Der Cyber-Raum strategisch betrachtet
Chancen und Risiken der digitalen Revolution

von Peter Härle, Studienleiter

Er ist nicht wahrnehmbar, dennoch nutzen wir ihn ständig, meist jedoch ohne uns dessen bewusst zu sein. Der Cyber-Raum ist zu einem unverzichtbaren, selbstverständlichen Teil unseres Lebens geworden. Wenn wir über Land fahren, durch die Luft fliegen oder über die Weltmeere segeln, begeben wir uns von Ort zu Ort. Den Cyber-Raum verlassen wir dabei jedoch nie, es sei denn, die Verbindung bricht aufgrund eines Funklochs ab. Unsere Anbindung erfolgt über inzwischen unverzichtbare Smartphones, die wir immer und überall griffbereit haben. Die Welt wurde zum „globalen Dorf“ und wir leben mitten drin. Einfacher ist unser Weltbild dadurch nicht geworden. Die Vielzahl der Informationen lässt ein vages Ordnungsschema erkennen, wonach alles irgendwie mit allem zusammenhängt. Mehr und mehr wird uns bewusst, dass wir mitten in einem unabwendbaren, gewaltigen Veränderungsprozesses stehen, der längst all unsere Lebensbereiche erfasst hat.

Potenzial der Digitalen Revolution

Die Erfindung und der Einsatz der Dampfmaschine führten beginnend in der zweiten Hälfte des 18. Jahrhunderts zur industriellen Revolution, die bahnbrechende Veränderungen nach sich zog. Plötzlich war nichts mehr so, wie es früher einmal war. Die Leistungsfähigkeit der Landwirtschaft konnte durch Maschinenkraft enorm gesteigert werden, wodurch letztlich die gesamte Wirtschaft wesentlich arbeitsteiliger organisiert werden konnte; der Zwang zur Selbstversorgung war nicht mehr gegeben. Die damit einhergehenden Veränderungen waren fundamental, wie immer gab es dabei Gewinner und Verlierer. Huf- und Nagelschmied wie auch Wagner hatten keine Zukunft mehr, dafür bildeten sich ganz neue Berufsgruppen wie Maschinisten, Lokomotivführer und Mechaniker heraus. Großbritannien, das Land, in dem Dampfmaschinen früh zum Einsatz kamen, stand über gut ein Jahrhundert an der Spitze der Industrialisierung, entsprechend groß war das damit verbundene politische Gewicht.

Die mit enormem Tempo fortschreitende Digitalisierung und der damit immer bessere Zugang zum Cyber-Raum und dessen zunehmend intensivere Nutzung, die mit Begriffen wie Internet der Dinge bzw. Industrie 4.0 umschrieben werden, haben ein gesellschaftliches Veränderungspotenzial, das alles bislang an Veränderung Dagewesene in den Schatten stellt. Die strategische Dimension des Cyber-Raumes und die daraus zu ziehenden Folgerungen sind daher von fundamentaler Bedeutung für unsere Zukunft.[1]

[1] vgl. Dr. Angela Merkel, Rede anl. des Jahrestreffens 2015 des World Economic Forum Davos, 22.01.2015, http://www.bundeskanzlerin.de/Content/DE/Rede/2015/01/2015-01-22-merkel-wef.html, Zugriff am 26.01.2015

Besonderheiten des Cyber-Raumes

Das Kunstwort Cyber-Raum umfasst die Gesamtheit aller Computer, Router, Speicher, Kabel sowie weitere Komponenten, die es ermöglichen, riesige Datenmengen in kurzer Zeit um die Welt zu schicken. Abstrakt betrachtet handelt es sich um einen von Menschenhand geschaffenen, künstlichen sowie grenzenlosen Raum, in dem Digitalisierung und Globalisierung mit Hilfe des Internets zusammengeführt werden. Der Cyber-Raum ist omnipräsent, zeitlich unbegrenzt nutzbar und, durch technischen Fortschritt bedingt, unablässig im Wandel.

Während die Kontinente, Weltmeere, der Luft- und Weltraum zu den tradierten, physikalisch fassbaren Global Commons zählen, ist mit dem Cyber-Raum ein weiteres, weltweites Allgemeingut hinzugekommen, das gleichsam alle anderen überwölbt und sich mit atemberaubender Geschwindigkeit weiterentwickelt.[2] Die damit einhergehenden, gewaltigen Veränderungen betreffen alle Dimensionen eines vernetzten, strategischen Denkansatzes. Politisch, diplomatisch, militärisch, ökonomisch, sozial, informatorisch, infrastrukturell, die Auswirkungen sind allumfassend. Besonders kommt es dabei auf die Interdependenzen an, wie die Weiterentwicklung von statten geht und wo der gesamte Prozess Eingriffsmöglichkeiten bietet und/oder -notwendigkeiten fordert.

Um die Global Commons bestmöglich zu nutzen, um sich „unfallfrei“ darin zu bewegen, bedarf es Regeln. Diese zu schaffen ist Aufgabe der Politik. Bezogen auf die natürlichen Allgemeingüter sind die heute vorhandenen nationalen und internationalen Regelwerke bedarfs- und erfahrungsorientiert über viele Perioden hinweg entstanden. Erleichternd wirkte dabei der Umstand, dass sich diese, vom Weltraum abgesehen, klar abgrenzen lassen und sich dadurch zuordnungsbare nationale Zuständigkeiten ergeben. Der Cyber-Raum erweist sich dem gegenüber als weit komplexer. Insbesondere seine nationale Zuordnungsbarkeit ist nicht gegeben. Hinzu kommt sein allmählicher Entstehungsprozess, der mitunter mehr durch anarchisches, als durch systemisches Handeln geprägt ist. Dem entspricht die Grundhaltung, dass erlaubt ist, was technisch machbar ist. Gerade aufgrund des mit dem Cyber-Raum und der fortschreitenden Digitalisierung verbundenen immensen Innovationspotenzials, kommt es insbesondere darauf an, die damit verbundenen zahlreichen Auswirkungen und tiefgreifenden Veränderungen frühzeitig zu erkennen und in politische Konzepte einzubinden. Analoges Denken war gestern, die neue Komplexität erfordert weit mehr Flexibilität und Kreativität.

Chancen und Risiken im Cyber-Raum [3]

Als weltweit nutzbares Allgemeingut schafft der Cyber-Raum im Zusammenhang mit der Digitalen Revolution sowie dem Umgang mit Big Data vollkommen neue bahnbrechende Möglichkeiten, die vor Jahren noch undenkbar waren. Er ist zu einem unverzichtbaren Aktionsraum von Staat, Wirtschaft, Wissenschaft und Gesellschaft geworden, der durch sein mit ihm verbundenes, enormes gesellschaftliches und strukturelles Veränderungspotenzial uns alle nachhaltig berührt.

Als Informations- und Kommunikationsraum, als sozialer Interaktionsraum, als Wirtschafts- und Handelsraum, als politischer Partizipationsraum oder als Steuerungsraum, der Cyber-Raum bietet vielfältige Nutzungsmöglichkeiten, die mit großen Chancen, aber auch ebensolchen Risiken verbunden sind, die durch die Erfassung und Auswertung von Big Data noch verstärkt werden.

---

[2] vgl. Brett Williams: Cyberspace: What is it, where is it and who cares?, Armed Forces Journal, 13.03.2014, http://www.armedforcesjournal.com/cyberspace-what-is-it-where-is-it-and-who-cares/, Zugriff am 16.01.2015

[3] vgl. Österreichische Strategie für Cyber Sicherheit, Wien, März 2013, S. 6, http://www.bka.gv.at/DocView.axd?CobId=50748, Zugriff am 19.03.2015

Mittels eines leistungsfähigen Internetanschlusses sind die Datenübertragung sowie der Zugriff auf Daten- und Informationsbestände nahezu verzugslos, uneingeschränkt und weltweit möglich. Längst hat die E-Mail den klassischen Briefverkehr oder andere Kommunikationsarten, wie Fernschreiben oder Fax, abgelöst. Weltweit werden pro Minute bereits mehr als 200 Millionen E-Mails versandt und über zwei Millionen Suchabfragen bei Google getätigt. Mehr und mehr werden auch Telefongespräche über das Internet und nicht mehr über die klassischen Telefonkabel geführt.

Soziale Netzwerke sind längst zu einem festen, viele unserer Lebensbereiche beeinflussenden Bestandteile geworden. Ob Job- oder Partnersuche, die Pflege sozialer Beziehungen sowie menschlicher Interaktionen, die Möglichkeiten sind fast unerschöpflich und täglich, wenn nicht stündlich, tun sich neue auf. Soziale Netzwerke, wie Facebook, Twitter, Xing u.a., haben in kürzester Zeit die Welt erobert. Längst werden diese dazu genutzt, Verabredungen zu treffen, wie auch politisch aktiv zu werden. Weltweit gibt es derzeit mehr als zwei Milliarden Internetnutzer, Tendenz steigend.

Innerhalb weniger Jahre ist der Cyber-Raum darüber hinaus zu einem Marktplatz von strategischer Bedeutung geworden. Amazon, Alibaba, Zalando, unzählige Reiseportale, die Aufzählung könnte nahezu unbegrenzt fortgesetzt werden. Wer im Handel- und Dienstleistungsgewerbe bestehen will, kommt zumindest um einen Internetauftritt, meist aber auch einen Internet Shop, nicht herum. Binnen zwei Jahren hat sich der mittels E-Commerce weltweit erzielte Umsatz nahezu verdoppelt. Der gesamte weltweite Zahlungsverkehr wird fast ausschließlich über das Internet abgewickelt. E-Banking und Geldautomaten haben die Kundenfrequenz der Filialbanken, von Beratungsgesprächen abgesehen, drastisch reduziert.

Längst hat auch der Staat mit E-Government die Chancen erkannt. Die Distanz zum Bürger ist geringer; zahlreiche, insbesondere administrative staatliche Leistungen können schneller und effizienter erbracht werden. Der Cyber-Raum hat Einfluss auf das Verhältnis von Staat und Gesellschaft. Auch politische Partizipation und Meinungsäußerung wurden erleichtert. Gleichzeitig ist damit die Erwartungshaltung an die Politik gestiegen. Es genügt nicht mehr, einen politisch erzielten Kompromiss zu verkünden; Transparenz und möglichst umfängliche Partizipation am politischen Prozess werden von den interessierten Wählern erwartet und bei den Volksvertretern eingeklagt und mitunter auch erzwungen.

Über den Cyber-Raum als Informations- und Kommunikationsraum hinaus geht dessen eng damit verbundene Rolle als Steuerungsraum. Eine Funktion, mit der nahezu die gesamte Infrastruktur im Verkehrs-, Energie-, Wirtschafts- und Industrie-, im Sicherheits-, sowie im Gesundheits- und Bildungsbereich bereits jetzt überwacht, betrieben und gewartet werden kann. Dies umfasst die gesamte kritische Infrastruktur (KRITIS) eines Staates. Internet 4.0 und Internet der Dinge sind die neuen Schlagworte für eine noch weitergehende Vernetzung. Damit verbunden ist letztlich die Vision, sein alltägliches Umfeld mit einer einzigen App vom Handy aus zu überwachen und zu steuern.

Berechnungen aus dem Jahr 2011 zufolge verdoppelt sich das weltweite Datenvolumen alle zwei Jahre. Big Data bezeichnet ursprünglich Datenmengen, die zu groß, zu komplex oder zu schnell Änderungen unterworfen sind, um diese mit klassischen Methoden der Datenverarbeitung auszuwerten. Mehr und mehr lassen sich inzwischen jedoch mit der Hilfe zahlreicher leistungsstarker Computer vielfältige Verknüpfungen auch großer Datenmengen sowie statistische Auswertungen realisieren, die Rückschlüsse auf Zusammenhänge und Verhaltensweisen ermöglichen. Wirtschaftsunternehmen erhoffen sich daraus u.a. Wettbewerbsvorteile, staatliche Stellen setzen auf bessere Ergebnisse z.B. in der Kriminalistik und Terrorismusbekämpfung oder aber bei der Vorhersage des Wählerverhaltens.

Wo viel Licht ist, gibt es naturgemäß aber auch viel Schatten. Zutrittsbeschränkungen zum Cyber-Raum gibt es nicht. Den Chancen und Möglichkeiten steht eine Vielzahl von Risiken und Bedrohungen gegenüber. Der Cyber-Raum ist auch Tatraum und dies leider in zunehmendem Maße. Die Bandbreite reicht von der gezielten Kontrolle und Beeinflussung der Bevölkerung, von Propaganda und bewusster Falschinformation

bis hin zur Cyber-Kriminalität, dem Identitätsmissbrauch, dem Missbrauch des Internets für extremistische Zwecke und letztlich gezielten massiven Cyber-Angriffen durch staatliche und nichtstaatliche Akteure, die den Cyber-Raum als Feld für ihr Handeln nutzen und dabei auch vor Landesgrenzen nicht Halt machen, sondern sich gerade die Entgrenzung des Raumes zu Nutze machen, um eigens Handeln zu kaschieren. Solche Angriffe können auch Teil militärischer Operationen sein.

Cyber-Awareness umfasst mehr als Cyber-Security

Gezielter Missbrauch innerhalb des neu geschaffenen Allgemeingutes Cyber-Raum führte bereits früh zu der Erkenntnis, dass Cyber-Security von wesentlicher Bedeutung ist, um den damit verbunden Risiken entgegen zu wirken. Operativ-taktische Maßnahmen zur Erhöhung der Cyber-Security sind heute jedem Anwender vertraut und werden mit der Veränderung des Cyber-Raumes ständig angepasst. Die Bundesregierung hat mit der Schaffung des Bundesamtes für Sicherheit in der Informationstechnik (BSI) bereits 1991 entsprechend reagiert.

Im Grundsatz zeichnen sich, strategisch betrachtet, drei handlungsrelevante Felder ab. Die mit der Digitalisierung verbundenen Chancen und Risiken haben rechtliche, wirtschaftliche sowie, quasi auf einer höheren Ebene, politische Konsequenzen.

Die Aktivitäten der amerikanischen NSA haben die Debatte um ein ausgewogenes Maß von Freiheit und Sicherheit im Cyber-Raum beflügelt.[4] Durch seine Entgrenzung ist der Cyber-Raum in besonderem Maße dazu geeignet, Informationen abzugreifen, aber auch manipulierend einzugreifen. Der Virus Stuxnet war in der Lage, gezielt in die Steuerung von Zentrifugen iranischer Atomanlagen einzugreifen und diese durch Drehzahlveränderungen unschädlich zu machen. Jegliche Art von Kritischer Infrastruktur (KRITIS), wozu auch Banken zählen, ist sicherlich einer besonderen Gefährdung ausgesetzt. Experten gehen davon aus, dass schon bald auch bislang ungeschützte SmartTV, quasi KRITIS im privaten Bereich, Angriffsziele krimineller Machenschaften sein werden, um mittels deren Sperrung bzw. Entsperrung Einnahmen zu generieren. Letztlich hilft gegen all diese Machenschaften nur, die eigenen Systeme bestmöglich abzuschotten und ständig auf Eindringlinge hin zu überprüfen. Auch für den Cyber-Raum bedarf es Regeln bzw. eines anerkannten Verhaltenskodexes. Ferner scheint es geboten zu sein, bestehende gesetzliche Regelungen im Hinblick auf deren Relevanz und Anwendbarkeit im Zeitalter der Digitalisierung zu überprüfen. Ein Beispiel ist hierfür das Urheberrecht, das noch weitgehend analog ausgelegt ist. Nur wenn es gelingt, geistiges Eigentum auch im Netz wirksam zu schützen, werden unabdingbare Bedingungen geschaffen, dass sich Start up in größerem Maße in Deutschland bzw. Europa herausbilden. Dabei gilt es zu bedenken, dass die heute wertvollsten Firmen der Welt, wie Apple, Microsoft, Google, einst alle als solche begonnen haben. Die Nutzung öffentlicher Hotspots, der Umgang mit Big Data, die Entwicklung und Nutzung autonom fahrender Automobile mögen weitere Bereiche aufzeigen, die heute noch nicht oder bestenfalls unzureichend rechtlich geregelt sind. Hinzu kommt, dass die digitale Revolution global erfolgt, Gesetze meist aber nur einen lokalen oder regionalen Geltungsanspruch haben.

In wirtschaftlicher Hinsicht scheint es so, als hätte Deutschland und Europa die Digitalisierung lange Zeit verschlafen.[5] Mehr und mehr hat jedoch inzwischen eine Aufholjagd begonnen. Die ersten Branchen sind bereits massiv von Umbrüchen betroffen. Die Firma Voith, einst Weltmarktführer in der Produktion von Papiermaschinen, konnte in den letzten drei Jahren keine ihrer hochkomplexen Maschinen verkaufen, da der Bedarf an Papier weltweit drastisch zurückgegangen ist. Jetzt wird das Unternehmen grundlegend umstrukturiert. Auf die strategische Industrie Deutschlands, den Automobilbau, kommen ebenfalls gewaltige

[4] vgl. Stefan Beutelsbacher u. Thomas Jüngling: Operation offene Tür, Wie die NSA mit einem Wunderprogramm in Hunderte Millionen Computer eindringt, Die Welt v. 18.02.2015, S. 10
[5] vgl. Carsten Knop: Digitaler Kaltstart in ein neues Jahr, Frankfurter Allgemeine Zeitung (FAZ) v. 14.02.2015, S. 32

Herausforderungen zu. Noch ist nicht entschieden, ob die sich am Horizont abzeichnenden autonom fahrenden Autos im Silicon Valley oder aber weiterhin in Stuttgart, München, Ingolstadt und Wolfsburg produziert werden.[6] Ein derartiger Einschnitt hätte drastische Konsequenzen nicht nur für die Automobilbauer, deren Zulieferer, die Werkzeugmaschinenindustrie und andere, letztlich wären die gesamte Wertschöpfungskette und damit unser aller Wohl davon betroffen. Der Industriestandort Deutschland wäre gefährdet. Mehr denn je kommt es daher jetzt darauf an, seitens der Politik die Digitalisierung fördernde Ausgangsbedingungen zu schaffen. Sich dessen bewusst hat Bundeskanzlerin Merkel das Bemühen darum bereits zur Chefsache erklärt. Die vom Bundeskabinett im August letzten Jahres verabschiedete „Digitale Agenda“[7] ist Ausdruck dieses Bemühens. Eine leistungsfähige Internetanbindung der Bevölkerung ist zwingende Voraussetzung für die weitere Entwicklung. Es ist daher konsequent, dass die Agenda digitale Infrastrukturen als primäres Handlungsfeld nennt. Auch die aufgekommenen Forderungen nach der Einrichtung von mit Sensoren ausgerüsteten Teststrecken für autonomes Fahren auf bestehenden Autobahnabschnitten ist in diesem Zusammenhang alles andere als abwegig, sondern eine zwingende Notwendigkeit, die strategische Industrie Deutschlands in das Zeitalter der Digitalisierung zu überführen.[8]

Eine neue App kann heute einerseits den Anfang vom Ende eines Wirtschaftsimperiums bedeuten,[9] andererseits neue Chancen eröffnen und zum Strukturwandel gestaltend beitragen.[10] Neben genialen Ideen und kühnen Visionen sind insbesondere eine breit angelegte, zukunftsweisende Aus- und Weiterbildung die Garanten dafür, die mit der digitalen Revolution verbundenen Chancen und Möglichkeiten zu erkennen und zu nutzen.[11] Big data macht nur dann Sinn, wenn die Datenmengen hinterfragt, sinnvoll ausgewertet und miteinander verknüpft werden können.[12] Die gezielte Förderung von Start-ups ist unabdingbar, um zumindest die Chance zu wahren, auch zukünftig am Weltmarkt eine respektable Rolle zu spielen. Die Schaffung einer flächendeckenden digitalen Infrastruktur ist zwingende Voraussetzung hierfür.

Wissen ist Macht, eine von der Aufklärung bis heute und vermutlich darüber hinaus gültige Erkenntnis. Nicht nur, dass die Informationsübermittlung immer schneller und kostengünstiger wird, auch der Umfang sowie die Analysemöglichkeiten zur Verfügung stehender Daten nehmen geradezu exponentiell zu. Gleichzeitig haben immer mehr Menschen Zugang zum Cyber-Raum und verfügen damit letztlich in nahezu Echtzeit über aktuelle Informationen. Diese zunehmende Transparenz führt jedoch gleichzeitig zu einer insgesamt zunehmenden Komplexität. Durch soziale Netzwerke bilden sich vollkommen neue Kommunikations- und Beziehungsstrukturen. Damit geht eine Umverteilung von Macht einher; letztlich resultiert daraus eine Neuausrichtung der Weltordnung. Polaritäten lösen sich auf, die Einflussmöglichkeiten großer und kleiner Staaten nivellieren sich, die Bedeutung der an Grenzen gebundenen Nationalstaaten nimmt ab. Politikgestaltung liegt dadurch mehr und mehr nicht mehr in der alleinigen Hand von Regierungen, ein größerer Einfluss global agierender Akteure aus der Wirtschaft sowie dem zivilgesellschaftlichen Umfeld ist damit einhergehend.[13]

---

[6] vgl. Nikolaus Doll: Fahrerloses Auto kommt in fünf Jahren, Die Welt v. 02.03.2015, S. 11

[7] Bundesministerium für Wirtschaft und Energie, August 2014, durch das Bundeskabinett am 20.08.2014 beschlossen, http://www.bmwi.de/DE/Themen/Digitale-Welt/digitale-agenda.html

[8] Bundesministerium für Verkehr und digitale Infrastruktur, Info-Papier „automatisiertes Fahren“: Aufbau „Digitales Testfeld Autobahn“. Eine entsprechend ausgestattete Teststrecke wird auf der A 9 in Bayern eingerichtet. Erste Maßnahmen zur Digitalisierung erfolgen noch in 2015. http://www.bmvi.de/SharedDocs/DE/Artikel/DG/automatisiertes-fahren-info-papier.html?linkToOverview=js

[9] vgl. Heinz Schulte: Vom Ende der Macht, griephan Briefe 07/15 v. 09.02.2015, S. 4

[10] Peter Diamandis, Geschäftsführer der Singularity University: „In zehn Jahren werden 40 Prozent der heute 500 größten Unternehmen der Welt keine Rolle mehr spielen.“, nach: Thomas Schulz: Das Morgen-Land, Der Spiegel 10/2015 v. 28.02.2015, S. 24

[11] vgl. Nina Trentmann: Die Zukunft ist programmiert. An britischen Schulen lernen schon Kinder den Umgang mit Quellcode und Computersprache. Sie sollen die Digital-Unternehmer von morgen werden, Die Welt v. 28.02.2015, S. 19

[12] Dr. Thomas Schweer, Entwickler des Pre Crime Observation System (Precobs): „Menschen handeln nach Mustern, das macht sie berechenbar“, nach: Jörg Schindler u. Wolf Wiedmann-Schmidt: Im roten Bereich, Der Spiegel 10/2015 v. 28.02.2015, S. 51; Harald Czycholl: Wie Big Data die Arbeitswelt verändert, Die Welt v. 13.02.2015, S. 17

[13] vgl. Joseph S. Nye: Macht im 21. Jahrhundert, Siedler-Verlag 2011, S. 175 ff.

Trotz der tendenziell schwindenden Einflussmöglichkeiten muss den Staaten daran gelegen sein, dass ihre Bürger einerseits an den mit der digitalen Revolution verbundenen Chancen partizipieren können, und dass andererseits jedoch damit verbundene Risiken abgewehrt werden. Die größten Risiken dürften dabei in der Manipulation bzw. dem Abgreifen von Daten im Bereich von KRITIS, der Wirtschaft oder im privaten Bereich liegen. Gesicherte Konten und verlässliche Aktien- und Börsenkurse sind genauso relevant wie ein problemlos funktionierender Zahlungsverkehr oder die stabile Stromversorgung. Einem Angriff auf Bits und Bytes haben tradierte polizeiliche oder militärische Wirkmittel nur wenig oder nichts entgegenzusetzen, zumal wenn dieser elektronisch erfolgt. Auch die Frage einer möglichen Reaktion ist neu zu definieren. Dabei sind auch schwierige Fragen zu klären, so auch, ob möglicherweise ein „Hack back" mit ggf. offenem Ausgang legitim, verantwort- und durchführbar ist.[14] Insgesamt sind nicht nur das Zusammenspiel von Absicherung, Abschreckung und Verteidigung neu zu gewichten und zu ordnen, sondern auch das neu entstandene Machtgefüge zwischen Nuklear- und/oder Cyber-Mächten und die daraus resultierenden Folgen neu zu beurteilen.

Cyber-Awareness bedarf einer ganzheitlichen, politikbereichsübergreifenden Betrachtung

In strategischer Hinsicht besteht noch erheblicher Diskussions- und Handlungsbedarf. Da so gut wie alle Lebens- und Politikbereiche von der Digitalisierung und deren Folgen betroffen sind, handelt es um eine ausgeprägte Querschnittsaufgabe, was einmal mehr die Zuordnung der Verantwortlichkeiten nicht erleichtert. Aufgrund des vielschichtigen Entwicklungsprozesses des Cyber-Raumes und der Vielzahl der verwendeten Systeme sowie den damit verbundenen Verantwortlichkeiten, erweisen sich bereits ressortinterne Abstimmungsprozesse mehr als komplex. Für ressortübergreifende Betrachtungen gilt dies in verstärktem Maße.

Die Digitale Agenda der Bundesregierung sowie die Cyber-Sicherheitsstrategie für Deutschland [15] des Bundesministeriums des Innern sind ein erster Anfang. Grundsätzlich sind der Cyber-Raum und dessen Möglichkeiten in alle strategischen Überlegungen mit einzubeziehen. Das mit der digitalen Revolution verbundene struktur- und machtverändernde Potenzial ist enorm. Die komplexen Herausforderungen des Cyber-Bereichs verlangen geradezu nach einem Vernetzten Ansatz. Nur wenn diesen ganzheitlich und politikbereichsübergreifend begegnet wird, besteht die Chance, dass Deutschland auch zukünftig seine wirtschaftliche Stellung und weltpolitische Bedeutung halten kann.

Ein nationaler Alleingang erscheint dabei ziemlich aussichtslos. Die Entgrenzung des Cyber-Raums einerseits, und die schwindende Bedeutung von Nationalstaaten andererseits, erfordern ein zumindest EU-gemeinsames Vorgehen, um im internationalen Konzert wahrnehmbar mitzuspielen. Es bedarf einer starken Digitalunion in der einheitliche digitale Spielregeln für alle gelten. Ein starker Binnenmarkt dürfte der Garant dafür sein, auch im digitalen Zeitalter den damit verbundenen Herausforderungen gewachsen zu sein. Dies bedeutet aber auch, der noch im IT-Bereich bestehenden Fragmentierung entgegenzuwirken. Gemeinsame Standards und Verhaltensregeln sind jedoch nicht nur regional, sondern weltweit zwingend. Es bedarf einer Global Internet Governance auf der Basis einer einvernehmlichen Verständigung der Völkergemeinschaft im Hinblick auf die Regelungen und Mechanismen für den Betrieb und die Nutzung des Netzes.

Chancen nutzen, Risiken vermeiden, muss die Devise lauten. Hat uns einst „Made in Germany" zur Weltgeltung verholfen, könnte es zukünftig „Backed up in Europe" sein. Dabei müssen digitale Souveränität ge-

[14] vgl. Carsten Knop: Black-out im Cyberkrieg, Frankfurter Allgemeine Zeitung (FAZ) v. 21.02.2015, S. 21
[15] Bundesministerium des Inneren, Februar 2011, durch das Bundeskabinett am 23.02.2011 beschlossen, http://www.bmi.bund.de/cln_174/SharedDocs/Downloads/DE/Themen/OED_Verwaltung/Informationsgesellschaft/cyber.html?nn=109632

währleistet und Vertrauen gegeben sein. Den negativen Erfahrungen mit der Datensicherheit im Zusammenhang mit der NSA könnte mit einer European Cloud entgegen getreten werden.[16]

Mit der digitalen Revolution sind enorme Chancen, aber auch Risiken verbunden. Nur wer die Chancen nutzt und dabei die Risiken beherrscht, wird auch zukünftig bestehen. Der Wettlauf ist bereits in vollem Gange und wird weiter rasant Fahrt aufnehmen. Einen Weg zurück gibt es nicht, denn der technologische Fortschritt lässt sich nicht aufhalten. Bereits Albert Einstein stellte fest: „Der Fortschritt geschieht heute so schnell, dass, während jemand eine Sache für gänzlich undurchführbar erklärt, er von einem anderen unterbrochen wird, der sie schon realisiert hat.“ [17]

Oberst i.G. Peter Härle ist Studienleiter an der Bundesakademie für Sicherheitspolitik.
Der Beitrag gibt die persönliche Auffassung des Autors wieder.

[16] Günther Oettinger: „Wir haben das Spiel in der IT-Branche verloren“, http://www.faz.net/aktuell/wirtschaft/netzwirtschaft/oettinger-auf-dld, Zugriff am 02.02.2015
[17] Albert Einstein, Physiker (* 14. März 1879 in Ulm; † 18. April 1955 in Princeton, New Jersey)