Metis

Studie

Großmächte und Digitalisierung – welche Folgen für unsere Weltordnung?

Nr. 08 | Oktober 2018

Institut für
Strategie & Vorausschau

Zusammenfassung

Die vorliegende Studie legt den Dreiklang aus Daten, ihrer Verarbeitung und damit ihrem Ummünzen in ökonomische und militärische Macht zu Grunde, um den Wettlauf der Großmächte USA und China um die Vormachtstellung im Digitalzeitalter zu beleuchten. Schlaglichtartig werden Rüstung und Rüstungskontrolle, strategische Stabilität und vorausschauend die Implikationen einer möglichen Quantencomputer-Revolution dargestellt. Am Schluss dieser Studie stehen einige weiterführende Überlegungen zu den Implikationen der Weltordnung im Digitalzeitalter für liberale Demokratien wie Deutschland.

Daten, Künstliche Intelligenz und Macht

Daten sind das Öl des 21. Jahrhunderts. Diese beliebte Analogie hinkt, aber sie macht doch auf einen für die vorliegende Studie entscheidenden Zusammenhang aufmerksam: Daten – die Fähigkeiten und Möglichkeiten zu ihrer Gewinnung, die Kapazitäten zu ihrer Verarbeitung mittels Künstlicher Intelligenz (KI)[1] und somit ihr Ummünzen in ökonomische und militärische Macht – werden für die Weltordnung im Zeitalter der Digitalisierung von entscheidender Bedeutung sein. Zivile Technologieunternehmen sind dabei die Innovationsmotoren. Private Investitionen übersteigen die des öffentlichen Sektors und des Militärs um ein Vielfaches.

In den USA sucht das Pentagon daher die Nähe zu Technologiefirmen im Silicon Valley. Washington stellt strategisch vom Anti-Terror-Krieg auf Großmachtkonflikt um. Die militärische Nutzung von Technologien aus dem Feld der KI soll die eigene konventionelle Überlegenheit absichern (Third Offset Strategy).

China formulierte 2017 das offizielle Ziel, bis 2030 globaler KI-Innovationsführer zu sein. Auch Peking arbeitet an zivil-militärischer Integration. Die Früchte seiner rasanten kommerziellen Aufholjagd will das Land auch militärisch nutzen („Intelligentisierung" der Kriegsführung).[2]

Am Beispiel Chinas und der USA werden über drei militärisch relevante Felder hinweg die Implikationen des Digitalzeitalters für Großmachtpolitik exemplarisch untersucht. Es werden schlaglichtartig Rüstung und Rüstungskontrolle, strategische Stabilität sowie vorausschauend die Nutzung von Quantencomputern analysiert. Die Schlussbetrachtung erweitert den Fokus. Sie fragt nach der Zukunft des liberaldemokratischen Gesellschaftsmodells in der Weltordnung des Digitalzeitalters.

Rüstung und Rüstungskontrolle

Die USA und China streben beide das Überführen von digitalen Innovationen aus dem zivilen Sektor in militärische Anwendungen an. Sie stehen dabei vor zwei Herausforderungen: Erstens der Diffusionsanfälligkeit digitaler Technologien (Monopole sind dadurch viel schwerer zu behaupten als im Falle bisheriger militärischer Hochtechnologie, wie etwa Stealth). Zweitens der Inkompatibilität militärischer Beschaffungsprozesse und Anforderungen mit den kurzen Entwicklungszyklen kommerzieller, bisweilen unzuverlässiger Produkte und Lösungen.

1 Der weite und nicht einheitlich definierte Begriff der Künstlichen Intelligenz umfasst eine Vielzahl unterschiedlicher softwarebasierter Techniken und Verfahren zur Automatisierung von spezifischen Einzelaufgaben, die bisher die Anwendung menschlicher Intelligenz erforderten.

2 Für China war der Sieg der Software AlphaGo (entwickelt von Googles DeepMind) gegen den Go-Champion Lee Sedol 2016 ein „Sputnik Moment".

Das Pentagon sucht mit seinem Defense Innovation Unit Experimental (DIUx) getauften Ableger im Silicon Valley schon seit 2015 Antworten auf diese Herausforderungen durch größere Nähe zu zivilen Technologieunternehmen. Allerdings ist das gezielte Herantasten des US-Militärs an den kommerziellen Sektor nicht unumstritten, wie das Pilotprojekt Maven beispielhaft zeigt. In dieser Zusammenarbeit zwischen Google und dem Pentagon sollte eine auf maschinellem Lernen beruhende Software automatisch Objekte und Personen in Videoübertragungen von Drohnen erkennen, um menschlichen Analysten Arbeit bei der Auswertung abzunehmen. Das Pilotprojekt stieß nach seinem Bekanntwerden innerhalb der Belegschaft von Google auf massiven Widerstand, die es als Vorbote einer algorithmisierten, entmenschlichten Kriegsführung ablehnte. Im Juni 2018 sah sich die Unternehmensführung gezwungen, den mit dem Pentagon noch bis März 2019 laufenden Maven-Vertrag nicht zu verlängern. In seinen im Anschluss erarbeiteten und veröffentlichten KI-Prinzipien schränkte das Unternehmen zudem seine Kooperation mit dem Militär ein und erteilte der Arbeit an Waffensystemen eine (nahezu)[3] komplette Absage. Google zog sich darüber hinaus aus dem Bieterwettbewerb um das rund 10 Mrd. USD schwere Projekt Joint Enterprise Defense Infrastructure (JEDI) zurück, mit dem das Pentagon eine militärische Cloud realisieren will. Googles Konkurrenten blieben davon zunächst unbeeindruckt; doch jüngst regte sich auch unter den „tech workers" bei Amazon und Microsoft organisierter Widerstand gegen JEDI.

Aus China sind keine vergleichbaren Entwicklungen bekannt. Das liegt auch an Geheimhaltung und Transparenzmangel aufgrund der semipermeablen Sprachbarriere. Letztere erlaubt es dem – in weiten Teilen im Ausland ausgebildeten und der englischen Sprache mächtigen – chinesischen Tech-Sektor, englischsprachige Gehalte zu rezipieren, während in umgekehrter Richtung kaum Informationsaustausch und Wissenstransfer stattfinden. Offene Quellen lassen jedenfalls keine weitreichenden Schlüsse darüber zu, inwiefern das chinesische Militär analog zum Pentagon Kooperationen mit Alibaba, Baidu oder Tencent pflegt und ob dies mit ähnlichen Bedenken oder Widerständen wie in den USA einhergeht. Die offen zur Verfügung stehenden Übersetzungen offizieller chinesischer Debatten und Dokumente (insbesondere des White Paper on Civil-Military Fusion and AI) legen den Schluss nahe, dass es intensive Bestrebungen gibt. Aber anders als im Westen, in dem – über die US-Beispiele Maven und JEDI hinausgehend – die militärische Nutzung von Techniken aus dem Bereich der KI generell von Zivilgesellschaft und Experten medienwirksam kritisch hinterfragt wird,[4] ist bisher aus China nur ein prominenter Fall eines namhaften KI-Forschers bekannt, der öffentlich in ähnlich kritischer Form Stellung bezieht.[5]

Mit der wachsenden Bedeutung von Daten und Software in militärischen Anwendungen steht auch die Rüstungskontrolle (unter Großmächten) vor gänzlich neuen Herausforderungen. Das quantitative Paradigma des 20. Jahrhunderts trägt nur noch begrenzt. In der nuklearen wie auch der konventionellen Rüstungskontrolle waren bisher numerische Grenzen und Zählregeln die Dreh- und Angelpunkte. Im Nuklearbereich wurden Sprengköpfe und Trägersysteme gezählt, im konventionellen Bereich Längen, Höhen, Breiten und Leergewichte gemessen. Bei in ihren Fähigkeiten zunehmend von Software geprägter konventioneller Hochtechnologie hat dieser Ansatz weniger, im Falle von Cyberfähigkeiten keinerlei Bedeutung mehr. Denn wenn die Effektivität eines physischen Waffensystems sich primär aus äußerlich nicht erkennbaren Faktoren wie etwa Autonomiegrad oder auch Zusammenwirken mit verteilten Sensoren und anderen Waffenplattformen ergibt, dann wird die Verifikation von Rüstungskontrollabkommen deutlich schwieriger.

Das quantitative wird im digitalen Zeitalter durch ein qualitatives Paradigma ergänzt werden müssen, wenn die Rüstungskontrolle ihre politisch stabilisierende Funktion behalten soll. Während diese Erkenntnis nicht neu und in Fachkreisen längst Diskussionsgegenstand ist, steht die Forschung zu Lösungen noch am Anfang. Fest steht jedoch zumindest, dass digitale Technologien nicht nur Herausforderung, sondern auch Chance für die Rüstungskontrolle sind. Erste Studien zur Nutzung von distributed ledger-Lösungen (Blockchain) im Bereich des nuklearen Nichtverbreitungsregimes legen beispielsweise nahe, dass sich nicht nur für die Rüstung, sondern auch für die Rüstungskontrolle im digitalen Zeitalter neue Horizonte auftun.

Strategische Stabilität

Die Möglichkeit zur Automatisierung von Prozessen ist ein wesentliches Kennzeichen des digitalen Zeitalters – im Zivilen wie im Militärischen.[6] Im hochsensiblen und

3 Die Prinzipien legen nahe, dass Google für ausschließlich gegen Objekte wirkende Waffensysteme – nach Abwägung – eine Ausnahme machen könnte. Nur gegen Munition wirkende Verteidigungssysteme wären dafür wohl ein plausibles Beispiel.

4 Exemplarisch seien hier die offenen Briefe des Future of Life Institute genannt, die stets von führenden Köpfen im Bereich der KI und angrenzenden Feldern sowie prominenten öffentlichen Intellektuellen unterschrieben werden. Die Liste reicht von Demis Hassabis und Mustafa Suleyman von Googles DeepMind über den jüngst verstorbenen Stephen Hawking bis hin zu Elon Musk.

5 Prof. Zhou Zhihua von der Nanjing Universität.

6 In Letzterem kann dies bis zur Auswahl und Bekämpfung von Zielen ohne menschliche Verfügungsgewalt reichen, siehe „Sicherheitspolitische Auswirkungen der Digitalisierung", Metis Studie Nr. 1 (2/2018).

notorisch konservativ gehandhabten Nuklearbereich stößt die Automatisierung von Prozessen an eine besondere Grenze. Die Entscheidung über den Gebrauch von Nuklearwaffen wird (auf absehbare Zeit) nicht automatisiert werden. Der Fall des Oberstleutnant Stanislaw Petrow, der 1983 als leitender Offizier den Alarm des sowjetischen Frühwarnsystems, das einen US-Nuklearwaffenangriff meldete, in Zweifel zog und damit eine wahrscheinliche nukleare Eskalation verhinderte, steht sämtlichen Nuklearwaffenstaaten (hoffentlich) klar vor Augen. Petrow begründete seine – korrekte – Entscheidung später damit, dass das Warnsystem neu gewesen sei, die geringe Anzahl der gemeldeten US-Raketen keinen Sinn für einen Erstschlag ergeben habe und sein Bauchgefühl ihn an der Echtheit des Alarms hatte zweifeln lassen. Menschliche Urteilskraft, das zeigt das Beispiel Petrow, beruht auf der Kompetenz, zahlreiche subtile Kontextinformationen auswerten zu können. Vergleichbare Entscheidungskompetenz wird auf absehbare Zeit nicht maschinell reproduzierbar sein.

So wenig wahrscheinlich wie das Delegieren der existenziellen Entscheidung eines Nuklearwaffengebrauchs an Algorithmen ist zudem die Gefährdung der strategischen Stabilität durch direkte Zugriffe über das Internet.

Dennoch verschärfen Internet und Digitalzeitalter bestimmte im Nuklearsektor angelegte Risiken,[7] insbesondere solche der Fehlkalkulation und Fehlperzeption. Zu diesen mittelbaren Risiken gehört die Manipulation der Informationslandschaft, in der politisch-militärische Entscheidungen stattfinden. Besonderes Aufsehen erzeugte hier jüngst die auf Deep Learning beruhende Technik der deep fakes, insbesondere deep fake-Videos, die sich in Echtzeit generieren und zu manipulativen Zwecken verbreiten lassen. Damit werden, in einer Zeit, in der der primäre Kommunikationskanal des US-Präsidenten Twitter und Nordkorea Nuklearwaffenstaat ist, neue Manipulations- und Eskalationsszenarien Realität.[8] Altbekannte risikomindernde Maßnahmen wie no first use-Doktrinen oder die Senkung des nuklearen Alarmstatus, um in Krisensituationen Zeit zu gewinnen, erhalten dadurch neue rüstungskontrollpolitische Relevanz.

Quantencomputer: Die kommende Revolution?

Den Transmissionsriemen zur Umwandlung von Daten in ökonomische und militärische Macht bildet derzeit die gewachsene Rechenkapazität herkömmlicher Computer in Kombination mit maschinellem Lernen. In den USA, China und Europa[9] wird inzwischen an Quantencomputern geforscht. IBM in den USA und Alibaba in China bieten zu experimentellen Zwecken bereits Prototypen für cloudbasiertes Quantencomputing an.

Quantencomputer wären, träten sie denn tatsächlich irgendwann den Schritt aus dem Labor in die tägliche Nutzungspraxis an, eine umwälzende Neuerung. Kommunikation, Sensorik und Navigation – um nur drei Felder zu nennen – würden revolutioniert. Quantencomputer nutzen primär zwei quantenmechanische Phänomene: Superposition und Verschränkung.

Superposition beschreibt eine Überlagerung von Zuständen. Konkret nutzen Quantencomputer Superposition in QBits, die, anders als Bits mit nur zwei diskreten Zuständen (1 oder 0) in herkömmlichen Computern, beide Zustände zeitgleich annehmen können. Ein Anwendungsszenario ist die Nutzung der aus QBits resultierende immensen Rechenleistung, um nach bisherigen Standards sicher verschlüsselte Daten in kürzester Zeit zu entschlüsseln. Die Auswirkungen auf Kommunikationsflüsse oder kritische Infrastrukturen wie das Finanzwesen wären weitreichend. Bis dato lagernde und nicht entschlüsselbare Datenbestände könnten mit einem Schlag offengelegt werden – nicht zuletzt für Geheimdienste ein Alptraumszenario.

Verschränkung beschreibt das Phänomen, nach dem zwei oder mehrere Teilchen (bspw. Photonen) auch über große Distanzen hinweg den stets gleichen Zustand annehmen. Konkret genutzt in Form quantenkryptographischer Anwendungen ermöglicht dies einen abhörsicheren Austausch von Informationen. Abhörsicher deshalb, weil die quantenmechanische Verschränkung es unmöglich macht, die Kommunikationsverbindung ohne leicht erkennbare Störung abzuhören – ein unbemerktes Mitlauschen ist bei Quantenkryptographie quasi naturgesetzlich ausgeschlossen. China startete mit Micius bereits 2016 den ersten „Quanten-Satelliten" der Welt, mit dem ein quantenkryptographisch gesicherter Videoanruf zwischen Peking und Wien demonstriert wurde. Sowohl in China als auch in den USA und Europa ist aktuell der Aufbau von Glasfaser-basierten Prototypen für ein „Quanten-Internet" im Gang.

Ein drittes Beispiel für eine relevante Anwendung von Quantencomputern liegt im Bereich extrem präziser Sensorik. Konkret beschäftigt Washington die Sorge, dass der chinesische Vorsprung in der Nutzung von Quantentechnologie für den Radarbereich die bisherige

7 Siehe auch Metis Studie Nr. 1 (2/2018), S. 4–5.

8 Bsp.: „You Won't Believe What Obama Says In This Video!" https://youtube.com/watch?v=cQ54GDm1eL0
Noch sind deep fake-Videos auf den zweiten Blick als Täuschung zu entlarven. In wenigen Jahren wird dies nur noch mit speziellen Hilfsmitteln möglich sein.

9 Die Bundesregierung hat im September 2018 ein mit rund 650 Mio. EUR gefördertes „Forschungsprogramm Quantentechnologie" beschlossen. Neben dem Bundesministerium für Bildung und Forschung sind auch Wirtschafts-, Innen und Verteidigungsressort an dem Vorhaben beteiligt.

US-Vormachtstellung im Bereich Stealth schlagartig zunichtemachen könnte.

Bisher sind Quantencomputer Laborexperimente ohne nennenswerten ökonomischen, geschweige denn militärischen Nutzen. Es ist unklar, ob und wie sich ihre Nutzung skalieren und generalisieren lässt. Dennoch muss das Feld vorausschauend beobachtet werden. Selbst ein auf nur wenige Spezialanwendungen begrenzter Parallelbetrieb zu herkömmlichen Computerinfrastrukturen könnte, militärisch genutzt, asymmetrierende machtpolitische Effekte haben. So könnte beispielsweise mit einer Vorreiterschaft im Feld der Quantencomputer-gestützten Ent- und Verschlüsselung die globale Dominanz im Informationsraum einhergehen.

Schlussbetrachtung: Deutschland in der Weltordnung des Digitalzeitalters

Die Transformation von Daten in Macht mittels Technologie spielt nur eine ermöglichende, großmachtpolitisch nichts determinierende Rolle. Mit Blick auf die Weltordnung des Digitalzeitalters gilt es unbedingt auch zu fragen, wie unterschiedliche Gesellschaftsmodelle mit dem technologischen Wandel wechselwirken.

Dampfmaschine, Telegraf, Verbrennungsmotor und Radio setzten in den vergangenen zwei Jahrhunderten der ökonomischen und politischen Zentralisierung Grenzen. Das Modell Sowjetunion zerbrach, aus ökonomischer Sicht, nicht zuletzt daran, dass aufgrund von Informationsmangel von Moskau aus weder die Verteilung der Weizenernte effektiv zentral gesteuert noch ein lokaler Brotpreis sinnvoll bestimmt werden konnte. Informationsarmut begünstigte die dezentralen Organisationsformen Marktwirtschaft und Demokratie. Dass beide jedoch nicht zwingend Hand in Hand gehen müssen, demonstriert China. Hinzu kommt nun die Datenflut des Digitalzeitalters. Informationsüberfluss, nicht -mangel, wird zur Regel. Zentralistisch und autoritär organisierte Systeme könnten erstmals einen historischen Vorteil genießen gegenüber solchen, in denen zentralisiertes Sammeln, Verarbeiten und Anwenden von Daten durch Normen, Gesetze und Institutionen begrenzt ist – der wohl ungleiche Widerstand in den USA und China gegen zivil-militärische Integration, inklusive konkreter Beispiele wie Projekt Maven, fügt sich in dieses Bild.

Die Anziehungskraft derart technisch unterfütterter autoritärer Systeme ist nicht zu unterschätzen. Die Mehrzahl der Staaten weltweit entspricht nicht dem OECD-Ideal einer Demokratie. Für Gesellschaften, in denen keine gewachsenen, gefestigten Vertrauensverhältnisse existieren, bietet Totalüberwachung in Kombination mit Social Credit-Systemen, wie in China derzeit erprobt, die attraktive Möglichkeit, ein funktionierendes Gemeinwesen ohne „lästige" demokratische und rechtsstaatliche Elemente herzustellen. So begrüßen erstaunlich viele Chinesen die reputationsbasierten Sozialkreditsysteme, weil sie sich von diesen mehr Korruptionsbekämpfung und Fairness versprechen.

Hinzu kommen neue technische Möglichkeiten zur Beeinflussung von Bevölkerungen durch Manipulation des Informationsraums und somit politischer Willensbildungsprozesse – auch hier sind liberale Demokratien besonders anfällig. Dass dieses Gesellschaftsmodell im noch jungen Digitalzeitalter aktuell von innen wie außen unter Druck steht, ist ein klares Warnsignal.

Die aus deutscher Sicht mit Blick auf die künftige Weltordnung entscheidende Frage reicht somit über den Bereich der Sicherheitspolitik hinaus. Sie lautet: Kann die liberale Demokratie aufrechterhalten und samt sozialer Marktwirtschaft für das Digitalzeitalter erneuert werden?

Anlass zu Optimismus gibt die Tatsache, dass das Wettrennen der Großmächte um den Vorsprung bei der Digitalisierung im Kern ein Wettbewerb um die besten Talente ist – erst sie bringen Innovation hervor. Noch haben die liberalen Demokratien, allen voran die USA, hier die Nase vorn. China ist dies bewusst, weswegen es im Ausland studierende oder arbeitende chinesische Talente aggressiv umwirbt und zu einer Rückkehr bewegen will. In der Attraktivität ihres Gesellschaftsmodells und den Chancen auf Freiheitsrechte, Sicherheit, Bildung und Wohlstand müssen offen, demokratisch, rechtsstaatlich, pluralistisch und marktwirtschaftlich organisierte Gesellschaften also (weiterhin) ihren Vorteil sehen. Soll dieses Modell im Digitalzeitalter stark und glaubwürdig bleiben, dann muss es weiterentwickelt werden. Daraus ergeben sich drei große Handlungsfelder für Deutschlands liberaldemokratisches Politik- und sein sozialmarktwirtschaftliches Wirtschaftsmodell:

- Regelsysteme entwickeln, die Informationsüberfluss mit den Prinzipien von liberaler Demokratie und Rechtsstaatlichkeit vereinen und die Gewalt über Daten auf das Individuum zurückverlagern;[10]

- Fortbildung ermöglichen, um die durch Automatisierung entstehenden Strukturveränderungen am Arbeitsmarkt abzufedern;

- Ökologie als feste politische Kategorie in die soziale Marktwirtschaft integrieren und dies international als Leitidee bewerben, um den sozialen und ökonomischen Externalisierungseffekten der Marktwirtschaft (insbesondere dem Klimawandel) zu begegnen.

10 Eine entsprechende Antwort wären offene Systeme, die Nutzern Sicherheit und Privatsphäre zurückgeben und es ihnen erlauben, Zugriffe durch Staaten und Unternehmen zu steuern. Der Erfinder des World Wide Web, Tim Berners-Lee, hat mit „Solid" ein solches Projekt aus der Taufe gehoben.

Metis

IMPRESSUM

Herausgeber

Metis Institut
für Strategie und Vorausschau
Universität der Bundeswehr
München
metis.unibw.de

Autor

Dr. Frank Sauer
metis@unibw.de

Creative Director

Christoph Ph. Nick, M.A.
c-studios.net

Titelbild

Daniel Chen auf Unsplash

ISSN-2627-0587