Zu den neuen Gefahrenlagen im digitalen Raum

Henning Wegener

Die digitalen Techniken setzen neue Paradigmen für Struktur und Betrieb unserer Gesellschaft. Sie haben schon jetzt einen sozialen Wandel ausgelöst, dessen Ergebnis weltweit als geschichtliche Zäsur wahrgenommen wird. Immer weitere Lebensbereiche werden mittels Einsatz digitaler Techniken gesteuert, vernetzt und von ihnen abhängig. Je mehr diese Abhängigkeit wächst, desto mehr werden Stabilität, Sicherheit und Verlässlichkeit der Systeme, Vertrauen in ihre Funktionsfähigkeit und den Schutz der Privatsphäre auch zur Funktionsvoraussetzung unserer Gesellschaft.

Informationssicherheit wird damit zu einer Schlüsselaufgabe politischen Handelns, einer Herausforderung, die allerdings noch der universellen Analyse und strategischen Antwort harrt. Die Verwundbarkeit der digitalen Endgeräte und der sie verbindenden Netze und ihres Betriebs wird unterschätzt, während die Gefahren und Schäden mit zunehmender Beschleunigung, und jeweils höherer technischer Sophistikation und Komplexität alarmierend und exponentiell wachsen.
Die Dynamik dieses Wachstums, das krebsartige Wuchern der Angriffe im *cyberspace* und die enorme Potenzierung der

Gefahren – und damit die Dringlichkeit des Handelns – sind das Thema dieses Artikels. Ihm liegt die Überzeugung zugrunde, dass wir in der Phase eines Quantensprungs der digitalen Bedrohungen stehen, die auch eine neue Dimension der Bewusstseinsnahme erheischt.

***

Die Segnungen, die die neuen Informations- und Kommunikationstechniken (ICT) einbringen, sind evident. Sie bringen beispiellose Chancen für Wachstum und Wohlstand, rentablere Produktion und Distribution, administrative Effizienz, den optimierten Betrieb der wesentlichen öffentlichen Infrastrukturen, menschliche Entwicklung und Bereicherung und die Heraufkunft der vielbeschworenen Informationsgesellschaft. Information und Kommunikation werden immer mehr zum entscheidenden Rohmaterial menschlicher Aktivität. ICT negieren die Relevanz von Raum und Grenzen, ja, auch der Zeit und bis zu hohem Grade der Kosten, und erlauben damit die Vision einer globalen Gesellschaft mit neuen Arbeitsteilungen und universalem Fortschritt, auch im Sinne individueller Chancen und höherer gesellschaflicher Integration.

Aber auch der digitale Planet hat seine dunkle, ja sinistre Rückseite. Wie alle modernen Techniken – die nukleare als Beispiel – ist die digitale mit Ambivalenzen besetzt. Den Chancen entsprechen die Verwundbarkeiten und systemischen Fragilitäten. Die digitalen Technologien vergrössern die Amplituden von Trends. Die Ausschläge werden grösser, die Proportionen verändern sich. Mehr Chancen und Gewinne, aber die begleitenden Risiken und Schäden wachsen mit, meist überproportional. *More good comes with more bad.* Wir leben in einer Weltrisikogesellschaft. Der digitale Raum ist ein zunehmend gefährliches Ambiente.

Die Missbrauchsmöglichkeit digitaler Techniken, die Möglichkeit der Angriffe auf die moderne Kommunikation und Informatik, liegt in diesen selbst. Dabei geht es nicht nur um das Internet, sondern um alle digitalen Datenträgerdispositive und die sie verbindenden Netze, – dazu später mehr. Sie sind leicht – und von überall – zugänglich, und damit auch überall angreifbar. Das Manipulieren von Daten und Systemen ist Individuen ebenso wie Gruppen mit krimineller Absicht und Staaten möglich; es geht um die gleichen Techniken und sie sind in allen Lebensbereichen gleichermassen anwendbar. Angriffe sind grundsätzlich anonym oder anonymisierbar. Sie können von jedem Punkt der Welt aus auf jedes vernetzte System

erfolgen: Informationssicherheit ist eine Herausforderung universaler Dimension. Angriffe wirken in Bruchteilen von Sekunden. Sie sind unsichtbar, ,,virtuell" und unmittelbar, aber ihre Folgen können oft auch lange unerkennbar bleiben. Zuordnung und Verfolgung, *tracing and tracking*, der Verursacher, sind ein Problem, das sich anderswo so nicht stellt. Angriffe im Internet und auf andere Netzwerke sind gratis oder jedenfalls extrem kosteneffizient, d.h. es gibt praktisch keine ökonomische Relation zwischen Cyber-Angriff und angerichtetem Schaden.

Selbstverständlch reagieren Regierungen und Gesellschaft auf diese Herausforderung. Die Regierungen nicht nur der entwickelten Länder schaffen Organe und gesetzliche Grundlagen, um den Kampf aufzunehmen. Je höher die digitale nationale Infrastruktur, umso höher die Gefährdung und der Bedarf an Gegenmassnahmen. Die USA investieren seit Jahren hunderte Millionen Dollars in den Schutz ihrer nationalen Infrastrukturen. Beispielhaft für das gestiegene Bewusstsein und eine entschlossene nationale Sicherheitspolitik ist die Erklärung Präsident Obamas vom 29. Mai 2009[1], in der er zu mehr Sicherheitsinvestition und nationaler Koordination aufruft und einen Chefkoordinator im Weissen Haus bestellt. In anderen

[1] The White House, Office of the Press Secretary

Staaten bleiben die Vorkehrungen lückenhaft und es fehlt an ausreichender Reaktionsfähigkeit und Koordination. Im privaten Bereich ist eine internationale Sicherheitsindustrie hohen technischen Niveaus mit zweistelligen jährlichen Wachstumsraten entstanden. Die Wirtschaft schützt sich, mit hohen Investitionen, auf Unternehmensebene und kollektiv. Durch teils öffentliche, teils private Initiative ist ein Netz von technischen Eingriffskommandos (CERT – Computer Emergency Response Teams) eingerichtet worden, das heute bereits in den meisten Ländern tätig ist und sich koordiniert. Die übernationalen und internationalen Organiationen, eingedenk der universalen Aufgabenstellung, reagieren. Die EU-Kommission hat, wie in der ganzen Digitaltechnik, umfassende regulatorische Intiativen ergriffen und eine eigene Netzsicherheitsagentur (ENISA) eingerichtet. Die NATO hat ein Schwerpunktprogramm *Cyber Defence*.[2] Der Europarat hat mit der Aushandlung der Convention on Cybercrime rechtliche Basisarbeit geleistet. In den VN-Gipfeln zur Informationsgesellschaft 2003/2005 ist das Thema Vertrauen und Sicherheit in den ICT gross geschrieben worden; die Internationale Fernmeldeunion (ITU) wurde zum Koordinator dieses Themas bestellt und hat seither hervorragende Arbeit

[2] NATO Erklärung von Bukarest, 4. April 2008, para. 47

geleistet, die ihr eine internationale Führungsrolle sichert[3]. Die VN Generalversammlung hat seit den 90er Jahren die Auswirkungen von Cyber-Angriffen auf die internationale Sicherheit problematisiert. Immer wieder haben die VN die Schafffung einer*Global culture of cybersecurity* gefordert. Nichts zu wünschen übrig lässt die wissenschaftliche Befassung mit den Cybergefahren. Die Literatur ist fast unüberschaubar und wächst, wie jede Internetsuche unter einschlägigen Stichworten zB bei Google zeigt.

Hier ist also bereits Bemerkenswertes geleistet worden, obwohl die Verteidungs- und Vorsorgemassnahmen immer wieder hinter den wachsenden Gefahren zurückbleiben. Die Cyber-Verteidigung hält mit den frenetischen Veränderungen im digitalen Raum und den neuen Gefährdungen einfach nicht Schritt. Oft wird deshalb international die Frage gestellt, ob der Kampf gegen die Cyber-Kriminalität angesichts der Allgegenwart digitaler Systeme überhaupt noch zu gewinnen ist. In dem zeitlosen Dilemma zwischen Angriff und Verteidigung scheint auch hier der Angriff in der Vorhand, zumal im digitalen Kampf der Angreifer den Angriffspunkt mit fast unbegrenzter technischer Freiheit wählen kann, während die Verteidigung reagieren, und Schwachstellen abdichten muss.

---

[3] vgl. *Henning Wegener, Harnessing the perils in cyberspace: who is in charge? DISARMAMENT FORUM, UNIDIR, 2007 n° 3*

Deutliche Fehlbestände gibt es noch im allgemeinen öffentlichen Bewusstsein. Hier werden das Ausmass der Bedrohung, die Dringlichkeit von wirksamen Gegenstrategien und die Abwehr- und Beteiligungsmöglichkeit der einzelnen noch nicht ausreichend wahrgenommen, es fehlen auch Beurteilungsmasstäbe; die öffentlichen Ängste machen sich lieber an meist irrational überhöhten Gefahren im Bereich des Nuklaren, des Klimas, der Umweltverschmutzung, an eventuellen Pandemien oder an der Wirtschaftskrise fest. Dieser relativen Trivialisierung der Bedrohungen im digitalen Raum ist entgegenzuwirken, und diesem Ziel sollen auch die nachstehenden Ausführungen dienen.

Dabei sollen zunächst einige technische Entwicklungen der letzten Jahre mit ihrem Wachstumspotential skizziert werden; es folgen Angaben zu Bedeutung und Ausmass der resultierenden Bedrohungen mit dem Schwerpunkt auf der sicherheitspolitischen Problematik von *cyber conflict – cyber terrorism* und *cyber war*. Im weiteren sollen in aller gebotenen Kürze und Vereinfachung Strategien zur Eindämmung und Bekämpfung der Bedrohungen erörtert werden, und schliesslich das dazu erforderliche rechtliche Instrumentarium.

***

Vorab eine definitorische Klärung. Der Kern der Computerdelikte, der cybercrimes, ist der direkte Zugriff auf Datenverarbeitungs-, und –speicherapparate, durch Verschaffung illegalen Zugangs, illegalen Datenraubs oder Datenmanipulation, oder Störung bzw. Zerstörung oder Missbrauch der Datenträgersysteme, - es handelt sich also um Delikte gegen die Integrität, Authentizität, Verfügbarkeit oder Vertraulichkeit von digitalen Systemen und ihren Daten; in diesem Sinne definiert auch die wegweisende Convention on Cybercrime des Europarats[4] die Delikte. Davon zu unterscheiden, wenn auch nicht weniger bedeutend, ist die Nutzung der enormen Kommunikations- und Multiplikatorfähigkeiten des Internets (und anderer digitaler Mittel) für illegale Inhalte (Pornographie mit Minderjährigen, Verletzung von copyright, Propagierung von Rassenhass, Anstiftung zu Krieg und Verbrechen, Werbung für Terrorismus, betrügerische Offerten aller Art, Anleitung zur rechtswidrigen Fertigung von Atombomben, Rezepte für Cyber-Kriminalität, etc.); die Konvention des Europarats pönalisiert davon die Kinderpornographie und die Copyrightsverletzungen, und in einem Zusatzprotokoll auch Xenonophie und Rassismus. Da für

[4] http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm

die grosse Zahl der sonstigen inhaltsbezogenen Internetdelikte „normale" nationale und internationale Sanktionen greifen, beziehen sich die nachstehenden Ausführungen vornehmlich auf den Kernbereich der Cyber-Delikte: die technische Manipulation von digitalen Systeme und den in ihnen gehandhabten Daten.

Die neue Dimension der Bedrohung ist zunächst quantitativ indiziert. ZZt. dürfte es weltweit mehr als 1,5 Mia. konventionelle internetfähige Computer geben, mit einem wachsenden Prozentsatz (in einigen Ländern nahe 100) von Breitbandzugang; Breitbandkapazität ist für alle grossen digitalen Steuerungsaufgaben und für Datentransport unabdinglich. Computer sind ein wichtiger Teil der Bedrohungslandschaft, aber potentielle Opfer von cybercrimes sind auch alle anderen Gerätschaften, in denen Mikroprozessoren digitale Daten handhaben. Dazu gehören insbesondere die Mikroprozessoren in eingebetteten Systemen (embedded devices), mobile Systeme von Mobiltelefonen zu Taschencomputern (hand-held devices) , die schon heute omnipräsenten Sensoren, zB RFIDs (Radio Frequency Identification). Hier sind wir bereits im zweistelligen Milliardenbereich. Die folgenden, als „next generation" etikettierten, aber schon sehr kurzfristig wirksam werdenden

technologischen Entwicklungen zeigen, wohin diese quantative Reise geht: Ultra-Miniaturisierung von digitalen Schaltkreisen, massiver Einsatz von Prozessoren mit Mehrfachkernen, vermehrter Einsatz von Glasfaser, rapide Zunahme des mobilen Datentransports, Entwicklung neuer potenter „smarter" Geräte, Reifwerden des Quantencomputing, Ubiquität von neuen miniaturisierten computing-Elementen, die auch zu ganz neuen, andersartigen Strukturen und Verarbeitungsmechanismen digitaler Netze (u.a. „artificial neural nets") konfiguriert werden und eingebetteten Systemen, Biometrie, die Entwicklung zum „Internet of Things" mit in Kleidung eingenähten oder in Brillengestellen untergebrachen Miniaturcomputern, die Konstruktion von autonom operierenden und sich selbst organisierenden Zwergcomputern, die automatisch mit anderen digitalen Geräten kommunizieren . . . alle diese Entwicklungen tragen zum explosiven Wachstum der digitalen Akteure und zu der Exponentialkurve der Konnektivitäten und damit zu einer neuen Grössenordnung der Verwundbarkeiten bei.

Zu diesen quantitativen Fakten treten die Phänomene von Migration und Konvergenz. Die Scheidung zwischen verschiedenen digitalen Handlungsebenen wird zunehmend aufgehoben. Die Festnetztelefonie wandert immer mehr in den

Bereich drathloser Kommunikation und ins Internet (Voice over IP), und die Computing-Vorgänge und die Speicherung grosser Datenmengen wandern aus den individuellen und Geschäftscomputer-Systemen in riesige externe Daten-Zentren (Server-Farmen oder auch ,,grid computing") mit tausenden von Servern und Speicherkapazität im Petabyte-Bereich ab, wobei die Rechen- und Speichervorgänge für den einzelnen Nutzer völlig intransparent sind und im Übrigen auch die traditionellen Zugangsschleusen (firewalls) funktionslos machen. Festnetze und drahtlose Netze konvergieren bis zur Ununterscheidbarkeit, zumal sich zunehmend ad-hoc-Netze für bestimmte Anwendungen und auf Zeit bilden lassen. So entsteht eine riesige integrierte Netzwerkstruktur mit einem zahlenmässig kaum noch fassbaren Universum von Konnektivitäten – und Verwundbarkeiten - , in dem wichtige Komponenten (viele mobile Systeme, RFIDs, eingebettete Mikroprozessoren mit wichtigen Steuerungsfunktionen) vor digitalen Angriffen völlig ungeschützt daliegen.

Nun zu den Techniken der Cyber-Delinquenten und den daraus resultierenden neuen Bedrohungen. Vom Beginn des Computerzeitalters in den letzten Jahrzehnten des 20. Jh. hat es gelegentliche Virusattacken, zT auch massiver Art gegeben, für die unschwer Antivirus-Software entwickelt werden konnte.

Aber dieses „romantische Zeitalter" ist endgültig vorbei. Die neuen Angriffsformen lassen sich nicht ohne einen intensiven Blick auf die Veränderung in der Täterlandschaft analysieren. An die Stelle von Einzeltätern, meist jugendlichen Hackern mit spielerischem Motiv, sind endgültig riesige kriminelle Konsortien mit hoher Professionalität und unbegrenzten technischen und finanziellen Mitteln getreten. Diese organisierte Kriminalität zur betrügerischen Gewinnerzielung konzentriert sich auf wenige – bekannte – Länder, kanalisiert aber ihre Attacken zwecks Anonymisierung („station hopping") über andere Staaten (Schwerpunkt: USA) und benutzt weltweit auch Individuen im Netz zB zur Geldwäsche. Diese Konsorzien verfügen über riesige Karteien von e-mail-Adressen, mit denen massiv spam-Nachrichten abgesetzt werden können, bei entsprechenden Auftraggebern eine lukratives Geschäft. Heute sind 80-90% des weltweiten e-mail Verkehrs spam, für den Einzelnutzer nur deshalb nicht in vollem Umfang bemerkbar, weil die Netzbetreiber (Internet Service Provider, ISP) relativ wirksame Spamfilter einsetzen. Spam-Nachrichten sind nicht nur eine Belästigung der Nutzer, sondern dienen auch als Vehikel für die Infektion mit Viren und anderer Schadens-Software („malware"), - nicht nur in e-mail-Anhängen, die tunlichst nicht geöffnet werden, sondern auch im eigentlichen spam-Text. Vor 10 Jahren wurden 40.000 Virus-Varianten gezählt; 2008

hat die Sicherheitsfirma Panda ihre Zahl auf 13 Millionen geschätzt. Bei allen Formen von malware wirken die Schutzprogramme nur gegen bekannte Versionen; die neuen Angreifer entwickeln jedoch, häufig mit überlegenen technischen Fähigkeiten und erstaunlichem Tempo, ständig neue Varianten, sodass die Verteidiger ohne Pause neue Verwundbarkeiten beseitigen müssen, - ein atemloses Rennen. Ein gutes Anti-Virus-Programm muss bis zu mehrfach täglich seine Datenbasis aktualisieren.

Vielleicht die gefährlichste neue Entwicklung ist das Entstehen von *botnets*. Der Terminus bezieht sich auf das für den Computernutzer nicht erkennbare Einpflanzen von Viren, die schlafend bleiben, vom Angreifer aber jederzeit aufgerufen werden können („Trojaner"). Sie machen die Computer zu „zombies", zu Robotern, und erlauben, wenn in grosser Zahl vernetzt, dem kriminellen Manager („bot herder" oder „bot master") jederzeit umfassende Operationen. Grosse botnets sind hierarchisch, ja geradezu militärisch organisiert. Der Befall mit unerkannten Trojanern wird in einigen Ländern auf 60% aller Computer geschätzt. Einige Varianten der botnet-Software sind in der Lage, selbstätig weitere Computer für das net zu rekrutieren. Zu den aktuellen Schadensformen gehört insbesondere das Ausspähen persönlicher Daten aus allen

Lebensbereichen, einschliesslich der benutzten privaten Passworte. Dies erlaubt nicht nur die Plünderung von Bankkonten, im Geschäftsleben den Raub von Geschäftszahlen, Kundenkarteien, Produktionsplanungen und –entwürfen, sondern auch die Verfälschung der entsprechenden Dateien. Die Datenspionage führt immer häufiger zu einem *identity theft*, mittels dessen der kriminelle Urheber sich völlig an die Stelle des Ausgespähten setzen und zu dessen Lasten agieren kann. Über die botnets können auch die Prozessfunktionen von Computern (Logikbomben) oder deren Daten zerstört oder verändert werden. Nicht weniger gravierend ist, dass die botnets durch gleichzeitiges Aufrufen einer grossen Zahl von Computern die e-mail- Adressen der Zielempfänger saturieren und lahmlegen und sogar dauerhaft beschädigen können („distributed denial of service", DDoS). Damit können nicht nur Unternehmen oder ganze Geschäftszweige, sondern auch essentielle Infrastrukturen (Regierung, Elektrizitätsversorgung, Steuerungscomputer im Bankwesen, Luft- und Eisenbahnverkehr, bei Talsperren, die technische ITC-Infrastruktur selbst, etc.) mit hoher Schadenswirkung ausser Funktion gesetzt werden. Das gleiche gilt, noch gravierender, für Einrichtungen im Verteidigungssektor. Die dreifache Nutzungsmöglichkeit der botnets für Datenspionage,

insbesondere Industriespionage, Logikbomben und DDoS ist in der Tat ominös.

Die von kriminellen Konsorzien aufgebauten botnets nehmen immer neue Grössenordnungen an. Das bisher grösste erkannte net hatte, so wird geschätzt, 1.5 Mio Computer versklavt. Die neueste Bedrohung, gegen die noch keine Gegenstrategien entwickelt worden sind, ist das botnet CONFICKER, das 5 Mio Computer in 122 Ländern einsetzen und steuern kann.

Andere gängige Methoden zur kriminellen Gewinnerzielung, mittels botnets oder auch ausserhalb, sind das phishing, die Umleitung von Computern auf gefälschte angebliche Internetseiten von Banken, zur Erlangung von Passwörtern, Kreditkartennummern, etc., die anschliessende Kontenplünderung erlauben (etwa 60% der direkten Angriffe); das pharming, das ebenfalls betrügerisch auf andere Seiten umlenkt, etc. Die Schäden der Wirtschaft durch Internetkriminalität erreichen jährlich zwei- bis dreistellige Milliardenbeträge; eine verlässliche Schätzung spricht von 180 Mia. Euro; freilich gibt es auch wesentlich bescheidenere Zahlen. Allerdings sind genaue Quantifizierungen nicht möglich, da die Unternehmen, und vornehmlich die Banken,

die Schäden oft selbst abdecken, im Interesse des Kundenvertrauens damit aber nicht an die Öffentlichkeit gehen.

Die vorstehenden Tatsachen erlauben nun einen Blick auf die eigentlichen Bedrohungen für die Stabilität des digitalen Raums und damit auch unserer Gesellschaftssysteme. Die riesigen Gewinne, die vor allem das organisierte Verbrechen durch digitale Wirtschaftskriminalität abschöpft, sind dabei nur ein Teil des Bedrohungszenarios. Wichtiger sind die neuen Möglichkeiten im Bereich des *cyber conflict*. Die Dimension der botnets erlaubt es, mit koordinierten gleichzeitigen Angriffen gegen das Wirtschaftssystem, wichtige nationale Infrastrukturen und das Verteidigungsdispositiv eines Landes – die ja alle auch einen hohen Grad von Interdependenz haben – in Sekundenschnelle praktisch alle wichtigen Lebensbereiche durch massives DDoS lahmzulegen. Die kürzlichen Vorgänge in Estland und Georgien geben von den anwendbaren Techniken und möglichen Ergebnissen einen Vorgeschmack. Über diese Probeveranstaltungen hinaus ist aber klar, dass die technischen Voraussetzungen für ein digitales Pearl Harbour – und mehr – heute eindeutig gegeben sind. Cyberwar-Szenarien werden an anderer Stelle in diesem Heft erörtert. Hier sei nur soviel gesagt, dass zu der massiven DDoS-Blockade der ITC-Netze – und alle Verteidungsministerien benutzen heute zusätzlich zu

geschützten Infranetzen, die freilich auch verwundbar sind, die zivilen Netze – auch die Spionage in die Verteidigungsplanung, das Verfälschen von Gefechtsfeld-Information, die Intervention in die Befehlsstränge und das Funktionieren von Waffensystemen, etc. treten können.

Die direkten gewinnträchtigen Aktivitäten der *bot herders* sind nur ein Teil ihres Geschäftsmodells. Im Internet kann *malware* letzter Aktualität erworben werden, können Hinweise auf die Schwachstellen kommerzieller Software und Instruktionen für den Diebstahl von Passworten oder Kreditkartennummern heruntergeladen werden. Umfangreiche Listen von e-mail-Adressen bis zum Millionenumfang stehen zum Verkauf. Von den Konsorzien können auch Cyber-Angriffsdienste gekauft oder stundenweise gemietet werden, sodass andere kriminelle Akteure, vor allem aber Terroristen – oder auch feindliche Regierungen – hinter derart unheiligen Allianzen ohne jede Gefahr der Identifizierung agieren können. Auch hier bietet der Estland-Fall mehr als Anhaltspunkte. Angesichts der Tätigkeit solcher Akteure werden die Grenzen zwischen den Kategorien *cybercrime, cyber terrorism* und *cyberwar* fliessend.

Fast alle Regierungen sehen diese möglichen Entwicklungen mit Sorge und treffen im Verteidigungsbereich Vorsorge, um die

Angreifbarkeit ihres Sicherheitsdispositiv zu mindern. Über die legitimen Vorkehrungen hinaus – Sicherung der eigenen ICT-Infrastruktur, ,,cyberwarfare countermeasures" - ist freilich problematisch, dass sich heute bis zu 140 Länder – darunter vor allem die grossen Mächte - mit offensiver Informatik ausrüsten und Cyber-Angriffsoptionen in ihre Planungen einbauen. Dabei ist freilich zuzugeben, dass eine klare Unterscheidung zwischen Angriffs- und Abwehrtechnologie schwer möglich ist; für die information weapon ist eine Definition noch nicht gefunden. Eine Unterscheidung ist freilich bei Absichten und strategischer Planung möglich; und Cyber-Angriffe, die sich im zivilen und militärischen Bereich ja der gleichen Techniken bedienen, sind klar definiert.

***

Wie steht es nun angesichts der geschilderten Kalamitäten und Perspektiven mit wirksameren Gegenstrategien? Sie können hier angesichts der Komplexität des Themas nur schematisch behandelt werden, was aber auch erlaubt, klare Prioritäten anzuzeigen[5]. Wichtige Aufgaben ergeben sich für nationale

---

[5] vgl. hierzu ausführlicher Top Cyber Security Problems That Need Resolution,
World Federation of Scientists, Geneva, May 2009,
http://www.unibw.de/infosecur/
documents/published_documents_cyber_security_problems

Regierungen, internationale Organisationen, die Wirtschaft und Industrie, und auch den einzelnen Nutzer.

- Vordringlich ist zunächst, in Ansehung des globalen Charakters der Bedrohung, das Netz der Verbots- und Sanktionsnormen weltweit zu komplettieren. Es darf keine rechtsfreien Räume geben, von denen aus Angriffe straffrei unternommen werden können. Hier hat die schon genannte, im Europarat ausgehandelte Conventon on Cybercrime, den Grund gelegt. Sie ist bisher von 26 Staaten ratifiziert, von weiteren 20 gezeichnet worden. Die Vorschriften haben aber über den Kreis der Vertragsparteien hinaus Modellcharakter. Die Konvention muss Standard für eine universelle, harmonisierte Pönalisierung von Cyberdelikten werden[6].
- Nicht weniger dringend ist die universelle Möglichkeit der Rechtsverfol-gung. Hier bietet die Europarats-Konvention Regeln für die internationale polizeiliche und gerichtliche Zusammenarbeit. Ein Kern ist die permanente Kontakt- und Informationsmöglichkeit der Rechtsverfolgungsbehörden (24/7-Mechanismus, ursprünglich von der G7 propagiert, an

---

[6] Die Konvention ist auch in das noch umfassendere „ITU Toolkit for Cybercrime Legislation", http://www.itu.int/ITU-D/cyb/cybersecurity/legislation.html

dem inzwischen ca. 50 Staaten teilnehmen), auch eine stärkere Rolle von Interpol und Europol in der Rechtsverfolgung dieser Delikte.

- Zur effektiveren Rechtsverfolgung sollte baldmöglichst und einheitlich das Internet-Protokoll IPv6 engeführt werden, um die Identifikation und Zuordnung und die Transparenz von digitalen Nachrichten an der Quelle (Autor und Systeme) zu erleichtern.
- Das Netz von nationalen CERTs muss komplettiert und zu einem Netz international operierender, multidisziplinärer Cyber Reponse Centers mit umfassenden Überwachungs- und Koordinierungsaufgaben ausgebaut werden.
- Die Industrie muss sich verantwortlich dafür fühlen, in ihre Designs von Geräten und Software von Anfang an mehr Sicherheit einzubauen; heute sind neue Anwendungen entschieden zu anfällig gegen Angriffe. Das gilt gerade auch für mobile Systeme, deren explosives Wachstum die integrierten Netze zunehmend gefährdet, und für die neuen Techniken im *grid computing* und *cloud computing*.
- Die Regierungen müssen sich den neuen Bedrohungen noch umfassender stellen und die organisatorischen und investiven Vorkehrungen für Vorsorge und Abwehr treffen, wobei einer raschen und effektiven nationalen Koordination grosse Bedeutung zukommt. Das Bewusstsein und die Kenntnis von

den Gefahrenlagen im digitalen Raum und verantwortungsvolle Nutzung muss ein integraler Teil der Erziehung besonders der jungen Generation für das Internetzeitalter werden; ihnen muss früh eine Kultur der Informationssicherheit vermittelt werden.

- Die Nutzer der ITC – die Wirtschaft, die Manager von Infrastrukturanlagen und die Individuen – müssen mehr Wachsamkeit und Selbstschutzinstinkte entwickeln (Aktueller Virusschutz, Verschlüsselung, Sorgfalt mit Passworten, Zugangskontrolle bei Computern mit Nutzeridentifizierung, Authentifizierung der benutzten Software, etc.). In den Unternehmen muss den mit Informationssicherheit betrauten Mitarbeitern ein höherer organisatorischer Stellenwert zugeordnet werden. Sie müssen ein quantitatives Risikomanagement für ihre Anlagen einführen.
- Die Sicherheitstechniken mittels Kryptographie, Zertifikationen, elektronischen Unterschriften, „trustworthy computing", etc. müssen weiterentwickelt werden, und zwar so, dass sie auch künftigen Herausforderungen (zB quantum computing) standhalten.
- Im internationalen Bereich sollte die technische und politische Führungsrolle der ITU als internationale lead agency in der Informationssicherheit gestärkt werden.

- Erarbeitung von Standards mit internationaler Gültigkeit für den Schutz der Privatsphäre und von Geschäftsdaten im Abgleich sowohl mit der zunehmenden Eindringfähigkeit von Spionagetechniken, Suchmaschinen, data mining, etc. wie auch den öffentlichen Sicherheitsinteressen.

Von vielleicht noch grösserer Bedeutung ist die Erarbeitung eines modernen völkerrechtlichen Rahmens für die Beurteilung der militärischen Nutzung von ICT (cyber war und cyber defence). Zwar lassen sich aus dem Vertragsvölkerrecht und aus den umfassenden Prinzipien-erklärungen der VN-Generalversammlung zu den Themen Agression und Intervention[7] einige allgemeine Standards ableiten, die Aufgabe einer Anpassung des Völkerrechts an die Erfordernisse de Digitalzeitalters ist aber ungelöst. Hier bedarf es einer

---

[7] „Definition of Aggression", Res. 3314 (XXIX), „Declaration on Principles of International Law concerning Friendly Relations and Cooperation among States in accordance with the Charter of the United Nations", Res. 2625 (XXV), „Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of Their Independence and Sovereignty", Res. 2131 (XX). Hierzu auch Sergei Komov, Sergei Korotkov, Igor Dylevski Military aspects of ensuring international information security in the context of elaborating universally acknowledged principles of international law. DISARMAMENT FORUM, UNIDIR, 2007 nº. 3. Russland hat sich um die Thematisierung dieser Fragen in den VN besonders verdient gemacht.

autoritativen Neuinterpretation der VN Charta (und des NATO-Vertrages) zu Begriffen wie ,,bewaffneter Angriff", ,,territoriale Integrität", ,,nationale Souveränität". Die rechtlichen Grenzen von ,,information operations" auf der einen, Selbstverteidigung unter Art. 51 der Charta auf der anderen, müssen anhand von realistischen cyberwar-Szenarien aufgezeigt werden. Es bedarf einer Definition der ,,information weapons" und ihres offensiven Einsatzes, ebenso wie der Entwicklung operativer Standards für die Anwendung von Kapitel VII der Charta, bzw. kollektiver Gegenmassnahmen unter dem NATO-Vertrag. In diesem Zusammenhang ist ernsthaft zu prüfen, ob der offensive Einsatz von cyber weapons nicht grundsätzlich geächtet werden sollte, ungeachtet der schwierigen Abgrenzung zwischen offensiver und defensiver Anwendung von ICT und den Problemen etwaiger Sanktionen.

Darüber hinaus stellt sich eine übergreifende ordnungspolitische Aufgabe. Ebenso wie die Weltmeere und der Weltraum bedarf auch die neue Domäne des ,,cyber space", des digitalen Raums, einer konzeptionellen Gesamterfassung. Für die Meere ist eine umfassende Kodifikation in der Seerechtskonvention gelungen, für den Weltraum zeichnet sich ein Regime mit wesentlichen Regeln ab. Auch für die digitale Sphäre ist schon nach einem internationalen ,,Law of

Cyberspace" als Ordnungsrahmen gerufen worden[8]. Er würde auch eine schlüssigere Bearbeitung der Probleme des cyber conflict und die Erarbeitung eines allgemeingültigen Cyber-Verhaltenskodexes ermöglichen, uns vielleicht auch einem Zustand näherbringen, bei dem an die Stelle einer Konfliktsperspektive mit hohem Destabilisierungspotential die Normalität eines cyber peace tritt.

Botschafter a.D. HENNING WEGENER ist Chairman des Permanent Monitoring Panel on Information Security der World Federation of Scientists, Genf

---

8 Vgl. Permanent Monitoring Panel on Information Security, World Federation of Scientists Toward a Universal Order of Cyberspace: Managing Threats from Cybercrime to Cyberwar, 2003, http://www.itu.int/dms_pub/itu-s/md/03/wsis/S03-WSIS-C-0006!!MSW-E.doc. Ahmad Kamal, The Law of Cyber-Space. An Invitation to the Table of Negotiations, UNITAR, 2005.