusions/.

48 Libicki, Martin C., Cyberdeterrence and Cyberwar, in: *RAND Corporation*, 2009, S. 93-99.

Wirksamkeit von „hack backs“

In politischen Debatten zu digitalen Gegenschlägen fehlt gegenwärtig die Diskussion rund um die Frage, ob Gegenangriffe als *ultima ratio* in Notsituationen überhaupt effektiv sein können. Generell ist die Wirksamkeit von Cyber-Angriffen ein Problem, das sich insbesondere auch bei destruktiven Cyber-Gegenangriffen stellt, die ein Zielsystem permanent lahmlegen sollen. Entgegen dem Offensiv-Dominanz-Mythos, der eingangs erwähnt wurde, kann sich der Angreifer im Vorfeld eines Angriffs keinesfalls sicher sein, dass sein Cyber-Angriff „wirkt“.[49] Insbesondere destruktive Cyber-Angriffe erfordern eine sehr genaue Kenntnis des Ziels und der darin eingesetzten Hard- und Software. Der Angriff muss schließlich auf die spezielle Konfiguration des Ziels angepasst werde. Dieser Prozess ist sowohl zeit- als auch kostenintensiv. Stuxnet konnte nur deshalb erfolgreich iranische Urananlagen zerstören, weil lange im Voraus intensive „reconnaissance“ der Zielsysteme betrieben wurde und Informationen über die verwendeten Siemens SCADA-Systeme (und ihre Sicherheitslücken) erlangt hat. Unter dem Codenamen „Operation Olympic Games” begannen die Planungen wohl bereits im Jahr 2005 und beinhalteten den Nachbau und die Simulation der spezifischen Zentrifugen-Anlagen.[50] Dazu kommt, dass es verschiedene Iterationen von Stuxnet gab, was darauf hindeutet, dass der Angriff zunächst nicht wirkte und daher angepasst werden musste.[51] Das gleiche Problem zeigt sich bei Cyber-Gegenangriffen, die in Notsituationen, d.h. mit geringer oder so gut wie keiner zeitlichen Vorbereitung durchgeführt – sozusagen „aus der Hüfte geschossen“ – werden. Ähnlich wie in Rids Attributrionsthese lässt sich argumentieren: je weniger Zeit es zur Vorbereitung („reconnaisance“ des Ziels) eines „hack backs“ gibt, desto geringer sind der Wirkungsgrad und die Zielgenauigkeit.[52] Das zuvor erwähnte Avalanche-Botnet, mit seinen rotierenden, dynamischen C2 zeigt dies ebenfalls. Ein Cyber-Angriff auf dieses Botnet hätte keine Wirkung gehabt, da das System beim Ausfall eines Servers dynamisch einen

49 Singer, P. W.; Friedman, A., “Cult of the Cyber Offensive. Why Belief in First Strake Advantage Is Misguided Today as It Was in 1914”, in: *Foreign Policy*, 15.01.2014. http://foreignpolicy.com/2014/01/15/cult-of-the-cyber-offensive/.

50 Lindsay, Jon R., “Stuxnet and the Limits of Cyber Warfare”, in: Security Studies 22 (2013): 365–404, S. 385.

51 Kaspersky Blog, “Stuxnet: Victims Zero”, *Kaspersky*, 2014. https://blog.kaspersky.com/stuxnet-victims-zero/6775/.

52 Lin, Patrick, “Ethics of Hacking Back. Six Arguments from Armed Conflict to Zombies”, wie FN 31, hier: S. 13.

anderen aktiviert hat.[53] In Notsituationen fehlt in der Regel aber das Wissen um solche Eigenschaften des Zielsystems.

Das Beispiel Avalanche ist instruktiv, da Cyber-Angreifer die Angriffe in der Regel von mehreren sogenannten „Launch"-Plattformen starten, die u.a. auch Teil eines Botnetzes sein können. Wird einer dieser Launch-Server durch einen Gegenangriff zerstört, wechselt der Angreifer zum nächsten „fallback"-Server. Der Verteidiger verliert dadurch jedoch die Kenntnis über die Position des Angreifers und weiß somit nicht mehr, von wo der nächste Angriff kommen wird. Im schlimmsten Fall verschießt der Verteidiger sein „Pulver" an gegnerischen „honey pots" und offenbart damit dem Gegner seine Gegenangriffsfähigkeiten.[54] Alternativ kann ein unbesonnener Gegenschlag Computer zerstören, auf denen sich potenziell wichtige forensische Informationen über den Gegner befunden haben. Ob dies der Fall ist, hängt vom technischen Know-How und der Sorgfalt des Gegners ab. Eine gut ausgestattete APT-Gruppe wird resilienter sein als Script-Kiddies. Mit wem man es aber zu tun hat, ist in zeitkritischen Situationen oft nicht klar.

Die Kosten von Cyber-Arsenalen

Es ist also keinesfalls gewährleistet, dass ein Cyber-Gegenangriff als Schnellschuss überhaupt effektiv ist. Um dies zu gewährleisten, müssten Planungen zum Einsatz von „hack back"-Verfahren beinhalten, dass man für geeignete unmittelbare Reaktionen auf Cyber-Attacken die möglichen Schwächen, potentiellen Sicherheitslücken und Zugriffspunkte („Angriffsvektoren") potentieller Gegner bereits im Vorfeld kennt. Folglich müsste man für alle Kontingenzen ein Arsenal vorkonfigurierter und auf bestimmte Zielsysteme verschiedenster politischer Gegenspieler angepasster „Cyber-Angriffswerkzeuge" oder zumindest passender Sicherheitslücken horten und diesen Bestand kontinuierlich aktualisieren. Anders als bei physischen Konflikten bräuchte man hier nicht nur nachrichtendienstliche Informationen über die Systeme geographischer Nachbarn, sondern Informationen von allen potenziellen und relevanten staatlichen und nicht-staatlichen Cyber-Aggressoren. Damit würde konzeptionell anstelle der defensiven Sicherung der eigenen IT-Systeme die – möglicherweise illegitime – Analyse fremder IT-Systeme in Friedenszeiten sowie die Sammlung und Geheimhaltung von Sicherheitslücken in den Fokus von – gegenwärtig in Deutschland ohnehin dünn aufgestellten – staatlichen Cyber-Einheiten treten.

Neben dem personellen Aufwand wäre das Aufstellen von Arsenalen mit einsatzbereiter digitaler Gegenschlags-Software enorm kostspielig. Komplexe Sicherheitslücken, sofern man sie nicht durch eigenen Personalaufwand entdeckt, kosten je nach Zielsystem Hunderttausende oder gar Millionen von Euro. Laut einer Studie der RAND Corporation haben 0-day-Sicherheitslücken eine durchschnittliche Lebenszeit von 6,9 Jahren. Cyber-Arsenale müssten also dauerhaft geprüft und erneuert werden, damit ihre Wirksamkeit gewährleistet werden kann.[55]

Neben Kosten- und Personalfragen stellt sich auch die Frage der Sicherheit. Die jüngsten Vault 7- und Shadowbroker-Leaks zeigen eindrucksvoll, dass Cyber-Arsenale selbst von den besten Geheimdiensten der Welt nicht geheim gehalten werden können.[56] Einstmals kostspielige NSA- und CIA-Angriffstools sind nun frei im Internet verfügbar und somit faktisch wertlos, da Verteidiger mit dem Wissen um diese Tools ihre Systeme schützen können. Dabei gibt es neben der Gefahr, die von Hackern ausgeht, auch die Gefahr von Insidern, die geheime Informationen wie z.B. über Angriffstools preisgeben. Laut einer Studie von Verizon sind Insider für 40 Prozent der Daten-Leaks in Regierungsinstitutionen verantwortlich.[57]

Die Beispiele Vault 7 und Shadowbroker zeigen zudem ein anderes Dilemma der digitalen Revolution: Sind Informationen im Internet erst einmal veröffentlicht, kann dieser Prozess nicht mehr rückgängig gemacht werden. „You cannot steal back a secret".[58] Aus diesem Grund wird auch die Idee eines „hack backs" zur Rettung von Daten vom amerikanischen Depart-

53. "'Avalanche' Network Dismantled in International Cyber Operation", *Europol*, January 12, 2016. https://www.europol.europa.eu/newsroom/news/"avalanche"-network-dismantled-in-international-cyber-operation.
54 Nakashima, Ellen, "It Was Hand-to-Hand Combat: Details of a Cyberattack at State", in: *Washington Post*, 04.04.2017. https://www.pressreader.com/usa/the-washington-post/20170404/281694024627764.
55 Ablon, Lilian; Bogart, Andy, "Zero Days, Thousands of Nights. The Life and Times of Zero-Day Vulnerabilities and Their Exploits", *RAND*, 2016.
56 McLaughlin, Jenna, "Trove of Stolen NSA Data Is 'Devastating' Loss for Intelligence Community", in: *Foreign Policy*, April 17, 2017. http://foreignpolicy.com/2017/04/17/trove-of-stolen-nsa-data-is-devastating-loss-for-intelligence-community/.
57 "Verizon 2017 Data Breach Investigations Report", wie FN 22, hier: S. 28.
58 "Into the Gray Zone. The Private Sector and Active Defense Against Cyber Threats", wie FN 16, hier: S. 12.

ment of Homeland Security als wenig ergiebig abgetan.[59] Hacker kopieren in der Regel gestohlene Informationen auf weitere Rechner, veröffentlichen diese im Darknet oder auf anderen Kanälen (siehe Wikileaks).

Außenpolitische Signalwirkung

Neben den technischen Problemen geht mit Blick auf die zunehmende Militarisierung des Internets[60] von den Debatten über "hack back"-Fähigkeiten und Befugnisse eine zweifelhafte außenpolitische Signalwirkung aus. Wenngleich meist betont wird, dass diese Fähigkeiten ausschließlich für defensive Zwecke im Sinne einer *ultima ratio*-Lösung vorgesehen sind, kann aus technischer Sicht die rein defensive Ausrichtung solcher Hilfsmittel gegenüber anderen internationalen Akteuren nicht glaubhaft belegt werden. Geheimdienste oder militärische Dienste mit Fähigkeiten zum "hack back" sind praktisch auch in der Lage diese proaktiv und explizit offensiv als Angriffsmittel einzusetzen. Eine Abgrenzung von „rein defensiven" "hack back"-Methoden, die über diesen Zweifel erhaben sind, ist nicht möglich. Die Selbstverpflichtung eines Staates zum ausschließlich defensiven Einsatz solcher Mittel ist gegenwärtig aufgrund der fehlenden international verbindlichen Normen zum staatlichen Einsatz von offensiven Cyber-Hilfsmitteln und insbesondere angesichts fehlender Verifikationsmaßnahmen im Cyberspace nicht nachvollziehbar. Damit konterkariert diese weitere Aufrüstung im Cyberspace das sicherheits- und stabilitätsfördernde Konzept der vertrauensbildenden Maßnahmen[61] im Sinne der glaubhaften Versicherung der Abwesenheit von Bedrohungen, sowie der Eingrenzung der eigenen staatlichen Möglichkeiten, in Krisensituationen Druck durch militärische Aktivitäten ausüben zu können.

„Hack back"-Akteure

Neben der Frage, ob es normativ gerechtfertigt und operativ sinnvoll ist, „zurückzuhacken", stellt sich zudem auch die Frage, wer für mögliche Gegenschläge verantwortlich sein sollte. In der Literatur werden folgende Akteure diskutiert: Strafverfolgungsbehörden (wie z.B. FBI oder Bundeskriminalamt), Geheimdienste (z.B. NSA, Bundesnachrichtendienst, Verfassungsschutz), militärische Einheiten (z.B. das Zentrum für Cyberoperationen des Kommandos Cyber und Informationsraum), private Cyber-Sicherheitsfirmen, multinationale Organisationen (NATO oder EU) oder unabhängige und somit vertrauenswürdige Drittparteien (wie etwa das deutsche BSI). Die Frage, welcher dieser Akteure am geeignetsten ist, hängt von den individuellen Fähigkeiten (Personal, Ressourcen, Know-How und Infrastruktur) sowie den rechtlichen Implikationen ab. Hier gibt es ein Dilemma zwischen Kompetenzen und Legalität.

Generell akzeptieren die meisten Staaten, dass internationale und nationale Gesetze im Cyberspace gelten. Viele Staaten haben sich auf internationale Standards geeinigt (Budapester Konvention 2004) und Gesetze erlassen (z.B. Deutschland per StGB § 202c oder in den Vereinigten Staaten der US Computer Fraud and Abuse Act von 1986), die das unbefugte Eindringen in fremde IT-Systeme unter Strafe stellen. Mit anderen Worten: das (in der Regel unbefugte) Hacken von Rechnern in fremden Staaten verletzt in den meisten Fällen lokale Gesetze, egal ob es von Strafverfolgungsbehörden, Privatunternehmen oder patriotischen APT-Gruppen ausgeht. „Hack backs" sind also nach der gegenwärtigen Rechtslage in den meisten Fällen illegal. Allerdings gibt es hier verschiedene rechtliche Grauzonen, etwa bei Hacks durch Nachrichtendienste zur Auslandsüberwachung.[62] Dass insbesondere Nachrichtendienste moderner Industrienationen über technische Fähigkeiten zu „hack backs" verfügen, steht mindestens seit den Leaks von Edward Snowden außer Frage. Aber auch Polizeibehörden wie das FBI entwickeln entsprechende Fähigkeiten. Im Rahmen regulärer Strafverfolungsprozesse ist es Polizeibehörden, häufig auf Richtererlass, zudem erlaubt, in Kernbereiche privater Lebensführung einzudringen, wenn es etwa um Wohnraumüberwachung geht. Beim Hacking bzw. der Quellen-Telekommunikationsüberwachung sind ähnliche Kompetenzen denkbar, auch wenn hier die verfassungsrechtlichen Implikationen sorgfältig geprüft werden müssen.[63] Komplizierter wird es bei den Fragen von internationalen Zu-

59 Vgl. FN 56.

60 Exemplarisch: "The Cyber Index International Security Trends and Realities", *UNIDIR*, Genf: 2013, http://www.unidir.org/files/publications/pdfs/cyber-index-2013-en-463.pdf.

61 Neuneck, G., "Krieg im Internet? Cyberwar in ethischer Reflexion", in: *Handbuch Friedensethik*, Springer Fachmedien, Wiesbaden: 2017.

62 Bitton, Raphael, "The Legitimacy of Spying Among Nations", in: *American University International Law Review* 29 (2014): 1010–65.

63 Bundesverfassungsgericht, Urteil vom 20. April 2016. https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2016/04/rs20160420_1bvr096609.html.

ständigkeiten und Gegenschlägen in Krisensituationen, wenn also Zielserver im Ausland stehen.

Neben der Frage des Rechts, die hier nicht abschließend diskutiert werden kann, stellt sich die Frage nach den Kompetenzen. Insbesondere private Cyber-Sicherheitsfirmen haben in den letzten Jahren eine enorme digitale Expertise aufgebaut.[64] Höhere Löhne, flexible Arbeitszeiten und ein genereller Fachkräftemangel führen in den meisten Staaten dazu, dass einige der besten Hacker in der Privatwirtschaft arbeiten, während staatliche Stellen enorme Rekrutierungsschwierigkeiten haben.[65] Einige Cyber-Sicherheitsfirmen wären technisch durchaus in der Lage zu gezielten digitalen Gegenschlägen. Firmen sind in der Regel die häufigsten Ziele von Cyber-Angriffen und bemerken diese in der Regel auch zuerst. Insofern wird das Argument vorgebracht, dass private Unternehmen in der Regel schneller, flexibler und somit besser auf Angriffe reagieren können als staatliche Stellen.[66] Hunter-Teams der deutschen Telekom könnten zum Beispiel im Angriffsfall vermutlich schneller reagieren als die staatlichen Computer Emergency Response Teams des nationalen Cyberabwehrzentrums. Dies ist auch eine Frage der Kapazitäten: Staatliche Behörden haben in der Regel gar nicht genug Personal, um für die aktive Verteidigung aller Unternehmen oder Betreiber kritischer Infrastrukturen eines Landes zu sorgen, insbesondere wenn diese simultan von einem Cyber-Angriff betroffen sind. Eindrucksvoll ist hier der Hack des Bundestages, der aufgrund fehlender Ressourcen bei staatlichen Stellen nur sehr langsam bewältigt werden konnte.[67] Insofern argumentieren einige, dass private Unternehmen entweder selbst bestimmte, nicht-destruktive "hack back"-Kapazitäten aufstellen oder zumindest vom freien Markt einkaufen sollten.[68] Dazu wird die Analogie von Privatdetektiven oder privaten Sicherheitsfirmen bedient, welche für bestimmte Gegenschläge autorisiert werden könnten. Hierzu müsste es aber einen rechtlichen Rahmen geben, der Fragen der Verantwortlichkeit im Schadensfall regelt und legitime/illegitime Praktiken unterbindet. Dies ist insbesondere ein rechtlich komplexes Unterfangen. In der Literatur werden hierzu verschiedene Modelle diskutiert: etwa „private public partnerships" wie sie heute bei Attributionsprozessen schon üblich sind, Lizenzmodelle, mit denen der Staat ad hoc bestimmte Unternehmen autorisiert im eigenen Namen Gegenschläge auszuführen[69] oder gar die Einrichtung internationaler Organisationen im Sinne der Vereinten Nationen. Microsoft fordert gegenwärtig eine internationale Organisation zur Attribution von Cyber-Angriffen, welche in einem nächsten Schritt auch für Gegenmaßnahmen beauftragt werden könnte.[70]

Gegen all diese Ideen sprechen Argumente der staatlichen Souveränität und des Gewaltmonopols. Nach dem Tallinn-Manual, welches Computer-Netzwerkoperationen verrechtlicht, können Cyber-Angriffe im Sinne des Völkerrechts als Gewaltakt verstanden werden. Wenn nun also private Firmen Cyber-Gegenschläge ausführen, könnte dies zu Vigilantismus bzw. einer Situation führen, die dem Hobbes'schen Naturzustand gleicht: jeder hackt jeden. Das ist insofern problematisch als gemäß dem Völkerrecht Staaten für jegliches Unrecht, das von ihrem Territorium ausgeht, verantwortlich sind („due dilligence").[71] Im Zweifelsfall wäre also der Staat für Schäden verantwortlich, die vom eigenen Territorium ausgehen. Dies würde zumindest dafür sprechen, „hack back"-Kompetenzen bei staatlichen Stellen anzusiedeln.

Ein weiteres Problem privater "hack back"- Akteure betrifft die Kontrolle derselben. Das Problem zeigt sich bereits heute bei Cyber-Sicherheitsfirmen, die für Kunden Cyber-Vorfälle analysieren. Computer-Forensik und -Analyse erfordert die Kenntnis intimster Details der betroffenen Rechner. Dies kann sowohl die

64 Rabkin, Jeremy; Rabkin, Ariel, "Hacking Back Without Cracking Up", in: *Aegis Paper* 1606 (2016), S. 7.
65 Biermann, Kai; Klormann, Sybille, „Freiwillige und Nerds – Was ist das für eine Truppe?" In: *Zeit Online*, 04.05.2017. http://www.zeit.de/digital/internet/2017-04/cyber-armee-bundeswehr-ursula-von-der-leyen.
66 Baker, Stewart; Kerr, Orin; Volokh, Eugene, "The Hackback Debate", *Steptoe Cyberblog*, February 11, 2012. http://www.steptoecyberblog.com/2012/11/02/the-hackback-debate/.
67 Beuth, Patrick; Biermann, Kai; Klingst, Martin; Stark, Holger, „Bundestags-Hack: Merkel und der schicke Bär", wie FN 23.
68 Rosenzweig, Paul; Bucci, Steven P.; Inserra, David, "Next Steps for U.S. Cybersecurity in the Trump Administration: Active Cyber Defense", in: *Backgrounder* 3188 (2017), S. 10.
69 Rabkin, Jeremy; Rabkin, Ariel, "Hacking Back Without Cracking Up", wie FN 64, hier: S. 5.
70 Charney, Scott; English, Erin; Kleiner, Aaron; Malisevic, Nemanja; McKay, Angela; Neutze, Jan; Nicholas, Paul, "From Articulation to Implementation. Enabling Progress on Cybersecurity Norms", Microsoft, 2016. https://www.microsoft.com/en-us/cybersecurity/content-hub/enabling-progress-on-cybersecurity-norms.
71 Bendiek, Annegret, "Sorgfaltsverantwortung im Cyberraum. Leitlinien für eine Deutsche Cyber-Außen- und Sicherheitspolitik." Berlin: *SWP-Studie* 2016/S 03, März 2016.

Privatsphäre von Individuen betreffen als auch Firmengeheimnisse und geistiges Eigentum. Gleiches gilt bei „hack backs“, so paradox es zunächst erscheint. Um die Gefahr des Missbrauchs durch „hack back“-Firmen zu mindern, müssten diese staatlich streng kontrolliert werden. Ob dies effizient und wirkungsvoll gestaltet werden kann, ist eine schwierige Frage.

Aus diesem Grund wird die Idee eines neutralen Akteurs diskutiert, welcher staatlich zertifiziert und kontrolliert ist, gleichzeitig aber kein Interesse am geistigen Eigentum seiner Kunden hat. Diese neutrale Institution würde sowohl von staatlicher als auch privater Seite als vertrauensvoll wahrgenommen. In Deutschland verdient das Bundesamt für die Sicherheit der Informationstechnik dieses Vertrauen. Die primäre Aufgabe des BSI ist die Verteidigung und Sicherung von staatlichen Systemen, etwa durch definierte Standards und Zertifizierungen, aber auch durch CERT-Teams, „awareness raising“, Schulungen und Weiterbildungen. Würde das BSI die Befugnis zu „hack back“-Fähigkeiten erhalten, also offensiv tätig werden, könnte dies seine defensive Funktion schwächen.[72]

Erstens gibt es einen aus den USA bekannten Interessengegensatz zwischen offensiven und defensiven Operationen: Der Angreifer braucht unsichere Systeme und unbekannte Schwachstellen für Cyber-Angriffe. Der Verteidiger will diese aber schließen. Liegen beide Funktionen bei derselben Behörde, kann ein offensiver Bias entstehen. Anstatt Sicherheitslücken zu schließen, werden diese offen gehalten. Offensive Cyber-Fähigkeiten schwächen also die defensive Mission der Behörden.[73]

Das zweite Problem betrifft das Vertrauen, welches unabhängige, neutrale Behörden genießen. Deutsche Firmen müssen z.B. darauf vertrauen, dass die Cyber-Sicherheitszertifizierungen und Produktempfehlungen des BSI keine geheimen Hintertüren oder absichtliche Schwachstellen beinhalten. Würde das BSI offensiv tätig werden, stünde wie bei den Geheimdiensten der Verdacht im Raum, dass diese z.B. Schwachstellen in bereits zertifizierten Geräten mandatieren. Die Snowden-Enthüllungen bestätigten z.B. das Gerücht, dass die NSA Sicherheitslücken in CISCO-Systemen mandatiert hat, ähnlich wie bei chinesischen Diensten davon ausgegangen wird, dass diese chinesische Hard- und Software mit Hintertüren versehen, weshalb sie nicht in Hochsicherheitsbereichen der US-Regierung eingesetzt werden.[74] Da Vertrauen essenziell für die Cyber-Sicherheit ist, ist eine organisationale Trennung von offensiven und defensiven Fähigkeiten zu bevorzugen. Aus dem gleichen Grund hat z.B. die Obama-Administration als eine der letzten ihrer Amtshandlungen die Doppelrolle der NSA in Cyber-Offensive und -Defensive innerhalb des US Cyber Commands beendet.[75]

Neben den Problemen des Vertrauens, Rechts und der Fähigkeiten muss allerdings festgehalten werden, dass die zuvor aufgeworfenen Fragen der zeitgemäßen Detektion, Attribution und angemessenen Reaktion sowohl für staatliche als auch nichtstaatliche Akteure gleichermaßen gelten.

Fazit

Digitale Gegenschläge in Krisensituationen zeigen ein interessantes Dilemma. Zwar mögen Gegenschläge bei einem großangelegten, destruktiven Cyber-Angriff völkerrechtlich legitim sein, um größeren Schaden abzuwenden, dennoch sind „hack backs“ in solchen Notsituationen wahrscheinlich ineffektiv und mit höheren Kosten als Nutzen verbunden. Es ist unklar, ob überhaupt rechtzeitig ein Gegner bestimmt werden kann oder ob man nicht in die Falle tappt und das falsche Ziel, etwa ein Krankenhaus, trifft. Findige Gegner könnten, je mehr Staaten digitale Gegenschläge legitimieren, bewusst auf die Strategie „menschlicher Schutzschilde“ setzen, um die Kosten für einen Gegenschlag in die Höhe zu treiben. Die Gefahr von Kollateralschäden ist insbesondere bei Schnellschüssen in Krisenreaktionen hoch. Ferner ist in Krisensituationen oftmals nicht genug Zeit um das Zielsystem,

72 Tanriverdi, Hakan, “Hacking Back: BSI diskutiert digitale Gegenschläge“, in: *Süddeutsche Zeitung online*, 21.06.2017. http://www.sueddeutsche.de/digital/it-sicherheit-bundesbehoerde-diskutiert-ob-sie-zurueck-hacken-soll-1.3554124.

73 Sasso, Brendan, “The NSA Isn’t Just Spying on Us, It’s Also Undermining Internet Security”, in: *The Atlantic*, April 29, 2014. https://www.theatlantic.com/politics/archive/2014/04/the-nsa-isnt-just-spying-on-us-its-also-undermining-internet-security/457038/.

74 Goodin, Dan, “Cisco Confirms NSA-Linked Zeroday Target Its Firewalls for Years”, in: *Ars Technica*, August 18, 2016. https://arstechnica.com/security/2016/08/cisco-confirms-nsa-linked-zeroday-targeted-its-firewalls-for-years/.

75 Nakashima, Ellen. “Obama Moves to Split Cyberwarfare Command from the NSA”, in: *Washington Post*, 23.06.2016. https://www.washingtonpost.com/world/national-security/obama-moves-to-split-cyberwarfare-command-from-the-nsa/2016/12/23/a7707fc4-c95b-11e6-8bee-54e800ef2a63_story.html?utm_term=.8e222a8b157c.

sofern man es findet, auf etwaige Fallen und „honey pots“ zu analysieren. D.h. ein Gegenschlag birgt auch die Gefahr, die eigenen Fähigkeiten zu offenbaren. Datenrettungsmissionen sind ebenfalls von ungewissen Erfolg, da Cyber-Kriminelle gestohlene Daten vervielfältigen. Insgesamt ist der Nutzen von digitalen Gegenschlägen mit dem Ziel, ein System zu zerstören, eher zweifelhaft. Andere, aktivere Maßnahmen der Verteidigung wie Hunter-Teams, das Umleiten von DDoS-Traffic oder „honey pots“ erscheinen da sinnvoller und rechtlich unproblematischer. Bei Botnetzen und Cyber-Kriminalität sieht die Sache anders aus. Aus Sicht von Strafverfolgungsbehörden und Nachrichtendiensten sind „hack backs“ mit dem Ziel der Informationsgewinnung dem bloßen Zerstören von Zielsystemen vorzuziehen. Andererseits kann man sich in solchen Fällen selten auf das Recht zur Selbstverteidigung berufen.

Sollten Gegenschläge trotz ihres zweifelhaften Nutzens legitimiert werden, müssen sich politische Entscheidungsträger zudem Gedanken über Verantwortlichkeiten, die Art des Gegenschlages sowie die Regeln und Grenzen solcher Operationen machen. Im Sinne guter Diplomatie mag es sinnvoll sein, Gegenschläge über diplomatische Kanäle anzukündigen, gleichzeitig vermindert dies vermutlich ihre Wirksamkeit. Versteckte Gegenschläge, sofern sie attribuierbar sind, können *ex ante* bestehende diplomatische Krisen noch verschärfen. Dies gilt insbesondere bei destruktiven Gegenschlägen, welche ein Ziel permanent zerstören. In den USA dürfen solche Schläge mit hohem Eskalationspotenzial nur auf Anordnung des Präsidenten ausgeführt werden. Sie dürfen auch nur eine *ultima ratio* sein, zu der man greift, wenn sich andere diplomatische Verfahren als wirkungslos herausstellen. Ferner sollte bei solchen Gegenschlägen ein multilateraler Prozess vorgeschaltet sein, der sicherstellt, dass man nicht versehentlich wichtige Beweismittel zerstört, die für strafrechtliche Ermittlungen relevant sind. Da das Internet ein globales Medium ist, sollte staatliches Verhalten auch zunehmend überstaatlich abgesichert sein.

Glossar

Advanced Persistent Threat – „Ein sogenannter Advanced Persistent Threat (APT) ist ein Netzwerk-Angriff, bei dem sich eine unautorisierte Person Zugriff auf ein Netzwerk verschafft und sich dort so lange wie möglich unentdeckt aufhält. Die Intention eines APT-Angriffs ist in erster Linie, Daten zu stehlen und keinen sonstigen Schaden anzurichten. Ziel solcher APT-Angriffe sind oftmals Organisationen in Bereichen, bei denen sehr wertvolle Informationen zu holen sind."[76]

Attributionsproblem – Das Attributionsproblem beschreibt die Schwierigkeit den Urheber einer Cyber-Attacke zu identifizieren, da diese oftmals nur schwer sichtbare digitale Spuren hinterlassen und Beweismittel leicht zu fälschen. Ferner kann technische Forensik in der Regel nur die Maschine identifizieren, von der ein Angriff ausging, was aber keine Rückschlüsse auf den Täter (Urheber) bzw. dessen Auftraggeber oder Sponsor zulässt (soziale bzw. politische Attribution).[77]

Beacon – „Beacons sind Codeteile die in sensitive Dokumente eingebettet werden und den Besitzer informieren, wenn auf diese Dokumente zugegriffen wird oder diese aus dem eigenen Netzwerk entwendet werden. Aggressive Beacons können selbst aus Schadsoftware fungieren und den Rechner des Diebes infizieren um etwa Informationen an den Besitzer zu schicken."[78]

Botnetz – „Ein Botnet, auch als Botnetz oder Zombie-Armee bekannt, ist eine Reihe von Computer, die ohne das Wissen ihrer Besitzer dazu verwendet werden, um Dateien (inklusive Spam und Viren) über das Internet an andere Computer zu senden. Ein solcher Computer wird oftmals als „Zombie" bezeichnet, im Endeffekt ist der Computer ein Roboter (oder kurz „Bot" genannt), der den Anweisungen eines Auftraggebers folgt, um Spam zu versenden oder andere Rechner mit Viren zu infizieren. Die meisten hiervon betroffenen Systeme sind private Computer."[79]

Computer Incident/Emergency Response Teams (CERT) – „Ein CERT-Team besteht aus EDV-Sicherheitsfachleuten, die bei der Lösung konkreter IT-Sicherheitsvorfälle mitwirken. Typische Anwendungsgebiete sind das Bekanntwerden von Sicherheitslücken, die Verbreitung neuartiger Viren oder gezielte Angriffe auf Server. Die Experten-Teams wirken bei der Problemlösung als Koordinatoren mit oder beschäftigen sich ganz allgemein mit Problemlösungen. Das Ziel der Tätigkeit liegt in der Vermittlung von Lösungsansätzen und der Warnung vor Sicherheitslücken."[80]

Command and Control (C2) Server – „Bei einem Command and Control Server (C&C-Server) handelt es sich um den zentralen Computer, der Befehle an ein sogenanntes Botnet absetzt und anschließend die zurückgesandten Berichte der ausgewählten Computer empfängt."[81]

DDoS – „Bei einem Distributed Denial-of-Service (DDoS)-Angriff wird eine große Zahl infiltrierter Systeme für den Angriff auf ein einzelnes Ziel mobilisiert. Das Ziel-System kann diesen Ansturm meist nicht bewältigen und ist dadurch für seine Nutzer nicht mehr erreichbar. Die Flut eingehender Nachrichten erzwingt eine Abschaltung des Systems und somit auch der über dieses System für legitime Nutzer bereitgestellten Dienste."[82]

Defacement von Websites - „Website Defacement (Beschmutzung) beschreibt das Beschmieren oder das Verändern von Inhalten auf Websites, um z.B. politische Botschaften zu verbreiten."[83]

Honeypot (Honigtopf) – „Ein Honeypot, auch Honigtopf genannt, ist ein Computersystem im Internet, das explizit darauf abzielt, Leute anzulocken und „einzufangen", die versuchen, in fremde Computersysteme einzudringen. Dies beinhaltet unter anderem Hacker, Cracker und sogenannte Script Kiddies."[84]

Hunter Team (Jäger) – „Jäger Teams durchsuchen proaktive eigene Netzwerke nach Eindringlingen und versuchen deren Modus Operandi zu identifizieren und die Bedrohung zu isolieren, solange sie im eigenen Netz existiert."[85]

Intrusion Detection System – „Ein IDS (Intrusion Detection System) ist ein Gerät oder eine Software-Anwendung, die einen Administrator im Falle einer Security- oder Policy-Verletzung benachrichtigt. Das System wird auch aktiv, sollte das IT-Netzwerk (Information Technology) des Administrators in irgendeiner anderen Form kompromittiert sein."[86]

76 http://www.searchsecurity.de/definition/Advanced-Persistent-Threat-APT
77 https://www.wired.com/2016/12/hacker-lexicon-attribution-problem/
78 https://cchs.gwu.edu/sites/cchs.gwu.edu/files/downloads/CCHS-ActiveDefenseReportFINAL.pdf
79 http://www.searchsecurity.de/definition/Botnet
80 http://www.egovernment-computing.de/was-ist-ein-cert-a-579250/
81 http://www.searchsecurity.de/definition/Command-and-Control-Server-CC-Server
82 http://www.searchsecurity.de/definition/Distributed-Denial-of-Service-DDoS-Angriff
83 https://www.trendmicro.com/vinfo/us/security/definition/website-defacement
84 http://www.searchsecurity.de/definition/Honeypot-Honigtopf
85 http://www.techrepublic.com/article/cyber-threat-hunting-why-this-active-strategy-gives-analysts-an-edge/
86 http://www.searchsecurity.de/definition/Intrusion-

Phishing – „Phishing bezeichnet einen per E-Mail durchgeführten Betrugsversuch, bei dem der Empfänger eine echt wirkende E-Mail erhält. Allerdings ist diese präpariert und soll ihn zur Preisgabe persönlicher und finanzieller Daten verleiten. Meist scheinen diese E-Mails von bekannten und vertrauenswürdigen Webseiten zu stammen."[87]

Penetration & Payload. Cyber-Angriffe laufen in mehreren Phasen ab. Die Phase der Penetration beschreibt das Eindringen in ein IT-System durch das Auskundschaften und Ausnutzen von Schwachstellen in der Verteidigung. Nachdem auf ein System zugegriffen wurde und dieser Zugriff dauerhaft gewährleistet ist, kann ein Payload, also eine konkrete Funktion, wie etwa key-logging, Datendiebstahl, Rechtediebstahl, löschen oder „wiping" von Daten etc., ausgeführt.

SCADA – „Unter Supervisory Control and Data Acquisition (SCADA) versteht man das Überwachen und Steuern technischer Prozesse mittels eines Computer-Systems."[88]

Social Engineering – „Der Begriff „Social Engineering" bezeichnet eine Vorgehensweise, bei der die Schwachstelle Mensch ausgenutzt wird. Oft werden dabei Mitarbeiter eines Unternehmens mit einem Trick überredet, die normalen Sicherheitsvorkehrungen zu umgehen und sensible Informationen preiszugeben."[89]

Watering Hole – „Ein Watering-Hole-Angriff ist ein Security Exploit, bei dem ein Cyberkrimineller eine bestimmte Gruppe an Endanwendern anvisiert. Dabei infiziert er Websites, von denen der Angreifern weiß, dass die Mitglieder der Zielgruppe diese immer wieder aufsuchen. Das Ziel ist es, den Computer eines Opfers zu infizieren und sich damit Zugriff auf das Netzwerk an dessen Arbeitsstelle zu verschaffen."[90]

Zero-Day (0-Day) – „Eine Zero-Day-Lücke ist eine Schwachstelle im IT-System einer Firma. Die betroffene Software, Hardware oder Firmware lässt sich zunächst nicht dagegen schützen. Ein potenzieller Angriff (Zero-Day-Exploit) erfolgt am selben Tag, an dem die Security-Lücke entdeckt wurde. Die Schwachstelle wird daher Zero-Day-Lücke genannt, da zwischen der Entdeckung des ersten Angriffs und der Sicherheitslücke Null Tage liegen."[91]

Detection-System-IDS
87 http://www.searchsecurity.de/definition/Phishing
88 https://de.wikipedia.org/wiki/Supervisory_Control_and_Data_Acquisition
89 http://www.searchsecurity.de/definition/Social-Engineering
90 http://www.searchsecurity.de/definition/Watering-Hole-Angriff-Auflauern-an-der-Wasserstelle
91 http://www.searchsecurity.de/definition/Zero-Day-Luecke