IPG

NEUE HIGH-TECH-KRIEGE 30.03.2015 | Robin Geiß

# Völkerrecht im „Cyberwar“

## Militärische Cyberoperationen bedrohen nicht nur Zivilisten, sondern fordern auch zentrale Grundannahmen des Völkerrechts heraus.

Dem Cyberraum wird spätestens seit der Stuxnet-Attacke gegen iranische Atomanlagen aus dem Jahr 2010 erhebliches militärisches Potenzial beigemessen. Längst sind sich Experten einig, dass Cyberattacken – etwa durch manipulative Eingriffe in Flugleitsysteme, die Stromversorgung oder andere zentrale Komponenten der (zivilen) Infrastruktur – erheblichen Schaden verursachen können. Darüber hinaus bietet der Cyberspace unzählige Möglichkeiten, die Handlungs- und Reaktionsfähigkeit gerade hoch moderner Armeen mit ihrem vernetzten Militärapparat zu manipulieren. Die USA und China haben den Cyberspace aus diesem Grund übereinstimmend als „neue Domaine der Kriegführung“ eingestuft und „Cyberdominanz“ in zukünftigen bewaffneten Konflikten jeweils zur strategischen Priorität erklärt. Auch die NATO hat die Cyberabwehr 2014 als Kernaufgabe kollektiver Verteidigung definiert.

Doch inwiefern reguliert das Völkerrecht das neuartige Phänomen Cyberwarfare adäquat? Mittlerweile herrscht zwischen den Staaten Einigkeit, dass der Cyberspace kein (völker-)rechtliches Vakuum ist. Völkerrecht gilt online ebenso wie offline. Diskutiert wird aber die Frage der Anwendung des bestehenden Rechts unter neuartigen technischen Bedingungen. Die globale Vernetztheit des virtuellen Raums, seine Losgelöstheit von den für das traditionelle Völkerrecht so grundlegenden Staatsgrenzen, Anonymität und die Geschwindigkeit der Abläufe fordern zentrale Grundannahmen der Völkerrechtsordnung heraus.

Dabei wirft das Phänomen Cyberwarfare aus völkerrechtlicher Sicht zwei grundlegende Fragestellungen auf. Erstens: Unter welchen Voraussetzungen überschreitet eine Cyberattacke die Schwelle zu einem bewaffneten Angriff und löst damit das in Artikel 51 der Charta der Vereinten Nationen verankerte Recht auf (militärische) Selbstverteidigung aus? Zweitens: Soweit es in zukünftigen bewaffneten Konflikten tatsächlich zum Einsatz militärischer Cybertechnologie kommt, stellt sich die Frage, inwiefern dies durch das vor allem in den

Genfer Konventionen von 1949 verankerte humanitäre Völkerrecht erfasst wird.

## Selbstverteidigung gegen Cyberangriffe?

Die Charta der Vereinten Nationen erkennt Staaten im Falle eines bewaffneten Angriffs „das naturgegebene Recht zur individuellen oder kollektiven Selbstverteidigung“ zu. Dieser Grundsatz gilt auch im Cyberspace. Mittlerweile besteht Einigkeit, dass eine Cyberattacke die in ihren Folgen mit den Konsequenzen eines herkömmlichen, militärischen Angriffs vergleichbar ist, als bewaffneter Angriff gilt und das Selbstverteidigungsrecht der UN Charta auslöst.

Klar ist auch, dass jedwede Antwort auf eine derartige Attacke dem Verhältnismäßigkeitsprinzip unterliegt und der Schwere des Angriffs angepasst sein muss. Nicht erforderlich ist es allerdings, dass ein Cyberangriff ebenfalls mit einer Cybermaßnahme beantwortet wird. Die Staaten sind in der Wahl ihrer Verteidigungsmittel grundsätzlich frei und könnten auch auf konventionelle militärische Mittel rekurrieren. Neu diskutiert werden muss im Rahmen dieser Schwellendiskussion allenfalls die Fragestellung, ob wirtschaftliche Gewalt, wie etwa eine schadhafte Manipulation der Finanzmärkte, nicht möglicherweise ebenfalls als ein das Selbstverteidigungsrecht auslösender Angriff zu qualifizieren sein sollte. Traditionell wird dies klar verneint. Da aber heutzutage unterschiedlichste Wirtschaftsabläufe und auch die Finanzmärkte in erheblichem Maße von einem funktionsfähigen Cyberraum abhängig sind und sich – vereinfacht gesagt – mit wenigen Mausklicks ein unter Umständen enormer wirtschaftlicher Schaden herbeiführen ließe, muss dies Position womöglich neu überdacht werden.

Für die Frage der Selbstverteidigung ist darüber hinaus auch die Zurechnung des Angriffs entscheidend. Problematisch ist, dass die unzähligen Verschleierungs- und Manipulationsmöglichkeiten des Cyberspace die Identifikation des Angreifers erheblich erschweren und bisweilen unmöglich machen. Selbstverteidigung aber darf es völkerrechtlich nur gegen einen klar identifizierten Angreifer geben. Eine Selbstverteidigung ins Blaue hinein hat der Internationale Gerichtshof in Den Haag ausdrücklich ausgeschlossen. Nicht alle Staaten wollen derart enge Schranken für das Selbstverteidigungsrecht akzeptieren. Mit Blick auf Cyberattacken gibt es daher durchaus Bestrebungen, einerseits die

hohe Schwelle für einen bewaffneten Angriff herabzusetzen und andererseits die strengen Zurechnungskriterien aufzuweichen.

Sicher, kein Staat Cyberattacken muss dulden. Das heißt aber nicht, dass bei einer Cyberattacke – selbst wenn sie gravierende Folgen haben sollte – automatisch und in jedem Fall das Selbstverteidigungsrecht zur Verfügung steht. Insbesondere ist nicht erkennbar, wie ein vereinfachter Rückgriff auf das Selbstverteidigungsrecht zu einem Mehr an Sicherheit beitragen sollte. Im Gegenteil: Die Auflockerung der strengen Kriterien des militärischen Selbstverteidigungsrechts untergräbt das völkerrechtliche Gewaltverbot und wird langfristig die Stabilität der internationalen Beziehungen gefährden. Auch und gerade im Cyberspace sollte das Recht zur militärischen Selbstverteidigung daher ein absolutes Ausnahmerecht bleiben.

## Es geht um Cyberdominanz

Welche militärischen Nutzungen des Cyberraums tatsächlich möglich und strategisch sinnvoll sind, lässt sich in Ermangelung entsprechender Staatenpraxis bislang nicht eindeutig beurteilen. Ein in den USA vieldiskutiertes Szenario ist etwa ein eskalierender Streit um Taiwan, in dessen Verlauf China durch Cybermaßnahmen versuchen könnte, eine amerikanische Reaktion zu verzögern, um innerhalb des so geschaffenen Zeitfensters irreversible Fakten zu schaffen. Daran wird deutlich, dass Cyberwarfare nicht als rein virtueller Konflikt verstanden wird, sondern als ein Element (neben vielen anderen) der modernen Konfliktführung.

Die USA, China und Russland scheinen sich gegenwärtig ein Wettrüsten im Cyberspace liefern. Ziel ist es, die technischen Voraussetzungen zu schaffen, um in einem möglichen Konfliktfall „Cyberdominanz“ zu gewährleisten. Das heißt, so wie es in der Vergangenheit im bewaffneten Konflikt darum ging, den Luftraum zu beherrschen, wird es in Zukunft (zusätzlich) auch darum gehen, die Kontrolle über den Cyberspace zu erlangen. Führt man sich vor Augen, wie schlagkräftig und manipulativ die NSA bereits in Friedenszeiten im Cyberraum operiert, lässt sich erahnen, wozu hoch moderne Militärs in der Lage sein könnten.

*So wie es in der Vergangenheit im bewaffneten Konflikt darum ging, den Luftraum*

Vor diesem Hintergrund stellt sich die Frage, inwiefern das humanitäre Völkerrecht derartige Operationen adäquat einzugrenzen vermag. Dabei wirft längst nicht jede militärische Cyberoperation komplizierte Rechtsfragen auf.

*zu beherrschen, wird es in Zukunft (zusätzlich) auch darum gehen, die Kontrolle über den Cyberspace zu erlangen.*

Direkte Angriffe auf die Zivilbevölkerung sind eindeutig verboten. Problematisch ist aber, dass in einem global vernetzen Raum selbst im Falle eines (grundsätzlich erlaubten) Angriffs auf militärische Systeme, unvorhergesehene Kaskadeneffekte eintreten könnten. Schwierigkeiten resultieren auch daraus, dass das humanitäre Völkerrecht die Zivilbevölkerung zwar vor physischer Zerstörung schützt, Cyberattacken der Bevölkerung aber auch – unabhängig von jeglicher Zerstörung in der realen Welt – erheblichen wirtschaftlichen Schaden zufügen können. Diese Schutzlücke sollte im Wege einer dynamischen – den modernen Verhältnissen angepasste – Interpretation geschlossen werden.

Weitaus schwieriger erscheint die rechtliche Bewertung, wenn Hard- und vor allem Softwarekomponenten der globalen Cyberinfrastruktur selbst zum strategischen Angriffsziel werden. In dem Maße, in dem Staaten wechselseitig um Cyberdominanz ringen, wird dieses Szenario zunehmend relevanter. Hier bestehen zum Teil noch erhebliche rechtliche Grauzonen. Problematisch ist vor allem, dass die Anwendung des völkerrechtlich zentralen Unterscheidungsprinzips zwischen militärischen (angreifbaren) und zivilen (geschützten) Objekten erheblich erschwert ist. Schließlich werden schon heute weitreichende Elemente der zivilen Cyberinfrastruktur auch für militärische Zwecke genutzt.

Das führt dazu, dass Komponenten der Cyberinfrastruktur auf Grundlage des geltenden Völkerrechts potentiell viel zu leicht als legitimes Angriffsziel qualifiziert werden können. Wenn Cyberdominanz das erklärte strategische Ziel ist, liegt es durchaus nahe, dass technologisch führende Staaten darin eher eine Chance als ein Problem sehen. Europäische Staaten, deren Gesellschaften in Zukunft immer stärker auf einen funktionsfähigen Cyberraum angewiesen sein werden, sollten sich hier klarer als bisher für eine enge(re) Auslegung stark machen.

Auch wenn das Schlagwort Cyberwarfare aus den Schlagzeilen kaum noch wegzudenken ist, Hysterie ist fehl am Platz. Bis heute hat noch keine der öffentlich bekannt gewordenen Cyberattacken die Schwelle zum bewaffneten Angriff im völkerrechtlichen Sinne erreicht. Gleichwohl muss eine sachliche Debatte um das Phänomen Cyberwarfare – losgelöst von überzogenen Worst-Case-Szenarien –

dringend geführt werden. Der Cyberspace hat enormes militärisches Potenzial. Die militärische Nutzung dieses Raums wird in Zukunft zunehmen. In dem Maße in dem die Vernetzung der Wirtschaftsabläufe und des gesellschaftlichen Lebens insgesamt fortschreitet, wird auch die Schutzbedürftigkeit der Zivilbevölkerung vor militärischen Cyberoperationen weiter steigen.

---



**Robin Geiß**
Glasgow

Robin Geiß ist seit 2013 Professor für International Law and Security an der Universität Glasgow. Davor war er Professor für International and European Law an der Universität Potsdam. Er ist Autor von *Failed States* (Duncker & Humblot 2005) und Ko-Autor von *Piracy and Armed Robbery at Sea* (OUP 2011).

## 3 LESERBRIEFE

### **Hans Oppenheimer** schrieb am 31.03.2015

Wo führt eigentlich die NATO Cyber-Attacken durch? Was läuft da in der Ukraine? Und hat Deutschland eigene vernünftige Abwehrfähigkeiten oder übernehmen das die Amerikaner (Stichwort: NSA)?

**Gerhard Fulda** schrieb am 31.03.2015

Es ist gut, dass IPG sich des Themas annimmt. In der Tat brauchen wir eine öffentliche Diskussion. Zumal die Bundesregierung daran nicht wirklich interessiert ist. Die digital stärker aufgerüsteten Länder (wie USA, Israel, Russland, China, UK, Frankreich und Deutschland) wollen eher ihrer Dominanz vertrauen als durch neue völkerrechtliche Regeln eingegrenzt werden.
Robin Geiss hat deutlich auf die Grauzonen und den Handlungsbedarf hingewiesen. Erstaunlich, dass er nicht das Tallinn Manual von 2013 erwähnt, in dem nach von der NATO organisierten mehrjährigen Beratungen von Nicht-Regierungsexperten bereits wichtige Vorarbeiten veröffentlicht worden sind - und an dem er selbst mitgearbeitet hat.
Zu Einzelfragen kann man Geiss weitgehend zustimmen. Er begründet allerdings nicht seine Auffassung, bis heute habe noch keine Cyber-Attacke die Schwelle zum "bewaffneten Angriff" im Sinne der VN-Charta überschritten und damit das Recht auf Selbstverteidigung begründet. Darüber kann man bei dem israelischen Stuxnet-Angriff auf die iranischen Zentrifugen zur Uran-Anreicherung durchaus streiten. Selbst der damalige

militärische Chefjurist des US Cyberkommandos hat das anders gesehen (auch wenn dann irrte, als er meinte, die Angreifer hätten sich wohl ihrerseits auf Selbstverteidigung berufen können).

PS Ich habe selbst 2013 über Cyberwar und Völkerrecht veröffentlicht. (ZENITH Nov. 2013 Seite 53)

---

**Pank Martin** schrieb am 01.04.2015

---

Es stellt sich noch immer die Frage wie eine Vorbereitungshandlung eines Staates für den Einsatzfall von "Cyberwar/intelligence - Komponenten" im Völkerrecht zu bewerten wäre.
Als Beispiel: Einflussnahme eines Staates in die Entwicklung von SW und HW der nationalen oder verbündeten Hersteller, um Implantate zu applizieren die im Anlassfall aktiviert werden können. (vgl. Snowden-Leaks zu Malware in Festplattenbootsystemen oder aktiven Netzwerkkomponenten, usw.). Natürlich sind technologisch gesehen viele Nationen in der Lage solche Vorbereitungshandlungen zu setzen und auf der anderen Seiten sind die "Kunden" nicht in der Lage diese zu prüfen. Eine nationale Unterstützung fehlt ebenso. Es

entsteht damit ein nicht zu unterschätzender "Machtraum" gepaart mit einer Paralyse des potentiellen Gegners, da die Mittel einer sauberen Prüfung der Komponenten des Cyberraumes, noch dazu in einem gestressten Wirtschaftsmarkt, nicht finanziert werden können. Nationalstaaten sind nicht gewillt solche Prüfungen mit Geldern der öffentlichen Hand zu finanzieren - damit steht dem Angreifer eine sehr offene "Flanke" zur Verfügung. Als Resultat muss davon ausgegangen werden, dass es einem hoch entwickelten Staat, unter der Voraussetzung der gezielten Einflussnahme auf seine Industrie, möglich sein kann die kritischen Infrastrukturen eines anderen Staates gezielt zu beeinflussen und u.U. zu zerstören.
Wie gehen Nationalstaaten in Zukunft mit dieser Bedrohung um? Haben diese überhaupt ein Bewusstsein zu dieser Bedrohung und werden wir jemals Mechanismen finden, die ein Vertrauen zulassen.
Zuoberst sollte, aus meiner Sicht, die Frage einer völkerrechtlichen Bewertung tatsächlich geklärt werden, um in weiterer Folge das Fundament für ein sicheres miteinander, zumindest in den kulturellen und wirtschaftlichen Partnerschaften zwischen Nationen, zu bilden.