**Zeitschrift:** ASMZ : Sicherheit Schweiz : Allgemeine schweizerische Militärzeitschrift

**Herausgeber:** Schweizerische Offiziersgesellschaft

**Band:** 177 (2011)

**Heft:** 3

**Artikel:** Cyberwar : digitaler Erstschlag?

**Autor:** Schneider, Henrique

**DOI:** https://doi.org/10.5169/seals-154222

# Cyberwar: Digitaler Erstschlag?

**Der Nationalrat überwies eine Motion «Massnahmen gegen Cyberwar». Das VBS schuf eine Stelle «Cyber Defense», um den virtuellen Raum und die dazugehörigen Infrastrukturen besser gegen Angriffe zu schützen. Doch was ist Cyberwar? Dem Begriff haftet die Mystik einer Mischung aus Raumschiff Enterprise und Wikileaks an. Aber wogegen muss man sich verteidigen?**

Henrique Schneider

«Wir müssen uns nicht so benehmen, als würden morgen sämtliche Netzwerke, die es auf dieser Welt gibt, lahmgelegt. Aber wir müssen uns mit der Tatsache befassen, dass man mit feindseliger Absicht in Netzwerke eindringen, und dass solches Eindringen ausserordentlichen Schaden verursachen kann.» So erklärte Ulrich Schlüer[1], Sprecher der SIK Mehrheit, in oben erwähnter Motion, den Begriff. Aus seinen Ausführungen geht hervor, die Schweiz befürchtet den digitalen Erstschlag.

### Wann erfolgte der Erstschlag?

Im 1999 musste das Weisse Haus drei Tage vom Netz genommen werden, da infolge des versehentlichen Bombardements der chinesischen Botschaft in Belgrad, chinesische Hacker die Websites der US-Regierung lahmlegten. Im 2007 wurden in Estland, nach der Entfernung eines russischen Kriegerdenkmals, Regierung und Unternehmen drei Wochen mit Hacker-Angriffen ausser Gefecht gesetzt.

## «Wogegen muss man sich verteidigen?»

Weitere Angriffe erfolgten im selben Jahr gegen Georgien, vor dem Krieg und im selben Muster, gegen Kyrgisien 2009. Ebenfalls 2007 gelang es israelischen Jagdflugzeugen, eine mutmassliche Atomanlage in Ostsyrien zu zerstören, nachdem es ihnen durch eine Täuschung der modernsten russischen Fliegerabwehr möglich war, den gesamten syrischen Luftraum unbehelligt zu durchfliegen.

Nachdem bereits 2003, beim grossen Stromausfall in den USA, der Verdacht aufgekommen war, dass dieser durch einen

Kriegsgerät im Cyberwar.

Computervirus ausgelöst wurde, mussten 2006 zweimal Atomkraftwerke nach Cyber-Angriffen abgeschaltet werden. Und im April 2009 gelang es Hackern, in die Stromnetzkontrolle der USA vorzudringen und dort Programme zu hinterlassen, die das System bei Bedarf unterbrechen hätten können. Im 2009 und 2010 griff der Stuxnet-Wurm iranische Atomanlagen an. Dieser Wurm verbreitete sich hochselektiv auf speziellen Steuerungseinheiten; anschliessend – nach einer festgelegten Anzahl von Infektionen – zerstörte er sich selbst.

### Abwehr – gegen was?

Die Nato nahm die Gefahr eines Cyberwars Ende 2010 in ihr neues strategisches Konzept auf.[2] Aber die Frage bleibt: wogegen richtet sich eine Abwehr? Obige Beispiele scheinen, ausser dem digitalen Charakter, wenig Gemeinsames zu haben. Eine originär-militärische Dimension hatte lediglich die israelische Operation, in der Cyberwars als operative Ergänzung zu konventionellen Massnahmen eingesetzt wurde.

Auf längere Sicht ist nicht davon auszugehen, dass zerstörerische Cyber-Angriffe ohne begleitende, bewegliche, militärische Operationen durchgeführt werden. Digitale Operationen können zwar wichtige Daten zerstören und die Kommunikation unterbrechen, möglicherweise wirken sie sich auch ernsthaft auf grosse Netzwerke, wie etwa die Stromversorgung aus. Doch grossflächige Angriffe sind sie nicht, sondern lediglich Machtdemonstrationen, oder sie können als Eskalationsstufe genutzt werden.

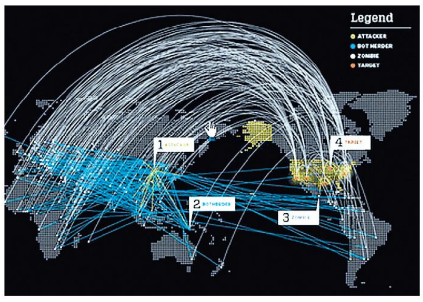
Wesentlich bedeutsamer ist die Kombination von Cyber-Angriffen mit «Klassischen» in zukünftigen Konflikten. Wie bereits Israel oder Russland gezeigt haben, kann die Unterstützung von militärischen Operationen zu Land, zu Wasser, in der Luft und im Weltraum durch begleitende Cyber-Attacken erfolgreich sein.

Die heutige Welt ist jedoch nicht nur von Kriegen und militärischer Macht geprägt, sondern auch von der stetigen Herausforderung durch Terrorismus und anarchistische Netzwerke sowie durch organisierte Kriminalität.

## «Cyberwar ist eine operative Ergänzung zu konventionellen Massnahmen.»

Terroristen nützen – wie jede andere Organisation – das Internet meist für kriminelle Aktivitäten zur Geldbeschaffung, aber auch zur Kommunikation. Cyber-Angriffe sind jedoch keine effektive Art,

Operationskarte im Cyberwar.



um Terror in die Zielbevölkerung zu tragen. Auch wenn Terroristen die Möglichkeit hätten, sophistizierte Cyber-Angriffe durchzuführen, würden sich diese kaum von den Attacken anderer Akteure unterscheiden. Terrorismus braucht aber eine Differenzierung, um erfolgreich zu sein, d.h. um Panik zu generieren.

### Was ist ein Cyber-Angriff?

Unter Cyber-Angriffen werden Massnahmen verstanden, «die unter Anwendung von digitalen Mitteln dazu dienen, den Zugriff auf Informationen in Computern oder Computernetzwerken zu stören, zu verhindern, zu verlangsamen oder die Information, die dazugehörigen Computernetzwerke oder die dazugehörigen Computer zu zerstören.»[3] Cyber-Angriffe können neben kriegerischer auch privater, kommerzieller oder krimineller Natur sein. Allerdings kommen bei allen Angriffen dieselben technischen Methoden zum Einsatz, was die Identifikation des Urhebers und die des Angriffsmotivs schwierig, mitunter sogar unmöglich macht.

Lageraum im Cyberwar.
Fotos: US Dep. Of Defense

Grundsätzlich kann man bei Cyber-Angriffen aktive, d.h. zerstörende, und passive Angriffe unterscheiden. Bei passiven Attacken werden Daten nur kopiert oder entfernt, ohne die angegriffenen Systeme zu zerstören. Diese Form ist eher bei kriminellen Aktionen der Fall, beispielsweise bei Diebstahl von Passwörtern oder Kreditkartendaten, aber auch bei Spionage im Netz, egal ob aus wirtschaftlichen oder politischen Motiven. In beiden Fällen soll das Ziel ja weiter zur Verfügung stehen.

Bei zerstörenden Attacken werden Systeme oder Netzwerkdienste durch gefälschte oder manipulierte Daten dazu gebracht, dass sie nicht mehr zur Verfügung stehen. Dies kann insbesondere bei kritischen Infrastrukturen verheerende Folgen haben. Das Muster von Angriffen ist grundsätzlich immer das gleiche: Zunächst geht es darum, Zugang zu Computern und Netzwerken zu erlangen. Danach wird dieser Zugang ausgenutzt, um Schadprogramme auf den Computern zu installieren. Mit Hilfe dieser Programme können Informationen entnommen oder manipuliert werden.

> Cyberwar: mit feindseliger Absicht in Netzwerke einzudringen, um in diesen Netzwerken ausserordentlichen Schaden zu verursachen.
>
> *oder*
>
> Unter Cyber-Angriffen werden Massnahmen verstanden, die unter Anwendung von digitalen Mitteln dazu dienen, den Zugriff auf Informationen in Computern oder Computernetzwerken zu stören, zu verhindern, zu verlangsamen oder die Information, die dazugehörigen Computernetzwerke oder die dazugehörigen Computer zu zerstören.

### Cyber Defense

Wie reagierten die Staaten auf diese neuartige Form der Bedrohung? In erster Linie mit der Aufstellung von Cyber-Einheiten. Neben den Cyber-Grossmächten USA, Russland, China und Frankreich werden in über hundert Staaten derzeit Cyber-Einheiten aufgestellt. Die USA verfügen über ein eigenes zentrales Cyber-Command mit rund 1000 Beschäftigten, in China sollen mehrere tausend Soldaten in Cyber-Regimentern arbeiten.

**«Cyber-Verteidigung bedeutet, die Systeme aufrechtzuerhalten.»**

Sowohl die Erkennung eines Angriffs als auch die Identifizierung der Angreifer wird bei guter Vorbereitung des Angriffs, dank der technologischen Weiterentwicklung, immer schwieriger, so dass auch die Abschreckung durch Vergeltung oder Gegenwehr erschwert wird. Die Kombination von extensiver Abhängigkeit von Cyber-Systemen und deren ständig vorhandene Verwundbarkeit gilt für lokale, nationale und globale Infrastrukturen gleichermassen.

Daraus folgt: Jegliche Steuerung mit Cyber-Mitteln muss prinzipiell als angreifbar gelten. Dieser Zusammenhang ist die eigentliche Grundlage der steigenden Ausnutzung solcher Technologien auch im Kriegsfall. Die zentrale Rolle im Cyberwar spielen zum jetzigen Zeitpunkt jedoch die Denial of Service Angriffe. Dabei verweigern Computer durch gezielte Überlastung, zum Beispiel mit sinnlosen Anfragen von aussen, ihren Dienst. Das heisst, der Schwerpunkt der Verteidigung wird sich darauf richten, die Systeme laufen zu lassen.

### Cyberwar – die Zukunft?

Die Zukunft des Krieges im 21. Jahrhundert liegt aber, trotz allem bisher Gesagten, nicht zwingend in der Hochtechnologie. Die Mehrzahl der Kriege wird auch weiterhin eher von niedriger Intensität sein und viel wahrscheinlicher die Form von Bürgerkriegen annehmen. Doch dürften Cyber-Angriffe am High-Tech-Ende des Konfliktspektrums und als Machtdemonstration verschiedenster Akteure eine Realität werden. Die Kombination dieser beiden Kriegsformen bezeichnet man als «hybride Kriege». Es zeichnet sich ab, dass die Armeen und Abwehren industrialisierter Staaten, unabhängig von den Konflikt-Szenarien, in friedenserhaltenden Einsätzen, wie auch in konventionell geführten Kriegen auf Digitalisierung, Vernetzung und Präzisierung ihrer Truppen angewiesen sein werden.

Der militärische Aufbau von Cyber-Einheiten hat erst begonnen. Es ist davon auszugehen, dass die Tausenden von Programmierern und angeworbenen Hackern in den nächsten Jahrzehnten die Kriegsführung entscheidend verändern werden; sie wird auch privater. ■

1 10.3625 – Amtliches Bulletin – Nationalrat – 02.12.10 – 08h00 – Provisorischer Text: 10.3625 Motion SiK-NR. Massnahmen gegen Cyberwar
2 NATO 2010. Active Engagement, Modern Defence; Absatz 12.
3 Olivier Minkwitz 2003. Ohne Hemmungen in den Krieg? Cyberwar und die Folgen; HSFK-Report 10/2003.

Prof. Dr.
Henrique Schneider
Consultant
A-2000 Stockerau