Aaron Lye

Quo vadis NATO?

Kurzer Bericht über die Tagung

Die Deutsche Sektion der IALANA (Juristinnen und Juristen gegen atomare, biologische und chemische Waffen. Für gewaltfreie Friedensgestaltung) veranstaltete gemeinsam mit dem Zentrum für Europäische Rechtspolitik (ZERP) der Universität Bremen und vielen weiteren Mitveranstaltern vom 26. bis 28. April 2013 in Bremen eine Tagung zum Thema Quo vadis NATO? – Herausforderungen für Demokratie und Recht.

Als Kernfrage wurde im Programm formuliert: „Ist das, was die NATO und ihre Mitgliedstaaten planen, finanzieren und tun, mit dem Friedensgebot des Grundgesetzes und der UN-Charta vereinbar?“ Der Schwerpunkt der Tagung lag auf einer kritischen Auseinandersetzung mit der Rolle der NATO in Vergangenheit, Gegenwart und Zukunft aus rechtlicher, friedenswissenschaftlicher und friedenspolitischer Sicht. Neben einer Reihe von Vorträgen bekannter Persönlichkeiten und Podiumsdiskussionen mit prominenter Besetzung gab es am Samstag Nachmittag acht parallele Arbeitsgruppen, von denen zwei einen starken informationstechnischen Bezug hatten: *Militärische Drohnen, Killerautomaten und das Recht* sowie *NATO, Cyberwar und das Recht*. Auf letztere Arbeitsgruppe soll im Folgenden näher eingegangen werden. Der Text basiert auf Stichworten zu den zwei Impulsvorträgen und der Diskussion in der Arbeitsgruppe.

Hans-Jörg Kreowski (Professor für Theoretische Informatik an der Universität Bremen und FIfF-Vorstandsmitglied) begann mit einem Vortrag zum Thema *Cyberwar – Schimäre oder reale Gefahr?*, der sich aus vier Teilen zusammen setzte: (1) Das Phänomen Cyberwar, (2) Bedrohungen durch Cyberwar, (3) Cyberpeace statt Cyberwar und (4) Thesen und Forderungen, was getan werden müsste, um Cyberwar zu unterbinden. Der Vortrag basierte auf Materialien von Sylvia Johnigk und Kai Nothdurft mit einer starken Orientierung an Sylvia Johnigks Vortrag *Cyberpeace statt Cyberwar* auf dem 29C3-Kongress *Not my Department!* im Dezember 2012 (vgl. Bericht in der *FIfF-Kommunikation 1/2013,* S.10/11).

Darauf folgte der Vortrag von *Michael Bothe* (ehemals Professor für Öffentliches Recht, Völkerrecht und Europarecht an der Goethe-Universität Frankfurt am Main) zu der rechtlichen Perspektive, inwiefern das bekannte Modell der Kriegsführung auf Cyberwar angewendet werden kann. Der Vortrag lässt sich in folgende vier Abschnitte einteilen: Einführung in den rechtlichen Rahmen von Kriegen, Parallelen zwischen konventionellen Kriegen und Cyberkrieg, Problematik bei Dual-Use-Infrastruktur und Anwendung von internationalem Recht auf Cyberwar.

Einführung in den rechtlichen Rahmen von Kriegen

Das Gewaltverbot besagt, dass Gewaltausübung in internationalen Beziehungen prinzipiell verboten ist und damit Kriege grundsätzlich völkerrechtswidrig sind. Wenn sie geführt werden, unterliegen sie rechtlichen Rahmenbedingungen und Regeln, die sowohl alte und neue Technologien und Prozesse betreffen.

Die Regeln, die militärische Gewalt einschränken, sind zu unterscheiden in *ius ad bellum* (right to war) und *ius in bello* (laws of war). Ius in bello, das Recht im Krieg, kann im Wesentlichen unter der Bezeichnung *Humanitäres Völkerrecht* zusammengefasst werden. Es besagt, wie gekämpft werden darf, und welche Mittel angewendet werden dürfen. Ius ad bellum (oder ius contra bellum) umfasst notwendige Kriterien, die erwogen werden müssen, bevor Krieg geführt werden darf. Nahezu jeder Angriff (als kriegerische Handlung) wird rechtlich begründet, wobei hier bestimmte Rechtfertigungsstrategien verfolgt werden, um diesen zu legitimieren und damit einen Angriff nicht als Verletzung des Gewaltverbots darzustellen. Ein solches Beispiel ist die Selbstverteidigung. Sie entkräftet das Gewaltverbot und ermöglicht militärische Gewalt. Laut internationalem Gerichtshof ist Selbstverteidigung auf Verdacht jedoch rechtswidrig. Ein Angriff muss prinzipiell einem Staat zurechenbar sein, da in internationalen Konflikten Staaten gegeneinander kämpfen, wobei allerdings auch nichtstaatliche Täter angreifbar sind.

Aaron Lye

Aaron Lye ist FIfF-Mitglied aus Bremen. Dort studiert er Informatik an der Universität Bremen und ist hochschulpolitisch aktiv.

Parallelen zwischen konventionellen Kriegen und Cyberkrieg

Um ius ad bellum und ius in bello auf Cyberwar anzuwenden und damit bestehende Rahmenbedingunen auf Cyberwar auszuweiten, ist es notwendig, Parallelen zwischen konventionellem Krieg und Cyberwar zu analysieren.

Neu beim Cyberwar sind die Formen der Schadenszufügung, also dem Angriff, und die Formen des Schadens. Hier wird zwischen direkten und indirekten Schäden differenziert. Auch indirekter Schaden kann verheerend sein, da dieser Auswirkungen auf große Systeme beabsichtigt und unter Umständen unser Leben vom Funktionieren dieser Systeme abhängig ist.

Im Bezug auf Cyberwar ist unklar, was überhaupt ein militärischer Angriff, und welche Gegengewalt gerechtfertigt ist. Besonders schwierig ist auch die Frage, gegen was und wen verteidigt wird, da eine Handlung häufig keinem Akteur zugeordnet werden kann und damit ein Attributionsproblem herrscht. Attribution ist bereits im konventionellen Krieg notwendig, allerdings ist hier die Zuordnung in der Regel einfacher. Dass Cyberangriffe nicht einfach zugeordnet werden können, ist eine Problematik von Cyberwar. Gleichzeitig ist dieses jedoch auch eine seiner Stärken für Angreifer. Deshalb ist es zu bezweifeln, dass Militärs und Regierungen gewillt sind, dieses Problem von sich aus zu lösen.

Ein Verbot von Cyberwar, wie es bei Landminen beispielsweise der Fall ist, löst das Problem nicht, da das Phänomen nach dem Verbot nicht aus der Welt geschafft wäre. Um das Phänomen rechtlich zu erfassen, bedarf es einer Analyse der Gewalt. Hierfür ist es notwendig, Parallelen von Cyberwar zum konventionellen Krieg zu finden. Eine wichtige Parallele ist der indirekte Schaden, der durch Angriffe verursacht wird. Beispielsweise entstand durch den Computer-Wurm *Stuxnet* direkter Schaden an Software; es wird allerdings davon ausgegangen, dass indirekter physischer Schaden an iranischer Uran-Anreicherungsinfrastruktur beabsichtigt war und dieser Fall auch eingetreten ist.

Problematik bei Dual-Use-Infrastruktur

Desweiteren gilt das Prinzip der Unterscheidung: Bei einem internationalen bewaffneten Konflikt kämpft ein Staat mit militärischen Mitteln gegen die militärischen Mittel eines anderen Staates. Wichtig ist die Unterscheidung zwischen militärischen und zivilen Infrastrukturen. Problematisch ist die Rechtslage bei Dual-Use-Infrastruktur (wie Energieversorgung und Verkehrswege). Diese darf angegriffen werden, allerdings entstehen unter Umständen gravierende Folge- und Kollateralschäden für die Zivilbevölkung. Deshalb sind diese Angriffe nur zulässig, wenn sie verhältnismäßig sind. Kollateralschäden sind bereits im konventionellen Krieg schwierig abschätzbar – im Cyberspace ist dieses mit Sicherheit nicht einfacher.

Anwendung von internationalem Recht auf Cyberwar

Man muss sich also genau damit auseinandersetzen, inwiefern sich internationales Recht, speziell ius ad bellum und humanitäres Völkerrecht, auf Cyberkonfikte und Cyber-Warfare anwenden lassen. Ein Ansatz bildet die Studie *Tallinn Manual on the International Law Applicable to Cyber Warfare*, die vom *NATO Cooperative Cyber Defence Centre of Excellence* in dreijähriger Arbeit erstellt und im März 2013 von der Cambridge University Press publiziert wurde. Dieses geschieht aus juristischer Sicht auch durchaus erfolgreich. Allerdings wird beim Tallinn Manual vorausgesetzt, dass das Attributionsproblem gelöst ist – deshalb ist Kritik an dieser Studie durchaus angebracht.

Aus rechtlicher Perspektive ist die Attribution die einzige Problematik, die gelöst werden muss. Internationales Recht anzupassen, löst die Problematik nicht, und auch informationstechnisch lässt es sich derzeit ohne totale Überwachung nicht lösen.

erschienen in der FIfF-Kommunikation, herausgegeben von FIfF e.V. - ISSN 0938-3476 www.fiff.de