

15. Jun. 2011

von Martin

in Cyber Security,  
Sicherheitskultur,  
Versicherheitlichung

Kommentare ( 0 )

## Bomben auf Botnets

von *Martin Schmetz*

Der Spruch “The internet is serious business” [[Quelle](#)] ist ein alter Witz unter Nerds und wird immer wieder gerne zitiert, wenn einige Nutzer online Dinge etwas zu ernst nehmen. Da Cybersecurity wohl endgültig im sicherheitspolitischen Mainstream [[Quelle](#)] angekommen ist, war es nur eine Frage der Zeit, bis das Internet auch dort “serious business” sein würde. Spätestens mit der Ankündigung der USA [[Quelle](#)], auf Cyberangriffe potentiell auch mit Waffengewalt zu reagieren, ist dies nun eingetreten. Ist ein Cyberangriff demnach in seiner Schwere äquivalent zu einem Angriff in der realen Welt, so muss der Angreifer mit Gegenschlägen mit konventionellen Waffen rechnen.

Die Idee der Äquivalenz hat es den Generälen dabei besonders angetan, ermöglicht sie doch elegant eine Brücke von Cyberangriffen zu Schäden in der physischen Welt zu schlagen: Wenn ein Cyberangriff in seinen Auswirkungen mit einem wie auch immer gearteten Angriff mit konventionellen Waffen vergleichbar ist – sei es durch den Tod von Bürgern, der Störung oder gar physischen Zerstörung von Infrastruktur - dann ist ein Gegenschlag ein legitimes Mittel der Selbstverteidigung.

Jedoch gibt es eine ganze Reihe von Problemen, die diese Ankündigung (hoffentlich) im Bereich der Rhetorik verbleiben lassen. Erstens sind Angriffe im Netz meist nicht einem einzelnen Akteur zuzuweisen, wenn dieser nicht konkret selbst die Verantwortung dafür übernimmt. Manchmal kann nach intensiver Recherche und mit einiger zeitlicher Distanz ein Angriff zugeordnet werden, zum Beispiel durch die Übernahme eines Botnets [[Quelle](#)]. Aber auch dies kann nur selten mit absoluter Sicherheit geschehen. Zweitens sind die von den USA gewählten Auswirkungen extrem vage und breit gewählt: Tote durch einen Cyberangriff hervorzurufen ist zwar denkbar, erscheint aber weit weniger wahrscheinlich als die Störung von Infrastruktur. Drittens wird nicht klar gemacht, welche Ziele als Begründung für einen Angriff herhalten müssten: Sind es lediglich staatliche Ziele oder gilt auch der Angriff auf nichtstaatliche Ziele (etwa der Hack bei Lockheed Martin [[Quelle](#)]) als legitimer Grund? Speziell letzteres Beispiel zeigt ein weiteres Problem der Gefahrenlage und ihrer Wahrnehmung auf: Man spricht zwar von gerne von Cyberwar, aber der Hack bei Lockheed Martin war, wie in den meisten Fällen, Industriespionage und kein Angriff. Ziel waren Informationen, nicht die Zerstörung von Eigentum oder Infrastruktur. Spionage alleine wird aber kaum als Kriegsgrund taugen können.

### SOCIAL MEDIA



### SUCHE

### TWITTER FEED

In den nächsten Wochen bei uns: Eine Beitragsreihe zu #Cyberpeace. Großartige Autoren, spannende Posts! [@fiff\\_de](http://t.co/z54MUpBFNc)  
3. Dezember 2014, 12:28 von &s

Ein kleiner Konferenzbericht zur #doeff14 von @seditioni und ein großes Lob an die Organisator\_innen! <http://t.co/tUtsCX4Vdg>  
1. Dezember 2014, 10:08 von &s

### TAGS

Andere Angriffe, etwa der von LulzSecurity auf ein dem FBI nahe stehendem Unternehmen [[Quelle](#)], stammen explizit nicht von staatlichen Akteuren und haben zudem den erheblichen Nachteil, dass die Angreifer vermutlich entweder in den USA selbst oder zumindest einem alliierten Land sitzen. Damit könnten sie mit strafrechtlichen Mitteln verfolgt werden, fallen aber aus der Zuständigkeit des Militärs heraus, womit die Androhung von Bomben sinnlos wird.

Im schlimmsten Fall spornt die Androhung von Bomben nichtstaatliche Hackergruppen sogar noch an. Im heute bekannt gewordenen Fall des Hacks der Webseite des US-Senats [[Quelle](#)] fragt LulzSecurity provokativ nach ob sie mit der Veröffentlichung der dort erhaltenen Daten einen Kriegsakt begehen.

Mit militärischen Mitteln auf Online-Attacken zu reagieren: Diese Drohung soll Länder vom Eindringen in amerikanische Systeme abhalten. Stattdessen wirkt sie irgendwie unangemessen, unrealistisch und ein wenig verzweifelt – man weiß sich scheinbar nicht anders zu helfen und holt den Vorschlaghammer raus. Früher sprach man oft davon mit Kanonen auf Spatzen zu schießen. Heute wirft man Bomben auf Botnets.

 Tags: [Botnet](#), [Cyberangriff](#), [Cyberwar](#), [Hack](#), [Infrastruktur](#), [LulzSec](#), [Online-Attacken](#)

« [Spundekäs' statt Salat](#) »

[Unsichere Natur?](#) »

BELIEBT KOMMENTARE NEU

Hell yeah, it's Political Science!  
Wissenschaftliche Podcasts

Das Internet darf ein cyberfreier  
Raum sein

Deutschlands Irak-Politik –  
Verantwortung nach außen,  
Intransparenz nach innen.

Wir haben Geburtstag!

„Mit Sicherheit nicht!“ Sexuelle  
Gewalt als politisches Mittel

## KATEGORIEN

[Außenpolitik \(59\)](#)

[Bürgerkriege \(16\)](#)

[Cyber Security \(40\)](#)

[Demokratisierung \(9\)](#)

[Drohnen \(15\)](#)

[Humanitäre Interventionen \(15\)](#)

[Innere Sicherheit \(24\)](#)

[Interviews \(10\)](#)

[Katastrophen \(4\)](#)

[Konferenz \(20\)](#)

[Militär \(27\)](#)

[Pandemien \(2\)](#)

[Podcast \(7\)](#)

[Popkultur \(20\)](#)

[Sanktionen \(8\)](#)

[Security Culture \(13\)](#)

[Sicherheits-Kommunikation \(14\)](#)

[Sicherheitskultur \(204\)](#)

[Sozialwissenschaft Online \(56\)](#)

**Bislang keine Kommentare**

**Einen Kommentar hinterlassen**

Name

Email

Webseite

Kommentar

Geben Sie den Text ein.  reCAPTCHA



 

[Datenschutz - Nutzungsbedingungen](#)

Benachrichtige mich über nachfolgende Kommentare per E-Mail.

[Stellenangebote \(41\)](#)

[Strategie \(10\)](#)

[Terrorismus \(14\)](#)

[Theorie \(2\)](#)

[Umwelt \(1\)](#)

[Versicherheitslichung \(21\)](#)

[Visualisierung \(5\)](#)

[Whistleblowing \(8\)](#)

[WikiLeaks \(17\)](#)

[WMD \(10\)](#)

[Zivilgesellschaft \(48\)](#)

## BLOGROLL

 [Arbeitskreis soziale Bewegungen](#)

 [Augen geradaus](#)

 [Dan Drezner](#)

 [Dart-Throwing Chimp](#)

 [David Campbell](#)

 [de.hypotheses.org](#)

 [Demokratieforschung Göttingen](#)

 [Duck Of Minerva](#)

 [Future and Politics](#)

[Hylaeen Flow](#)

 [Internet und Politik](#)

 [IR Blog](#)

 [Just Security Blog](#)

 [justsecurity.org](#)

 [Killer Apps](#)

 [Kings Of War](#)

 [netzpolitik.org](http://netzpolitik.org)

 [shabka.org](http://shabka.org)

 [Terrorismus in Deutschland](#)

 [theorieblog.de](http://theorieblog.de)

 [Verfassungsblog](#)

 [Vom Bohren harter Bretter](#)

 [whistleblower-net.de](http://whistleblower-net.de)

## ARCHIV

Wähle den Monat



Impressum | 

Dieses Werk bzw. Inhalt steht unter einer Creative Commons Namensnennung-NichtKommerziell-KeineBearbeitung 3.0 Unported Lizenz.

Über diese Lizenz hinausgehende Erlaubnisse können Sie unter [redaktion@sicherheitspolitik-blog.de](mailto:redaktion@sicherheitspolitik-blog.de) erhalten