Workshop zu „Völkerrecht des Netzes“
Montag, 8. September 2014
14.00 bis 18.00 Uhr

Protokoll:

Programm:

Begrüßung durch Prof. Dr. Dr. h.c. Ingolf Pernice, HIIG, und Prof. h. c. Dr. Norbert Riedel, Auswärtiges Amt

„Völkerrecht des Netzes“ (60 Min)

- Digitale Agenda der Bundesregierung & „Völkerrecht des Netzes“– Impuls von Dr. Norbert Riedel
- „Völkerrecht des Netzes“: Sicht der Praxis – Impuls von Dr. Pascal Hector, Auswärtiges Amt
- Diskussion

Fallbeispiele (je 45 Min)

Moderation: Prof. Dr. Anne Peters LLM (Harvard), Max-Planck-Institut Heidelberg

- Cyber-Sicherheit – Impuls von Prof. Dr. Geiss LLM (NYU), Universität Glasgow mit anschließender Diskussion

  - Pause -
- Menschenrechte – Impuls von Dr. Aust MLE, Humboldt-Universität mit anschließender Diskussion
- Ansätze jenseits des klassischen Völkerrechts – Impuls von Paul Fehlinger, Internet&Jurisdiction Project mit anschließender Diskussion

Zusammenfassung und Ausblick (20 Min)

Teilnehmer:

Aust, MLE	Dr. Helmut	Humboldt Universität	Wissenschaftl. Mitarbeiter
Baums	Ansgar	Hewlett-Packard	Executive Director Corporate Affairs Germany
Bender	Ulrike	Bundesministerium des Innern	Referentin
Berger	Cathleen	Auswärtiges Amt	Referentin
Beste	Ralf	Auswärtiges Amt	Stellv. Leiter des Planungsstabs
Decheva	Dr. Maria	Humboldt-Universität	Büro Prof. Dr. Dr. h.c. Pernice
Diekmann	Gesa	BITKOM	Leiterin Wissenschaftl. Dienst
Drohla	Dr. Jeannine	Bundesministerium der Verteidigung	Referentin
Fehlinger	Paul	Internet & Jurisdiction Project	Manager
Feldmann	Thorsten	JBB Rechtsanwälte	Rechtsanwalt
Fixson	Oliver	Auswärtiges Amt	Referatsleiter
Flockermann, LLM	Julia	Bundesministerium der Justiz und für Verbraucherschutz	Referentin
Fricke	Julian	Auswärtiges Amt	Referent
Geier	Karsten	Auswärtiges Amt	Leiter des Koordinierungsstabs Cyber-Außenpolitik
Geiss, LLM	Prof. Dr. Robin	University of Glasgow - School of Law	Professor of International Law and Security
Haase	Adrian	A.v. Humboldt Institut für Internet und Gesellschaft	Doktorand: Globaler Konstitutionalismus
Haupt	Dirk Roland	Auswärtiges Amt	Referent
Heckel	Dr. Peter	RA-Kanzlei Hengeler Mueller	Rechtsanwalt, Experte für Schiedsgerichtsbarkeit
Hector	Dr. Pascal	Auswärtiges Amt	Beauftragter für Fragen des allgemeinen und besonderen Völkerrechts
Josten	Katrin	Auswärtiges Amt	Referentin
Kottmann	Jan	Google Deutschland	Leiter Medienpolitik / Senior Policy Counsel
Lorentz	Jens	Auswärtiges Amt	Stellv. Leiter des Koordinierungsstabs Cyber-Außenpolitik
Mayer, LLM	Prof. Dr. Franz C.	Universität Bielefeld	Lehrstuhl für Öffentliches Recht, Europarecht, Völkerrecht, Rechtsvergleichung und Rechtspolitik
Metzger, LLM	Prof. Dr. Axel	Universität Hannover	Lehrstuhl für Informationstechnologierecht und Rechtsinformatik
Mielimonka	Matthias	Bundesministerium der Verteidigung	Referent
Moschtaghi	Dr. Ramin	Auswärtiges Amt	Referent
Münther	Jan		Experte für IT-Sicherheit
Niemann	Dr. Ingo	Auswärtiges Amt	Referent
Otto	Philipp	irights.info	

Pernice	Prof. Dr. Dr. h.c. Ingolf	A.v. Humboldt Institut für Internet und Gesellschaft	Direktor: Globaler Konstitutionalismus
Peters, LLM	Prof. Dr. Anne	Max-Planck-Institut für ausländisches öffentliches Recht und Völkerrecht	Direktorin
Peters, LLM	Emma	A.v. Humboldt Institut für Internet und Gesellschaft	Doktorandin: Globaler Konstitutionalismus
Riedel	Dr. Norbert	Auswärtiges Amt	Sonderbeauftragter für Cyber-Außenpolitik
Rotert	Prof. h.c. Michael	ECO Verband der deutschen Internetwirtschaft	Vorstandsvorsitzender
Saldías	Dr. Osvaldo	A.v. Humboldt Institut für Internet und Gesellschaft	Projektleiter: Globaler Konstitutionalismus und das Internet
Schaller	Dr. Christian	Stiftung Wissenschaft und Politik	Stellv. Forschungsgruppenleiter Globale Fragen
Schmitz-Buhl	Lina	Bundesministerium der Verteidigung	Referentin
Schöps	Dr. Thomas	Auswärtiges Amt	Referent
Schwarz	Michael	Humboldt-Universität	Wiss. Mitarbeiter Prof. Ingolf Pernice
Seidenberger	Dr. Ulrich	Auswärtiges Amt	Referatsleiter
Spies	Sylvia	Bundesministerium der Verteidigung	Referatsleiterin
Tomuschat	Prof. Dr. Dr. h.c. Christian	Humboldt Universität	Professor für Öffentliches Recht, Völker- und Europarecht
Uerpmann-Wittzack	Prof. Dr. Robert	Universität Regensburg	Lehrstuhl für Öffentliches Recht und Völkerrecht
	Dr. Lars	Humboldt Universität	Wissenschaftlicher Assistent
Wendel	Dr. Matthias	Humboldt-Universität	Wissenschaftlicher Assistent
Ziolkowski, LLM	Dr. Katharina	Bundesministerium der Verteidigung	Referentin

Ergebnisübersicht als möglicher Forschungsleitfaden:

I. Relevanz eines Völkerrechts des Netzes: Beobachtungen und Fragestellungen

- „There is no cyberspace, every space is cyber" – die Digitalisierung und das Internet umfassen bereits alle Lebensbereiche; die rechtliche Durchdringung kann mit der technischen Entwicklung nicht mithalten, so dass es noch viele Bereiche gibt, die nicht (hinreichend) geregelt sind.
- Ursprünglich war das Internet für die offene und direkte Datenübertragung von A nach B gedacht; mittlerweile hat sich das Internet aber weiterentwickelt, so dass die bei der Datenübertragung wiederum entstehenden Daten relevant geworden sind (Stichwort: Big Data und die Problematik, wie Staaten und Private damit umgehen).
- Das Internet wirft neue Fragen der staatlichen Souveränität auf, auf die Jellineks Souveränitätsbegriff möglicherweise nicht mehr passt.
- Stakeholder konstatieren: Mangelnde Vorhersehbarkeit rechtlicher Sachverhalte ist im Internet ein großes Problem, v. a. die Frage nach dem anwendbaren Recht. Freiheit des Internet geht mit einer Beunruhigung durch diese Freiheit einher: nach welchem Recht können die neuen Fragen angegangen werden?
- Fragmentierung des Rechts: Problematik, wer Regeln setzen kann und wer die Macht hat, diese auch durchzusetzen. Besser passt die Bezeichnung: „Balkanisierung des Internets im juristischen Bereich"
- Es geht nicht nur um klassisches Völkerrecht, sondern auch um Privatrecht, Wirtschaftsrecht, Wettbewerbsrecht – in allen Bereichen gibt es neue Fragen
  Daher wäre aufgrund der Fülle an betroffenen Rechtsgebieten ein besserer Begriff: **Internationales Internetrecht**
- Entwicklung des Völkerrechts des Netzes vollzieht sich nur in kleinen Schritten, obwohl sich das Internet in großen Schritten entwickelt; kann man die bestehenden Rechtsnormen auf das Internet übertragen oder gibt es Bereiche, die neu geregelt werden müssen?

II. Teilaspekte eines Völkerrechts des Netzes

1. Klassisches (Kriegs-)Völkerrecht und das Internet

Welche Elemente und Grundsätze des klassischen Völkerrechts können auf das Internet (modifiziert) übertragen werden?

- Kann man die Grundsätze zu Hoheitsgewalt und ihrer Abgrenzung übertragen – welcher Staat hat Regelungshoheit, wer hat eine Eingriffsberechtigung? Könnte man als substanziellen Anknüpfungspunkt das Territorium heranziehen oder führt dies im Cyber Space zu willkürlichen Ergebnissen?
  Wie sieht es mit dem (umstrittenen) Markt(ort)prinzip, das die EU als Anknüpfungspunkt ansieht, aus?
  Reicht die Abrufbarkeit eines Internetinhalts in einem Land (Stichwort: Leugnung des Holocaust) oder müssen kumulative Gesichtspunkte greifen?
- Kann man eine Parallele zum internationalen Seerecht ziehen und das Internet als *res omnium* ansehen (Gemeinverträglichkeitsprinzip)? Wäre es ungerecht, dass dann

bestimmte Staaten, auf deren Territorium sich terrestrische Stützpunkte des Netzes finden, stärker in Verantwortung genommen würden als andere? Oder entspräche dies nur dem anerkannten Prinzip, dass derjenige, der besondere Einflussmöglichkeiten habe, auch viel Verantwortung übernehmen müsse?
- Abwägung zwischen Hoheitsgewalt und Internetfreiheit angebracht

Internetvölkerrecht muss zwischen *Rechtssetzung* und *Rechtsbindung* unterscheiden.

Welcher Zurechnungsmechanismus ist im Cyber-Kriegsvölkerrecht anzuwenden?
- Alle Cyber-Infrastrukturen sind im Konfliktfall angreifbar.
- Großes Problem in diesem Bereich, Intensitätsschwelle (wann ist eine Attacke ein „bewaffneter Angriff"?) ist geklärt.
- Klassischerweise sollten hochintensive Verletzungen für die Bevölkerung durch das humanitäre Völkerrecht verhindert werden. Kann über diese Analogie hinaus auch die Cyberstruktur insgesamt als Schutzziel begriffen werden?
- Wahres Problem ist aber die Zurechnungsfrage. Besonders problematisch bei der Frage der Zurechnung ist, dass die Herkunft von Attacken technisch verhältnismäßig einfach zu verschleiern ist. Die wahre Herkunft lässt sich hingegen schwer aufdecken. Deshalb wurde diese Frage im „Tallinn Manual on the International Law Applicable to Cyber Warfare" mangels Einigung in der Expertengruppe ausgelassen.
- Zu bedenken: Es wird davon ausgegangen, dass Cyberattacken in Zukunft i. d. R. weniger den eigentlichen Angriff darstellen werden, sondern vielmehr als Verwirrungs-Szenario zur Vorbereitung eines analogen Angriffs dienen sollen.

Kann (und sollte) zwischenstaatliche (Wirtschafts-)Spionage völkerrechtlich geregelt werden?

2. Ansätze jenseits des klassischen Völkerrechts

Welche Rolle können innovative Normsetzungsverfahren einnehmen?
- Multi-Stakeholder-Ansatz
- Soft Law
- Internet Governance
- Deutsch-Brasilianische-Initiative bei den VN
- Globale Unternehmen setzen Standards (an welchen Stellen sollten nichtstaatliche Akteure zur aktiven Mitwirkung aufgefordert oder ihnen sogar bestimmte Regelungsbereiche vorrangig zur Regelung überlassen werden? Könne so zum Beispiel die Einflussnahme autoritärer Staaten zum Schutze der Meinungsfreiheit im Internet verhindert werden?)

Wäre ein Internationaler Gerichtshof für Cyberangelegenheiten mit regionalen Ablegern (vgl. NY-Convention) oder eine internationale Schiedsgerichtsbarkeit ein geeigneter Durchsetzungsmechanismus?
- In der internationalen Schiedsgerichtsbarkeit kennt man das Problem, unterschiedliche Ansätze und Grundvorstellungen aus verschiedenen Rechtskreisen zusammen zu bringen → hybrides Normenwerk als Lösungsansatz
- Verfahrensrecht spielt bei der Implementation eine besonders wichtige Rolle

3. Moderne Internetnutzung, Datenverarbeitung und die Menschenrechte

Verquickung von privater und staatlicher Datensammlung und -verarbeitung

- Recht auf Vergessen als Versuch der Selbstbehauptung des Persönlichkeitsschutzes; damit verbunden ist das Problem der (territorialen) Fragmentierung von Suchergebnissen → Gefahr der Fragmentierung des Internets insgesamt.
- Die Staaten bleiben als Akteure relevant (Beispiel NSA-Affäre): Wer übt Hoheitsgewalt über Daten aus?
- Andererseits scheint der problematische Akteur im Internet nicht nur der Staat zu sein, sondern auch private Unternehmen. Evtl. Ansatzpunkt für dieses Problem: Kartellrecht.

Das bestehende Datenschutzrecht und neue Herausforderungen – Big Data: Handelt es sich bei Big Data um eine per se rechtwidrige Praxis oder ist das geltende Recht überholt und muss für die Frage von Big Data weiterentwickelt werden?

- Kann das bestehende Datenschutzrecht die Fragen und Probleme, die Big Data und dessen Abkehr von der Relevanz der Personenbezogenheit von Daten und von der Kausalität (zugunsten von Korrelationen und Wahrscheinlichkeiten), beantworten bzw. lösen?
  Nach Ansicht vieler Teilnehmer ist davon auszugehen, dass das deutsche Datenschutzrecht keine Antworten auf diese Fragen findet – und auch im Übrigen nicht international skalierbar sei.
- Wer sammelt Daten und wer nutzt die freie Übertragung der Daten? Tun dies auch Kriminelle? Die IS soll angeblich Profile von möglichen Kandidaten für die Anwerbung erstellen. Problem: Dieselbe Datenübertragung kann sich positiv und negativ auf die Gesellschaft auswirken.
- Es ist weiterhin zwischen staatlichen und privaten Datensammlungen zu trennen.
- Nutzer haben Interesse an Internetdienstleistungen – und scheinen dabei auf Datenschutzrecht keinen gesteigerten Wert zu legen.
- Welche Schutzpflicht trifft den Staat hinsichtlich privater Datenverarbeitung, die „nur" aufgrund der Einwilligung von Nutzern zulässig ist, die jedoch regelmäßig gegenüber großen Internetkonzernen in einer wesentlich schwächeren Verhandlungsposition stehen? Zumindest in Deutschland/Europa ist man es gewohnt, die schwächere Partei zu schützen/paternalisieren. Ist dementsprechend ab einem gewissen Punkt nicht mehr von einer die Datenverarbeitung legitimierenden informierten Einwilligung auszugehen?

Wie können neue auf den Schutz der Menschenrechte bezogene Fragen beantwortet werden?

- Änderungen der Menschenrechtspakte → eher nicht erforderlich („same human rights online as offline").
- Internationale Gerichte können durch vorsichtige Rechtsfortbildung zu einem wirksamen Menschenrechtsschutz beitragen (z. B. der EGMR).
- Als Alternative kommt die eher faktische Rechtssetzung ohne Einigung aller/mehrerer Staaten im Rahmen eines Multi-Stakeholder-Ansatz in Betracht. Dieses Vorgehen hat aber auch Defizite wie mangelnde flächendeckende Akzeptanz, regelmäßige Beschränkung auf soft law.

- Dafür wäre die Vernetzung staatlicher und nicht-staatlicher Akteure entscheidend, um einen internationalen Konsens zu erreichen.
  Ein solcher ist im europäischen Raum denkbar, weltweit erscheint eine Konsensfindung hingegen schwierig.

Grundproblematik in der Konstruktion des Internets:
Alle drei Hauptakteure sind unzufrieden: Staaten sind frustriert, dass sie Recht im Internet nicht durchsetzen können. Mangels eindeutiger und geltender Regelungen wissen Unternehmen nicht, wie sie mit (staatlichen und privaten) Anfragen umgehen sollen; sie sind quasi gezwungen, Recht zu sprechen. Nutzer haben Angst um ihre Daten und vor Verletzungen ihrer Grundrechte.

- Wenn Unternehmen durch unterschiedliche nationale Rechtsanforderungen zum Rechtsbruch gezwungen werden (z.B. zu befolgendes staatliches Auskunftsverlangen auf der einen und Herausgabeverbot aus Datenschutzgründen auf der anderen Seite), werden die beteiligten Staaten ihrer Gewährleistungsfunktion zur Rechtsstaatlichkeit nicht gerecht. Sie müssen (u. U. auf klassisch völkerrechtlichem Wege durch internationale Verträge) tätig werden und (gemeinsam) Lösungen für die Problematik finden.
- Das Internet & Jurisdiction Project als Plattform für einen institutionalisierten Multi-Stakeholder-Ansatz:
  - Standardisierung von staatlichen „requests", die bei Unternehmen in einem anderen Land eingehen
  - Entwicklung prozess-orientierter Normen und Kriterien
  - transnationale Handhabung von Auseinandersetzungen zwischen öffentlichen und privaten Akteuren
- Ausarbeitung eines operationellen multi-stakeholder Regimes („policy standard") mit der Einbindung von Schlüsselakteuren, d.h. einer kritischen Masse von Staaten, Internationalen Organisationen, Unternehmen, technischen Betreibern und NGOs.
- Insbesondere soll die Geschwindigkeit der Entwicklung und die Langsamkeit des Rechts durch einen neuen Ansatz in Einklang gebracht werden.
- Der Cyberspace (bestehend aus grenzüberschreitenden Online-Räumen) darf nicht fragmentiert werden.
- Es gibt also kein fehlendes Recht im Internet, sondern ein Problem damit, welches Recht wie anzuwenden ist. Hier setzt der Internet & Jurisdiction Prozess an.

Inwieweit sind die aktuelle Konstruktion des Internets bzw. den Betrieb des Internets steuernden Regeln und Entscheidungsmechanismen dauerhaft festgelegt und welche Möglichkeiten haben Staaten(-gemeinschaften) und das internationale Recht Veränderungen vorzunehmen?

- Die aktuelle Konstruktion bzw. Regelsetzung des Internets kann geändert werden, z. B.:
  - ITU statt ICANN
  - Regionale/Nationale Fragmentierung des Netzes
  - Abschottung ganzer Staaten und Regionen
  - Sperrungen und Löschung von Inhalten
  - Kritische Größe der Relevanz von EU und USA in Regelungsfragen: bei Einigkeit kommt es auf andere Ansätze im internationalen Bereich gar nicht mehr an.

4. Rechtlicher Umgang mit Cyberattacken jenseits des Cyberwars

Muss bei Cyberattacken und Cyber(wirtschafts)spionage das Interventionsverbot cyberspezifisch begriffen werden, indem einerseits das Zwangselement durch ein Manipulationselement (z. B. das Überwinden sehr hoher technischer Sicherheitshürden als „Zwang") und andererseits der Handlungsort durch den Erfolgsort erweitert bzw. ausgetauscht wird?

Was kann von Staaten über das sog. No-Harm-Principle hinaus gefordert werden, damit auch keine indirekten Schädigungen vom Territorium eines Staates ausgehen dürfen, die nicht auf dessen eigenes Verhalten zurückgehen?

- Staaten, die angegriffen worden sind, bei denen die angegriffenen Server stehen bzw. durch deren Leitungen Angriffe verübt wurden, könnten Sorgfaltspflichten (due diligence Pflichten) auferlegt werden.
  Hierbei erscheint es nicht abwegig, die Pflichtendichte an die Einflussmöglichkeiten/Internetkapazitäten von Staaten anzupassen.
- Es erscheint sinnvoll, das materielle Strafrecht zur Abschreckung zu nutzen und dementsprechend anzupassen.
- Technik erneuern
- Codes of Conduct können einen Beginn darstellen.

Wie ist im Cyberbereich mit dem völkerrechtlichen Notstandsbegriff umzugehen?

- Begriff ist in der Staatenverantwortung bisher nicht unstreitig, insb. im Bereich der Rechtfertigung
- Spezielle Argumente werden schnell zu allgemeinen Argumenten, wenn man etwas für das Cyberrecht neu schafft.
  - USA nutzen den Notstandsbegriff extensiv zur Rechtfertigung von weitgehenden Maßnahmen. Gefahr oder Chance?
  - Lücke unterhalb der Schwelle zum Notstand; evtl. sind weniger intensive Maßnahmen bei Nichterreichen der Schwelle zum Notstand wünschenswert und daher völkerrechtlich zu regeln.

III. Ausblick

Der Workshop zum Völkerrecht des Netzes ist von seinen Teilnehmern aus Politik, Wirtschaft, Forschung und Zivilgesellschaft sehr positiv aufgenommen worden. Im Blog des Alexander von Humboldt Instituts für Internet und Gesellschaft haben Emma Peters (Link: HIIG-Blog/Peters) und Dr. Helmut P. Aust (Link: HIIG-Blog/Aust - der Beitrag wurde ebenfalls im Verfassungsblog veröffentlicht Link: Verfassungsblog/Aust) die Ergebnisse des Werkstattgesprächs bzw. den eigenen Beitrag zur Diskussion bereits kurzfristig in die Forschungs-Gemeinschaft hineingetragen. Darüber hinaus ist geplant, im Workshop aufgeworfene Aspekte/Forschungsansätze zu vertiefen - unter anderem sollen sich Workshops zu Einzelfragen des Internationalen Internetrechts stattfinden. Durch diese Konzentration auf spezifische Aspekte eines Völkerrechts des Netzes bzw. eines internationalen Internetrechts soll neben der notwendigen Erfassung des Themas in der Breite auch eine Bearbeitung in der Tiefe gewährleistet werden.

Stand: 13. Oktober 2014