AUSSEN- UND SICHERHEITSPOLITIK 17.01.2014 | Matthias Wolfram

Auch Deutschland ist in der Matrix

Weshalb ein Cyberkrieg möglich ist und Wegschauen nicht hilft

Der Begriff „Cyberkrieg“ wird heute oft undifferenziert im Zusammenhang mit kriminellen Machenschaften und Spionage oder aktuell der Überwachung des Internets genutzt. Die dem Konzept eigentlich zu Grunde liegende militärische Dimension ist dabei von den aktuellen Ereignissen weitgehend aus der Diskussion verdrängt worden. Noch vor einigen Jahren wurde alleine die Möglichkeit eines Cyberkriegs von vielen Beobachtern ausgeschlossen. Und auch heute noch wird die Frage nach der Wahrscheinlichkeit einer solchen Auseinandersetzung häufig belächelt und ohne tiefer gehende Analyse, meist mit dem Verweis auf empirische Erfahrungen, verworfen.

Cyberkrieg: So real wie Flugzeuge?

Zur angemessenen Gewährleistung der staatlichen Sicherheitsvorsorge ist die Frage im Sinne einer vorausschauenden Sicherheitspolitik von Bedeutung. Denn einen Cyberkrieg auf der Grundlage rückwärtsgewandter Betrachtungen rundweg auszuschließen, ist methodisch zumindest gewagt. Aus der Tatsache, dass ein Ereignis bis heute nicht aufgetreten ist, seine Unmöglichkeit zu folgern, ist offensichtlich weder schlüssig noch valide. Diese Haltung erinnert dabei frappierend an die des französischen Marschalls Foch, der dem Flugzeug 1911 jede militärische Bedeutung absprach.

Dabei trägt auch die Tatsache, dass jeder spezifische massive Cyberangriff eine „One-shot-weapon“ ist, die in dieser Form nur ein einziges Mal genutzt werden kann, zu der verbreiteten Verharmlosung bei. Mit einem Cyberangriff geht in der Regel die Offenlegung von Fähigkeiten und genutzten Cyberwirkmitteln, Hintertüren oder Schwachstellen einher. Daher ist er für den Urheber nur dann sinnvoll, wenn der Angriffszweck ausreichend wichtig ist, um die voraussichtlich nur einmal mögliche Attacke durchzuführen. Zudem tragen mit Sicherheit trotz der

Schwierigkeiten der Attribution auch die zu erwartenden politischen Auswirkungen dazu bei, eine vom Opfer potenziell als kriegerischer Angriff eingestufte Attacke nur im absoluten Ausnahmefall in Betracht zu ziehen.

Die Argumentation gegen die Wahrscheinlichkeit eines Cyberkriegs passt jedoch in ein vor allem in Deutschland weit verbreitetes Denkschema: Die Verknüpfung einer technischen Neuerung soll vor der militärischen Nutzung bewahrt werden, da der Einsatz von Gewalt grundsätzlich abgelehnt wird. Dabei erscheint nebensächlich, dass diese Argumentation im Hinblick auf möglicherweise notwendige militärische Einsätze hinkt und zudem den seit Menschengedenken existierenden Prozess der Nutzung neuer Entwicklungen für militärische Zwecke ignoriert. In der globalisierten und vernetzten Welt ist das einseitige Verharren in einer solchen Haltung schlichtweg sinnlos. Schließlich reicht es doch aus, wenn ein Akteur gleich welchen Zuschnitts sich das Potenzial von Cyberangriffen zu Nutze macht und damit auch die Bundesrepublik bedrohen könnte.

Cyberkrieg: Keine einheitliche Definition

Dabei fehlt eine allgemein anerkannte Definition eines Cyberkrieges noch immer und dürfte auch noch geraume Zeit auf sich warten lassen. Allerdings wird das Phänomen als kriegerische Auseinandersetzung im und durch den Cyberraum mit schwerwiegenden gewaltgleichen Auswirkungen in der physischen Welt für den Zweck einer grundsätzlichen Diskussion ausreichend gut beschrieben. Der Begriff ist jedoch zwangsläufig vielschichtig.

Dies führt oft zu stark unterschiedlichen Assoziationen, die sehr verschiedenen Wahrscheinlichkeiten unterliegen: Während ein langandauernder Cyberkrieg mit großflächigen, immensen Zerstörungen praktisch kaum vorstellbar ist, scheint ein in seiner Dauer und seinen Konsequenzen begrenzter Cyberangriff sehr wohl im Bereich des Möglichen zu liegen.

Die Möglichkeit, aus dem Cyberraum eine physische Zerstörung von Gegenständen herbeizuführen und auch

Die Möglichkeit, aus dem Cyberraum eine physische Zerstörung von Gegenständen herbeizuführen und auch direkt oder indirekt Menschenleben zu gefährden, kann dabei inzwischen als bewiesen angesehen werden. Damit ist grundsätzlich auch ein Cyberangriff

direkt oder indirekt Menschenleben zu gefährden, kann dabei inzwischen als bewiesen angesehen werden.

in großem Maßstab und mit strategischer Bedeutung denkbar. Auch wenn dieser eine erhebliche Vorbereitung und einen ebensolchen Mittel- und Personaleinsatz benötigen würde, ist eine breite, synchronisierte Attacke auf Personen, Einrichtungen oder zentrale Prozesse des alltäglichen Lebens grundsätzlich nicht auszuschließen und in bestimmten Szenarien durchaus plausibel. So ist beispielsweise eine großflächige Störung der Stromversorgung, herbeigeführt durch einen Cyberangriff, als politisches Druckmittel in einem nicht offen gewaltsam ausgetragenen Konflikt durchaus vorstellbar.

Sicher, diese Feststellung sagt zunächst noch nichts über die Wahrscheinlichkeit ihres Eintretens aus, die von verschiedenen Faktoren wie der Machtverteilung zwischen den Kontrahenten, der Fähigkeit zur Abschreckung oder der Verwundbarkeit und der Resilienz der Akteure abhängt. Sobald jedoch die grundsätzliche Möglichkeit eines Cyberkrieges besteht, darf diese Bedrohung auf Grund ihres potenziellen Ausmaßes nicht einfach ignoriert werden.

Die Möglichkeit und Plausibilität einer kriegerischen Auseinandersetzung im und durch den Cyberraum stellt die staatliche Sicherheitspolitik dabei vor das gleiche Dilemma wie auch andere gravierende, aber weniger offensichtliche Risiken: Ihre Vielzahl erfordert eine Schwerpunktsetzung der Sicherheitsvorsorge. Ein Staat kann sich kaum jemals auf die gesamte Bandbreite möglicher Bedrohungen umfassend vorbereiten. Dass dies zu einer Fokussierung auf die wahrscheinlichste Bedrohung führt, ist verständlich. Doch dies darf die Vorbereitung auf mögliche weitere Risiken nicht verhindern. Auch die Landesverteidigung, so wenig wahrscheinlich sie uns für Deutschland heute erscheint, ist auf Grund ihrer potenziell gravierenden Auswirkungen in den verteidigungspolitischen Richtlinien von 2011 noch immer als fester Bestandteil der Aufgaben der Bundeswehr aufgelistet.

Auch sicherheitspolitische Überraschungen großen Ausmaßes wie zwischenstaatliche Kriege, der Fall der Berliner Mauer oder der Arabische Frühling sind durchaus von einigen Beobachtern antizipiert worden. Meist jedoch unterlagen sie einer bewussten Ausblendung durch Analysten oder Entscheidungsträger, die die Szenarien für unmöglich oder unrealistisch hielten. Schon die hier genannten, zugegebenermaßen besonders prägnanten Fälle sollten daher Warnung genug sein.

Wenig wahrscheinlich aber potentiell desaströs...

Die Aufgabe strategischer Analyse ist es, voraus zu denken und auch neue, unter Umständen weit her geholt erscheinende Konstellationen und Risiken vorurteilsfrei zu prüfen. Dies ist umso mehr der Fall, wenn es sich wie im Falle von Cyberangriffen um eine sich noch immer weiter entwickelnde Technologie handelt, deren ganzes Potenzial derzeit noch nicht abgesehen werden kann.

Nach dem heutigen Stand der Erkenntnisse erfüllt ein Cyberkrieg langfristig gesehen die Bedingungen für einen Vorfall geringer Wahrscheinlichkeit, doch potenziell hohen Schadensrisikos.

Nach dem heutigen Stand der Erkenntnisse erfüllt ein Cyberkrieg langfristig gesehen die Bedingungen für einen Vorfall geringer Wahrscheinlichkeit, doch potenziell hohen Schadensrisikos. Dieses ist extrem schwer einzuschätzen, da die Sicherheitstests richtigerweise einer strikten Vertraulichkeit unterliegen. Schlichtweg davon auszugehen, dass Deutschland von gravierenden Entwicklungen verschont bleiben werde, wäre jedoch fahrlässig. Es ist daher Zeit für eine ideologiefreie, differenzierte Analyse des Phänomens, die nicht auf die Exekutive einerseits und nicht-staatliche Institutionen andererseits begrenzt bleibt.



Matthias Wolfram

Dr. Matthias Wolfram ist Generalstabsoffizier der Bundeswehr und hat an der Universität Erlangen-Nürnberg in Politischer Wissenschaft promoviert. Der Autor gibt ausschließlich seine eigene Meinung wieder.

2 LESERBRIEFE

Peter Cornelius schrieb am 21.01.2014

Sehr interessante Überlegungen, die sicher auch in die Politik getragen werden sollten

Gerimbeck schrieb am 28.03.2014

Der Gedanke von Herrn Wolfram spornt an, weiter darueber nachzudenken, da es uns alle betrifft. In diesem Zusammenhang darf ich auf den interessanten Beitrag in >Wikipedia - "Cyberkrieg", und vor allem auf das dortige Thema "Rezeption" verweisen.
Ich persoenlich tendiere mehr zu der Meinung von der Wissenschaftlerin Frau Miriam Cavelty-Dunn vom Crisis and Risk Network.
Nach meinem Dafuerhalten organisieren und verwirklichen sich Verhaltens-Situationen im neuronalen Netzwerk der Gehirne, und in der kommunikativen Vernetzungsarchitektur zu seinesgleichen. > Welches Gehirn welche Schlussfolgerungen fuer sich daraus ableitet ist eine neuronale Angelegenheit seiner Selbst, die existenzielle Reaktionen zu produzieren in der Lage

ist. Das Wort "Cyberkrieg" muesste, nach meiner subjektiven Anschauung, vom Autor, nach dieser denkweise definiert, eindeutiger zugeordnet werden, in welchem Kontext von "Sicherheits- und -Politik" dies von Ihm zu verstehen ist, was er damit sagen will, welchen geistigen Beitrag das bewerkstelligen soll. Dann koennte ich fuer mich einen produktiven Aha-Effekt abholen.
