Handelsblatt Konferenz – Cybersecurity 2011 – 13./14. Sept. - Berlin

Vom Cyberwar zum Cyberpeace

Die Diplomatie des Cyber-Friedens: Was soll verhandelt werden, und wo?

Henning Wegener

Der Begriff cyberwar erlebt gegenwärtig einen meteorischen Aufstieg zum Welt-Modewort. Es ist in aller Munde, auch im Munde derjenigen, die mit ihm nur ein dumpfes Gefühl wachsender Bedrohung durch einen unsichtbaren Feind verbinden. Sie wenden den Begriff undifferenziert auf Wikileaks, cybercrime und jede kriminelle und militärische Nutzung von ICTs an. Die Einschätzung der neuen Gefahren reicht von apokalyptischen Prognosen, einer existentiellen Bedrohung von Staat und Gesellschaft, zu bescheideneren Erwartungen von im schlimmsten Fall sektoriellen Schäden und regionalen Ausfällen.

Ich erwähne und quantifiziere die einzelnen Szenarien hier nicht, weise aber darauf hin, dass meine Arbeitsgruppe die Gefahren schon 2001 hoch veranschlagt hat[1]. Und zweifellos

[1] "Toward a Universal Order of Cyberspace: Managing Threats from Cybercrime to Cyberwar," 2001/2003, World Federation of Scientists – Permanent Monitoring

haben wir es mit Gefahren von realer strategischer Bedeutung zu tun, und tritt der cyberspace neben Land, Luft, See und Weltraum als fünftes mögliches Konfliktttheater in einer kriegerischen Auseinandersetzung. Cyber-Angriffe haben ein enormes physisches Schadenspotential, das auch massiv Menschenleben bedrohen und unkontrolliert auf unbeteiligte Länder überborden kann. Cyber-Angriffe im militärischen Zusammenhang gefährden in fast jedem denkbaren Fall die weltweite cyber stability.

Auch wenn es insoweit um die offensive militärische Nutzung von Informationstechnik geht, so gehört zum Komplex cyberwar neben der gezielten Störung und Zerstörung von ITSystemen und Netzen des Gegners, auch die Bereitstellung und Aufrechterhaltung der eigenen Kommunikations- und Kommandostrukturen sowie die Abwehr bzw. Vereitelung gegnerischer Angriffe auf diese, also cyber defense.

In der Diskussion über cyber-Krieg sind heute zwei gegenläufige und zT gegensätzliche Tendenzen zu beobachten, die sich im Spannungsfeld von cyberwar und cyber defense bewegen.

Auf der einen Seite haben – soweit abschätzbar – weit mehr als 100, ja wohl eher 150 Staaten eine nationale cyber-Kapazität

---

aufgebaut, meist im Rahmen personell und finanziell reichlich ausgestatteter nationaler Cyber Commands, die neben Reconnaissance-Missionen und informatischer Steuerung der Waffensysteme in einem ,,network-centric" Militärdispositiv vorwiegend offensive Möglichkeiten haben und mit eindrucksvoller Geschwindigkeit weiter entwickeln. Das ist heute sattsam erörtert worden, und lässt sich auch in der offenen Literatur nachverfolgen[2]. Cyber-Rüstung ist keine Prärogative grosser Mächte. Auch kleinere Staaten können sich den gleichmacherischen, asymmetrischen Effekt der digitalen Technologie zunutze machen und mit begrenzten Mitteln bedeutende offensive Potentiale aufbauen. Dabei fällt auf, dass weit mehr Kreativität und Ressourcen für Angriffstechnik und die Vorbereitung offensiver Aktionen aufgewandt werden – und das in fast unvorstellbaren Grössenordnungen - , als für Kriegsverhütung und Abwehr, und dass Dialogbemühungen gerade für letzteren Aspekt fehlen.

Ich halte dabei zunächst als bedenklich fest:

- Die wachsende Zahl der mit ,,cyber weapons" ausgerüsteten Staaten, Schurkenstaten eingeschlossen, und der sich beschleunigende Rhythmus des Wachstums dieser Rüstungsanstrengungen.

---

[2] ''Cyberspace: assessing the military dimension'', IISS The Military Balance 2011, p.27

- Den Mangel an Untersuchungen über, und Überlegungen zu, den möglichen Kaskadenwirkungen eines auch nur begrenzten cyber-Angriffs auf die intensiv vernetzten Gesellschaften, die angegriffen werden, und auf das internationale Umfeld, mit anderen Worten das Fehlen von Einschätzungen des grundsätzlichen Risikos des Einsatzes von cyber-Waffen.
- Den Ruf nach unbegrenzter Nutzung von cyber-Waffen („exploit potential fully", „maximum effect", „joint firing process", „retaliation", „punishing blow")
- Das Fehlen ausreichender rechtlicher Masstäbe für digitalkriegerische Handlungen und ihre Planung mit offensiver Zielsetzung. Hier ist oft eine Hemmungslosigkeit zu beobachten, die den digitalen Raum offensichtlich als rechtsfrei begreift: hierauf komme ich noch zurück
- Die terminologische Falle: der Militarisierung der Planung entspricht die Militarisierung des operativen cyber-Denkens („war-fighting doctrine"), was zu irreführenden und gefährlichen Analogien führen kann. Schon der Begriff cyberwar ist in dieser Hinsicht zu beanstanden, da er automatisch

militärische Denkschemen stimuliert; man sollte nur von cyber conflict sprechen.

Bei dieser militärischen Einordnung des cyber conflict verweile ich einen Augenblick. Wer auch beim Einsatz digitaler Mittel nur in militärischen Kategorien denkt, hat nicht nur die Begriffe cyber weapon, Abschreckung, „gezielter Gegenschlag", Retaliation, „Rules of Engagement" unzureichend durchdacht und die Spezifität eines cyber-Krieges verkannt, sondern kommt auch bei der analogen Anwendung des Kriegsvölkerrrechts (Verhältnismässigkeit, humanitäre Eingrenzung der Ziele, etc.) in Schwierigkeiten und gerät in die rein militärische Logik einer Eskalation mit kinetischen Waffen. Allzu bereitwillig wird dabei jeder cyber-Angriff als armed attack im Sinne des NATO-Vertrages und der VN-Charter eingeordnet und ungeachtet der Unlösbarkeit des Zurechnungsproblems auf militärische Antworten auch mit kinetischen Waffen gesetzt. Das kann nicht die Lösung sein.

Wir haben aber auch eine zweite, zunehmend stärker ausgeprägte Tendenz: Mit der Einsicht in das grosse Potential und die Zerstörungskraft von cyber-Angriffen und die Bedenklichkeit einer rein militärischen Betrachtung eines cyber-Konflikts rücken die Überlegungen, Cyberkriegsverhütung durch präventive Massnahmen, die Prioritarisierung von cyber defense und bessere

Zusammenarbeit aller stakeholders zu erreichen, in den Vordergrund.

Interessant ist, dass in einigen Ländern beide Tendenzen einigermassen unverbunden nebeneinander stehen. So hören wir bemerkenswert martialische Töne aus dem Kreise hoher amerikanischer militärischer Kommandos, während die Erarbeitung eines primär cyber-kriegsverhindenden, auf präventive Verteidung setzenden Konzepts aus der gleichen Behörde kommt: die Department of Defense Strategy for Operating in Cyberspace von Juli 2011 setzt in Fortführung früherer Überlegungen auf Verteidigung, enge Koordination innerhalb der Regierung und zwischen Regierung und Industrie, und internationale Zusammenarbeit. Die NATO-Gipfelerklärung von Lissabon (20. November 2010) – heute schon vielfach erörtert – unterschlägt nicht die Notwendigkeit der Verteidigung - , setzt den Schwerpunkt jedoch bei zentralem Cyber-Schutz und dem Ausbau kollektiver cyber-Verteidungsmöglichkeiten unter Ausschöpfung allianzinterner und internationaler Zusammenarbeitsmöglichkeiten (§ 40). Ausdrücklich - und wie ich meine richtigerweise - verzichtet die NATO auf eine pauschale Subsumierung von cyber-Angriffen unter den bewaffneten Angriff iS des Art. 5 des Washingtoner Vertrages, und stützt sich eher auf den Konsultations-mechanismus des Art. 4. Die NATO sieht die

Bewältigung von cyber-Angriffen im Rahmen eines neuen Sicherheitsparadigmas, bei dem Prävention und „resilience", also die Stärkung der bedrohten digitalen Infrastrukturen, und ein defensives „network of partnerships" im Vordergrund stehen.

Meine Arbeitsgruppe hat, in der gleichen Denkrichtung, bei der Behandlung von Cyber-Konflikten ihre Arbeit unter die Begriffe cyber stability und cyberpeace gestellt uund versucht, diese beiden Begriffe konzeptuell auszufüllen. Ich verweise hierzu besonders auf die Veröffentlichung „The Quest for Cyber Peace", die wir kürzlich gemeinsam mit dem Generalsekretär der Internationalen Telekommunikationsunion, Hamadoun Touré, herausgebracht haben. Als VN-Publikation ist das Buch in den sechs UNO-Sprachen abrufbar[3].

Cyberpeace soll in der Krieg-Frieden-Antinomie die Perspektive einer digitalen Friedensordnung in den Vordergrund stellen, in der die übergreifenden transnationalen Informationsnetze, die ein gemeinsames öffentliches Gut von hohem Wert darstellen, bewahrt werden und nicht unter militärischem Kalkül aufgeopfert werden. Grundidee ist, cyberwar so weit wie möglich zu delegitimieren, den digitalen Raum von Angriffen freizuhalten und eine

[3] www.itu.int/pub/S-GEN-WFS.01-1-2011. Siehe auch Henning Wegener, "Wer stoppt die Cyber-Krieger? Ein Plädoyer für Friedfertigkeit im digitalen Raum". Cicero, Magazin für politische Kultur, 21.12.2010 (Januar-Ausgabe 2011)

Güterabwägung zu fördern, die Selbstschutz, cyber defense und Zurückhaltung den Vorrang vor Angriff geben. Für die Einzelheiten dieses Friedenskonzepts, zB in der Auswirkung auf die Reaktion auf einen cyber-Angriff oder die Rules of Engagement darf ich auf anderwärts Geschriebenes verweisen[4]

Cyberpeace erfordert internationalen Konsensus über die Rechts- und Verhaltensregeln im digitalen Raum, ein Regelwerk, das auch dem Zeitdruck, der aus der bedrohlichen Lage im digitalen Raum erwächst, gerecht wird,

Die World Federation of Scientists fordert seit 2001 ein ,,Universal Law of Cyberspace" als Produkt einer weltweiten Verhandlung im VN-Rahmen; der Generalsekretär der ITU hat noch kürzlich nach einem ,,Global Cyber Treaty" gerufen, der die militärische Nutzung des digitalen Raums völkerrechtlch begrenzt und sanktioniert[5]. In der Tat ist mindestens für den dringend benötigten Rechtsrahmen im Endeffekt völkerrechtliche Verbindlichkeit erforderlich. Dennoch hat die Idee eines umfassenden Vertrages, so sehr sie ordnungspolitisch die richtige Zielperspektive aufzeigt, ihre Bedenklichkeiten. Für die

---

[4] Henning Wegener, "A Concept of Cyber Peace", in: "The Quest for Cyber Peace"
[5] Siehe auch Ahmad Kamal, "The Law of Cyber-Space. An invitation to the Table of Negotiations, UNITAR, Geneva 2005. Russland hat sich in den Vereinten Nationen über Jahre hinweg für den Abschluss eines Vertrages und das Verbot von Cyber-Waffen eingesetzt.

Anpassung und Neuinterpretation des existierenden Völkerrechts, einschliesslich des Kriegsvölkerrrechts, ist einer pragmatischen Evolution wohl der Vorzug zu geben. Erarbeitung, Akzeptanz und Ratifizierung eines weltweiten Vertragswerks, das die notwendigen Verhaltensregeln für die Staaten und die anderen digitalen stakeholders niederlegt, sind ungemein zeitraubend, in ihrem erfolgreichen Ausgang ungewiss, und vielleicht sogar unrealistisch. Immer mehr wird die Debatte deshalb unter dem Stichwort Verhaltenskodex geführt, was einzelne vertragliche Vereinbarungen nicht ausschliesst und im Übrigen eine dynamischere Problembehandlung erlaubt. Im Übrigen lassen sich nicht-staatliche Akteure, deren Mitirkung und Inpflichtnahme unabdinglich ist, einfacher einbeziehen als bei Vertragsverhandlungen zwischen Staaten. Aus den verschiedenen Diskussionsbeiträgen[6] lässt sich eine plausible Liste der regelungsbedürftigen und für eine Aushandlung des Kodex geeigneten Punkte ableiten.

---

[6] "Time to start talking about arms control on the Internet", The Economist, 1st July 2010, www.economist.com/node/16481504; Daniel Stauffacher et al., Ein internationaler Kodex für Cyber-Konflikte ist überfällig, ICT4Peace Foundation http://ict4peace.org, und NZZ, 11. Juli 2011."The Quest for Cyber Peace, op. cit. Eneken Tikk, Ten Rules for Cyber Security, Survival vol.53 no:3, June-July 2011. Siehe auch Richard A. Clarke (mit Robert K. Knake), Cyber War: the Next Threat to National Security and What to Do About It, New York 2010, dt. World Wide War. Angriff aus dem Internet, Hamburg 2011

Ich will zunächst versuchen, die wesentlichenThemen zu skizzieren. Ich stelle dann die Frage, wo solche Verhandlungen angesiedelt werden können, und wie die Ergebnisse operativ gemacht werden können.

Die prioritäre Aufgabe ist die Präzisierung des Rechtsrahmens. Der digitale Raum ist heute, wenn nicht ein rechtsfreier, dann mindestens ein rechtsarmer Raum. Die Schlüsseldokumente des Völkerrechts greifen nicht in direkter Anwendung, und dies gilt auch für die gewohnheitsrechtlichen Regeln des Allgemeinen Völkerrrechts und des Kriegsvölkerrechts. Unter den vertraglichen Regelungen ist insbesondere an die VN-Charter, den NATO-Vertrag, die Genfer Konventionen von 1949 und die Zusatzprotokolle von 1949 und 1977 hierzu, die Haager Konventionen von 1899 und 1907 und das VN-Waffenübereinkommen von 1980 mit seinen verschiedenen Zusatzprotokollen zu denken[7]. Pläne, Verträge wie die VN-Charter oder den Washingtoner Vertrag neuzuverhandeln oder im formalen Verfahren zu ergänzen, sind unrealistisch. Es muss deshalb darum gehen, diese Instrumente durch evolutive

---

[7] Zu anderen Völkerrechtsdokumenten, aus denen jedenfalls Prinzipien abgeleitet werden können, die Analogien erlauben, siehe Sergei Komov, Sergei Korotkov, Igor Dylewski, "Military aspects of ensuring international information security in the context of elaborating universally acknowledged principles of international law,"DISARMAMENT, April 2007, *ICTs and International Security*, United Nations Institute for Disarmament Research,

Konsensbildung über interpretative Ergänzungen an die Erfordernisse des Cyber-Zeitalters anzupassen und damit zu klären, was in einer digitalen Welt eine Kriegshandlung ist und wie offensive cyber-Handlungen mit dem Völkerrecht gefasst werden können.

Besonders definitionsbedürftig sind die Kernbegriffe bewaffneter Angriff – welche massiven und folgenreichen Einsätze von digitalen Techniken sind darunter einzuordnen, welche Szenarien müssen welche operativen Folgen unter Kapitel VII der VN-Charter auslösen?. Bei dem Begriff „territoriale Integrität" muss interpretativ klargestellt werden, dass kritische Infrastrukturen und ITNetzstrukturen und ihre Funktionsfähigkeit und Vertraulichkeit einbegriffen sind. Bei der Aufbereitung des NATO-Vertrages geht es zusätzlich ua darum, die Koordinaten für das kollektive Allianz-Handeln im Falle von cyber-Angriffen zu bestimmen. Die Genfer Konventionen, die sich natürlich zu Cyber-Angriffen auf kritische Infrastrukturen noch nicht äussern, müssen extensiv in der Weise interpretiert werden, dass bei cyber-Angriffen nicht nur zusätzliche Infrastrukturen, sondern auch essentielle Netzstrukturen, von deren Zerstörung und Ausfall unnötiges menschliches Leiden ausgehen können, in die Schutzvorschriften einbezogen werden. Zahlreiche andere Völkerrechtsinstrumente müssen auf die Analogiefähigkeit ihrer

Prinzipen untersucht werden. Die Kriegshandlungen begrenzenden Grundprinzipien des Kriegsvölkerrechts – ,,militärische" Notwendigkeit, Verhältnismässigkeit, Verbot der indiskriminierenden Angriffe, Unterscheidung zwischen zivilen und militärischen Zielen, Definition des Kombattantenstatus – müssen im Licht der spezifischen neuen Modalitäten überprüft und, vermutlich in einem sehr restriktiven Sinne, neubestimmt werden. Besonders kompliziert sind die Neutralitätsfragen – wie können Staaten unbeteiligt bleiben, wenn ein cyber-Angriff ihre Netze durchläuft, oder dort station-hopping und packet switching praktiziert werden?

Vielerorts – in Regierungen, in der Allianz und in der akademischen Welt – werden diese Probleme bereits intensiv behandelt. Die Arbeiten in der NATO sind in dieser Konferenz bereits ausführlich und überzeugend dargestellt worden. In der US Air Force ist eine Studie angelaufen, die alle defensiven und offensiven cyber capabilities vor ihrer Aufnahme in die Arsenale auf ihre Vereinbarkeit mit internationalem und nationalem Recht überprüft[8]. Wichtig ist jedoch, diese Klärungsbemühungen

[8] "Legal Reviews of Weapons and Cyber Capabilities, Air Force Instruction 51-402, 27. Juli 2011. Der US Congress hat am 18. Juli 2011 ein Hearing zu der Frage einer Definition von "cyber acts of war" abgehalten. Das US Verteidigungsministerium bemüht sich ebenfalls um Klärung, Jane's Defence Review, 27. Juli 2011

jetzt in einem repräsentativen internationalen Rahmen zusammenzuführen, um Konsenspositionen herauszuarbeiten.

Abgesehen von dieser übergeordneten rechtlichen Problemstellung kann man zahlreiche Elemente für einen internationalen Verhaltenskodex des cyberpeace identifizieren. Der Kodex soll Regeln für das Verhalten im digitalen Raum in Friedens- wie in Kriegszeiten beschreiben, und alle stakeholders – also auch die IT-Industrie , Server-Organisationen, internationale Organisationen – einbinden. Da hier das Bezugspaar cyberwar-cyberpeace im Vordergrund steht, konzentriere ich mich auf solche Verhaltenselemente, die in erster Linie die Staaten betreffen. Ich stütze mich bei meiner indikativen Liste vor allem auf die Prinzien für den cyber-Frieden, die die ITU vorgeschlagen hat und Vorschläge, die wir in meiner Arbeitsgruppe in den Vordergrund gestellt haben[9]. Das ergibt das folgende Vorschlagspaket:

Verbindliche Feststellung des Prinzips, dass eine cyber-Attacke gegen einen anderen Staat, direkt oder durch angeworbene Täter begangen, völkerrechtswidrig ist[10].

---

[9] Siehe auch Eneken Tikk, "Ten Rules of Cyber Security",s.o.

[10] Es wäre naheliegend, mit dem Verbot eines offensiven cyber-Krieges auch die Unzulässigkeit offensiver cyber-Strategien und die Forderung nach einem Verbot von cyber-Waffen zu verbinden. Ich sehe jedoch wegen der Schwierigkeit der Definition von cyber-Waffen hier davon ab; auch, wenn speziell entwickelte Angriffs-Software durchaus identifiziert werden kann, setze ich eher auf ihre graduelle "Ächtung", wobei sie nach und nach und zunehmend mit einem

Verpflichtung, keinen Ersteinsatz von cyber-Waffen gegen einen anderen Staat zu üben

Die Staaten verpflichten sich, national und im internationalen Rahmen, zu einer Politik der Prävention von cyber-Konflikten mit Priorität auf cyber-Verteidigung, und werden deshalb gemeinsam mit der Industrie ihre Systeme und Netze durch grösstmögliche Robustheit und Widerstandskraft gegen Angriffe (resilience), eingebaute Redundanzen, Netzsegmentierung, ,,cyber-Hygiene", effizientes Management, etc. sichern

Die Staaten orientieren sich im Falle eines erfolgten cyber-Angriffs oder einer schweren Störung der Netzstrukturen am Ziel einer frühestmöglichen Wiederherstellung intakter Netze und eines friedlichen, stabilen Kommunikationssystems

Erweiterter Schutz für kritische Infrastrukturen und Schutz (Unverletzlichkeit) transnationaler digitaler Netzstrukturen

Verpflichtung für alle Staaten, sich im Interesse eines einheitlichen bzw. harmonisierten internationen Rechtsschutzes mit einer umfassenden , Strafgesetzgebung zur Verfolgung von

---

kollektiven Unwerturteil belegt werden. Zur Definition von cyber-Waffen s. auch Barletta et. al "Cyber Conflict" in "The Quest for Cyber Peace", p. 59ff.

cyber-Delikten auszustatten – sei es durch Beitritt zur Convention on Cybercrime des Europarats, oder durch vergleichbar vollständige Regelungen – und die Rechtsverfolgung und dazu erforderliche internationale Zusammenarbeit effizient zu gestalten

Verpflichtung jeden Staats, seine Bürger im digitalen Raum schützen

Jeder Staat verpflichtet sich, keine cyber-Terroristen oder cyber-Delinquenten ungestraft auf seinem Staatsgebiet zu dulden

Der Einsatz von botnets und anderen irregulären cyber-Kriegern sollte verboten werden.

Die Neutralität ist auch im cyber-Zeitalter zu achten, und cyber-Angriffe dürfen nicht durch die Netze neutraler Staaten hindurch geführt werden

Staaten müssen sich bei der Aufklärung von cyber-Delikten gegenseitige Unterstützung leisten.

Die Staaten beteiligen sich an internationalen Informations- und Frühwarnsystemen (Beitritt zu den Vereinbarungen über 24/7-

Kontaktpunkte, internationale multidisziplinär ausgestattete CERT-Netzwerke)

Staaten werden ermutigt, zusätzlich zu multilateralen Verpflichtungen und Vereinbarungen auch bilaterale Abkommen mit gegenseitigen Nichtangriffsverpflichtungen und zur Verhinderung und gemeinsamen Abwehr von cyber-Angriffen und gegenseitige Unterstützung im Schadensfall abzuschliessen.

Insgesamt sollen die Regeln des Verhaltenskodez mehr Transparenz schaffen und das Vertrauen in die Integrität und Funktionsfähigkeit der Systeme und Netzstrukturen erhöhen, - ein entscheidendes Kriterium der Informationsgesellschaft und ein wichtiges Ingredienz des cyber-Friedens.

Bei der Frage,wo ein multilateraler Verhandlungsprozess angelagert werden kann, stehen mehrere Optionen zur Auswahl. Es könnte an eine selbständige Staatenkonferenz gedacht werden, die anschliessend auch eine Überwachungsstruktur für die Signatarstaaten schafft, um behauptete Verstösse gegen den Kodex zu überprüfen; die Teilnahme wäre freiwillig, neben den Staaten könnten sich auch die anderen Kategorien von stakeholders beteiligen. Frei von den universalen Konsenszwängen oder Abstimmungsregeln der VN könnte eine autonome

Staatenkonferenz ihre eigenen Regeln entwickeln, zB auch beschliessen, dass die teilnehmenden Staaten – am besten in Gruppen ähnlich denkender Teilnehmer - frei sind, Teile des Kodexes bereits frühzeitig für sich verbindlich zu erklären, was zwar zunächst dem Universalitätserfordernis nicht genügt, aber doch eine dynamische Konsensentwicklung auslösen kann. Eine derartige Konferenz könnte sich durchaus auch darauf einigen, statt eines Kodex zwei oder mehr sich ergänzende auszuhandeln, zB um den spezifischen Industrieinteressen und den Erfordernissen der Beziehung Staat-Wirtschaft Rechnung zu tragen.

Natürlich könnte auch das traditionelle Modell einer VN-Konferenz genutzt werden. Solche thematischen VN-Konferenzen mit der Beteiligung der gesamten VN-Mitgliedschaft haben schon in der Vergangenheit statt Verträgen Verhaltenskodices ausgehandelt, zB über Technologietransfer. Der Nachteil dieses Beispiels ist, dass das Verhandlungspaket als ganzes die Zustimmung der gesamten Weltgemeinschaft finden muss, was beim Technologietransfer auch in mehr als zwanzig Jahren nicht gelungen ist.
Eine andere Variante wäre, der ITU als dem Sachwalter der IT und der Informationssicherheit die Ausrichtung der Konferenz anzuvertrauen. Hier fehlt es nicht an der Sachkunde des

Sekretariats; im Übrigen ist die ITIndustrie ein organischer Bestandteil der ITU und kann deshalb problemlos einbezogen werden.

Mir selbst schwebt als Ort des Geschehens die Genfer Abrüstungskonferenz vor. Mit einer leichter handzuhabenden, aber immer noch repräsentativen Mitgliederzahl von 65 Staaten vereint die Conference on Disarmament Verhandlungserfahrung und spezifische Kompetenz für sicherheitspolitische Belange. Das 1979 formulierte Mandat der Konferenz würde, obwohl der Schwerpunkt meist bei der Aushandlung von Verträgen gelegen hat, die Beschäftigung mit einem internationalen Verhaltenskodex erlauben. Die Konferenz hat spefizischen Einblick in die Abrüstungsproblematik und kann deshalb die Spezifität eines cyber-Konflikts besonders gut beurteilen (Ubiquität der zugrundeliegenden dualen Technologie, Schwierigkeit der Definition von cyber-Waffen, Irrelevanz von Entfernung und Zeit, Automatisierung der Angriffe, Asymmetrie von Angreifer und Opfer, Verwobenheit der staatlichen Sicherheitspolitik und des privaten Sektors, Probleme der Zuordnung und der Verifikation, weitgehende Unwirksamkeit von Abschreckung). Die Konferenz ist

zZt übrigens praktisch arbeitslos und könnte ihre Ressourcen für die Problematik cyberwar/cyber peace durchaus einsetzen[11].

13.

September 2011

[11] Ich gehe davon aus, dass dieser Vorschlag auf den Widerspruch von Staaten führen wird, die mehr an Cyber-Rüstung als an Cyber-Frieden interessiert sind, führe das Thema jedoch aufgrund meiner langjährigen Befassung mit, und Kenntnis von, der Abrüstungskonferenz
In die Debatte ein.