Universidad Internacional Menéndez Pelayo

Sommerkurse 2014

***La Ciberseguridad y la***

***Protección de de la Información***

**Informationssicherheit in der Europäischen Union**

**Botschafter a.D. Henning Wegener**

**World Federation of Scientists**

**Santander**

**8. Juli 2014**

Vor diesem erfahrenen und fachkundigen Publikum bedarf es keiner Darstellung der grossen und wachsenden Gefahren im digitalen Raum. Ebensowenig ist es erforderlich, die Bedeutung einer umfassenden Strategie der Cybersicherheit zu unterstreichen und zu bekräftigen, dass es sich hier um eine der grosser Herausforderungen unserer Zeit handelt: die Meisterung der Gefahren im digitalen Raum - auch der Gefahren durch militärische Nutzung - ist Existenzbedingung für das Funktionieren unserer entwickelten Gesellschaften in einem umfassenden Sinne[[1]](#footnote-1). Und wir alle wissen, dass die Herausforderungen, die eine bis zur Totalität vernetzte, globale Informationsgesellschaft zu bestehen hat, nur durch enge internationale Zusammenarbeit und möglichst universale Normsetzung und Rechtsdurchsetzung zu bewältigen sind.

Globale Cybersicherheitspolitik bedeutet ein Zusammenwirken der Staaten dieser Welt, aber darüber haus auch aller digitalen Akteure. Der Ansatz der Multi-Stakeholder Community ist in aller Munde, aber deshalb, weil er unverzichtbar ist. Traditionelle Souveränitätskonzepte sind im Kampf gegen Cyber-Konflikte unzureichend, kein Staat, keine Staatengruppe, keine internationale Organisation sind eigenständig in der Lage, die erforderliche globale Cybersicherheitspolitik zu prägen

 Und regionale Aktionsfelder sind ebenso wichtig wie einzelstaatlche.

Der Europäischen Union kommt in diesem Zusammenhang eine besondere Bedeutung zu, nicht nur, weil sie 28 hochindustrielle Länder vereint, die in der digitalen Weltwirtschaft eine herausragende Rolle spielen[[2]](#footnote-2) und in denen die digitalen Technologien noch stärker als anderswo zum Paradigma der Wirtschaft und der Gesamtgesellschaft geworden sind. Sie sind auch proportional noch höher gefährdet als andere Länder. In dem Zuge, wie Cyberattacken zunehmend von internationalen Banden geführt werden, die international vernetzt auf höchstem technischen Niveau operieren, wird Cyber-Kriminalität zu einer grimmigen Realität, die hochvernetzte, sehr offene Länder wie die der EU besonders trifft. Deutschland wird einer Untersuchung von McAfee zufolge gemessen am Bruttosozialprodukt noch starker geschädigt als jedes andere Land: der jähriche Schadensumfang liegt bei 1,65% des BIP. Das sind viele Milliarden Euro[[3]](#footnote-3). Dabei erwähne ich nur die aktuell entstandenen und entstehenden wirtschaftlichen Schäden, nicht die darüber hinausgehenden sicherheitspolitisch relevanten Konfliktpotentiale und die Langfristfolgen der Cyberspionage..

Die EU ist gleichzeitig ein Verbund selbständiger Staaten, und eine Organisation mit gemeinsamen Instutitionen und Rechtsetzungsbefugnis[[4]](#footnote-4). Die Mehrzahl der Rechtsakte werden gemeinsam vom Europäischen Rat auf Vorschlag der Kommission und dem Europäischen Parlament in Kraft gesetzt. Verordnungen und Beschlüsse sind in allen ihren Teilen für die Mitgliedstaaten bindend, Richtlinien hinsichtlich des zu erreichenden Ziels. Das ist ein einmaliges Faktum. Die institutionelle Basis der europäischen Rechtsakte verleiht ihnen nicht nur die unmittelbare Rechtskraft nach innen, sondern auch eine starke Aussenwirkung. Europa wirkt beispielgebend, als institutionelles Laboratorium, in dem ausprobiert wird, was morgen auch auf der international Ebene darüber hinaus umgesetzt werden kann. Auf EU-Ebene zeigt sich, was und wie künftig global reguliert werden könnte. EU-Rechtsetzung ist ein Instrument innereuropäischer Koordinierung, aber auch ein Scharnier zur internationalen Regulierung.

Die europäische Cybersicherheitspoltik ist sowohl in internationale als auch innerstaatliche Regelungszusamenhänge eingebunden, sie wird im Kontext einer globalen Mehrebenen- und Multistakeholder-Struktur formuliert und interpretiert. Es liegt dabei in der Logik der europäischen Politik, dass innere und äussere Politik zunehmend verschmelzen, sie lassen sich in der europäischen Sicherheitspolitik kaum noch trennen. Damit verschwimmen auch die Zuständigkeitsbereiche der Innen- und Aussenpoltik. Die komplizierte Instititutionswirklichkeit in den 28-Staaten der Union zwingt zu einer sektorübergreifenden Kooperation und zu einer Vermischung traditioneller Rollen, natürlich auch zu einer Internationalisierung der Innen- und Justizpolitik, - alles wichtige Experimentalfelder mit Beispielwirkung für andere übernationale Regelungsversuche in der Cybersicherheitspolitik[[5]](#footnote-5).

Die Europäische Union hat bei der Förderung der Informationsgesellschaft und in der Cybersicherheitspolitik sehr frühzeitig, und dann kontinuierlich, eine hohe Aktivität entfaltet, geleitet von sehr aktiven und fähigen, besonders mit dieser Aufgabe betrauten Kommissar(inn)en. Seit Jahren figuriert Cybersicherheit weit oben auf der politischen Agenda der EU. Ich setze den eigentlichen Beginn dieser Politik mit der umfassenden Mitteilung der Kommission und des Rats von 2000 (COM(2000)890 final) an. In der Folge werde ich die einzelnen Etappen und Dokumente kurz zusammenfassen - und auch die dabei entstandenen institutionellen Vorkehrungen beschreiben - , um dann bei den beiden bedeutenden jüngsten Dokumenten, der Cybersicherheitsstrategie von 2013 JOIN(2013)1 final) und der im europäischen Gesetzgebungsgang stehenden Richtlinie für Netz- und Informationssicherheit (NIS) etwas ausführlicher zu verweilen.

Im Anschluss an diese kurze Analyse und die daraus gezogenen Schlussfolgerungen möchte ich, im Einklang mit dem Hauptthema dieses Kurses, die europäische Politik des Informations- und Datenschutzes in einer transatlantischen Perspektive, aber auch vor dem Hintergrund der technologischen Entwicklung beim Datenzugang – Big Data und mehr –behandeln, und mit einigen Empfehlungen hierzu enden. Datensicherheit und Datenschutz gehören durchaus zusammen.

Nach der genannten Mitteilung des Rats der EG von 2000 und einigem institutionellem Zögern – die Gemeinschaftskompetenz für den sog. Dritten Pfeiler war damals noch strittig, aber das Europäische Parlament drängte – hat die EU 2002 eine Rahmenrichtlinie zur Bekämpfung von Cyberangriffen und zur Harmonisierung des Strafrechts der Mitgliedstaaten und Zusammenarbeit in der Rechtsverfolgung verabschiedet, (COM(2002)173 endgültig), die im Oktober 2003 verabschiedet wurde. Sie war verbindlich, und musste von den Mitgliedern binnen eines Jahre in nationales Recht umgesetzt werden. Nach der EU-Erweiterung gilt sie auch für die neuen Mitgliedstaaten. Die Rahmenrichtlinie enthält eine Systematisierung von Cyberangriffen und einen Katalog strafrechtlicher Verbotstatbestände, die denen der fast zeitgleich unterzeichneten Budapest Convention on Cybercrime ähnlich sind, an deren Ausarbeitung die meisten EU-Staaten auch aktiv teilgenommen hatten.

Die Budapest Konvention ist weltweit und auch im transatlantischen Umgang mit Cyberstraftaten das zweifellos wichtigste Dokument, der bisher einzige Cyber-Vertrag, der die universale Harmonisierung nationaler strafrechtlicher Bestimmungen und strafrechtlicher Verfolgung für Internet-bezogene Straftaten zum Ziel hat. Nach Auffassung der EU sind Rahmenrichtlinie und Konvention voll vereinbar, und entsprechend haben nach und nach auch 23 der EU-Länder die Konvention ratifiziert. Wegen der identischen Zielsetzung der beiden Instrumente hat die Rahmenrichtlinie zweifellos eine gewisse Retardierung bei der Ratifizierung der Konvention mit sich gebracht, auch wenn EU-Dokumente und Tagungen verschiedentlich, zuletzt in der noch zu analysierenden EU Cybersicherheitsstrategie von 2013, die säumigen EU Mitglieder - es sind fünf, Griechenland, Irland, Luxemburg, Polen und Schweden - zu einer raschen Ratifizierung der Bundapester Konvention aufgefordert haben, um deren weltpolitischen Effekt und Impuls zu stärken.

Im Bestreben, den Schutz gegen Cyberangriffe auszubauen, sind in den nachfolgenden Jahren immer wieder gemeinsame EU-Dokumente verabschiedet worden. Ich nenne COM(2001)209), “Sicherheit der Netze und Informationen. Vorschlag für einen europäischen Politikansatz; im Jahr 2006 COM(2006)251, “Strategie für eine sichere Informationsgesellschaft”; aus 2009 eine Ratsentscheidung 2009/C.321.01 “Einen gemeinsamen europäischen Ansatz zur Netz- und Infomationssicherheit”, aus 2010 COM(2010)245 “Eine digitale Agenda für Europa”. Über mehrere Jahre setzte die EU einen Schwerpunkt beim Schutz kritischer Infrastrukturen und entwickelte ein “Europäisches Programm für den Schutz kritischer Infrastrukturen (EPCIP)” , COM(2006)786, die Richtlinie (2008)114/EG und die Mitteilung und den Aktionsplan COM(2009)149, aus 2011 die Mitteilung “Ergebnisse und nächste Schritte. Der Weg zur globalen Netzssicherheit”, COM(2011)163. Eine EU-Ministerkonferenz zu diesem Thema fand 2009 in Tallinn statt[[6]](#footnote-6). Als aktuelle Regelung mit strengen Auflagen für alle Teilnehmer am digitalen Verkehr ist noch die Verordnung vom Juni 2013 Nr. 611/2013 mit Meldepflichten bei der Verletzung des Schutzes personenbezogener Daten für die öffentich zugänglichen elektronischen Kommunikationsnetze zu erwähnen. An dieser Stelle jedes dieser Dokumente zu analysieren, erscheint nicht sinnvoll, da ihr Inhalt, im Zuge einer graduellen Weiterentwicklung, in die noch zu erwähnenden weiteren Entscheidungen und Dokumente – die Cybersicherheitsstrategie der Europäischen Union und die NIS-Richtline - eingegangen ist.

Von grosser operativer Bedeutung war die Schaffung 2004 der Europäischen Agentur für Netz- und Informationssicherheit (ENISA) unter Verordnung 460/2004, deren Auftrag und Ausstattung 2010 – wirksam 2013 – unter COM(2010)521 erheblich ausgeweitet werden konnte. Der Fächer der Tätigkeiten von ENISA in der Unterstützung und Förderung der EU-Cybersicherheitspolitik, auch im Zusammenspiel mit den Sicherheitsbehörden der Mitgliedsstaaten ist bemerkenswert. Auf der web-Seite von ENISA spiegeln sich diese weitgespannten Aktivitäten. Die EU verfügt mit ENISA über ein auch international anerkanntes Instrument, das allenfalls noch in den USA ein Entsprechung findet.

Anfang 2013 wurde das Europäische Zentrum zur Bekämpfung der Cyberkriminalität (EC3) als Teil des Europäischen Polizeiamts EUROPOL als zentrale Anlaufstelle für die Behandlung von Cyberangriffen eingerichtet, ebenso ein europaweit agierendes CERT, das CERT-EU, das mit den nationalen CERT der Mitgliedstaaten, deren Aufbau die EU in ihrer Digital Agenda befördert hat, zusammenarbeitet.

Kommen wir nun zur “Cybersicherheitsstrategie der Europäischen Union”. Die Verabschiedung eines solchen umfassenden, der Gesamthaftigkeit des Cyberproblems entsprechenden Strategiedokuments ist heute schon fast eine Modeerscheinung. Über die letzten Jahre haben etwa 35 Staaten, darunter auch Mitgliedsländer der EU wie Spanien und Deutschland, sich mit solchen Instrumenten der Analyse und der Koordination ausgestattet.

Das EU-Konzept ist umfassend. Die Strategie soll die Sicherheit von Informationstechnologien sowie die Einhaltung der Grundrechte und –werte der EU gewährleisten. Die Strategie identifiziert in jedem Kapitel Aufgaben für die EU-Organe, ENISA, die Mitgliedsländer, die Industrie.

Fünf strategische Prioritäten werden gesetzt und untersucht:

* Widerstandsfähigkeit gegenüber Cyberangriffen.
* Drastische Eindämmung der Cyberkriminalität
* Entwicklung einer Cyberverteidigungspolitik und von Cyberverteidigungskapazitäten im Zusammenhang mit der Gemeinsamen Sicherheits- und Verteidigungspolitik
* Entwicklung der industriellen und technischen Ressourcen für die Cybersicherheit
* Entwicklung einer einheitlichen Cyberraumstrategie der EU auf internationaler Ebene und Förderung der Grundwerte der EU

Von den fünf Schwerpunkten bezieht sich, deutlich sichtbar, nur einer auf die Probleme militärischer Sicherheit und den Ausbau militärischer und geheimdienstluicher Fähigkeiten, - ungeachtet der besorgniserrgenden und wachsenden Bedrohung durch ein ungebremstes und ungeregeltes Wettrüsten im digitalen Raum und der Proliferation von Cyber Commands und offensivn Cyberstrategien. Die anderen vier Prioritäten liegen in der Linie der EU-Cyberpolitik, aber mit neuen operativen Indices und Aufträgen und einer merkbar stärkeren Einbeziehung des Privatsektors, in dessen Hand ja schliesslich auch die Mehrzahl der kritischen Infrastrukturen liegt.

Um Mitwirkung des Privatsektors geht es auch in dem Richtlinienvorschlag für Netz- und Informationssicherheit (NIS), COM(2013)48 endgültig, den das Europäische Parlament - mit einigen Änderungen gegenüber dem Kommissionsentwurf – im Februar 2014 verabschiedet hat, der aber noch der Zustimmung ds Rats bedarf; es wird mit Abschluss des Verfahrens bis Ende 2014 gerechnet, sicher um den Preis noch weiterer Modifikationen. Vieles in dem Richtlinienvorschlag, auch das Ausmass der vorgesehenen Meldepflicht, ist noch strittig, aber die grundliegende Ausrichtung ist akzeptiert. Die Richtlinie vereinheitlicht zahlreiche Sicherheitspolitiken, zB bezüglich der Rolle der CERTs, nimmt die Betreiber kritischer Infrastrukturen in die Pflicht, zum Schutz der weltweiten digitalen Infrastruktur beizutragen und verpflichtet die Unternehmen, dafür zu sorgen, dass ihre Produkte und Dienstleistungen stets aktuellen Sicherheitsstandards genügen. Vor allem etabliert sie ein Meldesystem für Banken, Energieunternehmen, Internet-Handelsunternehmen, soziale Netzwerke, Unternehmen der Transport-Infrastruktur und andere Branchen, mit der Verpflichtung, signifikante Cyberangriffe bei einer nationalen Aufsichtsstelle zu melden, die mit den entsprechenden Stellen er anderen EU-Länder Informationen austauscht, und ggf. auch die öffentlichkeit oder private Betroffene informiert. Diese Regelung geht weit über das Meldeverfahren nach Verordnung Nr. 611/2013 das Kommunikationsunternehmen betrifft, hinaus und macht zu einer Meldepflicht, was bisher nur freiwllig war. Die Regelung ist auch mit den USA im HInblick auf die amerikanische *Disclosure Guidance* konsultiert worden. Eine Verletzung der Meldepflichten kann erhebiche Sanktionen nach sich ziehen. Die Richtlinie wird zweifellos eine bessere Analyse der kollektiven Gefahrenlagen erlauben und die Unternehmen veranlassen, ihren Cyberschutz und ihren Versicherungsschutz - zu verstärken.

Unter den weiteren aktuellen Massnahmen der EU sind zu nennen das 2013 begonnene, mit 15 Mio Euro ausgestattete PIlotprojekt zur Bekämpfung von botnets und Schadprogrammen, die Fazilität *Connecting Europe* , die die NIS-Kapazitäten der Mitgliedstaaten verknüpft, die European Public-Private Partnership for Resilience (EP3R) und Trust in Digital Life (TDL), und die zahlreichen, zunehmend operativen Aktivitäten, Konferenzen, Analysen, Berichte,Übungen zur Cybersicherheit (und die gemeinsame Planübung EU-USA “Cyber Atlantic 2011”), etc. von ENISA. Erwähnenswert ist auch die Europäische Cloud Computing Strategy (COM(20212) 529 endgültig), die nicht nur die Sicherheit und Vertrauenswürdigkeit europäische Datenzentren regelt, sondern auch – mit werbender Wirkung für europäische Nutzer – die volle Wahrung der europäischen Datenschutzbestimmungen und der entsprechenden Grundrechte in diesen Zentren

sicherstellt.

Zusammenfassend kann gesagt werden, dass die Cybersicherheitspolitik der EU und die getroffenen Massnahmen und Rechtsakte der gesetzten politischen Priorität im Ganzen gerecht werden. Bei der Harmonisierung und Vereinheitlichung der Rechtsnormen, Kompetenzen und administrativen Vorkehrungen, und bei der europaweiten Koordination unter den Regierungen und in der Multistakeholder Community sind grosse Fortschritte erzielt worden. Die unzureichenden internen Strukturen in kleineren Mitgliedstaaten werden zunehmend verbessert und integriert, was wichtig ist, um die Verwundbarkeiten der gesamten Union zu vermindern.

Der Schwerpunkt der EU-Politik liegt beim Aufbau von Widerstands-fähigkeit (resilience) und der Bekämpfung von Cyberkriminalität. Die Stichworte sind *cyber defense*. Schadensverhütung und Schadensminderung durch Zusammenarbeit und wirksames staatliches und privates Handeln.Die Schwerpunkte der “Cybersicherheitsstrategie der EU “ zeigen dies sehr klar. Ein Vergleich mit der US-Politik kann hier im Einzelnen nicht vorgenommen werden, aber es wird auch bei oberflächlicher Betrachtung deutlich, dass das US-Konzept ganz unterschiedlich aussieht. Im Vordergrund stehen dort die digitale Abschreckung und der Aufbau einer offensiven Angriffsfähigkeit, was sich in der technischen Ausstattung des US Cyber Command und dessen finanziellen Mitteln, aber auch in der Vielzahl mit Cyber Operations befasster Behörden niederschlägt. Die Sicherheitsagenda steht im Vordergrund; die Cybersicherheitspolitik der USA ist wesentlich von der Vorstellung geprägt, dass die nationale Sicherheit durch Cyberangriffe bedroht ist und dass dieser Bedrohung mit militärischem Denken und militärischen Mitteln begegnet werden muss. Abschreckung und die Drohung mit massiven Reaktionen sind heute, mindestens in der gängigen Interpretation, Kernelemente der US-Cybersicherheitspolitik[[7]](#footnote-7). Wir werden diese Tendenz zur Überordnung sicherheitspolitischer Gesichtspunkte wiederfinden, wenn wir uns anschliessend mit der Frage des Datenschutzes und den Grenzen des staatlichen Eingriffs in personenbezogene und unternehmens-bezogene Daten befassen. Allerdings sehen wir in der US-Politik auch ein gehöriges Mass an Ambivalenz In ihrer *International Strategy for Cyberspace* von 2011 sprechen sich die USA nachdrücklich für Zusammenarbeit, gerade auch internationale Zusammenarbeit, und friedliche Lösungen aus[[8]](#footnote-8). Dazu passt, dass sich die USA in letzter Zeit auch in den internationalen Gremien (in der VN-Generalversammlung, bei den Diskussionen über Vertrauensbildende Massnahmenm, in der Frage der Internet Governance) sehr regelungsfreudig und konziliant gegeben haben. Auf der anderen Seite wird auch zur Cybersicherheitspolitk der EU mancherorts kritisch angemerkt, sie unterliege einer gewissen “Versicherheitlichung”, d.h. sie werde unter dem Eindruck der neuen Cyber-Bedrohungslagen immer mehr zugunsten sicherheitspolitischer Massnahmen und zulasten von individuellen Freiheitsrechten und rechtsstaatlihchen Erfordernissen interpretiert.

Das Eindringen in digitale Datenträger – Computer, Telefone und andere Geräte – und das Kopieren, die Entnahme oder Veränderung und Weitergabe (der Oberbegriff ist Verarbeiten) von dort gespeicherten Daten ist ein Cyberdelikt. Hier berühren sich Cyberkriminalität und Datenschutz. Wir müssen in unserem Themenzusammenhang deshalb auch die europäische Datenschutzpolitik, soweit sie sich auf digital gespeicherte Daten bezieht, untersuchen, vor allem im Hinblick auf die aktuelle transatlantische Diskussion. Die EU-Datenschutzpolitik schützt personenbezogene Daten, also natürliche Personen. Kommerzielle und Firmendaten fallen zunächst nicht darunter.

Industriespionage, also der Gewinn überwiegend nicht personenbezogener, gewerblicher Daten ist völkerrechtlich nicht sanktioniert, wohl aber nach gemeinem Straf- und Zivilrecht. Strafrechtlich sind in den Mitgliedsländern der EU nach Art. 2 bis 5 der Budapester Konvention und ihrer jeweiligen innerstaatlichen Umsetzung derartige Eindringakte relevant, wobei freilich die Zurechnung eines Spähangriffs – wie immer Im digitalen Raum – schwierig ist. Selbstverständlich greift auch das Zivilrecht mit Schadensersatz-ansprüchen.

Das gilt strafrechtlich auch dann, wenn der Angriff von ausserhalb des nationalen Territoriums, wo der Schaden entsteht, ausgeübt wird. Das steht im Einklang mit dem allgemeinen strafprozessualen Grundsatz, dass Ort der Handlung auch der Ort des Schadenseintritts ist. Das Territorialprinzip, verankert in Art.22 der Konvention von Budapest, ist so zu interpretieren, dass die Schadenswirkung zählt, auch wenn der Verursacher von ausserhalb des Territoriums angreift. Dies wird in der Intepretationsregel Nr, 232 des Erläuternden Berichts zur Konvention eindeutig klargestellt. Da ein Cyberschaden oft nicht grenzgebunden ist, stehen wir hier an der Schwelle zu einem Weltstrafrecht bei digitalen Delikten.

Die Staatsanwaltschaft ist also mindestens in denjenigen Ländern, in denen bei Verdacht einer Straftat *ex officio* verfolgt werden muss, verpflichtet, ein Strafverfahren auch gegen Unbekannt zu eröffnen, wenn der vermutete oder wahrscheinliche Spionage-Angriff aus einem Drittland erfolgt ist, eine Praxis, die leider nur gelegentlich beobachtet wird. Sie ware aber politisch nützlich. Natürlich muss man den Dieb erst fangen, ehe man ihn hängt, aber eine Anklage hätte eine denunziatorische Öffentlichkeitswirkung, die abschreckend wirken kann. In Berlin hat die Staatsanwaltschaft Anklage gegen diejenigen “Unbekannten” erhoben, die – möglicherweis aus dem Inland, und aus nächster Nähe - , über längere Zeit Kanzlerin Merkels Telefon abgehört haben; man kann annehmen, dass es sich bei der Intrusion in die digitalen Geräte von Politikern nicht nur um die Abschöpfung personenbezogener Daten, sondern auch um den Gewinn politischer Fakten und Meinungen, also substantiell um Spionage handelt.

Der Schutz von personenbezogenen Daten und der Privatsphäre von Personen ist erst mit der Entwicklung der digitalen Datenspeicherung wirklich relevant geworden und hat Regelungsbedarf erzeugt. In der EU gilt (noch) die Datenschutzrichtlinie 95/46EG, mit Mindeststandards, die von den Mitgliedstaaten – bei einigen mit Schwierigkeiten – in der Folge umgesetzt wurden[[9]](#footnote-9). Die Richtlinie gilt für natürliche Personen und auch dann, wenn die Verarbeitung der Personendaten von einem nicht in der EU ansässigen Verarbeiter vorgenommen wird (wenn sie dazu dient, dem Betroffen Waren oder Dienstleistungen anzubieten oder die Beobachtung von dessen Verhalten zum Gegenstand hat). Die wichtigste Bedingung für rechtmässige Datenentnahme ist Einwilligung des Betroffenen, aber auch der Schutz von dessen lebenswichtigen Interessen, Vorhandensein einer Vertragsbindung und – in gewissem Rahmen - ein öffentliches Interesse. Die Datenweitergabe an Personen oder Unternehmen in Drittstaaten setzt eine Feststellung der EU-Kommission voraus, dass diese ein “angemessenes Schutzniveau” gewährleisten. Das Vorhandensein eines solchen Standards hat die EU auch bei den USA im Rahmen des Datenschutzabkommens “Safe Harbor”angenommen, das unter dem Abkommen registrierten und zertifizierten amerikanischen Unternehmen, die die Einhaltung einer Liste von Prinzipen gewährleisten, Datenzugang zu gewerbllichen und personen-bezogenen europäischen Daten gewährt. Safe Harbor soll sicherstellen, dass für Unternehmer auf beiden Seiten des Atlantik der gleiche Rechtsstandard gilt. Das Abkommen spiegelt auch die europäische Überzeugung wider, dass in der globalisierten Welt ein hohes Schutzniveau für private Daten, im Sinne von Datensicherheit und Datenschutz, weltweit ein Wettbewerbsvorteil ist.

Das Safe Harbor-Abkommen ist (ebenso wie das parallele SWIFT.Abkommen zu Bankdaten) in Schwierigkeiten. Nach Informationen, dass grosse amerikanische Unternehmen die vereinbarten Verpflichtungen (zB Datenverschlüsselung) nicht einhalten, sodass Geheimdienste Zugang zB zu Bankdaten erhalten, und unter dem Eindruck der Erkenntnisse über die massive Ausspähtätigkeit amerikanische Geheimdienste in Europa hat das Europäische Parlament im März 2014 mit sehr grosser Mehrheit die Aussetzung der Abkommen gefordert.Safe Harbor entspricht den Erfordernissen des EU-Datenschutzes nicht mehr. Kommission und Mitgliedsländer, vor allem die Wirtschaft, fordern Nachbesserungen, noch besser eine Neuverhandlung von Safe Harbor, widrigenfalls das Abkommen in der Tat – mit gravierenden Folgen – ausgesetzt würde. Die amerikanische Seite zeigt sich allerdings widerstrebend.

Die seit dem Erlass der Datenschutzrichtlinie 1995 technisch und politisch veränderte Situation hat die Kommission seit 2010 veranlasst, eine umfassende Neufassung ins Werk zu setzen. Sie hat den Entwurf einer Datenschutz-Grundverordnung, COM(2012)11 endgültig, - wohlgemerkt einer Verordnung mit unmittelbarer Rechtsverbindlichkeit, nicht nur einer Richtlinie -, an Ratsmitglieder und Parlament übersandt Der Entwurf soll den Datenschutzerfordernissen in einer neuen Digitalgesellschaft, die durch neue *social networks*, universale Konnektivitäten und eine immer weitere Durchdringung der Gesamtgesellschaft mit digitalen Datenträgern gekennzeichnet ist, Rechnung tragen und einen auch im Detail einheitlichen europäischen Rechtskorpus erzeugen. Die Gesamtverordnung nimmt die Regeln der früheren Richtlinie auf, präzisiert sie aber und macht sie im Ganzen stringenter. Sie verankert das individuelle Recht auf Datenlöschung (“right to forget”). Die Verfahrensregeln sind detaillierter. Bei Verletzungen des Datenschutzrechts werden jetzt Geldstrafen bis zu Millionenhöhe vorgesehen.Der Entwurf ist eine monumentale Kodifizierung in einem Umfang von nahezu 150 Seiten. Der EU-Ministerrat hat sich bis jetzt noch nicht auf den genauen Inhalt der Reform verständigen können. Die Behandlung im Rat dürfte sich bis Ende 2014 hinziehen.

Die Aktivitäten der amerikanischen Geheimdienste, vornehmlich der NSA, in Europa stellen nach der Richtlinie von 1995, aber mehr noch unter der wohl bald rechtskräftigen Grundsatz-Verordnung eine massive Verletzung von EU-Recht und Recht der Mitgliedsstaaten dar, soweit nicht – im Einzelfall – unter Mitwirkung europäischer Sicherheitsbehörden die verfahrensrechtlichen Voraussetzungen für einen rechtmässigen Datengewinn aus Sicherheitsgründen gegeben sind. Das unterliegt keinem Zweifel. Ebensowenig zweifelhaft ist, dass die amerikanischen Aktivitäten offenbar mit ihrer “Datensammelwut” weit über rationale, sicherheitsfördernde Eingriffe hinausgegangen sind.

Entgegen der Erregung und Empörung, die die Ausspähpraktiken der USA-Dienste und ihr Ausmass in manchen Kreisen in Europa hervorgerufen haben, möchte ich jedoch eine eher undramatische Bewertung der Ereignisse anbieten[[10]](#footnote-10).

Zunächst muss erkannt werden, dass der technologische Fortschritt heute ein Eindringen in digitale Netze und Datenträger und die Sammlung von Daten und ihre Aufarbeitung mit leistungsfähigen Suchmaschinen in einem Masse erlaubt, das noch vor wenigen Jahren völlig unvorstellbar war. Diese technologische Chance für die nationale Sicherheitspolitik des eigenen Landes – hier vor allem der USA - zu nutzen, ist nicht grundsätzlich zu verurteilen. Die neuen Techniken – Stichwort Big Data – werden auch Europa verändern. Neue Techniken werden genutzt, wenn sie nutzbar sind.

Dann ist auch zu sehen, dass nicht nur die USA, sondern auch die Nachrichtendienste der europäischen Staaten, häufig in engem Zusammenwirken, diese Techniken genutzt haben und nutzen und von amerikanischen Erkenntnisen beim Kampf gegen Terorismus, organisiertes Verbrechen, Drogenhandel, Geldwäsche profitieren. Das gilt besonders für Grossbritannien, das nicht nur amerikanische Erkenntnisse und Praktiken aus dem PRISM Programm ohne die üblichen “warrants” und ohne das Erfordernis von Verdachtsmomenten nutzt, sondern in grosser Dimension selbst Daten gewinnt, vor allem durch Datenausspähung in den Sozialen Netzen und in seinem umfassenden TEMPORA-Programm, das alle durch das UK laufenden Glasfaserkabel anzapft. Auch die EU-Kommission ist besorgt, dass Grossbritannien die rechtlichen Voraussetzungen nach EU-Recht, zB ausreichende gerichtlicne Kontrollen, nicht erfüllt. Auch andere Auslands-Intelligencedienste in der EU sind mindestens bei Aufklärungsaktivitäten im Ausland nicht kleinlich.

Unterbewertet wird in der europäischen Diskussion auch die sicherheitspolitische Relevanz der Spähtätigkeit, wobei über die Verhältnismässigkeit zwischen dem Ausmass des Eindringes in die Datennnetze und dem kriminiologischen Ergebnis natürlich diskutiert werden kann. Auf Datengewinn zu verzichten, rät niemand an. Und viele der von den USA ermittelten und auch den europäischen Alliierten mitgeteilten Daten und Erkenntnisse aus dem In- und Ausland übr acute Gefahren waren – und sind - für Europa eindeutig vorteilhaft.

Vorsicht ist auch bei dem Argument am Platze, die Autorisierung und Kontrolle in den USA, einschliesslich durch das nicht-öffentliche FISA-Tribunal sei so kursorisch, dass der Exekutive alles erlaubt sei. Daran ist richtig, dass die USA in den letzten Dekaden eine umfassende militärisch-industrielle Sicherheitsarchitektur aufgebaut haben und die Regierung den Sicherheitsdiensten weitgehend freie Handf gelassen hat. Aber auch wenn die sicherheitspolitischn Prioritäten in den USA wesentlich höher angesetzt werden, als in Europa, und pauschale Genehmigungen leichter zu erlangen sind, und auch wenn die IT-Firmen, Telefondienstleister und andere Unternehmen in den USA viel starker als in Europa denkbar, mit dem Zwang zur Datenüberlassung und -speicherung in Pflicht genommen werden, ist ein durchaus funktionierendes und verantwortungsvolles Kontrolldispositiv vorhanden.

Es gilt auch, dass nicht alle abgeschöpften Daten geoffenbart werden. Nach den NSA-Zahlen 1913 liegt die im Internet pro Tag zirkulierende Datenmenge bei 1.828 Petabyes. Davon kann die NSA nur etwa 1,2% erfassen, und davon auch nur einen Bruchteil zur Kenntnis nehmen. Das wären dann etwa 0,0004% des gesamten Datenverkehrs, bei dem überhaupt erst die Suchfilter der Behörde ansetzen. Wir müssen ein Gefühl für Dimensionen behalten.

Schliesslich ist auch das amerikanische Vorgehen Gegenstand einer heute lautstarken innenpolitischen Kritik. Die USA sind kein monolithischer Block, sondern eine lebendige Demokratie mit eingebauten Lerneffekten. Nicht auszuschliessen, dass wir im Abgleich der amerikanischen und europäischen Vorstellungen zum Datenschutz demnächst eine kongenialere Situation vorfinden. Im Januar 2014 hat der US-Präsident bereits einige schadensmindernde Massnahmen angekündigt (Datensammlung nur noch für ein sicherheitspolitische Zwecke, Telekommunikationsdaten von Amerikanern sollen künftig nur noch die Anbieter speichern, Zugang für NSA nur auf Gerichtsbeschluss, etc.)

Trotz meiner “Redimensionierung” des NSA-Ärgers ist aber festzuhalten:

* Das Verständnis für die Balance von Sicherheit und Freiheit, und für den Datenschutz sind auf beiden Seiten des Atlantik sehr verschieden ausgeprägt. Die USA haben keine vergleichbare Datenschutzgesetzgebung. Ihre Erfahrungen mit dem Terrorismus seit 2001 haben Bewusstsein und Politik starker geprägt. Wertskala und Prioritäten klaffen auseinander. Diese transatlantische Kluft lässt sich nicht grundsätzlich überbrücken, sondern allenfalls mildern. Europa kann aber von seinen hohen Schutzstandards nicht abweichen, sondern muss Respekt für seine Rechtsordnung einfordern.
* Die amerikanischen Praktiken sind unter internationalem (Konvention von Budapest), europäischem und nationalem Recht widerrechtlich und können in den einzelnen betroffenen europäischen Staaten auch strafrechtlich verfolgt werden, da die Wirkung des digitalen Eingriffs ja dort eintritt. Ein solcher Rechtsbehelf steht freilich unter dem Vorbehalt politischer Opportunität und begegnet dem Einwand der Souveränität, wenn eine ausländische Behörde unmittelbar tätig geworden ist (und nicht ein privater IT-Dienstleister), was hier meistens der Fall sein dürfte.
* Die sicherheitspolitischen Rechtfertigungen des amerikanischen Vorgehens sind aus europäischer Sicht rechtlich irrelevant, es müssten in jedem ausgespähten Land die Verfahren für eine sicherheitspolitisch begründete Überwachung eingehalten werden.
* Der Vertrauensverlust im transatlantischen Verhältnis ist ausserordentlich schwerwiegend, wird aber auf amerikanischer Seite offenbar in seinem Ausmass noch nicht ausreichend wahrgenommen. HInzu kommt der Verlust des Vertrauens der Bürger in die Integrität der digitalen Netze und ihrer Fähigkeit, Privatheit zu sichern.

Wenn ich mit einigen Empfehlungen enden soll, will ich sie auf wenige wesentliche beschränken.

In der EU-Cybersicherheitspolitik ist Wesentliches geleistet worden. Für die Fortführung enthält die Cybersicherheitsstrategie von 2013 eine Liste von Vorhaben und Aufträgen, die bald in Angriff genommen werden sollten. Wichtig ist, dass die Richtlinie für Netz- und Informations-sicherheit (NIS) bald endgültig verabschiedet wird.

Im Bereich des Datenschutzes ist ebenfalls erforderlich, dass der europäische Gesetzgeber die Grundsatz-Verordnung zum Datenschutz möglichst bald verabschiedet. Diese gemeinsame Rechtsgrundlage ist auch für die notwendigen weiteren Verhandlungen mit den USA notwendig.

Bei diesen muss es darum gehen, verlorenes Vertrauen wieder aufzubauen, ein möglichst hohes Einverständnis über ein tragbares Gleichgewicht zwischen Freiheit und Sicherheit zu finden, mehr Transparenz bezüglich der Aufklärung spolitik der atlantischen Partner und der in Anspruch genommen rechtlichen Basis dafür zu schaffen, und die Tätigkeit der ausländischen Dienste mit den europäischen Verfahren über erforderliche Überwachungsmassnahmen kompatibel zu machen. Eine Neuverhandlung des Safe Harbor-Abkommens müsste bald eingeleitet werden. Einige unerfreuliche Praktiken wie die illegale Ausspähung der Politiker befreundeter Staaten untereinander müssten einvernehmlich ausgesetzt werden; eine mündlich Zusicherung, in Zukunft Staats- und Regierungschefs von der Überwachung ihrer Kommunikation auszunehmen, reicht nicht. Es bedarf eines “no-spy”-Abkommens EU-USA, eines Spionageverzichts, oder mindestens eines Memorandum of Understanding in diesem Sinne, das mit einer noch engeren Zusammenarbeit der Geheimdienste beider Seiten verbunden werden kann.

Mittelfristig muss es Europa darum gehen, für ein internationales Rahmenwerk zu arbeiten, das die Balance zwischen legitimen Sicherheitsinteressen der Beteiligten und der Wahrung von Freiheitsrechten und Datenschutz einverständlich und verbindlich sicherstellt.

Viele Arbeiten müssen die EU-Staaten aber auch im eigenen Haus verrichten. Dazu gehört ein weiterer Ausbau der technischen Resilienz der Systeme und Netze, ein verbesserter Selbstschutz der Stakeholder Community, und ein stärkeres Sicherheitsbewusstsein (*awareness)*  aller Beteiligten, das auch zu höherer Datensparsamkeit, besseren back-up Praktiken, etc. führen kann.

Die EU-Staaten müssten auch sicherstellen, dass ihre eigenen Nachrichtendienste sich streng an die europäischen und nationalen Rechtsregeln halten und ihr Verhalten insoweit transparent machen, damit nicht von den Amerikanern mehr verlangt wird, als die Europäer selbst praktizieren. Dazu müsste auch ein internes EU-weites gegenseitiges Spionageverbot gehören

1. In der Liste der grössten Bedrohungen der Welt des Berichts Global Risk 2014 des World Economic Forum erscheinen die Cyberattacken als Weltrisiko an fünfter Stelle [↑](#footnote-ref-1)
2. Die EU ist nach wie vor die grösste Volkswirtschaft der Welt [↑](#footnote-ref-2)
3. Die durchschnittlichen Kosten eines Angriffs sind pro betroffenen Unternehmens kürzlich mit ca. 5 Mio € berechnet worden [↑](#footnote-ref-3)
4. Die materielle Zuständigkeit der EU-Organe für Cybersicherheit und die Informationsgesellschaft ergibt sich aus der Zuständigkeit fur Schaffung und Funktionieren des europäischen Binnenmarkts. Nach Art. 16 des Vertrages über die Arbeitsweise der Europäischen Union hat die EU auch die Kompetenz für den Erlass von Datenschutzvorschriften, zur Sicherung des Grundrechts auf den Schutz personenbezogenerer Daten, Art. 8 der Charta der Grundrechte der Europäischen Union [↑](#footnote-ref-4)
5. Auf internationaler Ebene ist die EU im Bereich der Cybersicherheit sowohl auf bilateraler als auch multilateraler Ebene enorm tätig, zB mittels der Arbeitsgruppe EU-USA zur Cybersicherheit und Cyberkriminalität und mit Beiträge in allen einschlägigen internationalen Organisiationen [↑](#footnote-ref-5)
6. www.tallinnciipeu.eu/?id=conference [↑](#footnote-ref-6)
7. Bei der Interpretation der zugänglichen Doktrin-Dokumente ist allerdings Vorsicht geboten. Sie sind umsichtig formuliert, und betonen, dass jede Cyber-Operation im Einklang mit dem Kriegsvölkerrrecht in seiner modernen Ausprägung stehen muss. [↑](#footnote-ref-7)
8. In der Strategie heisst es: “It is a call to the private sector, civil society, and end-users to reinforce (these) efforts through partnership, awareness, and action. Most importantly, it is an invitation to other states and peoples to join us in realizing this vision of prosperity, security, and openness in our networked world. These ideals are central to preserving the cyberspace we know, and to creating, together, the future we seek” [↑](#footnote-ref-8)
9. Sie wurde 2002 ergänzt durch die Datenschutzrichtlinie für elektronische Kommunikation, 2002/58/EG.Im weiteren internationalen Bereich gelten die OECD Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data, die eine weltweite Hamonisierung der wichtigsten Grundsätze zum Ziel hat, und die Europäische Datenschutzkonvention des Europarats, die für 46 Staaten völkerrechtlich verbindlich ist. In den Mitgliedstaaten der EU gelten nationale Gestze, so in Deutschland das Bundesdatenschutzgesetz von 1997, in das die Richtlinie 95/46EG eingearbeitet wurde. [↑](#footnote-ref-9)
10. Vgl.hierzu Nigel Inkster *The Snowden Revelations: Myths and Misapprehensions* SURVIVAL, February.March 2014, S. 51; Joachim Krause *Diskutieren statt moralisieren,* Internationale Politik, Januar-Februar 2014, S. 108 [↑](#footnote-ref-10)