

Cyber-War oder Cyber-Wahn?

Wenn Ungenauigkeiten im allgemeinen Sprachgebrauch juristische Unterscheidungen gefährden

ajv2016

2018-10-24T07:31:07

Der Cyberkrieg ist in aller Munde. Ein aktueller, in den Medien als [„Cyberkrieg“](#) bezeichnete Vorfall vom 4. Oktober betraf die Spionageaffäre in den Niederlanden. Vier Agenten des russischen Geheimdienstes hatten versucht, in das Computernetzwerk der Organisation für ein Chemiewaffenverbot (OPCW) einzudringen, mit dem mutmaßlichen Ziel, die Ermittlungen zum Giftgasangriff auf den abtrünnigen russischen Agenten Skripal und seine Tochter zu sabotieren. Prompt nachdem die niederländischen Behörden über die Spionageaktion informiert hatten, war vom [„russischen Cyberkrieg gegen den Westen“](#) zu lesen. Der „Cyberkrieg“ ist ein äußerst beliebtes Schlagwort. Die allermeisten Cyberangriffe, obwohl sie rechtswidrig sind, haben aus völkerrechtlicher Sicht allerdings nichts mit Krieg zu tun. Es wäre daher ratsam, nicht nur im Völkerrecht, sondern selbst im alltäglichen Sprachgebrauch genau zwischen Cyberkrieg und bloßer Verletzung der Cybersouveränität eines Staates zu unterscheiden.

Der Kriegsbegriff im Völkerrecht

Von einem Krieg kann aus rechtlicher Sicht frühestens die Rede sein, wenn das zwischenstaatliche Gewaltverbot gemäß Art. 2 Abs. 4 Charta der Vereinten Nationen (UN-Charta) verletzt wird. Konkret bedeutet dies, dass ein staatliches Organ mittels militärischer Waffengewalt einen anderen Staat schädigt und der Schaden über reine ökonomische Verluste, auch wenn diese immens sind, hinausgeht. Noch konkreter kann dann von einem Krieg gesprochen werden, wenn der geschädigte Staat in Ausübung seines Rechts auf Selbstverteidigung reagieren kann. Ab diesem Zeitpunkt erfolgt die Gewaltanwendung nicht mehr nur einseitig, da sich nun zwei Staaten gegenseitig mit militärischer Gewalt begegnen. Voraussetzung für die rechtmäßige Ausübung von Gegenangriffen im Rahmen der Selbstverteidigung nach Art. 51 UN-Charta ist das Vorliegen eines sogenannten „bewaffneten Angriffs“. Ein „bewaffneter Angriff“ ist etwa bei einer gravierenden physischen Zerstörung von Objekten oder beim Verlust von Menschenleben anzunehmen.

Cyberangriffe als Verstoß gegen das Gewaltverbot ?

Völkerrechtlich geht man davon aus, dass sich das Gewaltverbot [analog auf den Cyberraum](#) übertragen lässt, wenn man unter militärischer Waffengewalt Cyberwaffen miteinschließt. Als [Cyberwaffen](#) werden Software, Firmware oder Hardware bezeichnet, die für das Herbeiführen von Schäden über

Computernetzwerke entwickelt worden sind oder dafür eingesetzt werden. Der als Stuxnet bekannte Cyberangriff im Jahr 2010 auf das iranische Atomkraftwerk in Natanz kommt einer Verletzung des Gewaltverbots beispielsweise sehr nahe. Damals wurde ein Wurm in das Computersystem des Atomkraftwerks eingeschleust, der die Drehzahl der Uranzentrifugen in einer Weise manipulierte, dass diese zersprengten. Der Iran soll in der Folge etwa [1000 Uranzentrifugen](#) verloren haben, die zur Anreicherung von Uran gedient haben. Das Ziel von Stuxnet war, möglichst unauffällig das [iranische Atomprogramm](#) zu sabotieren. Mit größter Wahrscheinlichkeit vermutet man die Regierungen der [Vereinigten Staaten und Israel](#) hinter diesem Cyberangriff, eine offizielle Zurechnung ist allerdings nie erfolgt. Selbst in diesem Fall, als Objekte mittels eines Cyberangriffs physisch zerstört wurden, hüteten sich die Regierungen, rechtlich von einer Verletzung des Gewaltverbots und mithin von einem Krieg zu sprechen.

Ein Spionageakt mit oder ohne Cyberoperationen reicht nicht einmal aus, um in die Nähe des Gewaltverbots zu kommen – genauso wenig Wahlmanipulation, Sabotage oder Datenklau. In diesen Fällen wäre es akkurater, von einer Verletzung des Interventionsverbotes zu sprechen. Das Interventionsverbot schützt die Staaten vor Eingriffen in deren Souveränität, wenn ein Eingriff unter Anwendung von Zwang durch einen anderen Staat ausgeführt oder angeordnet wird. Der geschädigte Staat darf im Falle einer Verletzung des Interventionsverbots nicht dieselben Gegenmaßnahmen ergreifen wie er bei Verletzung des Gewaltverbots dürfte. Hinzu kommt, dass nicht abschließend klar ist, ob Spionageakte völkerrechtlich überhaupt gegen das Interventionsverbot verstoßen. Die Staatengemeinschaft betrachtete im Zeitpunkt der Gründung der Vereinten Nationen die Spionage als keine Verletzung des zwischenstaatlichen Interventionsverbots, weil sie sozusagen als [zulässiges Mittel zur geheimdienstlichen Informationsbeschaffung](#) dienen sollte.

Gefährden Ungenauigkeiten im allgemeinen Sprachgebrauch juristische Unterscheidungen?

Das Völkerrecht hat einen guten Grund, penibel zwischen Krieg und nicht-militärischer Verletzung der staatlichen Souveränität zu unterscheiden: Ein Krieg bringt weitreichende Konsequenzen mit sich, die nicht einfach rückgängig gemacht werden können. Damit gemeint sind über längere Zeit andauernde Zustände, gezeichnet durch den Verlust Hunderter von Menschenleben und Schwerstbeschädigung kritischer Infrastrukturen. Es sind insbesondere Verluste, die nicht einfach durch eine Schadenersatzzahlung aufgewogen werden können. Nicht-militärische Verletzungen der staatlichen Souveränität durch Cyberangriffe führten bisher zu zwar [enormen, aber dennoch rein finanziellen Schäden](#).

Die besondere Gefahr bei Cyberangriffen ist, dass sie mit gewissen Kontrollverlusten einhergehen. Einerseits können Cyberwaffen sehr schnell in falsche Hände geraten und beispielsweise für terroristisch motivierte Anschläge missbraucht werden. Andererseits bergen komplexe Angriffe wie man sie durch Stuxnet erfahren hat die Gefahr, nicht bloß bei einem rein finanziellen Schaden zu bleiben, sondern unter Umständen und je nach Örtlichkeit – man denke an das Atomkraftwerk – gar lebensgefährliche Explosionen zu verursachen. Im Fall von Cyberangriffen

ist durchaus denkbar, dass eine beabsichtigte, zunächst „einfache“ Verletzung der staatlichen Souveränität, dann vielleicht unbeabsichtigt die Gewaltschwelle erreicht. Wir sollten deshalb vorsichtiger sein und nicht jede Art von Eingriff in die staatliche Souveränität als Krieg bezeichnen. Das Schlagwort „Cyberkrieg“ darf in der Gesellschaft durch den alltäglichen Sprachgebrauch nicht salonfähig gemacht werden, weil damit schleichend auch die notwendige rechtliche Unterscheidung gefährdet wird. Dass Ungenauigkeiten im allgemeinen Sprachgebrauch juristische Unterscheidungen verschwimmen lassen, ist schnell geschehen: Ein aktuelles Beispiel wäre der Begriff [„Krieg gegen den Terror“](#), der post 9/11 ebenfalls als Schlagwort in den Medien verbreitet war. Dieser diffuse Ausdruck hat sich mittlerweile so eingebürgert, dass Staaten den Begriff „Krieg gegen den Terror“ dem Rechtsbegriff des internationalen oder internen bewaffneten Konfliktes vorziehen. Negative Auswirkungen zeitigte die Aufweichung des Rechtsbegriffs des bewaffneten Konfliktes etwa im Bereich der [Kriegsmaterialexporte](#). Teilweise wurden solche unter dem Vorwand bewilligt, ein Zielland befinde sich nicht in einem bewaffneten Konflikt, sondern beteilige sich lediglich am sogenannten „Krieg gegen den Terror“. Eine zu Beginn harmlose Ungenauigkeit des allgemeinen Sprachgebrauchs, und ein genereller Hang der Medien zur Dramatisierung, haben in diesem Fall zu einer Aufweichung eines Rechtsbegriffs geführt – mit [weitreichenden Konsequenzen](#).

Scheidungskrieg, Handelskrieg ... Cyberkrieg?

Der Begriff des Cyberkriegs darf nicht als dramatisierender Stimmungsmacher missbraucht werden. Schließlich steht der „Cyberkrieg“ im umgangssprachlichen Gebrauch nicht auf derselben Stufe wie der „Handelskrieg“ oder „Scheidungskrieg“. Bei den Letztgenannten weiß jeder, dass niemals ein tatsächlicher Krieg gemeint ist. Beim Cyberkrieg sieht es ganz anders aus: Gerade der graduelle Übergang von einer Verletzung des Interventionsverbots hin zur tatsächlichen Gewaltanwendung birgt im Falle von Cyberangriffen die Gefahr eines tatsächlichen Krieges. Eine scharfe Unterscheidung zwischen Verletzung des Gewalt- oder Interventionsverbots ist gerade in diesen Fällen von Bedeutung. Es ist bei Cybervorfällen unterhalb der Gewaltschwelle fahrlässig, von einem Krieg zu sprechen, ganz einfach deshalb, weil dadurch in der Gesellschaft falsche Erwartungen an die Möglichkeiten einer Gegenwehr geweckt werden. Der Westen schießt sich selbst ins Knie, wenn er lauthals „Cyberkrieg“ ruft, aber nicht völkerrechtskonform mit Gegenmaßnahmen reagieren kann, die in einem Krieg zu erwarten wären. Wird dieses Schlagwort für all die bloßen Eingriffe in die staatliche Cybersouveränität benutzt, fehlen dem Westen im Falle eines tatsächlichen Cyberkriegs plötzlich die Worte.

[Sanija Ameti](#) studierte Rechtswissenschaften mit Schwerpunkt im öffentlichen Recht an der Universität Zürich und promovierte zum Thema Cybersicherheit. Seit 2017 forscht sie als wissenschaftliche Assistentin am Institut für Völkerrecht und ausländisches Verfassungsrecht an der Universität Zürich. Bei ihrer vorangehenden Tätigkeit in der Direktion für Völkerrecht beim Eidgenössischen Amt für auswärtige Angelegenheiten befasste sie sich unter anderem mit dem „Tallinn Manual 2.0“ und dem Schweizer Export von Kriegsmaterial.

Cite as: Sanija Ameti, “Cyber-War oder Cyber-Wahn? Wenn Ungenauigkeiten im allgemeinen Sprachgebrauch juristische Unterscheidungen gefährden”, *Völkerrechtsblog*, 24 October 2018, (doi: folgt).

