

TERROR, CYBER-SECURITY, ETHIK UND FREIHEIT

Nikolaus Schatt

Lehrstuhl für Philosophie und Wissenschaftstheorie, Technische Universität München
Arcisstraße Nr. 21, D 80333 München, DE
nikolaus.schatt@tum.de

Schlagnote: *Terror, Sicherheitsataken, Cyber-Security, Ethik, Freiheit, Normen, Technik, Wissenschaftsphilosophie*

Abstract: *Terror und Angst lösen Forderungen nach mehr Sicherheit und Machtbefugnissen aus. Sicherheitsataken und Cyber-Security stehen für Probleme in der IKT-Welt. In Debatten werden wirksamere Abwehr-Maßnahmen bei immer kürzeren Entscheidungsfristen, Verschärfung von Normen und eine utilitaristische Sichtweise gefordert. Neue Grenzen stehen ethischen Grundsätzen (Freiheit, Rechtsphilosophie) gegenüber. Welche Argumentationen stehen für Verschärfung bzw. Gegenmaßnahmen bzw. welche stützen ethische Grundsätze zu Freiheit und der unantastbaren Würde des Menschen?*

1. Einführung und Fragestellung

Terror, Cyber-Security, Ethik und Freiheit betreffen aktuell unsere Gesellschaft. Terror löst in immer kürzeren zeitlichen Abständen Angst in der Bevölkerung aus, Bürger fordern mehr Sicherheit, Machtbefugnisse bis hin zur nahezu totalen Überwachung oder zum Militäreinsatz im eigenen Land. Verschärfung von Normen steht ethischen Grundsätzen unter Bezug auf Freiheit und die unantastbare Würde des Menschen gegenüber. Sicherheitsataken in der IKT-Welt haben noch im 20. Jahrhundert die breite Bevölkerung kaum tangiert. Durch vielfältige Einsatzgebiete der IKT, deren Einsatzverbreitung und die Digitalisierung der Gesellschaft nimmt die Bedeutung von Cyber-Security für Alle zu. Analysen zeigen gleichzeitig zunehmende Unwissenheit und wachsende Risiken. Die folgende Betrachtung der Cyber-Security konzentriert sich auf Szenarien und Randbedingungen des Terrors im Werte-Umfeld von Ethik und Freiheit.

2. Forderungen in der Gesellschaft und deren Grenzen

2.1. Herausforderungen der Gesellschaft

In Ergänzung der methodologischen Analyse zur Cyber-Security [vgl. SCHATT, IRIS 2016] konzentriert sich diese Arbeit auf Fragen der Gesellschaft zum weltweiten Terror in Verbindung mit Cyber-Security. Einer legitimen Verschärfung von Sicherheitsmaßnahmen stehen ethische Grundsätzen gegenüber. Das heutige Verständnis von Werten, Ethik, Normen, Freiheit und Würde des Menschen basiert auf philosophischen Sichtweisen der westlichen Welt. Die Gedanken reichen zurück in die Antike und finden sich beispielsweise in den Dialogen des Sokrates bei Platon, bei Aristoteles oder in Analysen zum Zusammenhang mit der römischen Verfassung [vgl. POLYBIOS 1861, Buch VI]. Sie sind Grundlage der Weiterentwicklung¹ in Mittelalter, Renaissance und Aufklärung. Auf Ethik wird in der Diskussion oft verwiesen, doch welche Ethik ist gemeint?

Die *formale Ethik*² beschreibt nach NOACK [2009, 12] nicht den Inhalt des menschlichen Handelns, sondern dessen Form. Die philosophische Interpretation hinterfragt die Orientierung des menschlichen Handelns, bei-

¹ Dazu sei an Arbeiten von William Occam, Niccolò di Bernardo di Macchiavelli, John Locke, Thomas Hobbes oder Adam Smith erinnert.

² Die formale Ethik findet sich bei Thales von Milet (625–545 v. Chr.). Er berechnete 585 v. Chr. die Sonnenfinsternis und zog einen neuen Schluss aus dieser Entdeckung. Aus der Berechnung der Sonne folgerte er, der Mensch denkt selbst, unabhängig vom Staat, der Religion und den Priestern [MANSFELD 1983, 44–55].

spielsweise bei Thales von Milet, «indem wir niemals das tun, was wir an anderen verurteilen». Sophisten und deren Vertreter Protagoras³ leiten als Grundprinzip ab «Der Mensch bestimmt also das Dasein und Sosein der Dinge». Somit kann jeder die Wirklichkeit erschaffen, wie sie ihm günstig ist, der sittliche Maßstab sei der Nutzen [VORLÄNDER 1969, 50–60]. Immanuel Kant begründet die Formalethik über das erkennende und handelnde Wesen Mensch, welches aus seinem eigenen Inneren seine nicht allgemeingültige Wertesubstanz⁴ bzw. Maxime ableitet. Kategorische Forderungen kommen bei Kant aus der reinen Vernunft, haben zwingenden Charakter und liefern das «So ist es». Die Gesetze der praktischen (handelnden) Vernunft haben fördernden Charakter und vermitteln das «So sollst du handeln». Kant sucht eine allgemeine Verbindlichkeit, und formuliert sein Prinzip «Handle so, dass die Maxime (Wünsche, Nutzen) deines Willens (Handelns) jederzeit zugleich als Prinzip einer allgemeinen Gesetzgebung gelten könne». Er verbindet das individuelle Handeln mit Allgemeingültigkeit und Pflicht. Formalethik wird als allgemeingültig betrachtet, verbunden mit wenig Aussagen, wie der Mensch konkret handeln soll [vgl. KANT 1924, 20–207]. Hans Jonas hat den Kant'schen kategorischen Imperativ mit seinem «Prinzip Verantwortung» weiterentwickelt⁵, vom «Prinzip Furcht» zur «Pflicht des Handelns» um Sorge und Verpflichtung⁶ für die Zukunft abgeleitet [JONAS 1984, 390 ff.].

Die *materiale beschreibende Wertethik* basiert auf Gedanken von Sokrates⁷, und begründet den Vorrang des Individuums. Die Wertethik von Platon formuliert den Gegenentwurf zur Sophistik. Platon gliedert die Wirklichkeit in drei Welten [PLATO, Politeia 509 c–510 e; 514 a–527 c] Immanenz⁸, Transzendenz⁹ und göttliche Welt (dem Einen, Unveränderlichen, dem Guten). Sittliche Grundsätze (als Elemente des Transzendenten) sind nicht in der empirischen Welt und Ideen sind nur dann sittlich, wenn sie am Guten teilhaben. Sie entzieht sich der Willkür des Menschen. Sie existieren unveränderlich in Ewigkeit als eine objektive Ethik. Aristoteles fügte diese Welten Platons als eine Einheit vom materiellem Ding und geistiger Form teleologisch zusammen [vgl. VOLLRATH 1978, 84–128] und vermittelt Handlungswerte wie vernunftgemäßes Verhalten, Triebe und Begierden zu beherrschen, Vernunft selbst zu entwickeln und zu stärken, also alle Extreme zu meiden und die gesunde Mitte einzuhalten. Diese Form der Ethik löst sich von der Willkür des Einzelnen, schließt den Wert und die Würde des Menschen ein und ist allen Mächten und Institutionen der Welt vorgeordnet¹⁰.

Der *Norm*-Begriff wird von Noack in die Sozialphilosophie und Soziologie¹¹ verortet. Er verweist auf eine zentrale Stellung bei Talcott Parsons «Theorie des sozialen Handelns». Der Einzelne hat Normen als verallgemeinertem Erwartungsmuster zu folgen, normenwidriges Verhalten wird sanktioniert und bestraft [vgl. PARSONS 1949, 46 f.; NOACK 2009, 11]. Normen bieten Orientierung, stabilisieren die Gesellschaft und geben der

³ Protagoras formulierte den Homo-Mensura-Satz, der Mensch ist das Maß aller Dinge [DIETZ 1976].

⁴ Dies wird durch das Bemühen gekennzeichnet, ein summum bonum, einen höchsten Wert und den Weg dorthin zu finden [vgl. NOACK 2009, 12; KANT 1924, 20–207; UEBERWEG 1924, 547–606].

⁵ Jonas spricht vom «wachsenden Bereich kollektiven Tuns, in dem Täter, Tat und Wirkung nicht mehr dieselben sind» [JONAS 1984, 26].

⁶ Jonas spricht dabei von der «Heuristik der Furcht» und von der «Theorie der Ethik» als «bescheidenes Ziel der Verantwortung für die Zukunft des Menschen» [JONAS 1984, 392/392].

⁷ Platon beschreibt dazu im Dialog Nomoi von Sokrates den Deus-Mensura-Satz (Gott (Ideen) ist das Maß aller Dinge): «Alle Sittlichkeit ist in mir, aber es ist die Stimme des Gottes in mir, der das Maß aller Dinge ist. Gott in mir ist allen Priestern und Herrschern, ja der gesamten Gesellschaft vorgeordnet» [vgl. PLATON, Apologie 31c–32 a; PLATON, Nomoi 716c4f; PLATON, Kratylos, 385e–386e; FINK 2007, 261].

⁸ Diese Immanenz ist gekennzeichnet durch die wahrnehmbare, die raumzeitliche Welt, mit Naturgesetzen, Koexistenz (räumliches und strukturiertes Nebeneinander) und Sukzession (zeitliches Nacheinander) und durch Werden und Vergehen [vgl. NOACK 2009, 15].

⁹ Die Transparenz ist charakterisiert als denkbare Welt der Begriffe und Ideen, also raum- und zeitlos, immateriell und seiend und mit übergreifenden Begriffen zu der erfahrbaren Welt; allerdings sind die Ideen auf die göttliche Welt ausgerichtet [vgl. NOACK 2009, 16].

¹⁰ Das bedeutendste Beispiel ist die Charta der Menschenrechte mit ihren 30 Artikeln «als das von allen Völkern und Nationen zu erreichende gemeinsame Ideal» [VEREINTE NATIONEN 1948].

¹¹ Begründung zum Normenbegriff vgl. Émile Durkheim, Georg Simmel, Ferdinand Tönnies [NOACK 2009, 11].

Gesamtheit Schutz. Die römische Verfassung ist als erfolgreiche Basis verschiedenster Regierungsformen beschrieben [vgl. POLYBIOS 1861, 647 ff.]. Als Kehrseite von Normen wird betont, dass sie persönliche Freiheit durch soziale Kontrolle einschränken und durch Sanktionen eine selbstständige Ethik unterbinden. Normen haben sich im Gegensatz zu Werten ständig verändert [NOACK 2009, 24]; was zur Frage nach ihrer Legitimität zwischen Konsens in der Gesellschaft und Durchsetzung der Norm führt [vgl. LUHMANN 1969, 27 ff.]. Eine Herausforderung unserer Gesellschaft liegt in der Suche nach der legitimen Balance zwischen Beibehaltung ethischer Grundsätze (Freiheit und unantastbare Würde des Menschen) und Abwehr von Terror und Kriminalität. Jede Verschärfung der Normen stößt auf Grenzen (z.B. in Deutschland im Grundgesetz formuliert), deren Aufhebung öffentlich kontrovers¹² diskutiert wird; einer Einführung utilitaristischer Sichtweisen widersprechen ethische Grundsätze von Freiheit und Ausprägungen der Rechtsphilosophie.

2.2. Aktuelle Entwicklung digitaler Grundrechte

Gedanken von Hans Jonas öffnen die Diskussion zur Einbeziehung der Ökologie mit Bezug auf *Resilienz*, *Reliability* und *Sustainability*¹³. Das Universum als gesamthafte Environment und Lebensraum des globalen Menschen wird im Rahmen der Digitalisierung zum Betrachtungshorizont der Weiterführung des «Prinzip der kritischen Vernunft» [JONAS 1984]. Dies führt zur Einbeziehung digitaler Daten in einem neuen kategorischen Imperativ. Diesen Weg beschreitet die neue Initiative¹⁴ *Digital Charta* in der EU, die in 23 Artikeln digitale Grundrechte für alle Bürger fordert [DIGITAL CHARTA EU 2016]. Deren Präambel stellt das Bewusstsein um «Anerkennung der angeborenen Würde und der gleichen und unveräußerlichen Rechte aller Menschen die Grundlage von Freiheit, Gerechtigkeit und Frieden in der Welt» voran; aus der «zunehmenden Digitalisierung» folgen «Veränderung der Grundlagen» und «Machtverschiebungen zwischen Einzelnen, Staat und Unternehmen». Auf Basis einer «zivilgesellschaftlichen Debatte» werden Forderungen für «Grundrechte und demokratische Grundprinzipien im digitalen Zeitalter» formuliert [DIGITAL CHARTA EU 2016]. Eine *Charta zur digitalen Vernetzung* hat der deutsche nationale IT-Gipfel als übergeordnete Grundlage initiiert¹⁵. Die darin niedergelegten zehn Grundsätze zur digitalen Vernetzung werden im wissenschaftlichen Bereich¹⁶, durch Einrichtungen, Verbände und durch immer mehr Unternehmen unterzeichnet. Diese regeln gesellschaftliche und wirtschaftliche Potenziale zum Umgang mit Daten, zur diskriminierungsfreien Teilhabe, Bildung und Qualifikation sowie zum gemeinsamen Dialog von Wirtschaft, Wissenschaft, Politik und Zivilgesellschaft [vgl. CHARTA DIGITALE VERNETZUNG 2016]. Eine weitere *Charta for the Digitally Connected World* haben im April 2016 die ICT Minister¹⁷ der G7 als international verabschiedet; sie sprechen sich u.a. gegen eine schärfere staatliche Regulierung des Netzes, für freien Informationsfluss und für einen Internet Governance Prozess aus [vgl. G7 CHARTER FOR THE DIGITALLY CONNECTED WORLD 2016].

Diese drei Initiativen fordern übergreifend eine Erweiterung verbindlicher Grundregeln bei der Digitalisierung der Gesellschaft. Der Bezug zur Cyber-Security ergibt sich in allen o.g. Papieren. beispielsweise ist im vierten Punkt der nationalen Charta Digitale Vernetzung formuliert: «Wir sind uns der Verpflichtung bewusst, mit personenbezogenen Daten und Informationen datenschutzgerecht und sicher umzugehen. Dies gewährleisten wir durch effektive technische und organisatorische Maßnahmen zum Schutz vor unberechtigtem Zugriff und missbräuchlicher Verwendung. Wir sehen ein einheitliches europäisches Datenschutzrecht als wichtige Rah-

¹² Beispielsweise steht der Forderung nach ausreichender Beteiligung der Legislative bei jeder einzelnen akuten Entscheidung der dazu erforderliche Zeitbedarf gleichzeitig immer kürzer werdenden Entscheidungsfristen entgegen.

¹³ Hier steht *Resilienz* für Widerstandsfähigkeit und Fähigkeit zur Krisenbewältigung und Weiterentwicklung, *Reliability* für Zuverlässigkeit und *Sustainability* für Nachhaltigkeit.

¹⁴ Diese Initiative hat 2016 das Papier dem Europäischen Parlament in Brüssel und der Öffentlichkeit zur weiteren Diskussion übergeben.

¹⁵ Schirmherrschaft durch den deutschen Wirtschaftsminister [vgl. CHARTA DIGITALE VERNETZUNG 2016].

¹⁶ Dazu gehört u.a. auch die acatech – Deutsche Akademie der Technikwissenschaften (auf der CEBIT 2016).

¹⁷ Deutschland war vertreten durch Staatssekretär Mathias Machnig (BMW).

menbedingung. Eine weitere internationale Harmonisierung rechtlicher Grundlagen muss zügig angegangen werden» [CHARTA DIGITALE VERNETZUNG 2016]. Entsprechende Prinzipien finden sich in der Internationalen Charta der G7 unter den Punkten 8 bis 15 [G7 CHARTER FOR THE DIGITALLY CONNECTED WORLD 2016].

Die *Digital Charta* spricht nahezu alle Problemfelder der Cyber-Security an. Deren Diskussion ist in der EU angelaufen, die internationale Diskussion und Verabschiedung gemeinsamer Formulierungen für alle Menschen der Welt ist notwendig. Die aktuelle Diskussion in der EU kann die Meinungsvielfalt der Mitgliedsstaaten integrieren und bekommt durch die Wirtschaftsmacht der EU Gewicht. Die Vorschläge konkurrieren mit Forderungen nach Verschärfung bzw. Vereinheitlichung bestehender nationaler oder europäischer Gesetze. In der globalen IKT-Welt sind nationale und internationale Initiativen wichtig, um Restriktionen von Freiheit zu vermeiden; wie durch die drei genannten Initiativen bzw. weitere Beschlüsse propagiert.

2.3. Einordnung von Terror

Neue *große Kriege* zwischen Ost und West konnten durch das «Gleichgewicht des Schreckens» verhindert werden. Dies führte zur Stabilität im kalten Krieg und wurde mit spieltheoretischen Ansätzen¹⁸ analysiert und erklärt. Robert J. Aumann untersuchte mit Methoden der Ökonomie die Frage um Krieg und die Anreize, um diesen zu verhindern bzw. den Frieden zu fördern. Er verweist, «Krieg sei ein steter Begleiter der Menschen, ein Phänomen, nicht aber eine Serie von Einzelereignissen». Seine Frage «Weshalb zieht Homo economicus – der rationale Mensch – in den Krieg?», beantwortete er mit «Krieg sei rational. Es ist ein grosser Fehler, Krieg als irrational abzutun» [AUMANN 2005]. Doch der Mensch handelt nicht immer rational [vgl. SELTEN 1965].

Terror wird inzwischen oft mit dem Attribut *Krieg* versehen und hat einen fließenden Übergang zu Kriminalität. Martin Hoch spricht bei Terror vom *kleinen Krieg*¹⁹ und bemerkt, «diese sind nicht notwendigerweise «kleiner» als die großen Kriege, weder in ihrer Intensität, noch ihrer Dauer, noch ihrer Zerstörungskraft. Charakteristisch für die *kleinen Kriege* ist die Abwesenheit bzw. Durchbrechung verbindlicher Regeln für die Kriegsführung und die fehlende Unterscheidung²⁰ zwischen Kombattanten und Nichtkombattanten, dem Herzstück des modernen humanitären Völkerrechts» [HOCH 2002, 20]. Die enge Verwandtschaft zwischen Terror und Kriminalität wird durch Hoch bestätigt, der feststellt, dass dies «zunehmend auch auf zwischenstaatliche Kriege [zutrifft]. Eine enge Verbindung mit mehr oder minder organisierter Kriminalität – etwa dem Drogenhandel [...] – ist für den kleinen Krieg²¹ ebenfalls typisch²²». Charakteristischerweise finden diese Kriege nicht mehr zwischen regulären Armeen statt, es treffen in *kleinen Kriegen* reguläre Einheiten und Exekutiven auf nichtstaatliche Akteure, organisiert als Kleingruppen und Einzeltäter. Perfide ist, dass sich (wie Hoch feststellt) die aktuelle Form der kleinen Kriege jeglicher Regeln entledigt hat und die gesamte Welt unter diesem Terror leidet. Es kommen alle Mittel zum Einsatz, und in seiner Brutalität werden auch Nichtkombattanten, Zivilisten, Unbeteiligte, Freizeiteinrichtungen, Krankenhäuser, Kindergärten, Schulen, Alte, Frauen und Kinder einbezogen, gefoltert, getötet und in ihrer Gesamtheit zum Feindbild erklärt. Dieser Mitteleinsatz erinnert an Phänomene des totalen Krieges²³ und an die Wiederkehr von Kriegsformen des Mittelalters [HOCH 2002]. Krieg, Terror und Kriminalität lösen mit ihrem Auftreten in immer kürzeren zeitlichen Abständen zunehmend Angst, den Wunsch nach besserem Schutz aber auch Widerstand gegen den Terror in der Bevölkerung aus.

¹⁸ Im Rahmen der Spieltheorie sei hier auf die beiden Nobelpreisträger Reinhard Selten mit seinem Konzept des «teilspielperfekten Gleichgewichts» [SELTEN 1965] und auf Robert J. Aumann mit seiner Erklärung von Krieg und Frieden verwiesen [AUMANN 2005].

¹⁹ Der Begriff des «kleinen Krieges» geht auf Carl von Clausewitz in Abgrenzung zu den zwischenstaatlichen «großen Kriegen» zurück [vgl. CLAUSEWITZ 1966, 208–599]. Der Begriff *Guerilla* steht für eine dieser Ausprägungen.

²⁰ Deshalb trifft für den kleinen Krieg der Begriff des «nicht-trinitarischen Krieges» zu, der die Unterscheidung zwischen Regierung, Streitkräften und Bevölkerung in modernen Staaten charakteristische Unterscheidung nicht kennt [CREVELD 1991, 35–62].

²¹ Synonyme Begriffe sind «lowintensity conflicts», «asymmetrische Kriege», «Partisanenkriege», «Guerillakriege» [HOCH 2002, 21] sowie «postnationaler Krieg» [BECK 1999, 984–990] und «neo-hobbesscher Krieg» [TROTHA 1999, 71–95, dort 92].

²² Ein Bezug zur Kriminalität als Strukturmerkmal im operativen Umfeldes westlicher Militäreinsätze im 21. Jahrhundert findet sich bei HILLS [2000].

²³ Vgl. KEELEY [1996, 175–176] oder TROTHA [1999, 75–79] sowie FÖRSTER [1999, 12–29, dort 13–14 und 29].

2.4. Auswirkungen auf die IKT

Anwendungen der IKT bekommen im Krieg, bei Terror und in Kriminalfällen immer mehr Bedeutung sowohl zur Unterstützung und Durchführung von Terror-Aktionen als auch bei Gegenaktionen, Spionage und Aufklärung. Zielgebiete der Angriffe betreffen das tägliche Leben, die Wirtschaft und die öffentliche Infrastruktur. Angriffe und Analysen reichen über die klassische IKT in alle gesellschaftlichen und politischen Bereiche. Die Bandbreite reicht über Verdachtsmomente einer gezielten Wahlbeeinflussung in USA mit Big Data Methoden über Robotik, Methoden von Artificial Intelligence (AI) und Missbrauch der Industrie 4.0. Die Weiterentwicklung der IKT-Technologien mit immer kleineren smarten Komponenten bis hin zu autonomen Systemen wie in Fahrzeugen, Drohnen bis zu soziotechnischen Systemen öffnet neue Risikofelder. Nach der Sicherheit in der klassischen IKT-Welt im 20. Jahrhundert verändert sich dies für die Bevölkerung mit den vielfältigen und zunehmenden Einsatzgebieten der IKT stark. Verbindungen in der IKT-Welt sind für alle Beteiligten sehr wichtig; es werden vielfältige Systeme der IKT, vor allem das Internet und das *darknet*²⁴ durch Angreifer genutzt. Aufgabenbereiche von Cyber-Security erweitern sich auf die vielen kleinen und im Regelfall bisher ungeschützten smarten Komponenten und unkontrollierter Zugriffe, Fehlnutzung und Manipulation.

Immer mehr Menschen fordern (durch Terror ausgelöst) zusätzliche Sicherheit; dies reicht bis zur totalen Überwachung und dem Militäreinsatz bei einer Terrorbedrohung. Geheimdienstliche Analysen sollen bereits im Vorfeld potentielle Angriffe erkennen sowie warnen. Der Exekutive sollen im Nachgang eines Terroraktes alle Auswertungen / Nutzungsdaten und nicht nur einzelne Beweisstücke zur Verfügung stehen. Ähnliche Forderungen stehen zur Verhinderung von organisierter Kriminalität und Verfolgung mafïöser Strukturen im Raum. Terror und Kriminalität sind nicht an nationale oder regionale Grenzen gebunden. Gegenüber dieser Beweglichkeit über staatliche Grenzen hinweg wirkt die Zusammenarbeit zwischen der Exekutive wie Polizei und Staatsanwaltschaften suboptimal. Ursachen finden sich in inkompatiblen Regeln, Datenstrukturen, Lücken im Datenaustausch und ineffektiven Kooperationen. Eine illegale Nutzung von IKT (durch Geheimdienste, kriminelle oder Terror- Organisationen) lässt sich in der Praxis nicht einschränken, bedingt durch die überregionale Verbreitung oder fehlende Auffälligkeit. Auf Grund der Eigennutzung und fehlendem Interesse (sich selbst zu blockieren) ist aber zu erwarten, dass aus diesen Kreisen keine generellen Attacken auf die globale IKT Infrastruktur erfolgen, aber spezifische Angriffe einzelner Stellen. Der technische Fortschritt und die nahezu überall mögliche Nutzung von IKT begünstigt nichtstaatliche kleinere Akteure und bietet diesen einen immer größer werdenden Hebel mittels Hacker-Angriffen. Das plakative Bild des Hackers, der «mit Laptop und Mobiltelefon am Pool eines Hotels in der Karibik, [...] die Wasserversorgung einer großen Stadt lahm legt» [Hoch 2002, 21] ist nicht mehr Science Fiction. Wenigen Personen ist es unter Zuhilfenahme moderner Technik und vergleichsweise kleinen Netzwerken möglich, einen Schaden anrichten, den man früher nur mit vielen Ressourcen staatlicher Einrichtungen erreichen konnte und das Risiko einer Enttarnung ist relativ gering, der physische Aufenthaltsort kaum ermittelbar oder angreifbar.

Lösungen über eine Cyber-Gegenstrategie stecken im Anfangsstadium. «Gegen diese Privatpersonen oder nichtstaatlichen Netzwerke [...] greifen] die klassischen Instrumente der internationalen Politik, die auf die Wirkung gegenüber Staaten optimiert sind (wie etwa Abschreckung durch die Drohung mit militärischer Macht), nicht mehr» [Hoch 2002, 21]. Er sieht als Gefahr, dass eine «Rückkehr des Mittelalters in der Sicherheitspolitik» durch die «zunehmende Privatisierung von Gewalt» zu einer «Auflösung des staatlichen Gewaltmonopols und das Nebeneinander bzw. die Konkurrenz staatlicher und nichtstaatlicher Machtausübung» führt. Weiter gibt es Risiken durch «eine Anzahl weiterer nichtstaatlicher Akteure, wie etwa global agierende Wirtschaftsunternehmen oder Nichtregierungsorganisationen, die aber als unmittelbar kämpfende Parteien in militärischen

²⁴ Das *darknet* basiert auf einem peer-to peer overlay network. In der Regel stellen die Nutzer die Verbindungen manuell her und damit ist deren Existenz nicht bekannt. Sie erhalten so ein höheres Maß an Sicherheit vor dritten Angreifern, denn neue Nutzer müssen quasi eingeladen werden. In diesem Netz haben sich beispielsweise Terroristen in Deutschland ihre Waffen besorgt. Im *darknet* werden Kontrollmöglichkeiten im Internet umgangen.

Konflikten (noch) nicht auftreten, auch wenn sie durchaus an Konflikten beteiligt sind bzw. auf diese Einfluss nehmen können» [HOCH 2002, 22]. Einflüsse von NGOs, Effekte der Digitalisierung wie bei Big Data, Risiken um die Berechenbarkeit der Welt und die neuen Entwicklungen von Analysemethoden nehmen stark zu. Es geht in der Cyber-Security um Verhinderung von Daten-Manipulationen im größeren Stil bzw. um deren Folgenvermeidung bei einzelnen Personen oder Gruppen. Ein neues Thema bekommt Bedeutung, die Übertragung klassischer Mobbing-Methoden in die sozialen Netzwerke (*Cyber-Mobbing*). Unliebsame Einträge bringen einzelne Personen in Misskredit; Betroffene erfahren nicht davon, wundern sich über geändertes Verhalten im sozialen Umfeld oder an der Arbeitsstelle; wogegen kaum etwas zu unternehmen ist, aber die Auswirkungen für die betroffene Person sind gravierend²⁵.

2.5. Prognosen, Vorsorge und Entscheidungen

Die Gesellschaft verändert sich durch Terror, Angst und Digitalisierung, die Berechenbarkeit von Verhaltensphänomenen mit Big Data. Dies führt zur Frage, ob unsere Zeit wirklich postfaktisch oder doch noch faktisch ist. Bedeuten heute noch Zahlen und Daten wirklich Fakten und Realität? Wir wissen wenig, «woher diese Datenströme kommen, wie sie entstehen und welche Gesetzmäßigkeiten ihnen zugrunde liegen» [MAINZER, 2014, 13]. Die manchmal so treffenden Zusammenhänge personalisierter Informationen muten merkwürdig an. Die Menschen sind sich nicht sicher, womit sie kontrollierbar und ihr Verhalten vorhersehbar werden.

Der Transhumanist Stefan Lorenz Sorgner setzt auf die «Vorzüge eines digital getunten Körpers» und verweist auf «die Verschmelzung von Mensch und Technik, [...], die bereits stattgefunden hat. Wir sind ja schon Cyborgs²⁶». Für Sorgner löst sich das vorherrschende christlich-kantische Menschenbild auf. Er verweist unter Bezug auf die deutsche Gesetzgebung, dass sich die «ontologisch-kategorial herausgehobene Sonderstellung des Menschen» ändern müsse, impliziert, nach «Darwin und Nietzsche ist diese metaphysisch-dualistische Anschauung nicht mehr haltbar» [INNERHOFER 2013]. Er stellt Grundrechte in Frage, geht davon aus, «Jeder kann für sich entscheiden, ob er eine Modifikation will oder nicht», gleichzeitig warnt er vor «totalitäre[n] Bevormundungs- und Überwachungsmechanismen, sei es von politischer wie industrieller Seite».

Diese Warnung stützt kritische Prognosen bei Martin Hoch, wonach es zur «*Vervielfältigung* der Konfliktszenarien [... kommen wird. ...]. Daneben wird es aber eine Vielzahl weiterer, asymmetrischer Konfliktszenarien geben, in denen nichtstaatliche Akteure eine zentrale Rolle spielen» [HOCH 2002, 23]. Er erwartet weiter, «dass durch die zahlenmäßige Zunahme von Akteuren das Geflecht der Beziehungen und Interaktionen in der internationalen Politik komplexer, und dadurch nicht zuletzt fehleranfälliger und weniger leistungsfähig werden wird. Dem Staat als bislang dominierendem Element des internationalen Systems ist [...] Konkurrenz durch inter- und supranationale Organisationen erwachsen. Für die Zukunft ist davon auszugehen, dass es auch im substaatlichen Bereich zu einer Zunahme von konkurrierenden Akteuren kommen wird. Die relative Dominanz der [nationalen] Staaten im internationalen System wird also abnehmen» [HOCH 2002, 33].

Seit den letzten Jahren verstärken sich nationalistische Tendenzen, die sich nicht mit digitalen Grenzen und Risiken in der Cyber-Security bei der gleichzeitigen Globalisierung der Bedrohungen decken. Die künftige Festlegung von Regeln²⁷, die bis dato bei kriegerischen Auseinandersetzungen galten, betrifft Unterschiede

²⁵ Diese Arbeitsfelder bieten sich an, um Anforderungen, Risiken und Verantwortung aus Betrieb und Einsatz in einer gesonderten Ausarbeitung näher zu betrachten.

²⁶ Sorgner setzt auf künftige Implantate, «um bei Bedarf eine neue Fremdsprache zu beherrschen oder auch als eine erweiterte Form des Gedächtnisses mit Zugriff auf das Wissen im Netz» und spricht vom «Cyborg-Enhancement» einer «Optimierung eines Organismus durch die Verschaltung mit digitalen oder mechanischen Maschinen [...] für einen kognitiv erweiterten Menschen» [INNERHOFER 2013].

²⁷ Vgl. Überblick zu gültigen Konventionen bei amnesty International [vgl. AMNESTY 2016] wie die Konvention über die Verhütung und Bestrafung des Völkermordes, Konvention über die Nichtanwendbarkeit von Verjährungsvorschriften auf Kriegsverbrechen und Verbrechen gegen die Menschlichkeit, Grundsätze für die internationale Zusammenarbeit bei der Ermittlung, Festnahme, Aus-

zwischen Terror-Regimes und Rechtsstaaten. Die Forderungen nach Verschärfung von Normen und einer Einführung einer utilitaristischen Sichtweise betreffen die rechtliche Grundlage zur gesellschaftlichen Vorsorge vor Angriffen und stehen ethischen Grundsätze der Freiheit und Kerngedanken in der Rechtsphilosophie gegenüber, wie etwa ob es legitim ist, einen Menschen oder eine Gruppe unbekannter Menschen zu opfern oder leiden zu lassen, um das Leben Einzelner oder gar Vieler zu schützen²⁸.

Die Art und Weise, wie Entscheidungen in der Cyber-Security zu treffen sind, ist individuell. Der Ernstfall ist für die einzelne Person bereits gegeben, wenn dessen persönliches IKT Umfeld betroffen und ausgefallen ist. Ein generell bedeutsamer Ernstfall betrifft große Versorgungsunternehmen der IKT und deren Services, etwa bei einem flächendeckenden Router-Ausfall, der nahezu das komplette Netzwerk lahm legt. Spezialisten im Unternehmen und Firmenleitung haben die notwendigen Entscheidungen zu treffen und sich mit wichtigen staatlichen Einrichtungen abzustimmen (gesetzliche Informationspflicht). Jeder Terrorangriff erfordert Entscheidungen, welcher Vorgehensweise Vorrang zu geben ist, Meist kann keine breite Diskussion geführt werden. Der Ernstfall, der eine öffentlich notwendige Infrastruktur zur Versorgung der Bevölkerung lahm legt, erfordert ein gutes Krisenmanagement. Sicher ist, im Nachgang wird es eine politische Debatte geben, was im Vorfeld oder in der aktuellen Entscheidung versäumt wurde. Aber noch handeln Menschen.

3. Neue Leitlinien als Lösungsansatz

Es gibt keine 100%ige Sicherheit und keinen Königsweg. Die zunehmende Geschwindigkeit der Weiterentwicklung in der IKT sowie zugehörige Risikofolgenabschätzung der Digitalisierung erzeugt immer wieder Korrekturbedarf. Foren zur Zusammenarbeit zwischen verschiedenen Disziplinen und Arbeitsfeldern in Recht und Informatik helfen zur Betrachtung und Diskussion einzelner Normen, ethischer Grundsätze, anderer Traditionen, deren Umsetzung in der Gesellschaft zur eigenen Positionierung zu Entwicklung und Einsatz der IKT. Die Diskussion und Legitimierung neuer Vereinbarungen und Grundregeln der digitalen Welt (wie in der o.g. Charta zur Digitalisierung vorgeschlagen) erfordert Partizipation in der Gesellschaft und wissenschaftliche Beiträge zur Stützung der Aussagen.

Unsicherheit braucht Leitlinien und Brücken zwischen Terror, Cyber-Security, Ethik und Freiheit mittels Normen und Technik. Neuerungen im IKT Umfeld verschieben Grenzen und erfordern Anpassungen der Normen, ohne dabei den Blick auf die Freiheit und die Würde des Menschen zu verlieren. Es gilt, «Grundrechte und demokratische Prinzipien auch in der digitalen Welt durch die Herrschaft des Rechts zu schützen [... und ...] eine rechtsstaatliche Ordnung im digitalen Zeitalter zu schaffen» [DIGITAL CHARTA EU 2016, Präambel].

4. Referenzen

ALDRICH, RICHARD J., US–European Intelligence Co-operation on Counter-Terrorism: Low Politics and Compulsion, *British Journal of Politics and International Relations*, Volume 11, Issue 1, 2009, 122–139.

AUMANN, ROBERT J., Vortrag an der ETH Zürich, <http://archiv.ethlife.ethz.ch/articles/tages/aumannlect.html>, 2005, abgerufen am 7. Dezember 2016.

BECK ULRICH, Über den postnationalen Krieg, in: *Blätter für deutsche und internationale Politik* 44 (1999), Nr. 8.

CHARTA DIGITALE VERNETZUNG E.V.I.G., <https://charta-digitale-vernetzung.de/die-charta-im-wortlaut/>, 2016, abgerufen am 9. Dezember 2016.

CLAUSEWITZ CARL VON, *Meine Vorlesungen über den kleinen Krieg*, gehalten auf der Kriegs-Schule 1810 und 1811. In: ders. (Hrsg), *Schriften, Aufsätze, Studien, Briefe*. Bd. 1. Göttingen 1966.

CREVELD, MARTIN VAN, *The Transformation of War*. New York 1991.

DIETZ KARL-MARTIN, *Protogoras von Abdera. Untersuchungen zu seinem Denken*. Bonn 1976.

lieferung und Bestrafung von Personen, die Kriegsverbrechen und Verbrechen gegen die Menschlichkeit begangen haben, Erklärung über den Schutz aller Personen vor dem Verschwindenlassen, Genfer Konventionen, Römisches Statut des Internationalen Strafgerichtshofs.

²⁸ Vgl. Diskussion zum Buch/Theaterstück/Film «Terror» [SCHIRACH 2016] und Publikumsentscheidungen.

- DIGITAL CHARTA EU, <https://digitalcharta.eu/>, 2016, abgerufen am 9. Dezember 2016.
- FINK FLORIAN, *Platons Begründung der Seele im absoluten Denken*, Berlin 2007.
- FÖRSTER STIG, Das Zeitalter des totalen Kriegs, 1861–1945. Konzeptionelle Überlegungen für einen historischen Strukturvergleich, in: *Mittelweg* 36 (1999), Nr. 8.6, 12–29, dort 13–14 und 29.
- G7 CHARTER FOR THE DIGITALLY CONNECTED WORLD, <http://www.international.gc.ca/g7/assets/pdfs/g7-2016-ict-charter.pdf>, 2016, abgerufen am 9. Dezember 2016.
- HILLS ALICE, *Doctrine, Criminality, and Future British Army Operations: A Half-Completed Understanding*. Camberley: The Strategic and Combat Studies Institute, 2000 (= *The Occasional*, Nr. 39).
- HOCH MARTIN, Die Rückkehr des Mittelalters in der Sicherheitspolitik, *WeltTrends* Nr. 35 2002.
- HÜGLI, ANTON, Wert: Einleitung. In: Joachim Ritter / Karlfried Gründer / Gottfried Gabriel (Hrsg.), *Historisches Wörterbuch der Philosophie*. Bd. 12. Darmstadt 2004, 555–558.
- INNERHOFER JUDITH E., Transhumanismus, Hirschrümmacher für alle, <http://pdf.zeit.de/2013/20/transhumanismus-philosoph-stefan-lorenz-sorgner.pdf>, 2013, abgerufen am 10. Dezember 2016.
- JONAS HANS, *Das Prinzip Verantwortung*, Frankfurt a. M. 1984.
- KANT, IMMANUEL, *Kritik der praktischen Vernunft*. In: Karl Vorländer (Hrsg.), *Sämtliche Werke*, Bd. 2. Leipzig 1924, 20–207.
- KEELEY, LAWRENCE H., *War Before Civilization*. Oxford 1996.
- LUHMANN, NIKLAS, *Legitimation durch Verfahren*, München 1969.
- MAINZER KLAUS, *Die Berechnung der Welt*, München 2014.
- MANSFELD, JAAP (Hrsg.), *Die Vorsokratiker*. Band 1, Stuttgart 1983, 44–55.
- NOACK, WINFRIED, *Herzensbildung als Erziehungsaufgabe*. In: Johannes Hartlapp / Stefan Höschle (Hrsg.), *Geschichte – Gesellschaft – Gerechtigkeit*. Berlin 2007, 109–125.
- NOACK WINFRIED, Wertekonstanz und Normenwandel in *Spes Christiana* 20, 2009, 11–30.
- PARSONS, TALCOTT, *The Structure of Social Action*. 2. Aufl. Glencoe 1949.
- PLATON, *Sämtliche Werke*, Hamburg 1958, Ausgabe 1981.
- POLYBIOS, *Geschichten Buch VI.1*, Übersetzung J. F. C. Campe, Stuttgart 1861, 647–720.
- SANDVOSS, ERNST R., *Immanuel Kant*. Stuttgart 1983.
- SCHATT NIKOLAUS, *Methoden der Cybersecurity in Anwendung und Recht. Eine methodologische Reflektion*. In: Erich Schweighofer / Franz Kummer / Walter Hötzendorfer / Georg Borges (Hrsg.), *Netzwerke / Networks*, Tagungsband des 19. Internationalen Rechtsinformatik Symposiums IRIS 2016, Wien/Bern 2016, 339–348.
- SCHIRACH, FERDINAND VON, *Terror*, München 2015.
- SELTEN REINHARD, *Spieltheoretische Behandlung eines Oligopolmodells mit Nachfrageträgheit*, Teil I: Bestimmung des dynamischen Preisgleichgewichts, und Teil II: Eigenschaften des dynamischen Preisgleichgewichts, in: *Zeitschrift f.d.ges. Staatswissenschaft* 121 (301–324 bzw. 667–689), 1965.
- TROTHA TRUTZ VON, *Formen des Krieges. Zur Typologie kriegerischer Aktionsmacht*. In: Sighard Neckel / Michael Schwab-Trapp (Hrsg.), *Ordnungen des Krieges. Beiträge zu einer politischen Soziologie der Gewalt und des Krieges*. Opladen 1999, 71–95, dort 92.
- UEBERWEG, FRIEDRICH, *Grundriß der Geschichte der Philosophie*. 3. Teil: Die Philosophie der Neuzeit bis zum Ende des Achtzehnten Jahrhunderts. 12. Aufl. Berlin 1924.
- VEREINTE NATIONEN, *Generalversammlung, Resolution der Generalversammlung, 217 A (III). Allgemeine Erklärung der Menschenrechte A/RES/217 A (III)*, 1948.
- VOLLRATH, ERNST, *Aristoteles*. In: Josef Speck (Hrsg.), *Grundprobleme der großen Philosophen*. Bd. 1. 2. Aufl. Göttingen 1978, 64–128.
- VORLÄNDER, KARL, *Philosophie des Altertums. Geschichte der Philosophie*. Bd. 1. Hamburg 1969.