Prof. Dr. Gebhard Geiger

Politik und Sicherheit im digitalen Zeitalter:
Deutschlands Herausforderung im modernen Informationskrieg.

1. Einführung

Die moderne informationstechnologische Revolution kann als eine grundlegende, weitreichende Umwälzung der menschlichen Zivilisation schlechthin verstanden werden. Als solche ist sie kulturgeschichtlich ohne Parallele. Binnen weniger Jahrzehnte hat sie nahezu sämtliche privaten wie öffentlichen Lebensbereiche von Grund auf verändert, weltweit, mit zunehmender Entwicklungsgeschwindigkeit, ohne daß sich ein Ende abzeichnen würde und ohne daß ihre langfristigen gesellschaftlichen Folgen klar absehbar wären. Mit ihr verbinden sich zudem viele Erwartungen und utopische Hoffnungen auf eine technisch, wirtschaftlich und politisch „globalisierte“ Welt, die im Feuilleton dann vollends zur „Weltgemeinschaft“ hochstilisiert wird.

Bei Licht besehen gibt jedoch die rasante informationstechnologische Umgestaltung weiter gesellschaftlicher Lebensbereiche zu utopischen Erwartungen keinen Anlaß. Wie die alltäglichen, ausufernden Fälle der Internetkriminalität, des sogenannten *computer hakking* und die zahllosen Techniken des „Informationskriegs“ zeigen, haben sich Leistungs- und Mißbrauchspotentiale der modernen Informations- und Kommunikationssysteme im Gleichschritt entwikkelt. Hinzu tritt eine weitere, nahezu unbemerkte politische Folge des informationstechnischen Wandels: Er hat einen Aspekt der Po-

litik und internationalen Sicherheit als höchst lebendig, modern und wirksam erwiesen, den viele in der aufgeklärten, wissenschaftlich-technisch fundierten Gesellschaft längst für überwunden glaubten. Es ist dies die wachsende Bereitschaft wirtschaftlicher und politischer Konkurrenten und Gegner, gesellschaftliche Konflikte mit allen verfügbaren Mitteln, rücksichtslos und jenseits jeglicher rechtlicher Schranken auszutragen – eine Bereitschaft, für die die vielgelobte „Anarchie des Internets" als Zustandsmerkmal des Informationszeitalters vielfache Anreize geschaffen hat. Ob der Rechtsstaat und die internationale Sicherheitspolitik im Verein mit Sicherheitstechnik und -wissenschaft diese Anreize jemals werden wirksam unterbinden oder zumindest einschränken können, ist keine Frage, über die man in der sicherheitspolitischen Zunft noch lange streiten sollte. Sie ist längst entschieden. Denn es ist davon auszugehen, daß sich auch Staaten durch elektronische Spionage, Sabotage und Überwachung des weltweiten Datenverkehrs selbst am Informationskrieg in dem Maße beteiligen, in dem sie im Konfliktfall hierin einen politischen oder wirtschaftlichen Vorteil sehen und im Übrigen der technische Entwicklungsstand sie und ihre Nachrichtendienste hierzu in die Lage versetzt.

Eine Ausnahme bietet hierbei allenfalls die Bundesrepublik Deutschland. Ihr sicherheitspolitisches Handeln orientiert sich von jeher weniger an der Äußerung und Durchsetzung der eigenen Interessen denn am *Appeasement* gegenüber dem Konkurrenten oder Gegner im Fall eines Interessenkonflikts. Beschwichtigung des Gegners ist jedoch keine erfolgreiche sicherheitspolitische Strategie. Sie beruht auf dem naiven Glauben, fremden politischen oder wirtschaftlichen Interessen nicht mit wirksamen Abwehrmaßnahmen, sondern mit voreiligen, einseitigen Zugeständnissen oder gut gemeintem, frommem Zureden begegnen zu können. Daß dieses

Vorgehen weniger eine Abschreckung denn eine Einladung an den Gegner bewirkt, seine Konfliktbereitschaft weiter zu steigern, zeigen insbesondere die technischen Mittel und Möglichkeiten, die der Informationskrieg bereitstellt, und die Anreize, sich ihrer angesichts der Anarchie des Internets weithin unentdeckt und ungestraft zu bedienen. Kurz, die wirtschaftlichen und technischen Leistungen der Informationsgesellschaft machen diese gleichzeitig anfällig gegenüber den Bedrohungen der Informationstechnik.

Die paradoxen Folgen dieser Entwicklung sind weder in der Theorie unbekannt noch in der geschichtlichen Erfahrung neu. Der englische Philosoph Thomas Hobbes hat bereits zu Beginn des Aufklärungszeitalters darauf hingewiesen, daß ein herrschaftsfreier Raum typischerweise als Schauplatz des „Krieges aller gegen alle“ dient. Hobbes vertrat die Auffassung, daß es kein vernünftiges Mittel gibt, diesen Krieg in einer herrschaftsfreien Gesellschaft zu verhindern. Sollte die hobbessche These auch auf die Informationsgesellschaft zutreffen, ist es wichtig, hierin eine Frühwarnung zu erkennen. Naiv ist es jedenfalls, im Internet eine „Weltgemeinschaft“ am Werk zu sehen, von der man glauben darf, daß sie in Bezug auf Datenschutz und Informationssicherheit nur lautere Absichten hegt.

2. Informationstechnik und Informationsgesellschaft

Rein theoretisch gesehen ist das Internet zwar weder ein rechts- noch ein herrschaftsfreier Raum. Der Betrieb und die Nutzung moderner elektronischer informations- und kommunikationstechnischer Systeme, allen voran des Internets, unterliegen – wie der Gebrauch herkömmlicher Technologien auch – der staatlichen Gesetzgebung und zahlreichen internationalen Regelungen. Flugverkehr, Schiffahrt, Funk- und

Telephonverkehr sind längst bekannte Beispiele für die politischen und sozialen Regelungsgebiete der Technik. Praktisch weist die moderne elektronische Kommunikation jedoch eine Reihe neuartiger technischer Merkmale auf, die eine wirksame rechtliche und politische Regelung ihrer Nutzung systematisch erschweren oder gar unmöglich machen. In dieser Beziehung trifft die Metapher von der Anarchie des Internets zu.

Kritisch an dieser Situation ist, daß die neuartigen Technologien keineswegs nur zum vertraulichen, wirtschaftlich effizienten, von gesetzlicher und bürokratischer Behinderung befreiten Datenverkehr genutzt werden. Die erste Erfindung nach der Erfindung des Internets war die der Internetkriminalität, und man fragt sich, was an ihr mehr hervorsticht, der Ideenreichtum, das technische Können oder die kriminelle Energie ihrer Protagonisten. Im Internet als dem Exerzierfeld des autonomen, nicht länger fremdbestimmten und staatlich schwierig zu kontrollierenden menschlichen Handelns zeigen sich praktisch kaum eingrenzbare Probleme und Herausforderungen für Wirtschaft, Gesellschaft und Sicherheitspolitik.

3. Neuartige Merkmale der Informationstechnik

Die digitale Kodierung oder kurz „Digitalisierung“ von Daten und Nachrichten ermöglicht eine radikale Vereinfachung und Vereinheitlichung sämtlicher Formen der Kommunikation, der Signalübertragung und Information: Bildliche, schriftliche, akustische, elektromagnetische usw. Darstellungen werden nur mehr mittels zweier Symbole, d. h. in einem Alphabet mit nur zwei Buchstaben niedergelegt. In allen Übertragungs- und Datenspeichermedien bleibt ein Text aus diesen Symbolen immer der gleiche. Seine Übertragung in andere Nachrichtenmedien besteht einzig in einem buchstabenge-

treuen Kopiervorgang, die Notwendigkeit der Textübersetzung und erst recht der Textinterpretation entfällt für den technische Vorgang der Nachrichtenübertragung. Grundsätzlich wird hiermit die Kopplung („Vernetzung“) aller technischen Systeme weltweit ermöglicht, nicht nur die Vernetzung nachrichtenverarbeitender Systeme („Internet der Dinge“, „Industrie 4.0“ u. a. m.).

Darüber hinaus entstehen Möglichkeiten der Vernetzung sämtlicher individueller, privater und öffentlicher Lebensbereiche, ebenso der dauernden Wechselwirkung zwischen ihnen. Dies gilt jedenfalls insoweit, als sich gesellschaftliche Beziehungen und Systeme auf technische Betriebsmittel stützen. Diese Systeme werden für praktisch jedermann vergleichsweise leicht zugänglich, sind auch aus der geographischen Distanz heraus angreifbar, während der Angreifer verdeckt und anonym bleibt und daher für die Strafverfolgung schwierig zu ergreifen ist. Die Folgen sind globale Formen des gesellschaftlichen Zusammenlebens und der Kooperation, aber auch des Konflikts bis hin zum mehr oder weniger totalen Informationskrieg.

4. Verwundbarkeit der Informationsgesellschaft

Virus-Angriffe auf elektronische Informationssysteme gehören heute zum Alltag im Internet, wenn sie auch nicht immer gleich weltweit Schäden verursachen. Umgekehrt sind Computersabotage, -spionage und Verletzungen des vertraulichen Datenverkehrs bei weitem nicht auf die Computerviren und die Angriffe der *computer hacker* mittels verdeckter, schädlicher Manipulationen von Rechnern, Netzwerken, Datenspeichern usw. beschränkt. Mit dem Ausbau der elektronischen Daten- und Telekommunikationsnetze haben sich vielmehr auch die politischen und wirtschaftlichen Konfliktpo-

tentiale und Mittel zur Konfliktaustragung in der zivilisierten Welt tiefgreifend verändert.

Von zentraler Bedeutung ist, daß die internationalen Beziehungen im Informationszeitalter weitreichenden, bisher unbekannten Gefährdungen ausgesetzt sind. Die neue sicherheitspolitische Lage ist dadurch gekennzeichnet, daß Handlungsfähigkeit und Überleben eines Staates oder Bündnisses in internationalen Krisen und Konflikten nicht mehr nur durch militärische Gewalt gefährdet sind, sondern zunehmend auch vom störungsfreien Betrieb staatlicher und internationaler Informations- und Kommunikationssysteme abhängen. Dies gilt insbesondere für die öffentlichen, informationsabhängigen Infrastrukturen der modernen Gesellschaft: Tansport und Verkehr, Nachrichten- und Kommunikationswege, das öffentliche Gesundheitswesen, Staat und Verwaltung, Wirtschaft, Banken und Finanzsysteme.

Zwar ist die moderne Gesellschaft ganz allgemein auf die uneingeschränkte Verfügbarkeit ihrer technischen Betriebsmittel angewiesen und bedarf daher aufwendiger Schutzmaßnahmen gegen technische Störfälle, Naturkatastrophen und gezielte (Zer-)Störungsakte beispielsweise krimineller oder terroristischer Art. Doch digitale Datennetze, allen voran das Internet, sind über weite Strecken öffentlich und anonym zugänglich, weltweit verknüpft und gegen den politisch oder kriminell motivierten Mißbrauch kaum ausreichend zu schützen. Insbesondere erweist es sich immer wieder als überraschend leicht, die Vertraulichkeit, Verfügbarkeit und Unverfälschtheit der übermittelten Daten zu verletzen. Die Verwundbarkeit des Datenverkehrs überträgt sich auf alle gesellschaftlichen Lebensbereiche, die elektronisch vernetzt sind und sich in ihrer Funktionsweise auf die ungestörte digitale Informationsverarbeitung stützten.

Zu den Folgen der elektronischen Vernetzung kommt der rasante informationstechnische Fortschritt, mit dem die Gesetzgebung und Strafverfolgung auf den Gebieten des Datenschutzes und der Informationssicherheit nicht Schritt halten können. In den internationalen Beziehungen, aber oft genug auch im Bereich der inneren Sicherheit, vollzieht sich praktisch der informationstechnische Wandel daher über weite Strecken in dem bereits erwähnten rechts- und herrschaftsfreien Raum, der „Anarchie des Internets".

Die zentrale Rolle der Informationstechnik legt es nahe, daß die von Konkurrenten und Gegnern genutzten Daten und Netze als Angriffsziele auf den globalen Märkten, aber auch bei internationalen Konflikten dienen. Denn computergestützte Angriffe, die sich gegen die Infrastruktur eines Landes richten, können militärische Gewaltanwendung sowohl unterstützten und ergänzen als auch um völlig neue Elemente erweitern, wenn nicht gar als Konfliktmittel ersetzen oder ganz erübrigen. Bedrohungen vom Typ des „Informationskriegs" gehen hauptsächlich von fremden Nachrichtendiensten, der militärischen aber auch der nichtmilitärischen Aufklärung und Sabotage, der internationalen Wirtschaftskriminalität sowie vom politisch motivierten Terrorismus aus. Zu nennen ist hier eine bunte Mischung aus politisch-weltanschaulichen Gruppen, Internetplattformen (etwa den bekannten „Wiki-leaks"), Aktionsbündnissen, *hacker*-Organisationen und vielen anderen mehr.

Für die Sicherheitspolitik liegt das Hauptproblem darin, daß die Verletzlichkeit der Informationsgesellschaft Angriffsflächen bieten, die sich bei internationalen Krisen und Konflikten von außen leicht nutzen lassen. Daher gibt es auch im Unterschied zu herkömmlichen Formen gewaltsamer internationaler Konflikte bei Angriffen von der Art des „Informationskriegs" kein geschütztes Staatsgebiet

mehr, das an seinen Grenzen mit militärischen Mitteln erfolgreich zu verteidigen wäre. Hinzu kommt, daß Frühwarnung, Abschreckung und Vergeltung bei elektronischen Netzangriffen wenig wirksam sind, da der Angreifer im Internet kaum jemals „dingfest" zu machen ist.

Sicherheit und Verteidigung der Informationsinfrastrukturen eines Landes sind Aufgabengebiete, die mit der globalen Vernetzung zunehmend der Kontrolle des einzelnen Staates entgleiten. Weltweite Nachrichtennetze greifen nach Aufgabestellung und Reichweite über alle herkömmlichen Gebiete der internationalen Politik und Beziehungen zwischen souveränen Staaten hinaus. Sie ermöglichen völlig neuartige Formen der internationalen Organisation und geben auch nichtstaatlichen Gruppen wirkungsvolle Mittel an die Hand, ihren Interessen über große räumliche Distanzen hinweg in kurzer Zeit international Aufmerksamkeit zu verschaffen. Das Spektrum der Möglichkeiten ist kaum begrenzt. Es reicht von grenzenlosen, weltweit operierenden Wirtschaftsunternehmen über Nachrichtenmedien, Interessen- und Umweltschutzverbände vom Typ der *Non-Governmental Organizations* (NGOs) bis zum politischen Terrorismus. Die weitere Entwicklung und Globalisierung der elektronischen Informations- und Kommunikationssysteme wird nichtstaatliche Organisationen in ihrer Fähigkeit zum organisierten Konfliktaustrag gegenüber Staaten auch in Zukunft wesentlich begünstigen.

Beispiele hierfür liefern seit vielen Jahren die internationalen Oppositionsbündnisse der „Globalisierungsgegner" gegen Tagungen der Welthandelsorganisation, der Weltbank und des Internationalem Währungsfonds sowie der sogenannten G7-, G8- und G20-Gipfeltreffen. Die gewalttätigen Aktionen werden von weltweit verstreu-

ten Gruppen über die elektronischen Medien vorbereitet und koordiniert.

Ähnlich verhält es sich mit dem informationsgestützten politischen, wirtschaftlichen und sozialen Einfluß einzelner Personen. Durch den gezielten Einsatz der elektronischen Nachrichtentechnik kann der Einfluß des Individuums in den unterschiedlichsten sozialen Rollen (Führer, Mitglied, Dissident einer Gruppe), Institutionen (Regierungen, Parteien, politische, soziale oder weltanschauliche „Bewegungen") oder Tätigkeitsfeldern (Wirtschaft, Medien, mediengesteuerte öffentliche Meinung) weltweit verstärkt und auf das Gebiet der internationalen Beziehungen ausgedehnt werden. So kann beispielsweise eine einzelne Person elektronische Postwurfsendungen vom Typ der *spam mails* dazu benutzen, mit dem geringstmöglichen Aufwand politische und weltanschauliche Agitation in milliardenfacher Vervielfältigung binnen weniger Stunden weltweit zu verbreiten – im Bedarfsfall völlig anonym und gegen den Widerstand aller nur denkbaren staatlichen und internationalen Einrichtungen.

Besonders kritisch für die Vertraulichkeit des elektronisch gestützten Daten- und Nachrichtenverkehrs ist die Rolle der „Innentäter". Unter Innentätern versteht man Mitarbeiter daten- und nachrichtenverarbeitender Systeme, die, dienstlich bedingt, Zugriff auf die zu verarbeitenden Informationen haben, diese unbemerkt kopieren und an außenstehende Auftraggeber oder Interessenten weiterleiten (verkaufen) können. Zumeist sind bei dieser Art des Verrats politische oder finanzielle Motive der Täter im Spiel. Auch für elektronisch hochgerüstete Systembetreiber, z. B. die Nachrichtendienste der Großmächte, bilden die Innentäter eine Schwachstelle, gegen die kaum ein „Kraut gewachsen" ist, das heißt die eine kaum auszu-

schaltende innere Bedrohung dieser Systeme selbst darstellen. Die weitreichenden Datenlecks, die sie in den letzten Jahren bei US-amerikanischen Behörden verursacht haben, heben die ganze Dramatik der Verwundbarkeit der Informationsgesellschaft hervor. Berühmt geworden sind insbesondere die Verratsfälle des NSA-Mitarbeiters Edward Snowden, des US-Soldaten Bradley Manning und ihrer internationalen Helfer in den Nachrichtenmedien (NSA ist der US-Geheimdienst National Security Agency). Sie haben amerikanische und britische Geheimdienste, aber auch die anderer Länder in einigen ihrer Kernaktivitäten weltweit bloßgestellt.

5. Politische Grundsatzfragen der deutschen Informationssicherheit

Die Bundesrepublik Deutschland, ihre Wirtschaftsunternehmen und ihre Bürger sind in vielen Bereichen Ziel von Datenschutzverletzungen in den elektronischen Medien und der Telephonüberwachung aus dem Ausland. Die Motive liegen weit verstreut, von der Wirtschaftsspionage bis hin zur politischen Überwachung und Manipulation des deutschen Verbündeten durch seine westlichen Partner. Vermutungen und Medienberichte hierzu wurden durch die Unterlagen des geflohenen NSA-Mitarbeiters Edward Snowden, aber auch bereits während vieler Jahren zuvor aus andern Quellen gespeist. Die Spitze des Eisbergs hat 2013 die Kontroverse um das Abhören von Telephongesprächen deutscher Bundeskanzler und Regierungsmitglieder durch amerikanische Geheimdienste sichtbar gemacht (der Fall „Merkelphone“).

Vieles, was hierzu in der Presse und im Internet im Einzelnen berichtet wurde, ist für Außenstehende kaum zu überprüfen. Aber jede Untersuchung und jede sicherheitspolitische Maßnahme der Bun-

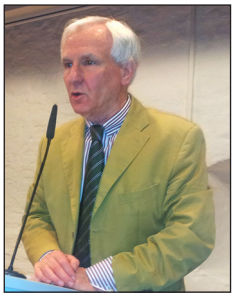
desregierung muß vernünftigerweise davon ausgehen, daß, wenn die technischen Möglichkeiten dazu bestehen, die amerikanischen, britischen und anderen westlichen Geheimdienste den Daten- und Nachrichtenverkehr auf deutschem Territorium elektronisch ausspionieren werden genauso wie russische oder chinesische Behörden oder ganz gemeine hacker, die privat auf eigene Faust aktiv sind. Presseberichten zufolge hat der damalige Kanzleramtsminister Roland Pofalla genau das bestritten. Im August 2013 berichtete er in Berlin, „sowohl der US-Geheimdienst NSA als auch der britische Geheimdienst hätten schriftlich erklärt, dass sie sich in Deutschland an Recht und Gesetz hielten und keine massenhafte Ausspähung betrieben“ (Wochenzeitung DIE ZEIT, 12. 8. 2013).

In Fachkreisen und den Medien ist über die Vorkommnisse und ihre Handhabung durch die deutsche Sicherheitspolitik viel debattiert worden. Der vorliegende Beitrag kann auf die breitgestreuten Befunde und die unterschiedlichen Einschätzungen, die sie erfahren haben, im Einzelnen nicht eingehen. Abschließend sind jedoch einige grundsätzliche Bemerkungen zum politischen Urteilshorizont der verantwortlichen Berliner Politiker und Parteien bei der Handhabung der Sicherheit der Bundesrepublik im Informationskrieg angebracht.

Ausgangspunkt sind die Erklärungen Roland Pofallas, mit denen der Kanzleramtsminister 2013 es in Abrede stellte, daß Deutschland von den Geheimdiensten einiger NATO-Partner routinemäßig ausspioniert wird. Diese Einschätzung der Sicherheitslage Deutschlands im Informationskrieg durch die Bundesregierung ist in einem Grade naiv, der an den elementarsten politischen Kompetenzen der Führung dieses Landes zweifeln läßt: Wenn ausländische Geheimdienste „schriftlich“ (!) erklären, daß sie in Deutschland nicht spio-

nieren, dann reicht das aus, ihnen zu glauben. Die Szene erinnert an das Märchen vom Wolf und den 7 Geißlein, in der der Wolf mit Kreide in der Stimme und einer weiß mit Mehl bestäubten Pfote junge Ziegen von der Lauterkeit seines Tuns überzeugt.

Eine professionell gehandhabte deutsche Sicherheitspolitik muß hingen davon ausgehen, daß fremde Geheimdienste sich nicht um deutsches Recht und die Gesetze scheren, wann immer sie einen Vorwand oder ein Motiv dafür haben. Sonst bräuchten sie erst gar nicht zu Mitteln der verdeckten Aufklärung zu greifen. Und weiterhin ist davon auszugehen, daß, wenn ein Geheimdienst ein Aufklärungsinteresse hat und über die technischen Mittel verfügt, sich die gewünschten Informationen zu verschaffen, wird er dies auch versuchen. Sonst könnte er sich den ganzen Spionageapparat und -aufwand sparen. Wohlgemerkt, es ist dabei nicht die Frage, ob die Bundesregierung oder der Bundesnachrichtendienst hierüber einen begründeten Verdacht oder sichere Informationen hat. Um eigene Abwehrmaßnahmen zu ergreifen, müssen sie im Zustand der Ungewißheit den Spionagefall annehmen, das heißt ihn hypothetisch voraussetzen und entsprechend planen und handeln – unabhängig davon, ob dieser Fall tatsächlich vorliegt. Mit Gewißheit vom Gegenteil auszugehen, daß nämlich der Geheimdienst eines verbündeten Landes dem deutschen Partner gegenüber keinen Vertrauensbruch begeht, wäre frommes Wunschdenken, das in der strategischen Analyse und sicherheitspolitischen Planung nicht nur nichts zu suchen hat, sondern eben für Deutschland sehr schädlich und im Zweifel brandgefährlich ist.



Gebhard Geiger, *Apl. Pof. Dr. phil. habil. Dr. rer nat.* Studium der Physik in Freiburg/Br., München und Cambridge/England. Mehrjährige Berufstätigkeit als Physiker an Forschungseinrichtungen im In- und Ausland. Zweitstudium der Politik und Philosophie in München und Los Angeles (UCLA). MA in Politischer Wissenschaft (UCLA) und Habilitation in Philosophie (Wissenschaftstheorie, Methodologie) an der Technischen Universität München (TUM). Langjährige Forschungs- und Lehrtätigkeit an der TUM auf den Gebieten der Methodologie der interdisziplinären Forschung, speziell der Risiko- und Sicherheitsforschung mit technischen und sozialwissenschaftlichen Anwendungen.