Klaus-Gerd Giesen

Umriss einer kantschen Cyberkriegsethik

Zusammenfassung
Der Text liefert einen Beitrag zur Erfassung des Cyberkrieges aus ethischer Perspektive. Nachdem die neue Kriegsform begrifflich erfasst und in den weiteren historischen und technischen Kontext eingeordnet ist, werden Normen internationaler Gerechtigkeit konkret entwickelt, indem auf die komplexe Kriegsethik Immanuel Kants zurückgegriffen wird. Besondere Aufmerksamkeit erhält dabei neben *Ius ad bellum* und *Ius in bello* vor allem das *Ius post bellum*, das als besonders relevant eingestuft wird, u. a. weil wegen der ständig wachsenden Bedeutung des Internet of Things völlig neue Gefahren für die Menschheit entstehen.

Abstract
The text contributes to the conceptualization of cyberwar from an ethical perspective. After this new form of war has been defined and placed in a wider historical and technical context, norms of international justice are developed in concrete terms by resorting to Immanuel Kant's complex war ethic. In addition to *ius ad bellum* and *ius in bello*, special attention is given to the *ius post bellum*, which is considered particularly relevant, among other things because the ever-growing importance of the Internet of Things is bringing entirely new dangers for humanity.

1 Einleitung: Cyberkrieg im Kontext

Seit Heraklit gibt es eine Philosophie des Krieges. Denn die Dichotomie von Krieg und Frieden strukturiert unser Leben. Fast alle bedeutenden Philosophen haben eine Philosophie des Krieges und des Friedens skizziert, einschließlich (im 20. Jahrhundert) Lévinas, Rawls, Derrida und Habermas. Sie alle zeigen Versuche auf, das Wesen des Krieges und/oder des Friedens zu erfassen und Gerechtigkeit in Bezug auf diesen Bereich zu definieren.

Der Cyberkrieg verändert unser Verständnis von Krieg bzw. Frieden sowie von der Beziehung zwischen Mensch und Maschine. Damit entsteht eine völlig neue militärische Dimension, für die ein ethischer Rahmen geschaffen werden muss, da sonst auf diesem Gebiet ein Naturzustand bestehen bleibt, in dem der stärkste Akteur fast uneingeschränkt herrschen kann.

Der Cyberkrieg ist eine völlig neue Dimension der Kriegsführung. Deshalb konnten sich internationale Normen noch kaum etablieren. Das Internet hat Einzelpersonen, verschiedenartigen Organisationen und Nationen eine nicht zu unterschätzende neue Schlagkraft gegeben, auf der die sich ständig weiterentwickelnde Netzwerktechnologie basiert. Für jedermann – Regierungen, Bürger, Soldaten, Spione, Propagandisten, Hacker und Terroristen – ist zum Beispiel Informationsbeschaffung, Kommunikation, Fundraising oder Öffentlichkeitsarbeit zunehmend digitalisiert.

Wir stehen erst am Anfang dieser Informationsrevolution. Der Computer ist sozusagen die neue Dampfmaschine. Das erleichtert ungemein den Erwerb und die Verbreitung von Wissen und Informationen durch den Aufstieg des Cyberspace. Heute sind mehr als zwei Milliarden Computer direkt mit dem Internet verbunden, und es gibt fast drei Milliarden Internetnutzer auf der Erde. Infolgedessen haben jetzt alle politischen und militärischen Konflikte auch eine Cyberdimension, deren Ausmaß und Auswirkungen noch immer schwer zu erfassen sind. Die im Cyberspace ausgetragenen Konflikte könnten in Zukunft vielleicht wichtiger sein als die Ereignisse in der physischen Welt. Im Cyberkonflikt ist die geographische Distanz zwischen Gegnern praktisch irrelevant, denn im Cyberspace ist jeder des anderen Nachbar: Mit Glasfaser- und Satellitenübertragungen bewegen sich Computersignale fast mit Lichtgeschwindigkeit. Die mächtigsten Waffen basieren nicht auf physischer Stärke, sondern auf Logik und Innovation. Cyberkriegsführung ist definitiv anders als traditionelle Kriegsführung, aber sie teilt einige Eigenschaften mit der historischen Rolle von Luftbombardierung, U-Boot-Kriegsführung und Spezialeinsatzkräften. Insbesondere kann sie einem Gegner aus der Ferne oder durch Ausnutzen des Überraschungsmomentes schmerzhaften, asymmetrischen Schaden zufügen (vgl. Geers 2011). Und Cyberkrieg ist vergleichsweise äußerst billig.

Die Vernetzung durch das Internet stellt eine enorme Bedrohung für die zivile Infrastruktur dar. Tatsächlich sind die meisten militärischen Netze auf zivile, vor allem kommerzielle Computerinfrastrukturen angewiesen, wie zum Beispiel unterseeische Glasfaserkabel, Satelliten, Router oder Knotenpunkte; umgekehrt sind zivile Fahrzeuge, Schifffahrt und Flugsicherung zunehmend mit Navigationssystemen ausgestattet, die auf Satelliten des Global Positioning System (GPS) basieren, welche auch vom Militär genutzt werden. Somit ist es mittlerweile äußerst schwierig, zwischen rein ziviler und rein militärischer Computerinfrastruktur zu

unterscheiden. Dies stellt eine ernsthafte Herausforderung bezüglich des allgegenwärtigen Unterscheidungsprinzips zwischen militärischen und zivilen Objekten dar (siehe unten). *Interconnectivity* bedeutet, dass sich die Auswirkungen eines Angriffs auf ein militärisches Ziel nicht auf dieses Ziel beschränken müssen. Tatsächlich kann ein Cyberangriff Auswirkungen auf verschiedene andere Systeme, einschließlich ziviler Infrastrukturen und Netzwerke, haben, beispielsweise durch die Verbreitung von *Malware* (bösartiger Software wie zum Beispiel Viren oder Würmer), wenn diese unkontrollierbar sind bzw. werden (vgl. Droege 2012).

Daher ist die zivile Infrastruktur aufgrund ihrer zunehmenden Abhängigkeit von Computersystemen sehr anfällig für Angriffe auf Computernetzwerke. Insbesondere eine Reihe kritischer Anlagen, wie Kraftwerke, Atomanlagen, Staudämme, Wasseraufbereitungs- und Verteilungssysteme, Ölraffinerien, Gas- und Ölpipelines, Bankensysteme (einschließlich Geldautomaten), Börsen und die übrige Finanzwelt, Krankenhaussysteme, Eisenbahnen und Flugsicherung sind auf Informationstechnologie angewiesen. Solche Systeme, die das Bindeglied zwischen der digitalen und der physischen Welt bilden, erweisen sich als extrem anfällig für äußere Einflüsse durch praktisch jeden potentiellen Angreifer. Es handelt sich um das sog. Internet of Things, d. h. aller Objekte, die direkt mit dem Internet verbunden sind.

Im Mai 2009 verkündete der amerikanische Präsident Obama: „Cyber-Eindringlinge haben unser Stromnetz untersucht […]. In anderen Ländern haben Cyber-Angriffe ganze Städte in Dunkelheit gestürzt" (The White House 2009). Journalisten kamen nach Recherchen zu dem Schluss, dass diese Anschläge in Brasilien stattgefunden haben, wo Millionen von Zivilisten im Bundesstaat Espírito Santo bereits im Jahr 2005 und in Rio de Janeiro im Jahr 2007 betroffen waren, und dass die Quelle der Anschläge noch unbekannt sei. Richard Clarke, der ehemalige Sonderberater von Präsident George W. Bush für Cybersicherheit, sagte später: „Angesichts der Ernsthaftigkeit, mit der die Obama-Administration die Cybersicherheit und das Stromnetz schützt, können wir gelassen die Art von Dingen erwarten, die in Brasilien geschehen sind, wo Hacker die Stromenergie erfolgreich zum Erliegen gebracht haben" (Mylrea 2009).

Nationale Sicherheitsplaner müssen heutzutage eingestehen, dass Elektrizität nicht ersetzt werden kann, und dass alle anderen Infrastrukturen, einschließlich Computernetzwerke, davon abhängen. Die Manipulation von elektrischen Netzmanagementsystemen ist daher derzeit wohl die größte zivile Bedrohung (vgl. Mele 2010). Darüber hinaus sind

Verteilsysteme für Lebensmittel, Wasser, Geld, Güter (Supply Chain Management) und Energie in jeder Phase auf IT angewiesen, ebenso wie Transport-, Gesundheits- und Finanzdienstleistungen. Möglicherweise katastrophale Szenarien wie Zusammenstöße zwischen Flugzeugen, die Freisetzung von Strahlung aus Kernkraftwerken oder toxischer Chemikalien aus Chemieanlagen und die Störung lebenswichtiger Infrastrukturen und Dienste wie Strom- oder Wassernetze, können nicht ausgeschlossen werden.

Im Jahr 2010 hat der Computerwurm Stuxnet, höchstwahrscheinlich ein amerikanisch-israelisches Joint Venture, das erreicht, was sämtliche Resolutionen des Sicherheitsrates der Vereinten Nationen nicht ermöglicht hatten: Irans Bau einer Atombombe zu unterbrechen. Ein halbes Megabyte Computercode ersetzte mögliche Luftangriffe der israelischen Luftwaffe. Stuxnet war deutlich effektiver als jeder konventionelle militärische Angriff hätte sein können – und das sogar ohne direkte Verbindung der iranischen Aufarbeitungsanlagen mit dem Internet (also per USB-Übertragung). Die Tatsache, dass die USA und Israel mit derart spektakulären Angriffen aufwarten können, stellt eine starke Versuchung für alle anderen Staaten dar, in Zukunft ebenfalls die Vorteile des Computer-Hackings zu nutzen.

Militärische Streitkräfte bilden natürlich keine Ausnahme. Die IT wird für das Management von Streitkräften eingesetzt – zum Beispiel gerade für die Führung und die Logistik. Schon heute ist es durchaus denkbar, dass ein ausländischer Staat die IT-Infrastruktur der gegnerischen Armee ganz oder teilweise kontrolliert und so manipuliert, dass diese Waffen – wie zum Beispiel atomar bestückte Raketen – auf die eigenen Städte und die eigene Bevölkerung abfeuert.

Die derzeitige Situation favorisiert den Cyberangreifer. Dies steht im Gegensatz zu unserem historischen Verständnis von Kriegsführung, bei dem der Verteidiger traditionell einen Heimvorteil genießt. Daher werden viele Regierungen in absehbarer Zeit zu dem Schluss kommen, dass die beste Cyberverteidigung ein gelungener Angriff ist.

Heutzutage kommt hinzu, dass Cyberangriffe auf politische Entscheidungsstrukturen, militärische Systeme oder den Durchschnittsbürger in vielen Fällen durch den zusätzlichen Vorteil der Anonymität des Angreifers unterstützt werden. Darüber hinaus macht die rasche Verbreitung von Internet-Technologien, einschließlich Hacker-Tools, unmöglich, dass jede Organisation, einschließlich der Armeen, mit allen diesen Neuheiten immer auf dem neuesten Stand ist. Häufige Software-Updates und

Netzwerk-Neukonfigurationen verändern unvorhersehbar und ohne Vorwarnung die Internet-Geographie. Cyberangriffe sind flexibler als jedes andere Waffensystem, das die Welt je gesehen hat. Sie können für Propaganda, Spionage oder die Zerstörung kritischer Infrastrukturen sowie großer Bevölkerungsgruppen eingesetzt werden. Die moralische Dimension des Cyberkrieges ist vorerst noch nicht sehr entwickelt, da es sich in erster Linie um die Nutzung und Ausbeutung von Informationen in Form von Computercode und Datenpaketen handelt; bisher gibt es kaum dadurch entstandenes menschliches Leid (vgl. Geers 2011). Aber das könnte sich eben bald ändern.

2 Begriffliche Bestimmung des Cyberkriegs

Aus ethischer Sicht ist es wichtig, zwischen einem Akt des Cyberkriegs und einem Akt zu differenzieren, der zwar moralisch falsch sein mag, aber gar nicht unter die Kategorie des Krieges fällt. Im Gegensatz zu vielen anderen Autoren (vgl. Einzinger 2011; Micewski 2011) soll hier für eine restriktive Definition plädiert werden, damit der Begriff nicht überfrachtet wird (vgl. Giesen 2013). Eines der Probleme besteht darin, dass im Cyberkonflikt Eingriffe auf das Staatsgebiet nicht unbedingt von Soldaten oder Fahrzeugen (Panzer, Flugzeuge usw.) vorgenommen werden. Insofern müssen zuerst einige Missverständnisse ausgeräumt werden.

Ein Cyberkrieg als solcher kann nur direkt zwischen zwei oder mehr *Staaten* stattfinden. Im Gegensatz zu Sean Watts (2012) soll hier jedoch die staatliche Zugehörigkeit nicht als einziges Kriterium für den Kombattantenstatus fungieren, d. h. die ansonsten restriktive Definition soll auch nichtstaatliche Akteure einschließen, die einer Staatsräson untergeordnet sind, wie z. B. nichtstaatliche Gruppen sogenannter „patriotischer Hacker" (in Russland, China, Israel und anderswo), die eng mit den nationalen Armeen zusammenarbeiten und von ihnen kontrolliert werden (vgl. Ventre 2011). Wie Michael Schmitt (2011, 579) zu Recht betont, bietet das geltende Völkerrecht hier einige interessante Analogien (der Fall Tadić des Internationalen Strafgerichtshofs für das ehemalige Jugoslawien, die iranische Geiselkrise 1979, der Fall Hisbollah 2006 usw.). Die Definition muss jedoch völkerrechtlich nicht anerkannte Gebietseinheiten wie die Türkische Republik Nordzypern, Palästina oder Transnistrien ausschließen.

Das Territorialitätsprinzip muss auch weiterhin als wesentliches Attribut der Staatssouveränität integraler Bestandteil der Definition sein (a contrario: Marie Stella 2003), obwohl aufgrund der dezentralen Natur des Internets jede Malware innerhalb von Sekundenbruchteilen viele Grenzen überschreiten kann, bevor sie ihr Ziel erreicht (vgl. Hare 2009). Es kann hier nur um die *Auswirkungen* eines Cyberangriffs auf ein nationales Territorium gehen.

Das im Völkerrecht viel diskutierte Prinzip der bewaffneten Aggression, das zur Rechtfertigung eines Kriegseintritts erforderlich ist (Art. 51 der UNO-Charta), sollte unbedingt beibehalten werden – allerdings mit der Ausnahme, dass sich die Bedeutung dessen, was als Waffe betrachtet werden kann, weiterentwickeln muss. Ein gezielter, mächtiger und zerstörerischer Computerwurm kann perfekt mit der Definition einer Waffe zusammenfallen (vgl. Delbasis 2009, 97). Auch hier kommt es auf die Wirkung an. Schließlich kann man mit einem Flugzeug auch Lebensmittel transportieren oder Städte bombardieren. Der Begriff des Cyberkrieges verlangt, dass Informationstechnologien für zerstörerische Zwecke genutzt werden.

Die Fachliteratur zelebriert das Wiederaufleben asymmetrischer Kriegsführung im Cyberspace (z. B. Schröfl u. a. 2011): Gegenüber einem Staat mit einer mächtigen Cyberarmee, wie den Vereinigten Staaten, Israel, China oder Russland, können alle anderen Länder in unterschiedlichem Maße offensive oder defensive Cyberkapazitäten besitzen und versucht sein, diese einzusetzen. Die Machtverhältnisse lassen jedoch vorerst keinen Zweifel am Ausgang eines solchen asymmetrischen Konflikts aufkommen. Dennoch ist im Cyberspace weder der totale Sieg noch die totale Niederlage wahrscheinlich.

Eine der Besonderheiten des Cyberkrieges liegt in der Möglichkeit eines sogenannten Sub-Rosa-Konflikts. In diesem Fall will weder der Angreifer noch der Verteidiger die Existenz eines Cyberkonfliktes öffentlich machen – auch nicht gegenüber der eigenen Bevölkerung. Dies kann entweder geschehen, um (für den angegriffenen Staat) im Falle einer Niederlage nicht das Gesicht zu verlieren, oder aus Angst vor der internationalen öffentlichen Meinung (für den Aggressorstaat), oder (für beide) um einen eskalierenden Konflikt durch einen Spillover-Effekt auf andere militärische Bereiche (konventionelle oder nukleare Kriegsführung) zu vermeiden, oder um Panik in der Bevölkerung zu vermeiden (vgl. Libicki 2009, 128–129). Der Sub-Rosa-Konflikt wirft das klassische Dilemma demokratischer Legitimität wichtiger militärischer Entscheidungen

versus technokratische Experteneffizienz erneut auf. Es ist klar, dass aus Sicht der internationalen Gerechtigkeit die größtmögliche Transparenz gefordert werden muss, damit die demokratische Kontrolle der Cyberwaffen erleichtert wird. Deshalb sollte ein Sub-Rosa-Cyberkrieg zumindest hinter verschlossenen Türen von den zuständigen parlamentarischen Verteidigungsausschüssen diskutiert und genehmigt werden.

Wenn man die genannten Voraussetzungen beachtet, kann man folgendes schnell ausschließen:

- *Cyberkriminalität*, auch durch nichtstaatliche Gruppen wie z. B. die russische Mafia. Der Europarat ist die einzige internationale Organisation, die Cyberkriminalität bislang reguliert hat.
- *Cyberpropaganda* und *Hacktivismus*, auch wenn sie DDoS-Angriffe auf Regierungswebsites beinhalten können.
- Eine einmalige *Cybersabotage* durch einen Staat: der Stuxnet-Virus bleibt damit deutlich unter der Schwelle, die den Cyberkrieg vernünftigerweise definiert.
- *Cyberspionage*: Tatsächlich ist Spionage mit neuen Technologien so alt wie die Beziehungen zwischen den Staaten. Das Hacken von Regierungscomputern oder Implantate – wie der mittlerweile berühmte *Flame*-Wurm oder der Diebstahl von Daten – bilden keine Ausnahme.
- *Cyberterrorismus* und *Cyberguerilla* sind das Ergebnis nichtstaatlicher Gruppen gegen einen oder mehrere Staaten und fallen daher nicht unter die Kategorie zwischenstaatlicher Konflikte.

So definiert sind die Grenzen zwischen den verschiedenen, im Internet stattfindenden aggressiven bzw. hinterhältigen Aktivitäten eigentlich gar nicht mehr so verschwommen.

3 Eine kantische Theorie des gerechten Cyberkriegs?

Nach der Begriffserfassung kann die Frage nach einer möglichen Grundlage für die Ethik des Cyberkriegs angegangen werden. Hier soll diesbezüglich die Theorie des gerechten Krieges mobilisiert werden, gerade weil es sich um einen sehr ausgereiften, von Cicero bis Walzer über viele Jahrhunderte entwickelten Ansatz handelt. Im Laufe der Zeit hat er sich an alle technologischen Revolutionen anpassen können. So führte zum Beispiel Vitoria im 16. Jahrhundert die wichtige Unterscheidung zwischen Kombattanten und Zivilisten mit dem damit einhergehenden Begriff

der Kollateralschäden infolge des Aufkommens von Artillerietechnik auf den Schlachtfeldern ein. Ein anderes Beispiel: In den vierziger und fünfziger Jahren diskutierten unter anderem die Theologen John Ford, Paul Ramsey und James Turner Johnson die höchst relevante Frage, ob selbst ein defensiver Atomkrieg überhaupt gerecht sein könnte. Die Theorie des gerechten Krieges ist also äußerst flexibel und entwicklungsfähig in Bezug auf neue Technologien der Kriegsführung.

Deshalb soll die klassische Theorie des gerechten Krieges hier auch erweitert werden: Rückgreifend auf Immanuel Kants *Rechtslehre* erscheint es logisch, dem traditionellen *Ius ad bellum* und *Ius in bello* ein *Ius post bellum* hinzuzufügen (Kant 1797, §§58–60; vgl. Giesen 2013). In der Tat war Immanuel Kant selbst nicht nur ein Friedensphilosoph, der für seine wegweisende Schrift zum Telos des ewigen Friedens bekannt wurde, sondern gleichzeitig auch ein Kriegsphilosoph, der in der *Metaphysik der Sitten* eine Theorie des gerechten Krieges entwickelt hat (vgl. Giesen 1997).

Wie schon in *Zum ewigen Frieden* (Kant 1795), aber im Gegensatz zu dem, was er einige Jahre zuvor in seiner *Idee zu einer allgemeinen Geschichte in weltbürgerlicher Absicht* (Kant 1784) bemerkt hatte, stellt Kant in der *Rechtslehre* fest, dass letztlich der „ewige Friede […] freilich eine unausführbare Idee ist" (Kant 1797, §61), zumal die allmähliche Ausdehnung des *foedus pacificum* auf die gesamte Erdoberfläche dazu führen würde, dass eine (Welt-)Regierung die Situation nicht mehr kontrollieren könnte, was zu vielen Bürgerkriegen führen würde. Das Problem des ethischen Status des Krieges bleibt daher ungelöst, da es eben um die Streitigkeiten von Staaten geht, die sich historisch gesehen noch außerhalb des republikanischen *foedus pacificum* befinden, sowie um die Beziehungen von republikanisch verfassten Staaten mit einem oder mehreren nicht-republikanischen Staaten. Eine normative Kriegsphilosophie ist somit notwendig. Die Paragraphen 56–60 der *Rechtslehre* sind deshalb der Definition von Kriterien für Gerechtigkeit oder Ungerechtigkeit solcher, vom *foedus pacificum* nicht gedeckten Kriege geschuldet.

Von Anfang an unterscheidet sich Kant von den Theorien des gerechten Krieges seiner Vorgänger. Erstens durch die Struktur seiner Argumentation: Zum traditionellen *Ius ad bellum* (§§56 und 57) und *Ius in bello* (§57) fügt er ein überraschendes *Ius post bellum* hinzu (§§58 und 60). Aber auch durch den Inhalt der entwickelten Kriterien. Kant geht hier auf die Kriterien von Aquinas zurück. Tatsächlich finden sich in den §§56 und 57 die vier thomistischen *Ius-ad-bellum*-Kriterien, wenn auch

in einer anderen Reihenfolge als in der *Summa Theologica*: 1. Das Ziel des Krieges muss ein vollkommenerer Frieden sein als vor dem Krieg (in den Worten Kants §57: „[…] den Krieg nach solchen Grundsätzen zu führen, nach welchen es immer noch möglich bleibt, aus jenem Naturzustande der Staaten […] herauszugehen und in einen rechtlichen zu treten"). 2. Der Krieg ist förmlich von der staatlichen Autorität zu erklären (vgl. Kant 1797, §55). 3. Der Krieg muss einen gerechten Grund haben (vgl. Kant 1797, §56 legt fest, dass er entweder nach einem Angriff, einer Drohung oder einem Vergehen erfolgen muss); 4. Eine rechte Intention: Für Kant bezieht sich dieses Gebot auf ein förmliches Verbot von Bestrafungs- und Vernichtungskriegen, welche den Herrscher aus moralisch „unreinen" Gründen in den Krieg führen können (Kant 1797, §56). In Aquinas, wie auch in Kant, fehlen die anderen drei Kriterien des üblichen Katalogs von *Ius ad bellum*, die zwischen den beiden Autoren von Vitoria und Suarez eingefügt wurden (vgl. Phillips 1984, 12–134), nämlich: 1. Krieg muss das allerletzte Mittel sein, um einen Streitfall zu lösen; 2. Es muss eine vernünftige Siegeschance bestehen, bevor man den Krieg erklärt; 3. Es soll unbedingt eine gewisse Verhältnismäßigkeit zwischen Fehlverhalten des Feindes und seiner Bestrafung gegeben sein.

Alle sieben *Ius-ad-bellum*-Kriterien (also auch die drei von Kant nicht einbezogenen) werden jetzt skizzenhaft auf den Cyberkrieg angewandt. Es muss dabei beachtet werden, dass der Katalog kumulativ ist, was bedeutet, dass sämtliche Kriterien erfüllt sein müssen, wenn ein Cyberkrieg als gerechter Krieg anerkannt werden soll.

4 Ius ad bellum

4.1 Das Endziel des Krieges: ein vollkommenerer Frieden (als vor dem Krieg).

Dieses erste Kriterium ist schwer zu erfüllen, weil Cyberkriege einfach dazu neigen, nicht enden zu wollen, da sie mit mehr oder weniger langen Pausen durchsetzt sein und möglicherweise auf der Sub-Rosa-Ebene weitergeführt werden können. Allerdings kann ein Krieg nur dann gerecht sein, wenn er ein Ende findet und wenn die Pläne für die Nachkriegsordnung diejenigen Mängel korrigieren, die schon vor dem Konflikt richtig erkannt wurden. Das bedeutet konkret, dass ein solcher Cyberkrieg nur eine gerechte Reaktion auf eine von einem

anderen Staat ausgelöste kinetische Aggression sein kann, wenn sie dazu bestimmt ist, das Schadenspotential des Gegners definitiv und für längere Zeit zu zerstören.

4.2 Die Autorität des Fürsten: die Kriegserklärung

Hier stehen wir vor zwei Herausforderungen: Zeit und Zuschreibung. Aufgrund der hohen Geschwindigkeit der Cyberkriegs-Ströme muss die formale diplomatische Kriegserklärung notwendigerweise auf ein Minimum reduziert werden, d. h. auf ein eindeutiges Computersignal, das wenige Augenblicke vor der Reaktion auf die Aggression gesendet wird – in Analogie zu einem Warnschuss in einer persönlichen Notsituation.

Andererseits liegt das Problem der Zuschreibung wiederum in der Tatsache, dass es im Cyberspace höchst problematisch ist, den Angreifer mit Sicherheit zu identifizieren, insbesondere wegen der möglichen Präsenz anderer Akteure auf dem virtuellen Schlachtfeld (vgl. Wheeler/Larsen 2007), aber auch wegen der wahrscheinlichen Nutzung von sogenannten Botnets (Third-Party-Servern), wie es zum Beispiel während des Cyberangriffs gegen Estland mit der illegalen Benutzung von mindestens einer Million Computern weltweit der Fall war. Während absolute Gewissheit im Cyberspace eigentlich nie möglich ist, können wir jedoch – ethisch gesehen – eine sehr hohe Wahrscheinlichkeit von 99 Prozent fordern. Mit anderen Worten: Es sollte sich ein probabilistischer Ansatz durchsetzen.

Dieses Kriterium schließt automatisch Hacker und private Auftragnehmer aus, die nicht einer Staatsgewalt unterstellt sind (z. B. durch Outsourcing), diplomatisch nicht oder kaum anerkannte Staaten wie Puntland und Abchasien, Cyberguerrilleros sowie terroristische Gruppen – es sei denn, sie werden von einem Staatsapparat geschützt bzw. sogar gefördert, der von ihren aggressiven Handlungen Kenntnis hat und nicht eingreift. Hier kommt die Analogie mit der Invasion Afghanistans im November 2001 durch die Vereinigten Staaten und ihren Verbündeten ins Bild: Die Taliban wussten nichts von der Vorbereitung der Anschläge vom 11. September, weigerten sich aber anschließend, Al-Qaida aus Afghanistan zu vertreiben. So kann ein Staat, der sich weigert, gegen aggressive nichtstaatliche Akteure auf seinem Territorium vorzugehen, selbst zum legitimen Ziel einer Cyberverteidigung des angegriffenen Staates werden, weil er eine schwere indirekte Verantwortung trägt (vgl. Tikk 2008, 22).

4.3 Eine gerechte Ursache

Jenseits der Selbstverteidigung gegen einen bewaffneten Angriff (ein ethisches Prinzip, das in Art. 51 der UNO-Charta juristisch verankert ist), die im Falle der Benutzung konventioneller Waffen (d. h. unter Annahme einer Cyberwaffenreaktion, zum Beispiel gegen die Besetzung eines Teils des Staatsgebiets) erst recht gilt, scheinen zwei weitere ethisch akzeptable Szenarien möglich zu sein: eine humanitäre Intervention (die vom Sicherheitsrat der Vereinten Nationen genehmigt werden muss) und ein Präventivschlag im Falle einer ernsten Bedrohung aus dem Ausland, welche das schiere Überleben des Staates gefährden kann. Hier greift die Analogie mit Michael Walzers Konzept der „supreme emergency" für den israelisch-arabischen Krieg, der am 5. Juni 1967 mit einem Präventivschlag begann (vgl. Walzer 1977, Kapitel 16).

4.4 Eine gerechte Absicht

Es muss zugegeben werden, dass dieses Problem aus theoretischer Sicht nicht richtig gelöst werden kann, denn gerade im Cyberspace kann jeder Akteur seine schlechten Absichten leicht verschleiern, gerade auch weil bestimmte Handlungen nicht sofort für jeden sichtbar sind. Deshalb muss auf größtmögliche Transparenz bestanden sowie eine gewisse Zeugenfunktion externen Beobachter (NGO-Watchdogs, neutrale Staaten usw.) eingeführt werden.

4.5 Verhältnismäßigkeit von Schuld und Strafe

Kant wies dieses Kriterium zurück, weil er seine Schrift zu Beginn der Ära des Massenkriegs und der Einführung der allgemeinen Wehrpflicht schrieb. Da Cyberkrieg aber genau das Gegenteil von Massenkrieg ist, werden die Kriterien hier beibehalten. Eigentlich handelt es sich um die Frage nach der Schwelle, ab der eine Cyberverteidigung jenseits des Sperrens von Zugängen (IP, Ports), der Umleitung und Verlangsamung von fremden oder eigenen Datenströmen oder dem einfachen Löschen von Schadsoftware beginnen darf. Offensichtlich reicht eine einfache DDoS-Attacke nicht aus. Es scheint notwendig, dass die Cyberaggression menschliche Opfer verursacht (insbesondere

über das Internet of Things) – zum Beispiel durch nukleare Strahlung oder schädliche Emissionen von Chemieanlagen oder durch schweren Störungen in Krankenhäusern – oder auf lebenswichtige Schlüsselinteressen des Staates abzielt (Strom- und Wasserverteilung, Börsen und Finanzsysteme, konventionelle oder nukleare Verteidigung, Sozialversicherungssysteme, Luftverkehrssysteme usw.). Um eine höhere Präzision zu erreichen – was außerhalb des Rahmens dieses Beitrags liegt – ist es sehr hilfreich, die sogenannte juristische „Schmittsche Analyse" zu verwenden, bei der eine qualitative Eins-zu-Zehn-Skala auf sieben Kriterien angewendet wird (vgl. Schmitt 1999; Michael u. a. 2003, 2; Wingfield/Michael 2004, 11–12).

Der große moralische Vorteil von Cyberwaffen liegt in der Präzision und Staffelung, mit der sich der Gegenangriff auf verschiedenen Ebenen und auf verschiedene Arten ausführen lässt. Da zudem ein reiner Cyberkrieg – ohne Beteiligung anderer Streitkräfte – ab einer bestimmten Aggressionsstufe eher unwahrscheinlich ist, kann der Gegenangriff auch durch die Nutzung des Multiplikatoreneffekts aus einer engen Vernetzung von Cyberarmee und Land-, Luft- und Seestreitkräften erfolgen. Mit anderen Worten, ein allmählicher Aufbau der Kriegsintensität ist durch die schrittweise Einführung des Cyberangriffs mit traditionelleren Mitteln des Krieges durchaus möglich und sogar wahrscheinlich (vgl. Sharma 2010, 63–67).

4.6 Krieg als letztes Mittel

Immanuel Kant hat dieses traditionelle Kriterium des *Ius ad bellum* nicht übernommen, weil er es vermutlich für heuchlerisch hielt. Im Cyberkrieg macht es auch tatsächlich keinen Sinn. Bei einem Cyberangriff bleibt nämlich nicht genügend Zeit für echte diplomatische Verhandlungen in angemessener Form. Das moralische Minimum besteht jedoch darin, dafür zu sorgen, dass die Aggression nicht zufällig erfolgt, zum Beispiel durch die unbeabsichtigte Verbreitung eines Virus, die der Angreifer selbst gar nicht bemerkt. Deshalb sollte es ein moralisches Gebot sein, strenge Kontrollen durchzuführen. Ein erster Schritt in diese Richtung wurde im Jahr 2011 mit der Einrichtung einer Hotline zwischen Washington und Moskau unternommen (wie in Zeiten des Kalten Krieges), um jegliches „Cyber-Missverständnis" auszuschließen.

4.7 Eine angemessene Hoffnung auf Erfolg

Dieses letzte Kriterium wurde ebenfalls von Kant nicht erwähnt, da es eine ausgewiesene Antizipationskapazität erfordert, die meistens nicht gegeben ist. Im Cyberkrieg gibt es für schwache Staaten die starke Versuchung, einen asymmetrischen Krieg gegen die wenigen Cybermächte zu führen – also Schikanen auf niedrigem Niveau. Hier könnte man einen Kompromiss zwischen Kant und den späteren Theoretikern des gerechten Krieges finden: Auch wenn alle anderen sechs Kriterien des *Ius ad bellum* erfüllt sind, erfordert dieses letzte noch den Verzicht auf jegliche Reaktion, wenn ein hohes Risiko des Scheiterns besteht, oder eine noch stärkere Gegenreaktion mit negativen Auswirkungen für die Zivilbevölkerung droht, oder wenn sie zu einer Eskalation mit den überlegenen kinetischen Kräften des Feindes führen kann. Daher ist auch im Cyberspace eine minimale Symmetrie der Kräfte erforderlich. So hat zum Beispiel Vietnam, wenn es von China angegriffen würde, keinerlei Interesse daran, darauf militärisch zu reagieren. Dasselbe gilt vorerst auch für Iran gegen Israel. Es geht um das Vorsorgeprinzip: In diesen Fällen erscheint es moralisch geboten, den Fall eher vor internationale Organisationen wie den UN-Sicherheitsrat zu bringen und/oder um Unterstützung und/oder Schutz durch eine Cybermacht zu bitten.

5 Ius in bello

In der *Metaphysik der Sitten* scheint Immanuel Kant auf Aquinas, d. h. auf die Tage vor Francisco de Vitoria, zurückzugehen, um sein *Ius in bello* zu definieren. Erstens entwickelt er in §57 den thomistischen Begriff der erlaubten und nicht-erlaubten Tricks: Spione, aus dem Hinterhalt agierende Attentäter, Giftmörder, Scharfschützen und Gerüchte werden explizit als illegale Mittel der Kriegsführung eingestuft, weil sie das für die Entwicklung eines zukünftigen (ewigen) Friedens notwendige gegenseitige Vertrauen zerstören. Zweitens gibt es in seinem *Ius in bello* ein (schwaches) Kriterium der Verhältnismäßigkeit, das – wie bei Aquinas – nur besagt, dass Plünderungen verboten sind.

Das Hauptproblem in dieser Parallele zwischen Kant und Aquinas liegt jedoch im „fehlenden" Element des *Ius in bello*: der Diskriminierung zwischen Kombattanten und Nichtkombattanten sowie der damit einhergehenden Möglichkeit von Kollateralschäden. Kant erwähnt dieses

von Vitoria eingeführte Kriterium nicht, was die Annahme untermauert, dass er eine traditionellere Doktrin für richtig hält.

Das Fehlen dieses Kriteriums zeigt uns deutlich, dass Kant in diesem Konzept etwas entdeckt zu glauben hat, das er für unangemessen hält. Der Grund für die Einführung durch Vitoria in seinem *De Indis* lag in der technischen Veränderung, die sich in der Kunst des Krieges im Zeitraum zwischen Aquinas und Vitoria vollzogen hatte: Er verweist auf die massive Einführung der Artillerie auf den Schlachtfeldern Kleinasiens im 14. und 15. Jahrhundert, insbesondere während des Sturzes von Konstantinopel 1453 durch Mehmed II. Diese Technologie fügte den Waffensystemen eine neue Dimension hinzu, da sie die räumliche Entfernung zwischen den verfeindeten Soldaten und eine gewisse Anonymität des individuellen Gegners auf dem Schlachtfeld ermöglicht, und da sie den unvermeidlichen Effekt hat, eine große Anzahl von Nichtkombattanten treffen zu können (vgl. Johnson 1981, 175–176). Daher erschien es Vitoria ethisch notwendig, zwischen Kombattanten und Nichtkombattanten zu unterscheiden, wobei letztere nur unabsichtlich getötet werden dürfen (Kollateralschaden).

In der *Rechtslehre* erwähnt Kant dieses wichtige Kriterium nicht. Eine Hypothese lautet, dass er die Relevanz einer solchen Unterscheidung aufgrund einer Diskontinuität in der Kriegskunst, die er selbst miterlebt hat, nicht erkennt. Tatsächlich war Immanuel Kant ein Zeitgenosse der Einführung des Massenkrieges. Er stellt fest, dass im revolutionären Frankreich sowie in Preußen des späten 18. Jahrhunderts die allgemeine Mobilmachung der Bevölkerung für militärische Zwecke etabliert wurde. (Vgl. Corvisier 1995, 162–163) Der Philosoph aus Königsberg erkennt, dass sich das Wesen der Kriegsführung grundsätzlich geändert hat: Sie umfasst fortan die gesamte Gesellschaftssphäre. Er zieht – so lautet die Hypothese – die wichtige Schlussfolgerung: Warum sollte das Kriterium der Unterscheidung von Kombattanten und Nichtkombattanten des *Ius in bello* beibehalten werden, wenn die gesamte Gesellschaft jetzt auf die eine oder andere Weise an den Kriegsanstrengungen beteiligt ist?

Es scheint, dass sein Schweigen zu diesem seit Vitoria bedeutsamen Kriterium – und damit die Rückkehr zur thomistischen Lehre – so interpretiert werden kann, als wollte Kant die Diskriminierung zwischen Kombattanten und Zivilisten aufheben. Die Massenkriegsführung macht eine solche Differenzierung irrelevant.

Die drei genannten Kriterien werden nun wieder nacheinander analysiert:

5.1 Erlaubte Täuschungen

Die Möglichkeit, den Feind bewusst zu täuschen, wird bereits von Aquinas in seiner *Summa Theologica* erwähnt. Man kann sich zum Beispiel vorstellen, dass ein Staat, um seinen Feind abzuschrecken, ihn in einem Gegenangriff irgendwie glauben macht, dass er weitreichende kybernetische Fähigkeiten besitzt, was aber nicht stimmt. Ein solches Verhalten erscheint moralisch ebenso zulässig wie Cyberpropaganda in Zeiten der Cyberkriegsführung, beispielsweise durch die Umleitung von Webseiten zur Verbreitung falscher Informationen oder gar Cyberspionage. Eigentlich gibt es bei diesem Kriterium nichts Neues zu diskutieren.

5.2 Verhältnismäßigkeit der Mittel

In diesem Zusammenhang ist ein Ansatz auf mehreren Ebenen erforderlich. Es ist wichtig, die Verhältnismäßigkeit zunächst in einer kohärenten Weise zu definieren. Beispielsweise sollte ein über das Internet of Things erfolgter Cyberangriff, der Hunderte von Todesopfern durch Abstürze ziviler Luftfahrtsysteme verursacht, natürlich weniger heftige Reaktionen hervorrufen als mehrere nukleare Explosionen mit erheblichen Strahlungseffekten, welche die Evakuierung eines Teils des Territoriums über viele Jahre erfordern. Das Kriterium ist daher in seiner Struktur fast schon utilitaristisch: Eine genaue Evaluierung der Folgen ist unerlässlich.

5.3 Die Diskriminierung zwischen Soldaten und Zivilisten

Es ist noch schwieriger, diese Unterscheidung im Cyberspace zu betreiben als auf dem konventionellen Schlachtfeld. Glücklicherweise gab uns Vitoria das erwähnte kasuistische Konzept par excellence: den Kollateralschaden, welcher ethisch erlaubt ist, wenn er nicht direkt beabsichtigt ist. Das bedeutet, dass der General, der einen Cyberangriff befiehlt und genau weiß, dass auch die Zivilbevölkerung davon betroffen sein wird, nur dann moralisch „sauber" bleibt, wenn seine Aktion in allererster Linie auf ein militärisches Ziel ausgerichtet ist, wie z. B. feindliche Computerserver oder konventionelle militärische Einrichtungen (z. B. die Kommunikationssysteme zwischen feindlichen Armeeeinheiten).

Das bedeutet, dass nur diskriminierungsfähige (d. h. gegen legitime Ziele gerichtete) Cyberwaffen eingesetzt werden können. Allerdings „sollten Cyberstrategen beachten, dass legitime Ziele auch zivile Objekte umfassen können, die eine duale militärisch-zivile Nutzung besitzen" (Dunlap 2011, 89). Die Ethik des gerechten Krieges erfordert ebenso, dass die zielenden Personen alles Mögliche tun, um sicherzustellen, dass das Ziel tatsächlich ein militärisches ist. In der Praxis scheint das – vorerst – technisch nicht möglich zu sein. Damit ist der oben erwähnte vermeintliche Vorbehalt Kants gegenüber dem Begriff des Kollateralschadens vorerst durchaus akzeptabel.

6 Ius post bellum

Die Ethik des gerechten Krieges braucht nicht zwingend bestimmen, dass ihre Normen durch Rechtsnormen – insbesondere durch die Weiterentwicklung bereits bestehender Bestimmungen des Kriegsrechtes – umgesetzt werden müssen, sofern sie anderweitig korrekt umgesetzt werden können. Daher sind neue rechtliche Vereinbarungen ethisch gesehen nicht zwingend erforderlich. Die umfangreiche juristische Literatur der letzten Jahre hat gezeigt, dass Normen des *Ius ad bellum* und *Ius in bello* auf das Recht des Cyberkonfliktes anwendbar sind, indem rechtliche Analogien aus der UNO-Charta und dem bestehenden Gewohnheitsrecht etabliert werden (vgl. Lin 2012; Jupillat 2015). Vor allem das sogenannte *Tallin Manual* der NATO aus dem Jahre 2013 ist hier wegweisend (vgl. Schmitt u. a. 2013).

Es scheint jedoch notwendig zu sein, die traditionelle Theorie des gerechten Krieges, die sich auf *Ius in bello* und *Ius ad bellum* beschränkt, durch Hinzufügen des kantschen *Ius post bellum* zu erweitern. Hier wird sich zeigen, dass die ethischen Normen des *Ius post bellum* durch einen neuen Völkerrechtsvertrag umgesetzt werden müssen.

Bislang wird das kantsche *Ius post bellum* kaum auf den Cyberkrieg angewendet. Die meisten Autoren, die sich auf die Theorie des gerechten Krieges beziehen, tun dies entweder rechtlich (vgl. Denning 2007; Roscini 2010, Dipert 2010) und/oder ignorieren das kantsche *Ius post bellum* völlig. Die wenigen Autoren, die sich damit beschäftigen (vgl. DiMeglio 2005; Ohrend 2000; Ohrend 2005), verwechseln zwei *Ius ad bellum*-Bestimmungen (das Endziel des Krieges und die Verhältnismäßigkeit von Schuld und Bestrafung), die sie irrtümlicherweise

für *Ius post bellum*-Normen halten. Sie beschäftigen sich ausschließlich mit der Art und Weise, wie der Krieg beendet wird und wie der Übergang vom Krieg zum Frieden organisiert werden soll. Einige schreiben sogar, dass Kant, „obwohl er die Notwendigkeit erkannte, ein *Ius post bellum* zu identifizieren und zu diskutieren, keine Kriterien für diese Kategorie spezifiziert hat" (DiMeglio 2005, 133). Kant ging es nicht um die Beendigung des Krieges oder um den Übergang vom Krieg zum Frieden, außer natürlich in den Bestimmungen des *Ius ad bellum*. Vielmehr ging es ihm beim *Ius post bellum* auf einer deutlich abstrakteren Ebene um die Folgen gewisser Kriegsakte für alle oder die meisten Länder des internationalen Systems seiner Zeit. Wir können hier zwei Kriterien herausfiltern:

Erstens ist Kant sehr besorgt über die „Verletzung [internationaler] öffentlicher Verträge, von welcher man voraussetzen kann, dass sie die Sache aller Völker betrifft, deren Freiheit dadurch bedroht wird" (Kant 1797, §60). Auf den Cyberspace übertragen kann diese Disposition folgendermaßen interpretiert werden: Die „Bombardierung" und Stilllegung aller dreizehn Root-Server, d. h. die Implosion des gesamten World Wide Webs für eine gewisse Zeit, stellt einen Verstoß gegen die Vereinbarung dar, die alle Nationen der Welt mit der Firma ICANN verbindet. Obwohl letztere formell ein privates Unternehmen in Kalifornien ist, besteht ihre Aufgabe darin, den freien Datenverkehr weltweit durch die ständige und zeitnahe Aktualisierung der einzigen globalen Registrierungsstelle für Domainnamen zu gewährleisten. Die Implosion des World Wide Webs, selbst für nur wenige Tage, würde solch gigantische wirtschaftliche und soziale Schäden anrichten, dass es als gerechtfertigt erscheint, dies ethisch in *jedem* anzunehmenden Cyberkriegsfall zu verbieten.

Darüber hinaus liefert Kant uns eine zweite Norm für das *Ius post bellum*: Ein ungerechter Feind ist derjenige, „dessen öffentlich […] geäußerter Wille eine Maxime verrät, nach welcher, wenn sie zur allgemeinen Regel gemacht würde, kein Friedenszustand unter Völkern möglich, sondern der Naturzustand verewigt werden müsste" (Kant 1797, §60). Hier erkennen wir eine Form des kategorischen Imperativs.

Ein solches Zurückwerfen auf den (politischen) Naturzustand scheint in einem einzigen Fall möglich: eine Malware, die in kürzester Zeit und dauerhaft alle oder die meisten Artefakte im Cyberspace zerstört: Computer, Mobiltelefone, Tabletts, Server, Satellitensysteme, GPS, TV, Digitalradio usw. mit unvorstellbaren Folgen für die Weltwirtschaft, die

Beziehungen zwischen den Staaten und den inneren Zusammenhalt der Gesellschaften. Sicherlich wären die Folgen in Malawi oder Kiribati relativ gering, aber die meisten entwickelten Staaten würden Schocks in einem nie dagewesenen Ausmaß erleben, so dass zumindest für eine längere Zeitspanne kein stabiler Frieden möglich wäre und eine Rückkehr zu einer Art Naturzustand unvermeidlich erscheint. Unsere Gesellschaften sind vom Cyberspace viel zu abhängig geworden.

Die beiden kantschen Kriterien des *Ius post bellum* des §60 der *Metaphysik der Sitten* mögen Anlass zur Besorgnis über eine Art virtuelles Armageddon geben, in dem das vorhandene elektromagnetische Spektrum genutzt wird, um viele Teile des Cyberspace als solches und viele Objekte, die mit dem Internet of Things verbunden sind, zu zerstören. Obwohl es sich bei beiden um Artefakte handelt, kann man sie heute als sogenannte Global Commons bezeichnen. Zumindest die entwickelten Staaten und die „emerging countries" der Welt setzen sie ununterbrochen ein. Der Cyberspace und das Internet of Things sind zur Grundlage der globalisierten Welt geworden (vgl. Schreier 2012, 13). In Analogie zur Biosphäre kann man sie als Infosphäre bezeichnen und ihre Zerstörung kann moralisch als das ultimative Übel im Cyberkonflikt betrachtet werden (vgl. Taddeo 2011).

Es ist die gemeinsame Pflicht aller Nationen, den internationalen Akteur zu ächten und ggf. zu bestrafen, der versuchen könnte, den friedlichen Datenfluss im internationalen System zu unterbrechen und die Welt wieder in ein Zeitalter vor der Digitalisierung zurückzuversetzen. Vor allem die anfälligen Industrieländer sollten diesen Schwachpunkt gleichermaßen fürchten. Leider kann nicht völlig ausgeschlossen werden, dass ein „Schurkenstaat" eines Tages einen Angriff auf den gesamten Cyberspace und/oder das Internet of Things startet. Darüber hinaus können transnationale Akteure – wie z. B. dschihadistische Gruppen – ausreichende technische Kompetenz erwerben, um zumindest einen Teil des Internets zu zerstören. Wir wissen nicht, was bereits in zehn Jahren technisch möglich sein wird.

Daher scheint es von großer ethischer Bedeutung zu sein, einen gemeinsamen, universellen (oder fast universellen) Konsens in diesen Fragen zu erreichen. Die UNO sollte verbindliche und sanktionskräftige Rechtsnormen formulieren, die jeden Versuch wirkungsvoll ächten, den Cyberspace und das Internet of Things zu vernichten, wie dies 2015 auch bereits vom UN GGE (United Nations Groups of Governmental Experts on Developments in the Field of Information and Telecommunications in

the Context of International Security) zum Teil bereits vorgeschlagen und von der UNO-Vollversammlung willkommen geheißen wurde. Möglicherweise könnten sie es sogar als Verbrechen gegen die Menschlichkeit bezeichnen, denn es zielt auf eines der Global Commons als solches ab. Ein verbindlicher Völkerechtsvertrag kann ggf. auch gegen den Willen der Vereinigten Staaten von Amerika zustande kommen, die natürlich einer solchen Initiative sehr reserviert gegenüber stehen, weil sie weltweit über die fortschrittlichsten Cyberkriegsfähigkeiten verfügen und jede verbindliche Vereinbarung oder Norm sie wahrscheinlich dazu zwingen würde, „tiefe Einschränkungen bei der Verwendung von Cyberwaffen und -techniken zu akzeptieren" (Gjelten 2010) und somit ihren Vorsprung zum Teil aufgeben müssten.

7 Schlussfolgerungen

Im Vorangehenden wurde versucht, eine von Kant inspirierte Ethik des Cyberkrieges zu skizzieren. Alle Kriterien des gerechten Krieges müssen natürlich deutlich vertieft und weiter ausdifferenziert werden. Es erscheint jedoch angebracht, einen ersten Umriss zu wagen.

Die wichtigsten Schlussfolgerungen lauten: 1. Dem kantschen *Ius post bellum* wurde in Sachen Cyberkrieg bislang bei weitem nicht genügend Aufmerksamkeit geschenkt; 2. Während das kantsche *Ius ad bellum* und *Ius in bello* durch die Annahme und Weiterentwicklung der bestehenden UNO-Charta und des Gewohnheitsrechts umgesetzt werden können (mehrere UN-Resolutionen und das oben genannte *Tallin Manual* deuten bereits in diese Richtung), scheint dies für das *Ius post bellum* nicht möglich zu sein. Hier ist ein völkerrechtlicher Vertrag notwendig, und zwar aus dem einfachen Grund, dass jede andere rechtliche Lösung erst dann zustande kommen kann, wenn es schon zu spät ist. Es ist moralisch notwendig, so bald wie möglich einen universellen Vertrag auf den Weg zu bringen, der jeden Versuch, den Cyberspace und das Internet of Things zu zerstören, ein für alle Mal verbietet.

Literatur

Corvisier, André (1995): La guerre. Essais historiques. Paris: Presses Universitaires de France.

Delibasis, Dimitri (2009): Information Warfare Concept of Operations Within The Individual Self-Defense. In: Karatzogianni, Athina (Hg.): Cyber Conflict and Global Politics. Abingdon: Routledge.

Denning, Dorothy (2007): The Ethics of Cyber Conflict, Draft of March 27. In: Himma, Kenneth E.; Tavani, Herman (Hg): Information and Computer Ethics. Hoboken: Wiley, .pdf of pre-publication version, online unter <*http://hdl.handle.net/10945/37167*>, abgerufen 28. 08. 2018.

DiMeglio, Richard (2005): The Evolution of the Just War Tradition: Defining Jus Post Bellum. In: Military Law Review 186, 116–163.

Dipert, Randall (2010): The Ethics of Cyberwarfare. In: Journal of Military Ethics 9(4), 384–410.

Dunlap, Charles J. (2011): Perspectives for Cyber Strategists on Law for Cyberwar. In: Strategic Studies Quarterly 5, 81–99.

Droege Cordula (2012): Get Off My Cloud: Cyber Warfare, International Humanitarian Law, and the Protection of Civilians. In: International Review of the Red Cross 94 (866), 515–531.

Einzinger, Kurt (2011): Cyber Warfare 2.0 – The Undertow of the Internet. In: Schröfl, Josef; Rajaee, Bahram M.; Muhr, Dieter (Hg.): Hybrid and Cyber War as Consequences of the Asymmetry. Frankfurt: Peter Lang.

Geers, Kenneth (2011): Strategic Cyber Secuity. Tallinn: CCD COE Publications.

Giesen, Klaus-Gerd (1997): Kant et la guerre de masse. In: Union scientifique franco-hellénique (Hg.): Droit et vertu chez Kant. Athens: Société hellénique d'études philosophiques, 331–341.

Giesen, Klaus-Gerd (2013): Towards a Theory of Just Cyberwar. In: Journal of Information Warfare 12 (1), 22–31.

Gjelten, Tom (2010): Shadow Wars: Debating Cyber 'Disarmament'. In: World Affairs 173, 33–42.

Hare, Forrest (2009): Borders in Cyberspace: Can Sovereignty Adapt to the Challenges of Cybersecurity? In: Czossek, C., Geers, K. (Hg.): The Virtual Battlefield: Perspectives on Cyber Warfare. Amsterdam: IOS Press, 88–105.

Johnson, James Turner (1981): Just War and the Restraint of War. A Moral and Historical Inquiry. Princeton: Princeton University Press.

Jupillat, Nicolas (2015): Armed Attacks in Cyberspace: The Unseen Threat to Peace and Security that Redefines the Law of State Responsibility. In: University of Detroit Mercy Law Review 92, 115–130.

Kant, Immanuel (1784): Idee zu einer allgemeinen Geschichte in weltbürgerlicher Absicht, Berlin: Akademie-Ausgabe, online unter <*https://korpora.zim.uni-duisburg-essen.de/kant/verzeichnisse-gesamt.html*>, abgerufen 16. 04. 2018.

Kant, Immanuel (1795): Zum ewigen Frieden, Berlin, Akademie-Ausgabe, online unter <*https://korpora.zim.uni-duisburg-essen.de/kant/verzeichnisse-gesamt.html*>, abgerufen 16. 04. 2018.

Kant, Immanuel (1797): Metaphysik der Sitten, Berlin, Akademie-Ausgabe, online unter <*https://korpora.zim.uni-duisburg-essen.de/kant/verzeichnisse-gesamt.html*>, abgerufen 16. 04. 2018.

Libicki, Martin C. (2009): Cyberdeterrence and Cyberwar. Santa Monica: RAND.

Lin, Herbert (2012): Cyberconflict and International Humanitarian Law. In: International Review of the Red Cross 94 (866), 515–531.

Mele, Stefano (2010): Cyber warfare and its damaging effects on citizens, online unter <*http://www.stefanomele.it/public/documenti/185DOC-937.pdf*>, abgerufen 10. 04. 2018.

Micewski, Edwin R. (2011): Cyber Warfare and Strategic Cultures – Information Technology and the Human Factor, in: Schröfl, Josef; Rajaee, Bahram M.; Muhr, Dieter (Hg.): Hybrid and Cyber War as Consequences of the Asymmetry. Frankfurt: Peter Lang.

Michael, James B; Wingfield, Thomas C.; Wijesekera, Duminda (2003): Measured Responses to Cyber Attacks Using Schmitt Analysis: A Case Study of Attack Scenarios for a Software-Intensive System. In: Proceedings Twenty-seventh Annual International Computer Software and Applications Conference, Dallas, online unter <*http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.111.4082&rep=rep1&type=pdf*>, abgrufen 28. 08. 2018.

Mylrea, Michael (2009): Brazil's Next Battlefield: Cyberspace. In: Foreign Policy Journal, 15, online unter <*www.foreignpolicyjournal.com/2009/11/15/brazils-next-battlefield-cyberspace*>, abgerufen 10. 04. 2018.

Orend, Brian (2000): War and International Justice: A Kantian Perspective. Waterloo: Wilfried Laurier University Press.

Orend, Brian (2005): War Effective Justice. In: Ethics & International Affairs 16 (1), 43–56.

Philipps, Robert (1984): War and Justice. Norman: University of Oklahoma Press.

Roscini, Marco (2010): World Wide Warfare – Jus ad Bellum and the Use of Cyberforce. In: Max Planck Yearbook of United Nations Law 14, 85–130.

Schmitt, Michael (1999): Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework. USAF Academy: Institute of Information Technology.

Schmitt, Michael (2011): Cyber Operations and the Jus ad Bellum Revisited. In: Villanova Law Review 56 (3), 568–605.

Schmitt, Michael u. a. (2013): Tallin Manual on the International Law Applicable to Cyberwar. Cambridge: Cambridge University Press.

Schreier, Fred (2012): On Cyberwarfare, Geneva, DCAF Horizon 2015 Working Paper No. 7.

Schröfl, Josef; Rajaee, Bahram M.; Muhr, Dieter (Hg.) (2011): Hybrid and Cyber War as Consequences of the Asymmetry. Frankfurt: Peter Lang.

Sharma, Amit (2010): Cyber Wars: A Paradigm Shift from Means to Ends. In: Strategic Analysis 34 (1), 63–67.

Stella, Marie (2003): La menace déterritorialisée et désétatisée: le cyberconflit. In: Revue internationale et stratégique 49, 165–171.

Taddeo, Mariarosaria (2011): Information Warfare: A Philosophical Analysis. In: Philosophy and Technology 25 (1), 105–120.

The White House (2009): Remarks By the President. On Securing Our Nation's Cyber Infrastructure, May 29, 2009, online unter <*https://obamawhitehouse.archives.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure*>, abgerufen 16. 04. 2018.

Tikk, Eneken; Kaska, Kadri; Rünnimeri, Kristel u. a. (Hg.) (2008): Cyber Attacks Against Georgia: Legal Lessons Identified. Tallinn: CCDCOE.

Ventre, Daniel (2011): Cyberespace et acteurs du cyberconflit. Paris: Hermes.

Walzer, Michael (1977): Just and Unjust Wars. New York: Basic Books.

Watts, Sean (2012): The Notion of Combatancy in Cyber Warfare. In: Czosseck, Christian; Ottis, Rain; Ziolkowski, Katharina (Hg.): 4th International Conference on Cyber Conflict, online unter <*https://ccdcoe.org/cycon/2012/proceedings/d2r1s10_watts.pdf*>, abgerufen 16. 04. 2018.

Wheeler, David A., Larsen, Gregory N. (2007): Techniques for Cyber Attack Attribution. Alexandria: Institute for Defense Analysis.

Wingfield, Thomas C., Michael, James B. (2004): An Introduction to Legal Aspects of Operations in Cyberspace. Monterey: Naval Postgraduate School.

Über den Autor

Klaus-Gerd Giesen, Prof. Dr., Professor für Politikwissenschaft an der Rechtswissenschaftlichen Fakultät der Université Clermont Auvergne in Clermont-Ferrand/Frankreich. E-Mail: klaus@giesen.fr.