Zur Verantwortung der Informatik in einer technologisierten Gesellschaft

Thomas Reinhold

English Title: The Responsibility of Computer Sciences in a Technology-Based Society

Abstract: The internet – or more generally cyberspace – is an essential part of modern societies, civil life, and directly as well as indirectly a crucial economic factor. The underlying technologies are an increasing target for economic or intelligence espionage and military activities. The access to this new domain "cyberspace", the control of its technologies, as well as the possibilities of its protection become more and more key for societal participation, economic and national welfare and, therefore, an integral part of internal and foreign security policies. The specific characteristics of cyberspace are major challenges for the application of established norms such as human rights, international cooperation and peace-keeping. Cyberspace is a completely man-made domain, and computer sciences are the essential designers of this domain. By means of historical examples, this article discusses the emerging role of computer sciences and the necessity to recognize its accountability. It aims to illustrate possibilities to actively take on this responsibility and to shape technological advancements for a peaceful and non-military application of cyberspace.

Keywords: Information Technology, Cyberspace, Cyberwar, Militarisation, IT-Security
Schlagworte: Informationstechnologie, Cyber-Raum, Cyberwar, Militarisierung, IT-Sicherheit

1. Einführung

Unser modernes Leben ist durchdrungen von digitalen Technologien. Computer und Software sind in vielen Bereichen selbstverständlicher Bestandteil des eigenen Lebens, zivilgesellschaftlicher Prozesse und außerdem ein wichtiger wirtschaftlicher Faktor. Dies bedeutet, dass der Zugang zu diesen Technologien und deren Kontrolle in zunehmenden Maße zum Schlüssel für individuelle gesellschaftliche Teilhabe, wirtschaftlichen Fortschritt und die sicherheitspolitische nationale Entwicklung wird. Exemplarisch wird dies unter anderem an den Debatten über eine stärkere Einbindung internationaler Gremien – wie der Internationalen Fernmeldeunion (ITU) als Sonderorganisation der Vereinten Nationen – in Fragen der Entwicklung, der technischen Struktur und der Verwaltung des globalen Internets deutlich; eine Veränderung die vor allem von Schwellenländern wie Brasilien seit Langem gefordert wird. Ähnlich prägnant ist die globale Verteilung der als „Internet-Backbone" benannten Glasfaserverbindungen, mit denen die weltweit verteilten eigenständigen Netzwerke per Kabel verbunden sind und bei denen ein signifikanter Unterschied in Anzahl und Bandbreite zwischen den globalen Ost-West-Verbindungen gegenüber den Nord-Süd-Verbindungen besteht[1] Das Internet und die zugrunde liegenden Netzwerke gelten in vielen Ländern als Bestandteil der sogenannten kritischen Infrastrukturen, deren Integrität und Verfügbarkeit als elementar für das nationale Wohl angesehen werden.

2. Gefahren der Militarisierung des Cyberspace

Dass Regierungen diese Entwicklung und Bedeutung auch im Sinne ihrer sicherheitspolitischen Ziele verstehen, offenbaren die Erfahrungen aus dem Arabischen Frühling oder die Enthüllungen aus dem Fundus von Edward Snowden[2] über die NSA, ihre Partner im Verbund der Five Eyes[3] sowie die Einbindung deutscher Nachrichtendienste[4]. Demokratische und autoritäre Staaten stehen sich gegenwärtig in ihren Bestrebungen, die Informationstechnik in ihrem Sinne zu beeinflussen und zu kontrollieren, nachrichtendienstliche Eingriffs- und Manipulationsmöglichkeiten zu etablieren oder auszubauen und Informationsströme zu überwachen und zu zensieren wenig nach. Flankiert wird diese Entwicklung von der Dominanz weniger global agierender IT-Unternehmen und den damit verbundenen Abhängigkeiten, Gefährdungen durch Sicherheitslücken und Schwachstellen sowie der Intransparenz von „IT-Monokulturen"[5] bei Hardware und Software. Auch aus militärischer Sicht werden die globalen IT-Strukturen und der als Cyberspace bezeichnete globale Raum aller vernetzten IT-Systeme und der darin enthaltenen Daten zunehmend zu einem relevanten Ziel und einer weiteren strategisch relevanten Domäne. Einer Studie des United Nations Institute for Disarmament Research (UNIDIR) zufolge gab es 2013[6] bereits 47 Staaten, die ihren nationalen Sicherheitsstrategien zufolge militärische Programme für den Cyberspace betreiben, zehn dieser Staaten[7] dabei mit explizit offensiver Ausrichtung. Neben

1 Vgl. http://www.submarinecablemap.com/.
2 Exemplarisch: https://edwardsnowden.com/de/revelations/.
3 "Five Eyes" ist der inoffizielle Name des Geheimdienstbündnisses der NSA (USA), des GCHQ (Großbritannien), des DSD (Australien), des Communications Security Establishment Canada (Kanada) und des GCSB (Neuseeland). Das Bündnis geht auf die 1947 vereinbarten Geheimdienstkooperationen "UKUSA" der USA und Großbritanniens zurück und wurde danach sukzessive um weitere Partnerländer erweitert.
4 Exemplarisch die Dokumentation des NSA-Untersuchungsausschusses im Deutschen Bundestag: https://de.wikipedia.org/wiki/NSA-Untersuchungsausschuss.
5 Als "IT-Monokulturen" wird die Dominanz einiger weniger Anbieter bei Software und Hardware verstanden, die aus der technologischen Entwicklung hervorgegangen ist. Beispiele dafür sind die Verbreitung von Microsoft Windows Betriebssystemen und Office-Anwendungen, der PDF-Betrachter der Firma Adobe oder Notebooks und Telekommunikationsgeräte der Firma Apple. Sicherheitslücken in diesen Produkten gefährden damit immer sehr viele Geräte und Anwender auf einmal.
6 UNIDIR 2013. The CyberIndex. International Security Trends and Realities, New York and Geneva, 2013. http://www.unidir.org/files/publications/pdfs/cyber-index-2013-en-463.pdf.
7 Die öffentlich verfügbaren Informationen zu Argentinien, Frankreich, Deutschland, Indien, Niederlande, Polen, Südkorea, Südafrika, Großbritannien, USA legen den Schluss nahe, dass diese Staaten offensive militärische Cyber-Einheiten aufbauen oder bereits über diese verfügen.

DOI: 10.5771/0175-274X-2016-4-253

nationalen Aktivitäten wie den kürzlich veröffentlichen Plänen der Bundeswehr zum Aufbau eines eigenen militärischen Organisationsbereichs auf Ebene der bestehenden drei Teilstreitkräfte Heer, Marine und Luftwaffe[8] hat sich der Cyberspace auch für Verteidigungsbündnisse wie die NATO zu einem ständigen Thema entwickelt[9].

Diese Entwicklung unterstreicht, dass mit der zunehmenden Technologisierung entscheidende gesellschaftliche und sicherheitspolitische Herausforderungen aufgeworfen werden. Dazu gehört bspw. die Wahrung von Menschenrechten wie das Recht auf freie Meinungsäußerung und die freie Entfaltung der Persönlichkeit und deren Gefährdung durch Überwachung und umfassende Speicherung und Analyse von persönlichen Daten. Ebenso bedeutend sind die Möglichkeiten der gesellschaftlichen Teilhabe durch das Angebot und den Zugang zu frei verfügbaren, barrierefreien und nicht-kommerziellen Dienstleistungen wie die verschiedenen sozialen Netzwerke, Informationsquellen, politische Mitwirkungsplattformen oder – global betrachtet – der generelle Zugang zu Möglichkeiten der digitalen Kommunikation und Vernetzung.

In der Industrie hat die Technologisierung in den letzten Jahrzehnten zu einer zunehmenden Vernetzung der Geräte und Prozesssteuerungsanlagen geführt. Diese alten, oft unzulänglich geschützten Systeme von Kraftwerken oder Fabriken werden zunehmend zum Ziel für Angriffe aus dem Internet, ein Umstand, der gerade im Bereich der kritischen Infrastrukturen mittlerweile stark bemängelt wird. Diese Probleme mit der Abhängigkeit und Anfälligkeit von IT werden seit der Entdeckung eines Vorfalls in einer iranischen Nuklearanreicherungsanlage im Jahr 2010 auch über Fachkreise hinaus mit Besorgnis wahrgenommen. Die Anlage wurde über mehrere Jahre hinweg mit einer Schadsoftware namens Stuxnet manipuliert,[10] die maßgeschneidert auf die technischen Gegebenheiten der Industrieanlage zugeschnitten war und mit deren Hilfe Zentrifugen durch die verborgene Veränderung von Rotationsgeschwindigkeiten einer höheren Belastung und damit einem schnelleren Verschleiß ausgesetzt wurden. Aufgrund der Komplexität der Schadsoftware, den benötigten Entwicklungsressourcen und notwendigen fachlichen Kenntnissen über die Anlage wurde Stuxnet mutmaßlich durch die Nachrichtendienste eines anderen Staates eingesetzt. Interviews mit hochrangigen US-Militärs in der New York Times[11] sowie der Washington Post[12] zufolge wurde Stuxnet durch US-amerikanische Dienste in Kooperation mit israelischen Geheimdiensten hergestellt und eingesetzt. Entwicklungen und Vorfälle in den Jahren nach Stuxnet legen den Schluss nahe, dass es weitere staatliche Akteure gibt, die kritische Infrastrukturen als potenzielle Ziele für Cyberoperationen wählen.

Angriffe auf solche IT-Systeme können jedoch unkalkulierbare Risiken bergen, da diese zumeist für die Kontrolle nachgeschalteter Systeme verantwortlich sind und mit der unbefugten Manipulation wichtige Regelungssysteme gestört werden können oder Schadsoftware sich auf andere angeschlossene Systeme ausbreiten kann. International geben insbesondere das Agieren staatlich militärischer und nachrichtendienstlicher Kräfte und die Planungen zum Aufbau offensiver „Cyber-Wirkmittel" Anlass zur Besorgnis. Bislang gibt es keinen Konsens über die Anwendung völkerrechtlicher Regeln und Gebote auf diese neue Domäne und die militärische Cyber-Aufrüstung einiger Nationen befeuert neuerliche Rüstungswettläufe, wie die UNIDIR-Studie deutlich zeigt. Dem gegenüber stehen vertrauensbildende Maßnahmen oder die Harmonisierung und Entwicklung gemeinsamer Termini, die sich spezifisch auf die neue Domäne Cyberspace beziehen, erst am Anfang. Dies wird bereits an den unterschiedlichen internationalen Sichtweisen auf die Sicherheit von IT-Systemen deutlich. Der US-amerikanisch und europäisch geprägten Auffassung der Integrität technischer Systeme mit ihrer Hard- und Software als Kern von IT-Sicherheit steht das Konzept der Informationssicherheit, ein gemeinsamer Vorschlag Russlands und Chinas an die UN, gegenüber. Letzterer schließt explizit die politische Hoheit und Kontrolle über verbreitete Informationen im jeweils nationalen Teil des Cyberspace ein und steht damit im Konflikt zum Recht auf eine freie Meinungsäußerung im Internet.

3. Verantwortung der Informatik

Der Informatik, ihren Fachkräften und Ausbildungseinrichtungen kommt angesichts dieser Situation eine besondere Rolle zu. IT-Produkte und Dienste haben eine enorme Breitenwirkung und einen direkten oder indirekten Einfluss auf die unterschiedlichsten Bereiche unserer Gesellschaft und der Staatengemeinschaft. Dabei ist der Cyberspace eine vollständig vom Menschen definierte und kontrollierte Domäne, in der die Informatik eine zentrale Position als Gestaltungskraft der Regeln dieser Domäne sowie deren Prozesse und Systeme einnimmt. Neben dieser Funktion fällt der Informatik angesichts der enormen Komplexität von IT-Hardware, Software und deren Verwendung und Wechselwirkungen oft die – ursprünglich dem Nutzer zugedachte – Rolle des alleinigen Kontrolleurs dieser Technologie zu. Exemplarisch wird dies an den globalen IT-Wirtschaftsunternehmen im Bereich der Kommunikation und sozialer Medien deutlich, deren Geschäftsmodelle immer wieder aus Datenschutz- und persönlichkeitsrechtlichen Gründen in der Kritik stehen. Nutzer dieser Dienste müssen in aller Regel zustimmen, dass Daten über ihr Verhalten gesammelt werden, können dabei jedoch selten kontrollieren oder überblicken, in welchem Umfang dies geschieht, inwiefern diese aggregierten Informationen durch den Dienstanbieter vermarktet werden oder ob ein nachrichtendienstlicher Zugriff erfolgt.

Leider ist mit Blick auf den akademischen und zivilgesellschaftlichen Bereich festzustellen, dass – abgesehen von wenigen Initiativen – die kritische Selbstreflexion der Informatik und

8 AbschlussberichtAufbaustab Cyber- und Informationsraum. http://www.bmvg.de/resource/resource/MzEzNTM4MmUzMzMyMmUzMTM1MzMyZTM2MzIzMDMwMzAzMDMwMzAzMDY5NmU2ODYyNzc2MzY5NzMyMDIwMjAyMDIw/Abschlussbericht%20Aufbaustab%20CIR.pdf.

9 Exemplarisch: Übersicht der NATO-Maßnahmen im Bereich der Verteidigung im Cyberspace http://www.nato.int/cps/en/natohq/topics_78170.htm.

10 Auch wenn die Anlage nicht direkt vernetzt war, ist es den Angreifern gelungen, Datenaustauschkanäle "nach draußen" zu etablieren, was u.a. daran deutlich wird, dass inaktive Versionen von Stuxnet sehr weit verbreitet entdeckt worden sind.

11 David E. Sanger: "Syria War Stirs New U.S. Debate on Cyberattacks", New York Times 24.02.2014.

12 Ellen Nakashima und Joby Warrick: "Stuxnet was work of U.S. and Israeli experts, officials say",Washington Post 02.06.2012.

ihrer Rolle kaum ausgeprägt ist. Die Informatik folgt in ihrem Gestaltungswillen in erster Linie ingenieurswissenschaftlichen Prinzipien, die eine möglichst optimale technische Lösung eines Problems als Ergebnis betrachten. Fragen der Verantwortung und nach den Folgen ihrer Entwicklungen werden in aller Regel außen vor gelassen und notwendiges philosophisches Handwerkzeug, wie die Selbstreflextion oder eine kritische Technikbewertung wie dies in der 1970er Jahren im Rahmen der Entwicklung erster Systeme künstlicher Intelligenz noch üblich war, werden selten gelehrt. Aspekte der Sicherheit und des Schutzes werden in erster Linie unter dem Blickpunkt technischer Eigenschaften von IT-Systemen, selten jedoch in ihren Implikationen für nationale und internationale Sicherheit oder Konzepten wie Menschenrechten, Krieg und Frieden betrachtet. Deutlich wird dies unter anderem an dem sehr mäßigen Erfolg zivilgesellschaftlicher Kampagnen für die Einhegung der militärischen Nutzung des Cyberspace[13] oder dem mühseligen Einsatz gegen die deutsche Vorratsdatenspeicherung[14]. Insbesondere angesichts der zunehmenden Militarisierung des Cyberspace und dem militärischen Ideal der kostengünstigen und gering-invasiven Cyberwaffe ist ein Blick auf historische Beispiele derartiger Entwicklungen geboten. Eindringlich haben unter anderem die Wissenschaftler der „Göttinger Erklärung", die als Physiker an der Entwicklung der Nukleartechnologie beteiligt waren, auf die Verantwortung für die Konsequenzen ihrer Forschungen hingewiesen[15]. Auch in der Informatik gab es in ihren frühen Jahren wichtige mahnende Stimmen, die heute kaum mehr bekannt sind, wahrgenommen oder bei der Ausbildung von Fachkräften vermittelt werden. Um es mit den Worten Josef Weizenbaums zu formulieren: *„Wir können die Technik nicht aus unserem Leben verbannen, die Verkehrsmittel nicht und inzwischen auch die Computer nicht. Umso wichtiger aber ist es, daß wir darüber nachdenken, wie wir mit den Errungenschaften der Technik in Zukunft umgehen sollen und wollen."*[16].

Angesichts der dargestellten Probleme und Herausforderungen bieten sich für die Informatiker/-innen vielfältige Möglichkeiten, ihre Rolle als kritische Gestalter/-innen wahrzunehmen. Mit Blick auf die Möglichkeiten der technologischen Selbstbestimmung, insbesondere angesichts der zunehmenden mobilen Kommunikation sind dies bspw. die weitere Förderung offener, von globalen IT-Unternehmen unabhängiger Software, die Benutzern bzw. Benutzerinnen die Kontrolle und Hoheit über ihre Daten ermöglicht. Eng damit verbunden ist die Entwicklung einfacher, zugänglicher und für den Einzelnen nachvollziehbarer Verfahren der sicheren Datenverschlüsselung und der verschlüsselten, für den Zugriff Dritter verborgener Kommunikationsmöglichkeiten. Die Erfahrungen des Arabischen Frühlings haben deutlich gemacht, dass aus Sicht repressiver Staaten ein enormer Bedarf für die Überwachung von Kommunikation, sozialen Medien und Computern existiert, ein Markt an dem übrigen auch deutsche Firmen partizipieren[17] und dem es gilt sichere und geschützte Alternativen entgegenzustellen.

Eine stärkere Diskussion der Implikationen entsprechender Technik und deren Einsatz ist dringend geboten, ebenso wie eine Fortsetzung der Debatte über den Umgang entdeckter Sicherheitslücken. Diese spielen für den verdeckten und unauthorisierten Zugriff auf fremde IT-Systeme eine entscheidende Rolle, da mit ihrer Hilfe unter Ausnutzung der Fehlfunktion der Zugang zum Zielsystem oft erst ermöglicht wird. Informationen über derartige Lücken in populärer Software, die breit verwendet wird, wie Internet-Browsern, Office-Anwendungen oder Server-Programmen sind für Nachrichtendienste und andere Bedarfsträger daher von hohem Wert. So wurde beispielsweise durch die Snowden-Enthüllungen bekannt, dass die US-amerikanische NSA teilweise die Fehlerberichte abgefangen und ausgewertet hat, die von Windows-Betriebssystemen nach Fehlfunktionen zum Teil automatisiert an den Hersteller Microsoft gesendet wurden. Die Bedeutung von Sicherheitslücken wird darüber hinaus auch an dem internationalen Handel mit diesen Informationen deutlich. Unternehmen wie die Firmen "Vupen", "Zerodium" oder "Hacking Team" kaufen entsprechende Informationen und geben diese an hochrangige Kunden weiter. Insbesondere unbekannte Sicherheitslücken, für die es noch keine Korrekturen des Herstellers gibt (sog. "Zero dayexploits"), stehen dabei hoch im Kurs. Angesichts dieser Situation stehen IT-Sicherheitsfachleute vor der Entscheidung derartiges Wissen um Sicherheitslücken zum Wohle aller zu veröffentlichen, an den jeweiligen Hersteller zu melden und offizielle zentrale Meldestellen, wie zum Beispiel das deutsche Bundesamt für Sicherheit in der Informationstechnik (BSI), zu informieren. Diese ethischen Herausforderungen betreffen in gleichem Maße den Wirtschaftszweig der militärischen IT-Entwicklungen, der angesichts eines größer werdenden Bedarfs nach „offensiven Cyber-Wirkmitteln" zukünftig absehbar wachsen wird. Die Informatik kann und muss der damit verbundenen Schwächung globaler IT-Strukturen und dem dargestellten sicherheitspolitischen Konfliktpotenzial entgegenwirken. Wichtige Maßnahmen könnten die internationale Vernetzung und der Austausch von IT-Fachkräften und Wissenschaftler/-innen explizit zu diesen Themen sein, ebenso wie dies bspw. Physiker/-innen seit vielen Jahrzehnten im Rahmen der Pugwash-Konferenzen[18] im Kampf gegen nukleare Bedrohungen tun. Weitere Ansatzpunkte betreffen die notwendige Forschung zur Übertragung wichtiger Instrumente der internationalen Sicherheitspolitik auf die Domäne des Cyberspace und die damit verbundenen Schwierigkeiten angesichts spezifischer Eigenschaften von Software wie Immaterialität oder Virtualität. Wie können etablierte Maßnahmen der Rüstungskontrolle oder der Verifikation vertraglicher Vereinbarungen zur Rüstungsbeschränkung für militärische Cyberprodukte umgesetzt werden? Wie lassen sich bspw. Verfahren der Software-Lizenzierung und Authentifizierung, wie sie im privatwirtschaftlichen Bereich zum Schutz geistigen Eigentums oder der Beschränkung auf legale Vertriebskanäle

13 Z.B. http://cyberpeace.fiff.de/Kampagne/Home.
14 Exemplarisch: Dokumentation des Arbeitskreises Vorratsdatenspeicherung http://www.vorratsdatenspeicherung.de/content/view/46/42/lang,de/.
15 Originaltext der Erklärung: https://de.wikipedia.org/wiki/G%C3%B6ttinger_Achtzehn.
16 Josef Weizenbaum und Klaus Haefner, Sind Computer die besseren Menschen?, Zürich 1990.
17 Exemplarisch die Aktivitäten der deutschen Firmen Gamma: https://netzpolitik.org/2014/gamma-finfisher-ueberwachungstechnologie-made-in-germany-gegen-arabischen-fruehling-in-bahrain-eingesetzt/ und Trovicor: http://www.cora-netz.de/cora/wp-content/uploads/2016/01/CorA-ForumMR_Steckbrief-Trovicor.pdf.
18 Siehe https://pugwash.org/.

eingesetzt werden, auf die Anforderungen der Proliferationskontrolle und Vermeidung von Cyber-Rüstungsgütern anwenden? Entgegen der empfundenen Virtualität des Cyberspace lassen sich alle Daten und IT-Systeme im Cyberspace auf konkrete Hardware zurückführen, die sich wiederum in aller Regel auf dem Boden von Nationalstaaten befindet. Ebenso ist die Menge der Verbindungen zwischen Übertragungsnetzwerken begrenzt und metaphorisch betrachtet stellen diese Knotenpunkte Grenzübergange dar. Damit bilden diese Strukturen die Grundlage, um das sicherheitspolitisch wichtige Prinzip der staatlich territorialen Souveränität und Verantwortlichkeit im Cyberspace abzubilden. Ausgehend von diesen Überlegungen ließe sich das Problem der schwierigen Attribuierbarkeit von Angriffen im Cyberspace bearbeiten. Die Kenntnis über die tatsächliche Herkunft einer Attacke stellt eine Voraussetzung für das Recht auf Selbstverteidigung eines Staates nach Art. 51 der UN-Charta dar. Während eine eindeutige weltweite Identifizierbarkeit im Cyberspace für den zivilen Bereich aus Menschenrechtsgründen nicht wünschenswert ist, wäre eine solche Maßnahme mit Hilfe der Möglichkeiten des neuen Internet-Adressierungs-Verfahrens IPv6[19] für militärische IT-Systeme umsetzbar und könnte einen wichtigen Beitrag zur Eingrenzung des „fog of war“[20] darstellen. Die staatlichen Konfliktparteien hätten damit eine Möglichkeit, das gegenseitige Handeln zu kontrollieren, Zusagen zu überwachen oder in akuten Krisensituationen Einblicke in IT-Netzwerke zu gewähren, um Fehlzuweisungen von Cyberattacken zu vermeiden.

Die dargestellten Herausforderungen digitaler Technologien sollen zeigen, dass die Forschung und Entwicklung von IT, Software und Algorithmen selten wertfrei und in aller Regel mit weitreichenden Konsequenzen verbunden sind. Andererseits existieren durchaus Ansatzpunkte für technische Möglichkeiten der Konfliktvermeidung und der aktiven Gestaltung einer friedlichen Nutzung des Cyberspace. Es ist an der Zeit, dass die IT-Branche, die Institutionen der IT-Ausbildung und die Informatik als Wissenschaft dies als eigene Verantwortung anerkennen, ihrer Rolle als Wegbereiter dieser Technologien gerecht werden und das notwendige ethische Rüstzeug vielmehr als bisher in die Ausbildung zukünftiger IT-Fachkräfte einfließen lassen.

Thomas Reinhold hat Informatik und Psychologie studiert und arbeitet als wissenschaftlicher Fellow am Institut für Friedensforschung und Sicherheitspolitik der Universität Hamburg zu Cyberbedrohungen, Cyberwar und Rüstungskontrolle im Cyberspace.

19 Einen Überblick über IPv6 und die Adressierung jeglicher Geräte im Internet bietet https://de.wikipedia.org/wiki/IPv6.

20 Das Konzept des “fog of war” bezeichnet allgemein die in spezifischen Situationen unklare Entscheidungsgrundlage für kriegerische Situationen aufgrund diverser weiterer Aspekte über die trotz Aufklärung keine Vorhersage getroffen werden kann. Im Kontext des Cyberspace betrifft dies in erster Linie die unklare Einschätzung der eigenen Gefährdungslage, der unklaren Verwundbarkeit eigener IT-Systeme sowie die Bewertung des Bedrohungs- und Zerstörungspotenzials von Cyberwaffen auf Seiten potenzieller Gegner für die bislang keinerlei Klassifikationsgrundlagen existieren.