20. Dez. 2010

von Martin

in Cyber Security, Sicherheitskultur, Versicherheitlichung

Kommentare (0)

Krieg im Internet?

Die Macht und Ohnmacht von Staaten

von Martin Schmetz

> *„As a doctrinal matter, the Pentagon has formally recognized cyberspace as a new domain of warfare.“* – William J. Lynn, US Deputy Secretary of Defense [Quelle]

Man befindet sich im Krieg: Mit der zunehmenden Vernetzung der Welt entstehen neue Sicherheitsherausforderungen. Angriffe im Internet sind keine Seltenheit mehr und die Frage, wie man damit umgeht steht überall auf der Tagesordnung. Die NATO führte mit der „Cyber Coalition 2010 Exercise“ erstmals ein Cyberwar-Manöver durch und die USA aktivierten 2010 eine reine Cyberwar-Einheit [Quelle]. Sowohl auf staatlicher als auch zwischenstaatlicher Ebene haben sich die Räder in Bewegung gesetzt um den neuen Bedrohungen zu begegnen.

Derweil erklärt Anonymous als nichtstaatlicher Akteur all jenen den Krieg , die sich nach ihrer Ansicht gegen freie Meinungsäußerung im Netz stellen, z.B. in dem sie Wikileaks das Nutzen ihrer Infrastruktur verbieten. Anonymous als ein loses Kollektiv von Internetaktivisten rund um die Welt, die sich Freiheit im Netz auf die Fahnen geschrieben haben, ist dabei nur ein besonders extremes Beispiel von einem entstaatlichten Akteur.

Stuxnet, der Virus, der vermutlich das iranische Atomprogramm sabotieren sollte, hat eindrucksvoll bewiesen, dass auch komplizierte Angriffe gegen sehr spezielle Ziele, durchgeführt von einem großen Team und über einen langen Zeitraum, nicht länger ein rein theoretisches Gefahrenszenario darstellen. Chinesische Hacker dringen in die Computersysteme von amerikanischen Unternehmen und Regierungsinstitutionen ein und sorgen so für zusätzliches Bedrohungspotenzial. Befinden wir uns schon in einem Krieg im Internet?

Keiner führt Krieg, aber alle reden davon

Die Wortwahl vieler Akteure mag markig ausfallen, aber man muss feststellen, dass der Cyberwar noch nicht eingetreten ist und es auch recht fraglich ist, ob er in absehbarer Zeit eintritt. Die Länder, denen im Allgemeinen die größte Schlagkraft im Feld des Cyberwars zugesprochen wird – Russland und vor allem China – hängen genau so vom Internet ab

wie Europa oder die USA. Verwunderlich bei dieser technologischen und verbalen Aufrüstung ist dann, dass bis jetzt kein Staat nachweislich kriegerische Handlungen im Netz gegen einen anderen durchgeführt hat (soweit dies bekannt ist). Die Angriffe auf Estland oder Georgien und der vermutete Angriff auf das iranische Atomprogramm mittels Stuxnet legen nahe, dass staatliche Akteure involviert waren, aber stichhaltig bewiesen werden kann das nicht.

Der Großteil der Cybersecurity-relevanten Aktivitäten, vor allem Seitens Russlands und Chinas, ist nicht Cyberwar oder die Vorbereitung dessen, sondern Cyber Spionage. Das Einbrechen in Systeme um an Informationen zu gelangen oder im Zweifelsfall subtil Prozesse zu manipulieren stand bis jetzt klar im Vordergrund. Dies ist durchaus nachvollziehbar: Der Profit, den derartige Aktionen im Vergleich zu möglichen negativen Konsequenzen abwerfen ist größer als der eines Angriffs auf einen Staat.

Beispiele für derartige Spionageangriffe gibt es viele: Die Wikileaks-Depeschen berichten vor allem von chinesischen Spionageattacken auf amerikanische Regierungsinstitutionen, aber zum Beispiel auch auf Google. Bei letzterem Angriff scheinen vor allem die E-Mails chinesischer Dissidenten von Interesse gewesen zu sein (siehe Depesche 09STATE67105). 2005 gab es von China aus Hackerattacken auf Netzwerke der amerikanischen Streitkräfte [Quelle]. Noch umfangreicher war Operation Aurora in der zweiten Jahreshälfte 2009, die diesmal vor allem amerikanische Unternehmen ins Visier nahm, vor allem aus dem IT- und Rüstungssektor. Dort wurden gezielt Informationen im großen Stil abgegriffen.

Nützliche Kriegsmetaphern

Dass das Internet versicherheitlicht wird ist wohl eine wenig umstrittene Feststellung. Interessant ist aber der Diskurs, in dem dies stattfindet: Konfrontationen im Netz werden mit einer Kriegsmetaphorik präsentiert, sei es von staatlicher oder nichtstaatlicher Seite. Auf staatlicher Seite übernehmen zunehmend klassische Militär- und Geheimdienstorgane die Kompetenzen in diesem Bereich oder versuchen es zumindest. In den USA gibt sich der Cyber Czar der Regierung Obama Howard Schmidt alle Mühe, den Kriegsbegriff aus der Diskussion herauszuhalten [Quelle], aber vor allem Vertreter von Geheimdiensten und Militär verwenden ihn gerne und oft, verbunden mit dem Aufruf, ihre Zuständigkeiten zur Verteidigung des Landes in diesen Bereichen zu erweitern [Quelle].

Die bisherigen Vorfälle widersprechen dabei dieser Darstellung: Angriffe wurden vor allem mit dem Ziel, Informationen zu erhalten oder subtil Sabotage auszuüben, durchgeführt. Kritische Infrastruktur zu zerstören spielte bislang eine eher zweitrangige Rolle.

Die für den Normalnutzer leichter erkennbaren Auswirkungen von Attacken sind ironischerweise die, die wohl eher nichtstaatlichen Akteuren angelastet

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)

werden können: Webseiten, die auf Grund von Angriffen nicht mehr erreichbar sind, so wie zuletzt im Fall von Operation Payback die Seiten von Visa, Mastercard, PayPal und Anderen. Ob derartige Angriffe, die Server mit sinnfreien Anfragen fluten und so verlangsamen oder lahmlegen, aber überhaupt eine Form des Cyberwar darstellen ist umstritten. Möglicherweise handelt es ich schlicht um eine neue, globalisierte Form des Bürgerprotests [Quelle].

So bleibt zu konstatieren, dass der Sicherheitsbegriff sich mit Cybersecurity erweitert und das Internet zunehmend versicherheitlicht wird. Die damit verbundene Bedeutung des Begriffs scheint aber im Diskurs eine andere zu werden, nämlich Krieg, als die tatsächliche Gefahrenlage dies nahe legen würde. Krieg im findet sich im Internet heute eher in den Worten als in den Taten.

Tags: Anonymous, Cyber Spionage, Cyberwar, Hacker, Internetaktivisten, Kriegsmetaphorik, Stuxnet, Wikileaks

« Neue Software, alte Hardware? Die NATO 3.0 als Risikomanager
Profiling am Flughafen: Wandel globaler Sicherheitskultur? »

Bislang keine Kommentare

Einen Kommentar hinterlassen

Name

Email

Webseite

Kommentar

Stellenangebote (41)
Strategie (10)
Terrorismus (14)
Theorie (2)
Umwelt (1)
Versicherheitlichung (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
Hylaean Flow
Internet und Politik
IR Blog
Just Security Blog
justsecurity.org
Killer Apps
Kings Of War
netzpolitik.org
shabka.org
Terrorismus in Deutschland

Geben Sie den Text ein.

reCAPTCHA

Bestätigen

Datenschutz - Nutzungsbedingungen

Kommentar senden

☑ Benachrichtige mich über nachfolgende Kommentare per E-Mail.

theorieblog.de
Verfassungsblog
Vom Bohren harter Bretter
whistleblower-net.de

ARCHIV

Wähle den Monat