15. Aug. 2014

von Martin

in Cyber Security

Kommentare (0)

Stell dir vor es ist Cyberkrieg und keiner merkts: Wieso der NSA Hack syrischer Router ein ziemliches Problem für das Konzept des Cyberkriegs ist

Edward Snowden verkündete in einem Interview mit Wired, dass der Ausfall des kompletten syrischen Internets im Jahr 2012 gar nicht vom Assadregime ausging, wie damals vermutet, sondern von einem missglückten Hack syrischer Router durch die NSA. Und wir haben ein Problem, denn wir wissen nicht so richtig, wie wir das deuten sollen. Ist das nun Cyberkrieg? Sollen wir Angst haben? Auf der einen Seite wird gewarnt, dass Cyberkrieg direkt vor der Tür steht und überhaupt, ja, wir alle sollten sehr, sehr viel Angst haben. Andere bezweifeln es – Cyberkrieg wird niemals stattfinden. Die verbitterten spielen Buzzwordbingo und sind wahrscheinlich schon mit dem Wort Cyberkrieg bedient. Dabei ist man sich nicht einmal einig, was Cyberkrieg eigentlich ist, schon gar nicht aus der Sicht internationalen Rechts. Es wurde bis jetzt sehr wenig dazu geschrieben, was auf internationaler Ebene relevant wäre. Ein wichtiges, wenn auch nicht rechtlich bindendes Dokument, ist das Tallinn Manual der NATO. Vielleicht kann uns das ja weiterhelfen.

Gott sei Dank müssen wir nicht weit lesen, um fündig zu werden: Die Regel 1 des Tallinn Manuals beschäftigt sich mit Souveränität und sagt im Abschnitt 6:

> *„A cyber operation by a State directed against cyber infrastructure located in another State may violate the latter's sovereignty. It certainly does so if it causes damage. [...]“*

Der Ausfall der syrischen Router war die Folge einer nicht geglückten Infektion mit einem Schadprogramm. Ob auch das als Angriff zu werten ist, darüber sind sich Experten nicht einig, so die Regel. Im Allgemeinen geht man bei Schadsoftware davon aus, dass diese die Funktionsweise der Hardware nicht fundamental beeinträchtigt, das ist auch schlicht zu auffällig als Angriff. Im vorliegenden Fall war die Infektion nicht erfolgreich, dafür aber die Hardware zerstört und Syrien offline. Ist das nun ein Angriff? In Abschnitt 7 der Regel 1 wird eine wichtige Unterscheidung gemacht zwischen

SOCIAL MEDIA

SUCHE

Suche...

Suche

TWITTER FEED

Ben Kamis: The concept of #cyberpeace is linguistic trolling. Cyberpeace: post-war is war, only more so http://t.co/fkaHhcgekK #cyberwar

ungefähr 51 Minuten her von &s

Wer wissen will was #cyberpeace ist, sollte wissen was dieser sog. #cyberkrieg ist: Matthias Schulze dazu bei uns http://t.co/LyvFdE29dN

8. Dezember 2014, 11:08 von &s

Neue #Jobs für Politikwissenschaftler_innen! http://t.co/f3vSzfJpMG

5. Dezember 2014, 9:03 von &s

TAGS

Angriffen und Eingriffen, die nicht als Angriff zu werten sind: Angriffe sind in der Regel „coercive“, man möchte durch den Angriff also einen anderen Staat dazu zwingen, etwas zu tun oder zu lassen.

Und ein derartiger Angriff wäre tatsächlich auch nach internationalem Recht als solcher zu werten – der so angegriffene Staat dürfte sich also wehren. Regel 9 führt aus:

> *„A state injured by an internationally wrongful act my resort to proportionate countermeasures, including cyber countermeasures, against the responsible State.“*

Ein Staat darf also im verhältnismäßigen Rahmen zurückschlagen, auch mit Cyberangriffen. Allerdings wird in der Regel weiter ausgeführt, dass dies nur im Rahmen internationalen Rechts erfolgen darf und erst nachdem man dies auf diplomatischer Ebene kritisiert hat.

Davon kann im vorliegenden Fall nicht die Rede sein. Syrien hat den Angriff offiziell nie als solchen bezeichnet, möglicherweise nie bemerkt. Wired vermutet, dass man zu sehr damit beschäftigt war, die Router zu reparieren, als dass man Zeit für eine Auswertung gehabt hätte. Auch der Zwangsaspekt (also „coercive“) ist nicht gegeben: Ziel der NSA war es, möglichst viele Daten abzugreifen. Der Hack selbst sollte gar nicht bemerkt werden. Damit kann man natürlich dementsprechend auch keinen Staat zu etwas zwingen – wäre der Hack erfolgreich gewesen, hätten die Syrer nichts gemerkt.

Aber der Zwangsaspekt muss nicht gegeben sein, um einen Angriff darzustellen. Dabei helfen uns die Regeln 11 und 13, die sich mit „use of force“, also Gewaltanwendung befassen. Gewaltanwendung ist illegal und Staaten dürfen darauf im Rahmen der Selbstverteidigung mit Gewalt antworten (Regel 13). Demnach ist der Zwangsaspekt (also „coercive“) zwar der beste Indikator für Gewaltanwendung, aber nicht der einzige: Als konkretes Beispiel für einen Angriff wird in Regel 13 Stuxnet genannt. Stuxnet hatte keinen direkten Zwangsaspekt – man wollte das Anreicherungsprogramm des Irans stoppen oder verzögern. Idealerweise hätte der Iran den Cyberangriff nie bemerkt, sondern an anderer Stelle immer weiter gesucht und so viel Zeit verloren. Ein offener Zwang war also nicht geben. Aber Regel 11 führt aus:

> *„A cyber operation constitutes a use of force, when its scale and effects are comparable to non-cyber operations rising to the level of a use of force.“*

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 (42)

Demokratisierung (9)

Drohnen (15)

Humanitäre Interventionen (15)

Innere Sicherheit (24)

Interviews (10)

Katastrophen (4)

Konferenz (20)

Militär (28)

Pandemien (2)

Podcast (7)

Popkultur (21)

Sanktionen (8)

Security Culture (14)

Leider bleibt der weitere Text auch hier unscharf, jedenfalls was es den vorliegenden Fall angeht. Demnach wäre beispielsweise die Unterstützung von Hacktivists keine Gewaltanwendung. Um herauszufinden, ob der Angriff einem konventionellen Angriff entspricht, gilt es diesen in mit einem solchen zu vergleichen (Regel 1, Abschnitt 6). Genauer schaut man dazu auf die Schwere der Auswirkungen des Angriffs im Vergleich zu kinetischen Angriffen. Wie schwer sind die Auswirkungen, wie direkt (zeitlich und kausal), wie stark ist der Eingriff in die Gesellschaft/Infrastruktur des Landes, wie messbar sind die Effekte, hat das ganze militärischen Charakter usw. (Regel 11, Abschnitt 9).

Vermutlich würde man demnach antworten: Ja, dann handelt es sich um einen Angriff. Immerhin wurde hier ein komplettes Land vom Netz genommen. Derart die Kommunikationsinfrastruktur eines Landes zu lähmen ist auch Teil eines konventionellen, kinetischen Angriffs. Entsprechend kann man wohl gerade was die Schwere und den Eingriff in das Funktionieren des Landes angeht durchaus von einem Angriff sprechen.

Trotz des sehr detaillierten Tallinn Manuals (300 Seiten!) bleibt man aber unbefriedigt zurück: War das nun ein Angriff oder nicht? Hätte Syrien sich wehren dürfen? Wir wissen es nicht, aber wir sollten auch nicht verwundert sein: Wer rechnet schon damit, dass der Angegriffene nicht bemerkt, dass er angegriffen wird, und dass der Angreifer den Angriff so eigentlich gar nicht durchführen will?

Aber damit haben wir nun auf mehreren Ebenen ein Problem: Erstens wissen wir nicht, ob es als Angriff zählen soll, weil zwar die Effekte ganz klar dafür sprechen, aber die syrische Reaktion, die Tatsache, dass es eigentlich ein Unfall war, sowie der Mangel an Zwang dagegen sprechen. Rein rechtlich helfen unsere Regeln uns nicht weiter.

Zweitens haben wir ein großes Problem für die Disziplin der Internationalen Beziehungen und ihre ganze Diskussion um Balance von offensiven und defensiven Fähigkeiten im Bereich Cyberwar: Es gibt sowieso schon nicht viele Beispiele für Cyberwar. Ein bis jetzt hypothetisches, aber beliebtes Katastrophenszenario war aber gerade das Abschalten des Internets in einem ganzen Land. Man war sich sicher: Das würde als Cyberkrieg gewertet und entsprechende Antworten nach sich ziehen. Nun ist genau das passiert und niemand hat es bemerkt, wohl auch weil in Syrien sowieso schon Krieg herrschte.

Aber gerade der letzte Punkt ist immens wichtig für die Diskussion um Cyberkrieg: Welchen strategischen Sinn macht ein Angriff mit derartigen Auswirkungen außerhalb eines größeren Kriegskontexts? Wenn man die Konfusion, die durch die temporäre Kommunikationsstörung ausgelöst wird, nicht zeitnah durch einen konventionellen Angriff ausnutzt, wird man ein Land wahrscheinlich zu nichts zwingen können. Aber genau darum geht es im Krieg. Wie Clausewitz schrieb: “Der Krieg ist also ein Akt der Gewalt, um

Sicherheits-Kommunikation (14)
Sicherheitskultur (205)
Sozialwissenschaft Online (57)
Stellenangebote (42)
Strategie (10)
Terrorismus (14)
Theorie (2)
Umwelt (1)
Versicherheitlichung (22)
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
Hylaean Flow
Internet und Politik
IR Blog
Just Security Blog
justsecurity.org
Killer Apps
Kings Of War

den Gegner zur Erfüllung unseres Willens zu zwingen."

Syrien aber nahm den Angriff nicht als solchen war, entsprechend wurde es auch zu keiner Verhaltensänderung gezwungen – nicht, dass dies jemals die Absicht gewesen wäre. Und es ist auch nicht das erste mal (wir denken wieder an Stuxnet), dass ein Akt des Cyberkriegs, der nicht Teil eines größeren Angriffs inklusive konventionellen Waffen war, keine Verhaltsänderung erzwingen sollte oder konnte. Macht es dann aber überhaupt noch Sinn, von Cyberkrieg als separatem Phänomen zu sprechen? So wie es aussieht, haben wir es entweder mit nachrichtendienstlichen Aktivitäten zu tun, die zwar hochproblematisch sind, aber bei denen es sich nicht um Krieg handelt, oder aber es findet in einem größeren Kriegskontext statt. Dann aber sind Cyberangriffe nur eine Waffe unter vielen und kein eigener Krieg.

Tags: Cyber Security, cyber sicherheit, Cyber War, Cyberkrieg, cybersicherheit, Cyberwar, Hack, Internet, nsa, snowden, Syrien

« Stellenanzeigen Juli 2/2

Stellenanzeigen August 1/2 »

Bislang keine Kommentare

Einen Kommentar hinterlassen

Name

Email

Webseite

Kommentar

Geben Sie den Text ein.

reCAPTCHA

netzpolitik.org

percepticon

shabka.org

Terrorismus in Deutschland

theorieblog.de

Verfassungsblog

Vom Bohren harter Bretter

whistleblower-net.de

ARCHIV

Wähle den Monat

Bestätigen

Datenschutz - Nutzungsbedingungen

Kommentar senden

☑ Benachrichtige mich über nachfolgende Kommentare per E-Mail.