Michael Bothe

Der Computer-Krieg und die NATO

Das sogenannte Talinn-Manual soll Rechtsfragen beim Cyber warfare der NATO klären helfen. Dafür wurde eine Kommission aus unabhängigen Experten und Expertinnen berufen, die die Ausübung von Gewalt im völkerrechtlichen Rahmen analysiert und Regeln für den staatlichen Cyberkrieg vorschlägt.

„Cyber warfare“ ist eine neue Form von zwischenstaatlicher Schadensstiftung, die eine neue Form von Schaden verursacht. Die Schädigung erfolgt über eine elektronische Kommunikation, die schadensstiftende Informationsgehalte (Viren, Würmer, Trojaner) übermittelt. Der dadurch unmittelbar verursachte Schaden ist die Beeinträchtigung der Funktionsfähigkeit von Computer-Systemen. Diese Computer-Systeme sind aber wesentliche Elemente des Funktionierens lebenswichtiger Dienstleistungen (Energie, Transport, Finanzdienstleistungen) und militärischer Fähigkeiten (Aufklärung, Übermittlung von Informationen an Entscheidungsträger). Deshalb stellt sich die Frage, ob die traditionellen Regeln des Völkerrechts, die grenzüberschreitende Schädigungshandlungen verbieten, auf diese neue Form von Schädigung und Schaden anwendbar sind. „Warfare“ heißt Ausübung militärischer Gewalt. Sind die bestehenden Regeln über die Ausübung militärischer Gewalt auf solche Schädigungen anzuwenden?

Dieser Frage hat sich eine NATO-Einrichtung mit dem wohlklingenden Namen „Cooperative Cyber Defence Center of Excellence“ in Talinn durch Einberufung einer Expertenkommission angenommen, die vor kurzem ihre Ergebnisse in Form eines „Manual“, d.h. von Richtlinien mit Kommentaren, in einem international angesehenen wissenschaftlichen Verlag veröffentlicht hat.[1] Die Regeln sind einfach und allgemein formuliert, die Streitpunkte stecken in den Kommentaren. Das Manual ist keine offizielle NATO-Doktrin, so ausdrücklich die Einleitung. Aber die Arbeit dürfte nicht allzu fern von dem sein, was in den militärischen und politischen Kreisen der NATO über Rechtsfragen des Computerkriegs gedacht wird. Solche Experten- und Expertinnenarbeiten haben ihre eigene Wirksamkeit. Sie pflegen, wenn sie überzeugend sind, die Überlegungen von Entscheidungsträgern und Entscheidungsträgerinnen und Richtern und Richterinnen (wenn es je zu Kriegsverbrechens-Prozessen wegen Computer-Angriffen kommen sollte) zu prägen. Irgendwoher müssen die Entscheidungsträger und Entscheidungsträgerinnen ihre Maßstäbe nehmen. Sie greifen gern auf die Arbeit von Experten und Expertinnen zurück. Deren Akzeptanz wird nur erhöht, wenn Unei-

nigkeit der Experten und Expertinnen in Einzelfragen nicht verschwiegen wird. Dieser Mechanismus war der NATO-Institution, die das Gremium einberufen hat, wohl bewusst. Darum lohnt eine inhaltliche Analyse dieser Arbeit nicht nur wissenschaftlich, sondern auch militärisch und politisch.

Völkerrechtliche Regeln über die Ausübung militärischer Gewalt gibt es auf zwei Ebenen. Auf der ersten Ebene ist geregelt, ob überhaupt militärische Gewalt ausgeübt werden darf, in traditioneller Terminologie das *ius ad bellum*, besser *ius contra bellum*, da es bei diesen Regeln gerade um das Verbot militärischer Gewalt geht. Auf der zweiten Ebene wird geregelt, wie denn Gewalt ausgeübt werden darf, wenn sie trotz des Verbots (rechtmäßig oder rechtswidrig) ausgeübt wird (*ius in bello*). Wegen der Schwäche der Durchsetzung der Regeln der ersten Ebene ist diese zweite Ebene notwendig, um Schlimmeres zu verhindern. Das Manual befasst sich mit beiden Ebenen.

Grundregel des *ius contra bellum* ist das Verbot zwischenstaatlicher Gewaltausübung. Die wesentliche Ausnahme vom Gewaltverbot ist das Recht der Selbstverteidigung gegen einen bewaffneten Angriff. Es stellt sich also die Frage, ob und unter welchen Umständen die umrissene elektronische Schadensstiftung „Gewalt" im Sinne des Gewaltverbots darstellt. Die NATO-Experten sehen das Kriterium, das diese Frage beantworten soll, in der Gleichwertigkeit der Wirkung der Schadensstiftung („scale and effects comparable to non-cyber operations rising to the level of a use of force"). Eine Maßnahme des Cyber warfare ist Ausübung von militärischer Gewalt, wenn ihre unmittelbare oder auch mittelbare Wirkung der Schadensstiftung durch militärische Maßnahmen gleichkommt. Das ist jedenfalls bei erheblicher physischer Zerstörung der Fall, etwa bei Öffnen der Schleusen eines Staudamms durch einen Computer-Angriff auf sein elektronisches Steuerungssystem. Bei dem bekannten Angriff auf iranische Atomanlagen durch „Stuxnet" wurden durch eine Manipulation des Steuerungssystems die Zentrifugen physisch beschädigt.

Mit dieser Theorie der gleichwertigen Wirkung wird die gesamte gegenwärtige Debatte um zulässige Angriffshandlungen in die Frage des Cyber warfare hineingetragen. Dies prägt das Manual. Es nimmt deswegen auch zu allgemeinen Streitfragen zulässiger Gewaltausübung Stellung (u.a. Selbstverteidigung und Beteiligung an Kampfhandlungen). So gerät das Manual über das Thema des Cyber warfare hinaus zu einer Art Lehrbuch darüber, wie das heutige Völkerrecht militärische Gewalt regelt, jedenfalls nach Auffassung NATO-naher Experten und Expertinnen. Das sei an wenigen Beispielen gezeigt.

Der „bewaffnete Angriff" ist eine intensive Form der Gewaltausübung, die das Selbstverteidigungsrecht auslöst. Darum ist die Definition des bewaffneten Angriffs entscheidend für die Definition von Selbstverteidigung. Mit dieser Definition wird Politik gemacht. Es geht um die Überzeugungskraft von Rechtfertigungsstrategien für den Einsatz militärischer Gewalt. Da die gebräuchlichste Rechtfertigung für den Einsatz militärischer Gewalt die Selbstverteidigung ist, vertreten Staaten, die aktive Optionen des Einsatzes militärischer Gewalt verfolgen und diese Optionen rechtlich rechtfertigen wollen, eine weite Definition des bewaffneten Angriffs. Denn diese hat eine weiter reichende Rechtfertigung von angestrebten militärischen Optionen zur Folge. Das Manual verfolgt die amerikanische Linie einer weiten Definition von als

Selbstverteidigung zulässiger Gewalt (wobei abweichende Meinungen, in dem Expertengremium eine Minderheit, nicht verschwiegen werden).

Herkömmlich wird als bewaffneter Angriff nur solche Gewalt angesehen, die von einem Staat gegenüber einem anderen Staat ausgeübt wird. Um den Tatbestand der Verletzung des Gewaltverbots oder des bewaffneten Angriffs zu erfüllen, muss eine Maßnahme einem Staat zurechenbar sein. Das wird seit 9/11 bestritten. Konnte denn dieser Angriff Afghanistan zugerechnet werden? Die Mehrheit der NATO-Experten und -Expertinnen ist der Auffassung, dass ein bewaffneter Angriff im Rechtssinn auch von einem nicht-staatlichen Akteur wie Al Qaeda ausgehen kann und dass Selbstverteidigung dann auch auf dem Gebiet eines Staates ausgeübt werden kann, dem der Angriff gar nicht zuzurechnen ist, jedenfalls wenn dieser nicht willens oder in der Lage ist, seinerseits gegen den von seinem Gebiet aus operierenden nicht-staatlichen Akteur vorzugehen. Der Kommentar verschweigt wenigstens nicht, dass der Internationale Gerichtshof das ganz anders sieht. Auch die Mehrheit der Völkerrechtler und Völkerrechtlerinnen der Welt teilt nicht unbedingt die Meinung der Mehrheit der NATO-Experten und -Expertinnen.

Mit der Zurechenbarkeit ist man bei der zentralen Schwierigkeit der rechtlichen Regelung des Cyber warfare. Die Rückverfolgung einer solchen Maßnahme zu ihrem eigentlichen Urheber ist häufig nicht möglich. Die Urheber des Stuxnet-Angriffs auf die iranischen Atomanlagen wurden nie einwandfrei identifiziert. Die Tatsache, dass eine Schädigung von einem bestimmten Server aus erfolgte, reicht nicht aus, um diese Schädigung dem Staat zuzurechnen, auf dessen Territorium der Server steht. Das sagt das Manual ausdrücklich (Regeln 7 und 8). Häufig ist nicht festzustellen, ob eine zweifellos vorhandene massive Schädigung als bewaffneter Angriff von einem bestimmten Akteur oder gar einem bestimmten Staat ausgeht. Nur wenn eine Zurechenbarkeit mit hinreichender Sicherheit feststeht, ist Selbstverteidigung gegen diesen Staat zulässig. Selbstverteidigung auf Verdacht ist es nicht, wie der Internationale Gerichtshof in einem anderen Fall gewaltsamer Reaktion auf Schädigungshandlungen unklaren Ursprungs entschieden hat. Selbstverteidigung wird also in vielen Fällen von Cyber warfare rechtlich nicht zulässig und übrigens auch militärisch oder politisch nicht sinnvoll sein – eine Schlussfolgerung, die das Manual nicht zieht.

Zum *ius in bello*: Seine Grundregel ist das Prinzip der Unterscheidung. Im bewaffneten Konflikt zulässig sind Schädigungshandlungen („Angriffe“) durch Angehörige des Militärs (Kombattanten) gegen die militärischen Anstrengungen des Gegners, d.h. gegen seine Streitkräfte und gegen sog. militärische Ziele. Das sind Objekte, die wirksam zur militärischen Anstrengung des Gegners beitragen und deren Zerstörung bzw. Eroberung oder Neutralisierung darum einen militärischen Vorteil mit sich bringt. Zivilisten und zivile Objekte dürfen nicht angegriffen werden. Im Rahmen des Cyber warfare stellt sich darum die Frage, welche Art von Schädigungshandlungen, die die Funktionsfähigkeit von Computer-Systemen beeinträchtigen, in diesem Sinne überhaupt Angriffe darstellen. Auch für diese Frage ist die Gleichwertigkeit der Wirkung mit der herkömmlicher Angriffe ausschlaggebend. Angriffe in diesem Sinne sind darum Handlungen, so das Manual (Regel 30), von denen vernünftiger Weise angenommen werden kann, dass sie Verletzung oder Tod von Personen oder Schaden an Sachgütern verursachen werden.

Computer-Systeme, die allein militärischen Zwecken dienen, sind militärische Ziele. Denkbar sind aber auch Angriffe auf Objekte, die zivilen Zwecken dienen, z.B. Steuerungssysteme der Energieversorgung, Einrichtungen der Telekommunikation. Wenn solche Einrichtungen zugleich auch militärischen Zwecken dienen (sog. „dual use"-Objekte), sind sie militärische Ziele. Vor einem Angriff müssen „praktisch mögliche" Maßnahmen ergriffen werden, um festzustellen, ob das der Fall ist. Wie im Falle von Computer-Systemen die bei dieser Prüfung anzuwendende Sorgfalt zu bestimmen ist, ist eine schwierige Frage. Das Manual spricht von „ständiger Sorgfalt" (constant care, Regel 52), ohne zu bestimmen, was das bedeutet. Hier sind wir erneut beim Problem der Internet-typischen Unsicherheiten.

Nur Kombattanten und Kombattantinnen (d.h. zur Teilnahme an Kampfhandlungen berechtigte Angehörige der Streitkräfte) und Zivilisten und Zivilistinnen, die unmittelbar an den Kampfhandlungen teilnehmen, dürfen gezielt angegriffen werden, letztere auch nur für die Zeit einer solchen Teilnahme (Regel 35). Im Bereich des Cyber warfare tummeln sich Privatpersonen, die in der Tat nicht den Streitkräften angehören, Hacker und Hackerinnen (Hacktivists), Programmierer und Programmiererinnen von Schadprogrammen u.v.m. Das Manual vertritt insofern eine weite Definition der unmittelbaren Teilnahme, die den Kreis der anzugreifenden Personen weit zieht. Teilnahme ist nicht nur der Angriff im Sinne der genannten Definition, sondern alles, was Streitkräften im Kampf schadet (also etwa Störung von militärischer Kommunikation). Unsicher sind die Experten und Expertinnen bei der Frage, wie nahe eine Unterstützungshandlung (etwa das Schreiben von Programmen zur Durchführung von Computer-Angriffen) an einer den Feind schädigenden Handlung sein muss, um als unmittelbare Teilnahme zu gelten, die den Programmierer zum rechtmäßigen Ziel von Angriffen macht. Ein Teil der Experten und Expertinnen scheint da recht geringe Anforderungen an diese Nähe zu stellen: die Hacktivists leben nach dem Manual ziemlich gefährlich.

Das Manual vertritt einerseits in seinen Stellungnahmen zu aktuellen Streitfragen der rechtlichen Schranken militärischer Gewalt konsequent eine Tendenz, die der Politik großer Militärmächte freundlich ist. Andrerseits verfolgt es einen an sich billigenswerten Ansatz: Es verwirft nicht etwa die bestehenden Rechtsregeln als obsolet oder irrelevant. Es versucht vielmehr, diese Regeln konsequent auf das neue Phänomen des Cyber warfare anzuwenden, indem es auf die gleichwertige Wirkung der Schädigungshandlung abstellt. Verboten sind solche Angriffe, die einen physischen Schaden verursachen, der dem gleicht, der durch herkömmliche militärische Operationen verursacht wird und der nach den für diese geltenden Regeln rechtswidrig ist. Das ist letztlich die traditionelle juristische Methode, neue Entwicklungen rechtlich einzugrenzen. Die Methode hat freilich ihre Grenzen. Es gibt neue Entwicklungen, für die die alten Regeln wirklich nicht ausreichen. Beim Computer-Krieg ist dies die Schwierigkeit, den wahren Urheber einer schadensstiftenden Handlung festzustellen und so die Handlung einem verantwortlichen Rechtssubjekt zuzuordnen. Aber eben darauf beruht die Wirkung von Rechtsregeln im Allgemeinen und von Völkerrecht im Besonderen.

Die Autoren des Manual haben das Problem gesehen, aber nicht wirklich lösen können oder wollen. Die Frage bleibt eine Herausforderung für die Rechtsentwicklung. Da

gilt es staatliche Kontrollpflichten zu bedenken und zu schaffen, die verhindern, dass unverantwortliche Akteure auf Kriegsschauplätzen mitmischen. Eine wesentliche staatliche Verantwortung geht auch dahin, die Verwundbarkeit lebenswichtiger Steuerungssysteme zu verringern. Das ist eine Herausforderung für die Entwicklung von Technologie, aber auch für eine wie auch immer zu denkende Entwicklung des Rechts. Das Manual kann nicht das letzte Wort in Fragen des Cyber warfare sein.

MICHAEL BOTHE ist Rechtswissenschaftler und als solcher Professor emeritus an der J.W. Goethe Universität Frankfurt/Main. Schwerpunkt seiner Tätigkeit ist der Bereich Völkerrecht, insbesondere mit den Themen Friedenssicherungsrecht, Rüstungskontrolle, humanitäres Völkerrecht, internationales Umweltrecht und vergleichendes Staats- und Verfassungsrecht. Bothe leitet seit 1995 den „Fachausschuss Humanitäres Völkerrecht“ des Deutschen Roten Kreuzes (DRK) und war von 2001 bis 2005 Vorsitzender der Deutschen Gesellschaft für Völkerrecht. Er gehörte außerdem von 2001 bis 2011 der Internationalen humanitären Ermittlungskommission an und war ab 2007 deren Präsident.

Anmerkungen:

1 Talinn Manual on the International Law Applicable to Cyber warfare. Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Center of Excellence. General editor: Michael N. Schmitt. Cambridge University Press 2013, XIX, 282 S., £ 35,00.