nehmen den umworbenen Ministerien anzubieten hatte, blieb allerdings bis zuletzt unklar. Im April 2021 meldete es schließlich Insolvenz an.

Dieses Schicksal droht der Investmentgesellschaft In-Q-Tel nicht, denn diese wird direkt aus dem Haushalt des US-amerikanischen Auslandsgeheimdienstes CIA finanziert. Nach Angaben des deutschen Verfassungsschutzes vergibt es „Risikokapital an junge Unternehmen, insbesondere im Bereich der Informationstechnologie“[12], wobei es offenbar darum geht, die entsprechenden Technologien für das US-amerikanische Militär bzw. die Geheimdienste zugänglich zu machen oder zumindest dem Zugriff Dritter zu entziehen. Ende 2020 war In-Q-Tel beim Dresdner Startup *Morpheus Space* eingestiegen, einer auf Antriebe für Nano-Satelliten spezialisierte Aus
zuvor auf verschiedenen Ebenen
chen Hand erhalten hatte. Dies s
nen Seiten.

erschienen in der FIfF-Kommunikation, herausgegeben von FIfF e.V. - ISSN 0938-3476 www.fiff.de

Dass öffentliche Gelder in private Profite überführt werden, indem Risiken sozialisiert und Gewinne privatisiert werden, ist jedoch eine zentrale Funktion des angestrebten Ökosystems und eine – gar nicht so neue – Form der politischen Steuerung technologischer „Innovation“.

Anmerkungen

1 Walter Dornberger (2020) Peenemünde – Die Geschichte der V-Waffen. RhinoVerlag, Ilmenau 2. Auflage 2020.

2 Vgl. beispielhaft: Petra Molnar, Lex Gill (2018) Bots at the Gate: A Human Rights Analysis of Automated Decision-Making in Canada's Immigration and Refugee System, https://citizenlab.ca/wp-content/uploads/2018/09/IHRP-Automated-Systems-Report-Web-V2.pdf.

3 Einen sehr guten Überblick über diskutierte Anwendungsbereiche liefert z. B. das Programm der Tagung „Künstliche Intelligenz – Chancen und Risiken für die Bundeswehr“ der Studiengesellschaft der Deutschen Gesellschaft für Wehrtechnik mbH, einsehbar unter: https://www.dwt-sgw.de/fileadmin/redaktion/SGW-Veranstaltungen/2019/9F9_KI2/9F9_KI_Bw_Programm_281019.pdf

4 Die Stellungnahme findet sich unter: https://www.mpg.de/11543958/Stellungnahme-Wissenschaft-und-Industrie.pdf.

5 Martin Stratmann (2017) Der Staat muss auch riskante Projekte fördern, Tagesspiegel (18.10.2017), dokumentiert unter: https://www.mpg.de/11679923/der-staat-muss-auch-riskante-projekte-foerdern.

6 Asgard, Roland Berger (2018) Artificial Intelligence – A strategy for European startups, https://www.rolandberger.com/publications/
i_strategy_for_european_startups.pdf.
nd weitgehend gleichlautend einem
men, der sich mitsamt der jeweiligen
den lässt: https://www.imi-online.
-dammbruch-der-ruestungsforschung/

8 Das Thesenpapier, aus dem alle Zitate in diesem Abschnitt entnommen sind, findet sich hier: https://www.bundeswehr.de/resource/blob/156024/d6ac452e72f77f3cc071184ae34dbf0e/download-positionspapier-deutsche-version-data.pdf.

9 Larissa Holzki (2021): Bundeswehrgeneral fordert: „Auch bei klassischen militärischen Problemen jetzt mit Start-ups zusammenarbeiten“, Handelsblatt.de (29.07.2021).

10 Siehe: https://migration-control.info/bobusi/.

11 Zitiert nach dem entsprechenden Eintrag in der „Border Business Liste“, siehe: https://migration-control.info/bobusi/pandora-inteligence (Stand 2.11.2021).

12 Bundestags-Drucksache 19/23509, https://dserver.bundestag.de/btd/19/235/1923509.pdf.

Thomas Reinhold

Zur Rolle und Verantwortung der Informatik für die Friedensforschung und Rüstungskontrolle

Die Ursprünge des Internets, so wie wir es heute kennen, basierten auf der Idee eines Austauschs von Ideen, Informationen und Codes. Obwohl die technischen Konzepte bereits durch den Wunsch nach einem staatlichen und militärischen Kommunikationssystem motiviert waren, welches auch nukleare Angriffe überstehen konnte, waren ein Großteil der ohnehin wenigen Nutzer:innen Akademiker:innen und Wissenschaftler:innen. Im Laufe der Jahre entwickelten sie so eine Technologie, die den freien Informationsfluss unterstützt. Dabei sah es lange Zeit danach aus, als könnte sich diese Idee hin zu einem weltweit freien und zugänglichen Netz entwickeln. Seit einigen Jahren, spätestens jedoch seit der Entdeckung von Stuxnet im Jahr 2010, wissen wir jedoch, dass auch Militär und Geheimdienste den sogenannten Cyberspace als Domäne für ihre Zwecke entdeckt haben. Angesichts der Abhängigkeiten moderner Gesellschaften von IT-Diensten und den zugrunde liegenden Infrastrukturen ist es zweifelsohne notwendig, die nationale IT-Sicherheit zu fördern und militärische Abwehrkapazitäten in diesem Bereich aufzubauen. Allerdings zeigen die Snowden-Enthüllungen oder der UNIDIR-Cyber-Index[1], dass immer mehr Staaten den Cyberspace auch als militärische Domäne betrachten, in der sie offensive Fähigkeiten entwickeln (müssen) oder diese bereits einsetzen. So ist es bei den US-Streitkräften inzwischen Pflicht, dass jeder Einsatz im Feld durch eine eigene Cyber-Einheit begleitet wird, die für Aufklärung, strategische Unterstützung und offensive Operationen zuständig ist. Diese Entwicklung ist auch an Deutschland nicht vorbeigegangen, wo die Bundeswehr eine eigenständige militärische Einheit, das Kommando *Cyber- und Informationsraum* (KdoCIR), eingerichtet hat, welche ab diesem Jahr voll einsatzfähig sein soll[2]. Inwieweit dieses neue Kommando offensive Fähigkeiten entwickeln und einsetzen darf (und auch wird), ist allerdings trotz zahlreicher öffentlicher Nachfragen und parlamentarischer Debatten weiterhin offen. Vieles deutet jedoch darauf hin, dass die bereits bestehenden Fähigkeiten der Vorgänger-Einheit *Computer-Netzwerk-Operationen* für solche Zwecke weitergenutzt und ausgebaut werden.

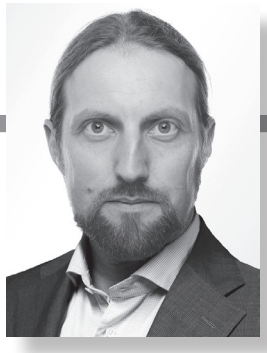
Wo militärische Kräfte in den Cyberspace vordringen, hat die internationale Gemeinschaft nach wie vor Schwierigkeiten, die in den letzten Jahrzehnten für die internationale Sicherheits-

und Außenpolitik entwickelten Regeln und Standards auf diesen neuen Bereich anzuwenden. Obwohl mittlerweile weitestgehend Einigkeit über die Gültigkeit des internationalen Völkerrechts auch im Cyberspace herrscht, bleibt die konkrete Anwendung dieser Normen oft unklar. Dies ist vor allem darauf zurückzuführen, dass der Cyberspace einige spezifische technische Merkmale aufweist, die sich stark von den bisherigen militärisch genutzten Domänen Luft, Wasser, Land und Weltall sowie deren technologischen und physikalischen Eigenschaften unterscheiden. So liegen beispielsweise der Cyberspace und die darin gespeicherten Informationen im Wesentlichen in virtueller Form vor. Auch wenn sich die Hardware einem bestimmten Standort zuordnen lässt, trifft dies nicht zwingend für die gespeicherten oder verarbeiteten Daten zu, insbesondere im Zeitalter des Cloud-Computing. Hinzu kommt, dass Software, wie alle anderen Daten, nahtlos dupliziert werden kann, sodass etablierte Maßnahmen der Rüstungskontrolle, welche auf dem Prinzip der Lokalisierung oder Quantifizierbarkeit beruhen, auf den Cyberspace nicht übertragbar sind. Die Virtualität und die zahllosen Möglichkeiten eines Angreifers, sich zu verbergen oder gar falsche Spuren zu legen, erschweren die Zurechnung von Cyberangriffen (Attribution), stellen jedoch eine zentrale Voraussetzung für jede nationale Selbstverteidigungsmaßnahme im Rahmen der UN-Charta dar[3]. Das letzte der offenkundigsten Beispiele für die technischen Besonderheiten des Cyberspace betrifft den ausgeprägten Dual-Use-Charakter von IT-Hard- und Software, der es erschwert, zwischen zu regulierender militärischer und zulässiger ziviler Nutzung betroffener Geräte zu unterschieden.

In Ergänzung zu diesen Schwierigkeiten ergibt sich eine weitere Herausforderung für die Sicherheit, Verfügbarkeit und Integrität der IT: die Nachfrage staatlicher Organisationen wie nationaler Nachrichtendienste, Strafverfolgungsbehörden oder der Streitkräfte an Schwachstellen in Hardware und Software zum Zwecke ihrer – zugegebenermaßen diskutablen – Aufgabenerfüllung. Neben Cyberkriminalität fördert diese Praxis die Entwicklung von Märkten für den Handel mit Sicherheitslücken und erhöht damit die Anreize, das Wissen über Schwachstellen zu verbergen und zu monetarisieren, anstatt es zur Stärkung der öffentlichen IT-Sicherheit offenzulegen. Die *EternalBlue*-Vorfälle im Zusammenhang mit den *WannaCry*[4]- und *NotPetya*[5]-Malware-Kampagnen, die immense wirtschaftliche Schäden verursachten, haben eindrucksvoll gezeigt, wie schnell sich ein solches Verhalten sowohl auf Wirtschaftssysteme als auch auf Zivilgesellschaften weltweit auswirken kann.

Aus Sicht der internationalen Sicherheit haben diese Entwicklungen der Militarisierung des Cyberspace zu einer Situation geführt, in der sich Streitkräfte einerseits zunehmend auf offensive Operationen in diesem Bereich vorbereiten. Andererseits fehlen gleichzeitig geeignete Maßnahmen, um diese Gefährdung der internationalen Sicherheit einzugrenzen oder überhaupt einschätzen zu können. Im Gegensatz zu konventionellen Waffen wie Raketen ist zum Beispiel noch unklar, wie der potenzielle Schaden einer Cyberwaffe gemessen oder kategorisiert werden kann. Dieses Ungleichgewicht hat zu nationalen Sicherheitsbedenken, unter anderem aufgrund von Vermutungen über das militärische Leistungsvermögen potenzieller Gegner, geführt und ein neues Wettrüsten mit Cyberwaffen ausgelöst, wodurch die internationale Lage zunehmend destabilisiert wird.

Dabei war die internationale Gemeinschaft in der Vergangenheit bereits mit solchen Situationen neuer technologischer Entwicklungen und deren „militärischer Vereinnahmung“ konfrontiert, wie im Fall von atomaren, biologischen und chemischen Waffen. Die politische Antwort auf diese Bedrohungen bestand stets in der Ausarbeitung von Vereinbarungen und Verträgen zur Eingrenzung der militärischen Nutzung dieser Technologien. Auch wenn dies oft langer Verhandlungsphasen bedurfte, in vielen Fällen mit Rückschritten und Enttäuschungen verbunden war und einige Probleme noch immer Gegenstand von Debatten und Auseinandersetzungen sind, so stellen derartige politische Maßnahmen wichtige Schritte auf dem Weg zu einer Rüstungskontrolle oder Nichtverbreitung von Waffen dar. Diese benötigen allerdings eine gemeinsame Grundlage für eine effektive Um- und Durchsetzung: Mittel zur gegenseitigen Kontrolle der Einhaltung jeglicher Art von Vereinbarungen. Bei diesen Verfahren der so genannten Verifikation handelt es sich um praktische Maßnahmen, die auf der Zählung, Messung oder Überwachung bestimmter technologischer Entwicklungen, Arsenale, Produktionsanlagen oder zuvor vereinbarter Limitierungen beruhen. Für das bekannteste Verifikationsregime ist die Internationale Atomenergie-Organisation (IAEO), eine internationale Organisation unter Führung der Vereinten Nationen, zuständig. Diese überwacht, unter anderem, das zivile Atomprogramm des Iran durch Besuche und Inspektionen von Kernkraftwerken und Anreicherungsanlagen, um so die Mengenbegrenzung von atomwaffenfähigem Kernmaterial zu kontrollieren. Wie bereits erwähnt, ist die Adaption derartiger Maßnahmen auf den Cyberspace aufgrund seiner spezifischen technischen Eigenschaften jedoch nicht möglich. Darüber hinaus ist es noch weitgehend unklar, ob alternative Verfahren existieren oder wie diese funktionieren könnten. Gleichsam verfügt der Cyberspace jedoch über einen wichtigen und einzigartigen Vorteil gegenüber allen früheren technologischen Entwicklungen: Er ist eine vollständig von Menschen geschaffene Domäne, deren „Naturgesetze“ von Informatiker:innen und IT-Praktiker:innen geschaffen und weiterentwickelt werden. Informatiker:innen setzen sich seit langem für IT-Sicherheit, Datenschutz und die Um-



Thomas Reinhold

Thomas Reinhold ist wissenschaftlicher Mitarbeiter und Doktorand am Fachgebiet Wissenschaft und Technik für Frieden und Sicherheit (PEASEC) der TU Darmstadt. Er befasst sich mit IT-gestützten Möglichkeiten für Rüstungskontrolle militärischer Aktivitäten im Cyberspace sowie den Problemen einer Militarisierung von Künstlicher Intelligenz.

setzung und Wahrung demokratischer Rechte in Software, Diensten und Infrastrukturen ein. Neben diesen Persönlichkeitsrechten erfordert die neue Situation bezüglich geheimdienstlicher und militärischer Akteure nun jedoch die Stärkung weiterer gefährdeter Werte, wie etwa des internationalen Friedens und der Sicherheit sowie der Unversehrtheit globaler IT-Infrastrukturen. Gleichzeitig müssen Maßnahmen wie die friedliche Nutzung und Weiterentwicklung der Domäne Cyberspace in den zugrunde liegenden technischen Systeme etabliert werden. So stellt sich beispielsweise die Frage, wie das Zerstörungspotenzial von *Cyber-Waffen* begrenzt oder geheimdienstliche und militärische Aktivitäten im Cyberspace transparent und kontrollierbar gestaltet werden können. Während Anonymität für Zivilist:innen im Cyberspace notwendig ist und geschützt werden muss, könnten militärische Netzwerke – also Teilsysteme, die in der Regel ohnehin bereits besonderen politischen Regeln unterliegen und aufgrund ihres spezifischen Zwecks stark reguliert sind – modifiziert werden, um Zugriffe auf fremde Netzwerke nachvollziehbar zu gestalten.

Diese Gedankenspiele führen zu einer sehr wichtigen Schlussfolgerung: Wenn es die Informatiker:innen sind, die den Cyberspace gestalten und seine zukünftige Entwicklung entscheidend mitbestimmen, dann sind auch sie es, denen in Anbetracht der oben beschriebenen Herausforderungen die Aufgabe der Entwicklung technischer Lösungsansätze zufällt. Der Schwerpunkt sollte darauf liegen, wie IT gestaltet werden muss, um eine friedliche und sichere Entwicklung des Cyberspace zu ermöglichen. Davon ausgehend ergibt sich eine Vielzahl von Fragen und Herausforderungen, die es zu lösen gilt: Wie können Rüstungskontrolle und Nichtverbreitungskontrolle von Cyberwaffen in der Praxis funktionieren? Wie könnten neue Ansätze zur Sicherung und Kontrolle der Entwicklung, des militärischen Einsatzes und der Nichtverwendung solcher Technologien aussehen, welche die Prinzipien etablierter Regeln und Normen für staatliches Verhalten in dieser Domäne abbilden? Welche messbaren Parameter und Eigenschaften gibt es für Software und Hardware, die für eine Dual-Use-Differenzierung herangezogen werden können? Lassen sich Kriterien finden, um potentiell eher unkritische, defensive Maßnahmen der Cyberverteidigung von solchen Maßnahmen oder Werkzeugen, die auch offensiv gegen Gegner eingesetzt werden, abzugrenzen? Und zu guter Letzt: Wie können Verifikationsmaßnahmen von militärischen Cyber-Fähigkeiten als Grundlage für Vereinbarungen und Verträge aussehen?

Vielleicht gibt es auf viele dieser Herausforderungen keine zufriedenstellenden Antworten. Aber es ist dringend geboten, diese Fragen anzugehen. Um es mit den Worten von J. F. Kennedy zu formulieren: „Wann, wenn nicht jetzt? Wer, wenn nicht wir?“

Anmerkungen

1 *Der Cyber-Index – Internationale Sicherheitstrends und Realitäten“ http://www.unidir.org/files/publications/pdfs/cyber-index-2013-en-463.pdf*
2 *https://www.bmvg.de/de/themen/cybersicherheit/cyber-verteidigung/entwicklung-des-org-bereich-bei-der-bw*
3 *Charta der Vereinten Nationen – http://www.unric.org/de/charta*
4 *Informationen zur EternalBlue-Sicherheitslücke und zur WannaCry-Schadsoftware-Kampagne https://cyber-peace.org/cyberpeace-cyberwar/relevante-cybervorfalle/wannacry-eternalblue/*
5 *Informationen zur NotPetya-Schadsoftware-Kampagne https://cyber-peace.org/cyberpeace-cyberwar/relevante-cybervorfalle/petya_notpetya/*

Christian Heck

War on Error

Am 15. August 2021 hatten die militant-islamistischen Taliban praktisch kampflos die afghanische Hauptstadt Kabul eingenommen. Niemand hat damit gerechnet, so Heiko Maas, Bundesminister des Auswärtigen, *„das war offensichtlich eine Fehleinschätzung, die die komplette internationale Gemeinschaft, auch ich und die Bundesregierung hatten.“* In der Nacht zum 31. August 2021 verließ die letzte US-Militärmaschine das Land.