KONRAD ADENAUER STIFTUNG

Quantentechnologie und Deutschlands Sicherheitspolitik

Eine geopolitische Notwendigkeit

Manuel Steudle

#KAS4SECURITY

kas.de

Quantentechnologie und Deutschlands Sicherheitspolitik

Eine geopolitische Notwendigkeit

Auf einen Blick

- Quantentechnologie ist eine sicherheitspolitische Schlüsseltechnologie: Sie gilt als Emerging and Disruptive Technology (EDT) mit enormem Potenzial für militärische und zivile Anwendungen.
- Quantencomputing bedroht heutige Verschlüsselungssysteme: Die Fähigkeit von Quantencomputern, gängige Verschlüsselungen zu entschlüsseln, stellt eine Bedrohung für Cybersicherheit, kritische Infrastrukturen und militärische Kommunikation dar.
- Quantensensorik revolutioniert Aufklärung und Navigation: Sie könnte die satellitenunabhängige Navigation und präzisere Ortung zum Beispiel von Hyperschallwaffen oder U-Booten ermöglichen.
- Quantenkommunikation erlaubt sicherere Datenübertragung: Mit solchen Verfahren kann abhörsichere Kommunikation gewährleistet werden – ein entscheidender Vorteil in hybriden und konventionellen Konflikten.
- Spill-Over-Effekte auf andere Technologien: Quantentechnologie verstärkt und beschleunigt Entwicklungen in KI, Hyperschalltechnik, Materialforschung und Raumfahrt – sie ist somit ein zentraler Katalysator für andere EDTs.
- Mangelhafte Einbindung in deutsche Sicherheitsarchitektur: Die Bundeswehr ist bislang konzeptionell und strukturell unzureichend auf die Integration von Quantentechnologien vorbereitet.
- Risiken für innere Sicherheit und den Datenschutz: Quantenfähige Angriffe auf Verschlüsselungssysteme gefährden personenbezogene Daten, kritische Infrastrukturen und ermöglichen neue Formen der Überwachung und Desinformation.
- Deutschland droht, im internationalen Wettbewerb um Quantentechnologie zurückzufallen, insbesondere gegenüber den USA und China, was sicherheitspolitische Abhängigkeiten und Risiken verstärkt.
- „Quantum Readiness“ für Deutschland: (a) Quantentechnologien müssen systematisch in die nationale Sicherheitsstrategie, Bundeswehrplanung und Rüstungsdokumente integriert werden. (b) Die Innovationsarchitektur muss reformiert werden: durch eine vergabefähige Agentur, gezielte Förderung von Dual-Use-Start-ups, Abbau bürokratischer Hürden und Anreize für Risikokapital. Ziel ist eine agile, sicherheitsrelevante Technologieförderung mit schneller Umsetzung in die Praxis. (c) Deutschland sollte seine internationale Zusammenarbeit mit NATO, EU und technologisch führenden Staaten strategisch ausbauen, um Souveränität in Quanteninfrastruktur und -anwendungen zu sichern. Gleichzeitig gilt es, gesellschaftliche Auswirkungen zu erforschen, Normen zu setzen und digitale Souveränität sowie Datenschutz zu wahren.

Inhalt

Abkürzungsverzeichnis

CAS	Chinese Academy of Sciences
CIH	Cyber Innovation Hub
CIR	Kommando Cyber- und Informationsraum
DARPA	Defense Advanced Research Projects Agency
EDT	Emerging and Disruptive Technologies
KI	Künstliche Intelligenz
MDB	Multi-Domain-Battlefield
MDO	Multi-Domain-Operation
OPCW	Organisation for the Prohibition of Chemical Weapons
PLAISF	People's Liberation Army Information Support Force
PLASSF	People's Liberation Army Strategic Support Force
QKD	Quantum Key Distribution
RSA	Rivest-Shamir-Adleman
USTC	University of Science and Technology of China

Einführung

Anlässlich des hundertjährigen Jubiläums der Entdeckung der Quantenmechanik startet 2025 in Deutschland das Quantenjahr: eine breit angelegte Forschungsinitiative im Bereich der Quantentechnologie. Die Quantentechnologie und ihre Anwendung in den Bereichen Computing, Sensorik und Kommunikation werden seit Längerem als Schlüsseltechnologie mit enormem Potenzial angesehen. Als Technologie, die von der NATO und im englischsprachigen Diskurs als Emerging and Disruptive Technology (EDT) bezeichnet wird, trägt sie ähnlich wie künstliche Intelligenz (KI) oder Weltraumtechnologie aber nicht nur Charakteristika, die der Menschheit förderlich sind. EDTs haben immer auch einen disruptiven Charakter, der sich auf die Gesellschaft, die Politik und die Sicherheitspolitik auswirkt.

In der Vergangenheit gab es stets eine enge Verzahnung von technologischem Fortschritt und schädlicher Anwendung neuer Technologien. Das prominenteste Beispiel aus der jüngeren Geschichte ist wohl die Entdeckung der Kernspaltung: Einerseits läutete sie energiewirtschaftlich ein neues Zeitalter ein, andererseits ermöglichte sie die Entwicklung von Atombomben. Technologien, die eine solche doppelte Verwendungsfähigkeit aufweisen, werden als Dual-Use-Technologien bezeichnet. Das sind technische Anwendungen, die sowohl dem zivilen als auch dem militärischen Bereich einen Nutzen versprechen oder innerhalb dieser Bereiche verwendet werden können.

Neue Technologien finden heute sehr schnell Anwendung in Konflikten. Zugleich lässt sich beobachten, dass Deutschland bei der Entwicklung und Anpassung solcher Technologien zurückfällt. Zwar ist die deutsche Grundlagenarbeit international konkurrenzfähig, doch letztlich sind es Unternehmen und Einrichtungen aus den USA und China, die die Kommerzialisierung und breite Nutzung neuer Technologien, wie es gegenwärtig im Bereich KI zu beobachten ist, ermöglichen. Eine vergleichbare Entwicklung gilt es im Bereich der Quantentechnologie zu verhindern. Dies ist nicht nur wichtig, um den Industriestandort Deutschland wettbewerbsfähig zu halten, sondern auch, um die nationale Sicherheit zu gewährleisten.

Ziel dieses Beitrags ist es, die Herausforderungen der Quantentechnologie für die Sicherheitspolitik Deutschlands in einer zunehmend volatilen Welt zu skizzieren, die damit verbundenen Gefahren herauszustellen und politische Handlungsoptionen aufzuzeigen.

Strategische Herausforderung

Während Staaten wie die USA, China und Frankreich die sicherheitspolitischen Implikationen disruptiver Technologien seit Jahren strategisch berücksichtigen, hat Deutschland diese Entwicklung lange vernachlässigt. In vielen Fällen – sei es bei der Digitalisierung oder der Forschung und Entwicklung von KI – fokussierte sich die Bundesregierung vor allem auf die wirtschaftliche oder zivile Entwicklung und ließ damit sicherheitspolitische Implikationen außer Acht.

Die neue Bundesregierung scheint sich dieser Herausforderung jedoch bewusst zu sein und will neue Technologien stärker in die sicherheitspolitische Planung einbeziehen. Die angekündigte Stärkung der Dual-Use-Forschung, die Förderung zivil-militärischer Kooperationen sowie der verstärkte Technologietransfer in die Streitkräfte sind dafür erste wichtige Schritte. Auch wenn Quantentechnologien darin bislang keine explizite Rolle spielen, deutet die geplante Veröffentlichung der Weltraumsicherheitsstrategie beispielsweise auf ein wachsendes Problembewusstsein hinsichtlich neuer technologischer Entwicklungen hin.

Diese Prioritätenverschiebung lässt sich auch an der Struktur der Ministerien ablesen. So wurde neben der Schaffung eines Digitalministeriums der Fachbereich Bildung aus dem Ministerium für Bildung und Forschung ausgegliedert und die Bereiche Technologie und Raumfahrt hinzugefügt. Damit soll die Forschung in der kommenden Legislaturperiode noch deutlicher als Innovationstreiber verstanden und gefördert werden. Aus diesem Grund ist auch die Förderung der Forschung und Entwicklung im Bereich Quantentechnologie in diesem Ministerium verortet. Die sicherheitspolitischen Implikationen der Quantentechnologie spielen in diesem Zusammenhang allerdings keine gewichtige Rolle. Eine Verknüpfung der wirtschaftlichen und sicherheitspolitischen Aspekte fehlt also derzeit noch. Gegenwärtig ist auch unklar, ob und wie die Quantentechnologie unmittelbar im sicherheitspolitischen Kontext von den neuen fiskalischen Spielräumen im Verteidigungsbereich profitieren könnte. Einzig das jüngste Papier zur Nationalen Sicherheits- und Verteidigungsindustrie-Strategie erkennt Quantentechnologien als Schlüsseltechnologien an, ohne deren sicherheitspolitisches Potenzial jedoch umfassend zu adressieren.

Diese Lücke ist strategisch riskant. Während im aktuellen sicherheitspolitischen Diskurs weiterhin die Debatte um klassische Rüstungssysteme dominiert, spielen innovative Technologien wie KI, unbemannte Systeme oder militärische Raumfahrtanwendungen weiterhin eine eher untergeordnete Rolle, obwohl sie die Kriegsführung bereits heute tiefgreifend verändern. Die sicherheitspolitischen Implikationen von Entwicklungen in der Quantentechnologie werden diese Veränderungen jedoch noch übertreffen und auch die anderen EDTs sowie deren Entwicklung und Einsatz maßgeblich beeinflussen.

Deutschland steht damit sicherheitspolitisch vor einem Wendepunkt. Ein strategischer Umgang mit Quantentechnologien ist dringend erforderlich, um internationale Anschlussfähigkeit sicherzustellen und technologische Souveränität im sicherheitspolitischen Bereich zu gewährleisten. Die Herausforderung besteht dabei nicht nur in der technologischen Entwicklung, sondern auch in ihrer gezielten sicherheitspolitischen Analyse und Integration. Nur wenn Quantentechnologien systematisch in Strategien, Risikoanalysen, Strukturen und Fähigkeitsprofile eingebunden werden, kann Deutschland den sicherheitspolitischen Quantensprung aktiv gestalten.

Quantum-Warfare

Neue Kriegsführung und Informationen

Der militärische Nutzen, der sich aus der Quantentechnologie ergibt, sowie das daraus entstehende sicherheitspolitische Erfordernis, entsprechende Rahmenbedingungen für ihre Erforschung und Entwicklung zu schaffen, werden gerade anhand der neuen Art der Kriegs- und Konfliktführung besonders deutlich. Seit den 1990er-Jahren, als der Begriff „Information Warfare“ in US-Militärkreisen aufkam und spätestens bei der Operation Desert Storm in die Praxis überführt wurde, versetzt diese bis heute im Kern gültige Militärdoktrin die Komponente der Information in den Mittelpunkt jeglicher Kriegs- und Konfliktführung.

Dabei werden Informationen sowohl als Ziel, Waffe, Quelle als auch Einsatzfeld verstanden. Sie sollen eine Überlegenheit in Friedens- und Kriegszeiten gewährleisten. Konkret bedeutet dies einerseits, die Informationskanäle des Gegners zu sabotieren, auszuspionieren oder Informationen zu manipulieren – und andererseits, die eigenen Informationen und Informationskanäle gegen feindliche Angriffe abzuschirmen.

Das Ziel besteht also darin, im Kriegsfall die Kill-Chain des Gegners zu stören, während die eigene intakt bleibt. Die Kill-Chain beschreibt den Ablauf von der Auswahl eines Ziels bis zu dessen Ausschaltung. In jedem einzelnen Schritt sind Informationen zur Erfüllung der Mission wesentlich. Innerhalb dieses Prozesses sind sowohl die Gewinnung als auch die Verarbeitung und die Verbreitung von Informationen erforderlich. Kommt es auch nur zu einer Störung in einem dieser drei Bereiche, kann die Kill-Chain nicht mehr reibungslos funktionieren und es besteht die Gefahr, die Informationshoheit zu verlieren. Durch das Anwachsen der Rechenleistung, Verbesserungen im Cyberbereich und Ähnliches wurde dies in den letzten Jahrzehnten noch wichtiger und erhielt eine weitere Dimension.

Mittlerweile sprechen die USA, die NATO und auch die Bundeswehr als Teil der NATO von der sogenannten Multi-Domain-Operation (MDO) beziehungsweise dem Multi-Domain-Battlefield (MDB), siehe Abbildung 1. Dabei werden die Methoden und Konzepte des Information Warfare in ein komplexes, mehrdimensionales Schlachtfeld überführt. Ziel ist die simultane Vernetzung und Orchestrierung aller Domänen (Land, Luft, See, Weltraum und Cyber), was eine umfassende Echtzeit-Informationsgewinnung, schnelle Informationsverarbeitung und gesicherte Informationsverbreitung über alle Domänen hinweg erfordert.

Manche sprechen in diesem Zusammenhang vom Transfer des in der Wirtschaft bereits diskutierten „Internets der Dinge“ zum „Internet der militärischen Dinge“. Dies ist unter anderem auch ein Grund, weshalb die Diskussion über Weltraum-Kapazitäten in deutschen und europäischen Sicherheitskreisen immer präsenter wird. Der Weltraum ist neben der Quantentechnologie eine von der NATO aufgelistete Technologie und betrifft vor allem die Bereiche Informationsgewinnung und -verbreitung. Die Quantentechnologie betrifft alle drei Bereiche dieses Komplexes und nimmt somit einen erheblichen Einfluss auf die Verteidigungs- und Angriffsfähigkeit.

Da hybride Kriegsführung oftmals so unterschwellig ist, dass Aktionen nicht als direkter Kriegsakt gewertet werden, spielt der Themenkomplex Information ebenfalls eine große Rolle. Die Quantentechnologie wird daher nicht nur in Kriegs-, sondern auch in Friedenszeiten erhebliche Auswirkungen auf die Sicherheitspolitik eines Landes haben. Dazu zählen unter anderem Desinformationskampagnen,

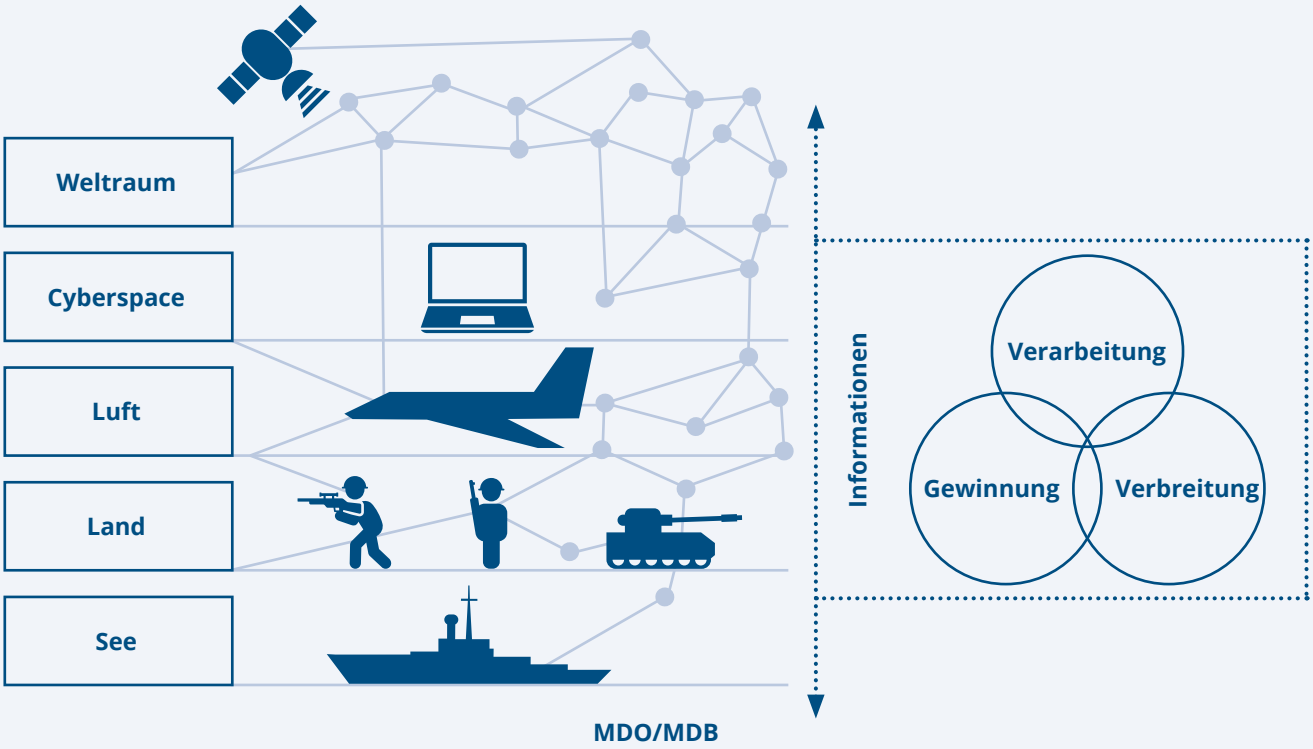


Abbildung 1: Eigene Darstellung der MDO/MDB-Doktrin

wie sie beispielsweise die Russische Föderation in westlichen Staaten, darunter Deutschland, betreibt, sowie Cyberangriffe mit dem Ziel der Extraktion von Informationen oder der Disruption von Informationskanälen. Deshalb ist es wichtig, im Rahmen der Fortschritte in den Quantentechnologien von einer Gefahr für die innere und äußere Sicherheit zu sprechen und dabei sowohl die militärische als auch die zivile Anwendung und deren sicherheitspolitische Implikationen im Blick zu behalten.

In unserer heutigen vernetzten Welt spielt der Informationsbereich eine Schlüsselrolle für die Sicherheit eines Landes – sowohl im zivilen als auch im militärischen Bereich. Die Auswirkungen von Entwicklungen in der Quantentechnologie auf die Informationssphäre im Allgemeinen veranlassen viele Akteure der Sicherheitspolitik, vom kommenden „Zeitalter des Quantum-Warfare“ zu sprechen. Dieses Zeitalter wird durch eine enorme Steigerung der Leistungsfähigkeit von Computern, Sensorik, Navigation, autonomen Waffensystemen, Kryptografie, Radarsystemen und elektronischer Kriegsführung geprägt sein. Diese Leistungssteigerung wird Kriege insgesamt schneller, präziser und gefährlicher machen und die Bedeutung der determinanten Information nochmals deutlich erhöhen. Deutschland muss daher seine Informationshoheit im Zeitalter des Quantum-Warfare wahren und ausbauen, um die innere und äußere Sicherheit zu gewährleisten.

Anwendungsbereiche

Quantencomputing: Kryptoanalyse, Simulation und Optimierung

Der Bereich des Quantencomputings ist derzeit wohl der am stärksten wahrgenommene Anwendungsbereich der Quantentechnologie im öffentlichen und politischen Diskurs. Quantencomputer können deutlich leistungsfähiger sein als herkömmliche Computer, da sie nicht auf klassische Schaltkreis-Chips zurückgreifen, sondern die Eigenschaften von Atomen nutzen. Das erlaubt eine deutlich umfangreichere und schnellere Informationsverarbeitung. Im sicherheitspolitischen Kontext bezieht sich das Quantencomputing vor allem auf den Bereich der Informationsverarbeitung, der wiederum in die drei

Bereiche (i) **Kryptoanalyse**, (ii) **Simulation** und (iii) **Optimierung** unterteilt werden kann.

Kryptoanalyse

Für Sicherheitskreise ist der wohl brisanteste Anwendungsbereich von Quantencomputern die Kryptoanalyse. Dieser Bereich umfasst Wissenschaft und Technik zur Entschlüsselung von verschlüsselten und somit sensiblen Informationen. Gängige Verschlüsselungen – seien sie militärisch oder zivil – verlassen sich üblicherweise auf die sogenannte Primzahl-Faktorisierung, auch Rivest-Shamir-Adleman (RSA)-Verschlüsselung genannt. Die zivilen und militärischen Bereiche unterscheiden sich hier zumeist nur durch die Stärke der identischen Grundverschlüsselung.

Ein herkömmlicher Computer bräuchte mehrere Milliarden Jahre, um einen gängigen RSA-Schlüssel zu entschlüsseln. Ein Quantencomputer allerdings würde für diese Entschlüsselung nur wenige Stunden benötigen, wie Peter W. Shor bereits in den 1990er-Jahren mit einem entsprechenden Algorithmus bewiesen hat. Die Entschlüsselung von RSA-Schlüsseln mithilfe eines Quantencomputers und das Freilegen selbst streng geheimer, militärisch oder politisch relevanter Informationen stellt also ein enormes Sicherheitsrisiko in Friedens-, aber vor allem in Kriegszeiten dar.

In Fachkreisen wird die Entwicklung eines solchen vollumfänglichen Codebrecher-Quantencomputers bis zum Ende der 2030er-Jahre erwartet. Sie kommen zu diesem Fazit, da es noch große technische Probleme gibt. Dies wird in Berichten und als Replik auf Erfolgsmeldungen von beispielsweise Google oder IBM immer wieder deutlich. Die größten Probleme sind nach wie vor die Fehlerquoten, die mangelnden Speicherkapazitäten und die enorme Kühlung. Eine sogenannte Quantensuprematie, die oft nach der Entwicklung eines neuen Quantencomputers ausgerufen wird, ist also noch nicht erreicht. Der Meilenstein der Quantensuprematie ist dabei klar definiert. Er ist erst erreicht, wenn ein Quantencomputer sämtliche Aufgaben erledigen kann und heutige Computer somit in jedem Aufgabenbereich ablöst.

Nichtsdestotrotz darf der Gedanke an einen Quantencomputer im Bereich der Kryptoanalyse heute nicht beiseitegelegt werden. Die heute gängigen Sammeln-und-morgen-entschlüsseln-Angriffe und die Unsicherheit bezüglich der Entwicklungsgeschwindigkeit machen es notwendig, sich bereits heute sowohl mit der Defensive als auch mit der Offensive zu beschäftigen. Dies ist unabdingbar für die Wahrung der Informationshoheit in Kriegs- und Friedenszeiten. Nicht ohne Grund gab die NSA bereits im Jahr 2022 das Ziel aus, alle sensiblen Daten bis spätestens 2035 mit selbst für Quantencomputer schwer bis gar nicht entschlüsselbaren Codes zu versehen.

Simulation

Eine weitere Anwendung, die derzeit vor allem im medizinischen Sektor intensiv erforscht wird, ist die Simulation komplexer Vorgänge mithilfe von Quantencomputern. Durch die hohe Rechenleistung und die parallele Modulation von Geschehnissen mithilfe der Qubits ist es möglich, komplexe Vorgänge zu simulieren. In der Medizin, Materialforschung und anderen Bereichen bezieht sich das auf das Verhalten von Organen oder Materie im Allgemeinen. Das kann einerseits zur Entdeckung neuer Medikamente und somit zur Rettung von Menschenleben führen, andererseits aber auch zur Entwicklung neuer chemischer und biologischer Kampfstoffe. Im Bereich der Materialforschung können zudem neue Legierungen entwickelt werden, die eine höhere Stealth-Fähigkeit für Kampfjets ermöglichen.

Als direkte Anwendung der Simulation könnte der Quantencomputer mit einer großen Zahl an Informationen über Flugabwehrstellungen, mobile Bodeneinheiten, Abfangjäger usw. sowie eigenen Angriffskapazitäten gespeist werden. Anschließend könnte der Computer den besten Einsatzplan unter Berücksichtigung einer bestimmten Bedingung (z. B. die höchste Überlebenschance der eigenen Truppen) berechnen. Dies könnte sowohl vor dem Angriff als auch synchron zum Angriff selbst durchgeführt werden. Dadurch werden die verschiedenen Domänen im Sinne der MDO-Doktrin verknüpft und die verschiedenen Einheiten orchestriert, was nochmals deutlich effizienter und schneller erfolgt. Die Verarbeitung der wichtigsten Ressource des 21. Jahrhunderts, der Information, wird somit in allen Bereichen deutlich beschleunigt.

Optimierung

Da das Militär selbst in Friedenszeiten, aber vor allem in Kriegseinsätzen, ein sehr komplexer Bereich ist, gibt es viele Optimierungsmöglichkeiten. Besonders im von der breiten Öffentlichkeit unterschätzten Teilbereich der Logistik. Abseits von großen Waffensystemen wie Panzern und Kampfjets ist die Logistik der Dreh- und Angelpunkt eines Kriegseinsatzes und ermöglicht erst den Einsatz dieser Waffensysteme. Gerade für Deutschland, das im NATO-Kontext oft als Logistikdrehscheibe bezeichnet wird, ist dies von immenser Bedeutung.

Die Relevanz der Logistik wurde zuletzt beim russischen Angriffskrieg deutlich, als die russische Armee massive logistische Probleme hatte. Die USA haben die Wichtigkeit der Logistik schon seit Langem erkannt und beherrschen sie sehr gut. Bereits 2021 startete die Defense Advanced Research Projects Agency (DARPA), das Flaggschiff für militärische Forschung und Entwicklung – ein Programm, das Erkenntnisse aus der Quantencomputer-Forschung für klassische Computer adaptiert, um die Logistik effizienter zu gestalten. Das Ziel besteht darin, komplexe logistische Probleme zu lösen und somit diesen Prozess zu optimieren. Allein durch diese Anpassung auf klassischen Computern soll die Effizienzsteigerung laut einem Bericht der DARPA immens sein und den Faktor 10.000 der derzeit verfügbaren Quantencomputer übersteigen. Sollte im Laufe der Jahre die Quantensuprematie erreicht werden, wird dieser Faktor nochmals deutlich überschritten und es werden massive Optimierungsmöglichkeiten gehoben.

Quantensensorik: Koordination, Aufklärung

Sensoren jeglicher Art sind aus der heutigen Kriegsführung und Verteidigung zur Informationsgewinnung nicht mehr wegzudenken. Die hohe Sensibilität gegenüber externen Störungen, die bei der Entwicklung von Quantencomputern ein großes Problem darstellt, kann bei der Sensorik genutzt werden, um die Leistung deutlich zu erhöhen.

Quantensensorik bezeichnet die Verwendung quantenmechanischer Systeme zur Messung verschiedener physikalischer Größen, darunter elektrische und magnetische Felder, Schwerkraft, Beschleunigung sowie Rotation. Phänomene, die beim Quantencomputing als störend gelten – etwa der Einfluss von Temperatur oder Schwerkraft auf Qubits, werden in der Quantensensorik gezielt genutzt. Anstatt diese äußeren Einflüsse zu unterdrücken, macht man sie messbar. So werden dieselben Interferenzen, die im Quantencomputer zu Fehlern führen, bei der Quantensensorik zu einer wertvollen Informationsquelle.

Diese Messung findet im militärischen Bereich breite Anwendung, da sie das sogenannte Situationsbewusstsein im Einsatz deutlich verbessert. Betrachtet man das heutige Situationsbewusstsein, so stellt man fest, dass hierfür vor allem orbitale Infrastruktur – also Satelliten – verwendet wird. Die Störung solcher Satelliten durch Jamming und Spoofing wird in Fachkreisen häufig problematisiert. Dies kann die Fernaufklärung erschweren oder Einheiten auf der Erde orientierungslos zurücklassen. Beides erschwert die Orchestrierung der verschiedenen Einheiten im Sinne der Militärdoktrin des 21. Jahrhunderts und greift die Informationshoheit im Bereich der Gewinnung und Verbreitung an.

Koordination

Im Bereich der Koordination militärischer Einheiten ist eine satellitengestützte Positionsbestimmung heute unverzichtbar. Daher haben viele Staaten eigene Systeme entwickelt. Die USA nutzen GPS, die Russische Föderation GLONASS, die Volksrepublik China Beidou und die EU Galileo. Doch diese Systeme sind anfällig für Störungen im Datenaustausch mit den Satelliten, weshalb viele nach neuen Möglichkeiten der Positionsbestimmung suchen.

Die Quantensensorik bietet mit Magnetometern, Gravitations- und Beschleunigungsmessern sowie hochsensiblen Quantenuhren eine nicht orbital gebundene Lösung, da damit eine hochgenaue Positionsbestimmung ohne Satelliten möglich ist. In Situationen, in denen satellitengebundene Systeme nicht zur Verfügung stehen, nutzt man bereits sogenannte Trägheitsnavigationssysteme. Diese sind allerdings sehr fehleranfällig und müssen immer wieder mit einem Satelliten kalibriert werden. Werden die klassischen Sensoren durch Quantensensoren

ersetzt, ist keine weitere Kalibrierung nötig und die Genauigkeit wird stark erhöht, sodass eine Navigation ohne Satelliten möglich wird.

Hier werden bereits sogenannte superleitende Quanteninterferenzgeräte getestet, die derzeit jedoch noch eine extreme Kühlung benötigen. Viele dieser Sensoren basieren auf Ionen und Atomen, die in einer magneto-optischen Falle positioniert werden. Die externen Interferenzen mit diesen Ionen oder Atomen werden gemessen und ermöglichen eine hochentwickelte Sensorik von Magnetfeldern, elektrischen Feldern, Temperaturänderungen, Druck, Geschwindigkeit usw. und somit eine genaue Positionsbestimmung. Die Funktionsweise ist klar und die Marktreife liegt nicht mehr allzu weit in der Zukunft. Das Ziel besteht darin, diese Sensoren so zu konstruieren, dass sie aus einer Testumgebung in den tatsächlichen Einsatz überführt werden können.

Aufklärung

Im Bereich der (Fern-)Aufklärung, für die heute Satelliten, aber auch Radar-/Sonar-Systeme verwendet werden, wird die Quantensensorik ebenfalls eine neue Realität schaffen, mit der sich sicherheitspolitische Kreise auseinandersetzen müssen. Einige kennen möglicherweise bereits die LiDAR-Technik – eine Technik, die mithilfe von Lasern (Photonen) in den Urwäldern Mexikos längst überwucherte Pyramiden der Maya aufdeckte. Auf derselben Funktionsweise basierend kann ein LiDAR-System durch Quantenphotonik in seiner Detektionsbandbreite, Mehrwellenanwendbarkeit und Abtastrate deutlich verbessert werden. Dadurch ist es möglich, mit einem LiDAR-System höhere und detailliertere Auflösungen zu erzielen und im militärischen Bereich Systeme zu entdecken, die Tarnkappentechnologien nutzen.

Durch diese Quantenneuerung eröffnet sich aber auch ein neues Anwendungsfeld für LiDAR: Es kann zur punktgenauen Verfolgung von sehr schnellen Objekten, wie etwa Hyperschallraketen, eingesetzt werden. Damit kann die lange beschworene Unverwundbarkeit von Hyperschallraketen durch ihre Schnelligkeit negiert werden und ein Abfangsystem effizienter und genauer arbeiten. Das gilt auch für Interkontinentalraketen, die aufgrund ihrer Flugbahn im Orbit sehr schwer zu verfolgen sind.

Neben der verbesserten Verfolgung wird auch die Anzahl der benötigten Stationen reduziert, da ein Quanten-LiDAR-System einen größeren Bereich abdecken kann.

Ein chinesisches Team der University of Science and Technology of China (USTC), welche unter der Verwaltung der Chinese Academy of Sciences (CAS) steht, bewies im Jahr 2024 in einem experimentellen Einsatz die verbesserten Fähigkeiten des Quanten-LiDAR. Da sowohl die USTC als auch die CAS sehr eng mit dem chinesischen Militär zusammenarbeiten, ist die Nähe der Forschung zur militärischen Anwendung nicht von der Hand zu weisen. Dieses Experiment zeigt, dass wir uns im Bereich der Quantensensorik allgemein mit einem wesentlich kürzeren Zeithorizont zur Marktreife beschäftigen als im Computing-Bereich.

Eine weitere entscheidende Technologie der Quantensensorik zur Aufklärung ist die Schwerkraftmessung beziehungsweise die absolute Schwerkraftgradiometrie. Mithilfe dieser Technologie können Lufteinschlüsse in fester Materie erkannt und lokalisiert werden. Diese Technologie wird im Sicherheitsbereich mit großem Interesse, aber auch mit Sorge verfolgt, da damit unterirdische militärische Anlagen lokalisiert und genau kartiert werden können. Noch dramatischer ist, dass mit dieser Technik auch ein U-Boot in großer Tiefe aufgespürt werden kann. Beides, insbesondere Letzteres, gefährdet die gesicherte Zweitschlagfähigkeit, die als wichtigster Baustein der nuklearen Abschreckung gilt.

Wenn strategische U-Boote, die nach der Zerstörung des Heimatlandes Atomraketen zum Gegner tragen, lokalisiert und ausgeschaltet werden können, ist die Abschreckungswirkung eines initialen Einsatzes von nuklearen Interkontinentalraketen nicht mehr vorhanden. Zwar kann darüber spekuliert werden, dass infolge der Entwicklung solcher Technologien gegensätzliche Entwicklungen in der Quantentechnologie zur Verhinderung einer solchen Lokalisierung erfolgen, jedoch wird es zumindest einen Zeitraum geben, in dem die nukleare Abschreckung nicht mehr uneingeschränkt gilt. Dies würde die globale Sicherheit massiv beeinträchtigen.

Insgesamt birgt die Quantensensorik – auch wenn der Computing-Bereich häufiger im Fokus steht – im

militärisch-sicherheitspolitischen Sinne die größten Potenziale und Gefahren. Gerade im Rahmen der Wichtigkeit von Informationen und der Informationsgewinnung in der modernen Kriegsführung wird der Krieg der Zukunft massiv von dieser Technologie beeinflusst werden. Die Förderung der Forschung und Entwicklung muss daher für Deutschland eine hohe Priorität haben. Gerade im Bereich der klassischen Sensorik sind deutsche Firmen global relevant und verfügen über großes Know-how, was eine gute Voraussetzung für eine Führungsrolle Deutschlands in der Quantensensorik ist.

Quantenkommunikation

Kommunikation ist und bleibt das Rückgrat jeder militärischen Operation – insbesondere in Zeiten eines immer komplexeren und dynamischeren Gefechtsfelds. Der Trend geht dabei weg von der reinen akustischen Sprachübertragung hin zu umfassenden Datenverbindungen. Diese ermöglichen die schnelle Bereitstellung von Lagekarten, Echtzeitbildern und Videodaten – also der Informationen, die auf dem Schlachtfeld des 21. Jahrhunderts unabdingbar sind. Der Preis dafür ist jedoch hoch: Die Anforderungen an die Leistungsfähigkeit und Ausfallsicherheit der Kommunikationssysteme steigen rapide, ebenso wie ihre Verwundbarkeit.

Ein vielversprechender Ansatz ist die Nutzung sogenannter atombasierter Rydberg-Antennen. Diese ermöglichen es, elektromagnetische Felder mit bislang unerreichter Präzision zu detektieren. Während herkömmliche Antennen je nach Frequenzbereich mehrere Dezimeter bis Meter groß sein müssen, können Rydberg-Antennen auf wenige Millimeter reduziert werden. Dadurch wird das Potenzial für kompakte, breitbandige Empfangssysteme eröffnet – insbesondere in Szenarien, in denen Größe, Gewicht und Energieverbrauch kritisch sind. Noch sind diese Sensoren auf starke Kühlung angewiesen und befinden sich in einem frühen Stadium der Entwicklung. Wenn die technischen Hürden erfolgreich überwunden werden, verspricht diese Technologie jedoch einen tiefgreifenden Wandel im Bereich der Gefechtsfeldkommunikation.

Mit der steigenden Datenmenge und Vernetzung rückt die Sicherheit der militärischen Kommunikation zunehmend in den Mittelpunkt. Derzeit dominieren asymmetrische kryptografische Verfahren, deren langfristige Sicherheit durch Quantencomputer – wie bereits erwähnt – bedroht sein wird. Symmetrische Systeme bieten zwar theoretisch eine höhere Sicherheit, sind in der Praxis jedoch schwer umzusetzen, da die initiale Schlüsselverteilung problematisch ist. An diesem Punkt setzt die Quantenkryptografie an – insbesondere das Verfahren der Quantum Key Distribution (QKD), das auf den physikalischen Grundlagen der Quantenmechanik basiert. QKD nutzt das sogenannte No-Cloning-Theorem, bei dem ein Quanten-Zustand als Schlüssel verwendet wird, der nicht kopiert oder entschlüsselt werden kann. Zudem kommt es bei jedem Abhörversuch zu messbaren Störungen, wodurch die Integrität der Verbindung direkt überprüfbar ist. Überschreitet die Fehlerrate einen bestimmten Grenzwert, wird die Verbindung automatisch als kompromittiert erkannt, sodass die Weitergabe sensibler Daten effektiv unterbunden wird. Dies ist besonders für den Themenkomplex der Cybersicherheit relevant.

Der heutige Entwicklungsstand stößt allerdings noch an seine Grenzen. Photonensignale verlieren auf langen Strecken stark an Intensität und die derzeit erreichbare Schlüsselgenerierungsrate von über 100 MB/s reicht noch nicht für breitflächige Echtzeitanwendungen aus. Dennoch zeigen Entwicklungen wie das chinesische Hochleistungs-QKD-Netzwerk mit einer Länge von 4,6 Kilometern, dass die praktische Umsetzung solcher Systeme schneller voranschreitet als bislang angenommen. Diese Systeme sind derzeit noch sogenannte Hybride, da sie gängige Kommunikationstechnologien mit quantentechnologischen Bestandteilen verschmelzen. Im chinesischen Fall und in dem geplanten EU-Projekt werden zudem Satelliten verwendet, um den Schlüssel an eine Bodenstation zu senden. Somit enthalten sie auch eine orbitale Komponente, die gegenüber Anti-Satelliten-Angriffen (sowohl physischer als auch elektromagnetischer Natur) verwundbar ist.

Eine weitere der Kommunikation zuzuordnende Technologie ist die Schaffung eines sogenannten Quantennetzwerks, bei dem Quantensensoren direkt mit Quantencomputern verlinkt werden und somit auf quantenmechanischer Ebene miteinander interagieren. Diese Interaktion könnte über verschränkte Partikel realisiert und die Informationen in Echtzeit

von einem zum anderen Gerät ausgetauscht werden. Die Entfernung der Partikel voneinander wäre in diesem Fall irrelevant für die Geschwindigkeit des Austauschs. Auch die Sicherheit des Austausches wäre gewährleistet, da ein Abhören, Unterbrechen oder Verfälschen von zwei miteinander verschränkten Partikeln derzeit theoretisch nicht möglich ist. Diese Anwendung der Verschränkung zur Kommunikation steckt noch in den Kinderschuhen, wird aber bei Voranschreiten der Forschung und Entwicklung realisiert werden.

Die Quantenkommunikation hebt die zahlreichen Synergien der gängigen Dreiteilung in Quantencomputing, -sensorik und -kommunikation hervor. Fortschritte in einem dieser Bereiche betreffen somit auch direkt die anderen Bereiche. Diese Synergien verdeutlichen, dass für Fortschritte in der Quantentechnologie ein wissenschaftlich stark differenziertes Forschungsfeld und ein Austausch über Fachbereiche hinweg benötigt wird.

Spill-Over-Effekte

Die NATO hat 2022 eine eigene Strategie für EDTs veröffentlicht. Insgesamt wurden neun Bereiche festgelegt: Dazu zählen KI, autonome Systeme, Biotechnologie, Weltraum, Hyperschalltechnologie, Materialforschung, Energieerzeugungs- und Antriebstechnologie, Kommunikationssysteme sowie Quantentechnologie. All diese Technologien verfügen mehr oder weniger über dieselben Charakteristika: Sie befinden sich derzeit noch in der Entwicklung, ihr wie auch immer geartetes Potenzial ist enorm und schwer vorhersehbar, sie beeinflussen sich teils gegenseitig in der Entwicklung und sie sind dual nutzbar – also sowohl militärisch als auch zivil/wirtschaftlich relevant.

Die Quantentechnologie ist die Technologie innerhalb dieser Gruppe, die perspektivisch die meisten Synergien zu den anderen Technologien schafft. So können Quantencomputer beispielsweise die Leistungsfähigkeit von KI-Systemen durch ihre Rechenleistung deutlich erhöhen und den Energieverbrauch reduzieren, der zunehmend zu einer Herausforderung wird. Mithilfe der Simulation können neue Materialien (neue Legierungen usw.) und Verbesserungen des menschlichen Körpers schneller entwickelt beziehungsweise entdeckt werden. Die Quantensensorik wird Potenziale im Bereich der Abwehr und Steuerung von Hyperschallwaffen erschließen und durch neue Satellitentechnik zur Fernaufklärung auch den Weltraum als Domäne beeinflussen. Die Quantenkommunikation wird neue Kommunikationswege schaffen und im Rahmen dessen auch die Interaktion von autonomen Systemen deutlich verbessern.

Die Quantentechnologie nimmt somit eine Sonderrolle innerhalb der Gruppe der EDTs ein. Es verwundert deshalb nicht, dass in diesem Zusammenhang auch immer häufiger der Begriff „Quantenrevolution“ fällt.

Rahmenbedingungen für die Bundeswehr

Die Bundeswehr wird heute in vielen Bereichen für ihre mangelnde Ausrüstung kritisiert. Seit dem Angriffskrieg Russlands auf die Ukraine stehen vor allem der Mangel an großen und teuren Waffensystemen sowie die Fähigkeitslücken in den Bereichen Digitalisierung, Luftabwehr, Radartechnik und Drohnenkampf im Fokus der Öffentlichkeit und Politik. Der jahrelange Sparkurs hat an vielen Stellen Lücken in die Fähigkeiten der Bundeswehr gerissen, die nun geschlossen werden sollen, um die Einsatzbereitschaft sicherzustellen. So ist beispielsweise die flächendeckende Einführung des Digitalfunks, der allen zur Verfügung steht, immer noch nicht durchgesetzt. Dies schwächt die Bundeswehr im Bereich der Informationsverbreitung wesentlich und verdeutlicht die mangelnde Anpassung an die Digitalisierung. Zugleich nimmt die militärische Bedeutung von EDTs wie Quantentechnologie dramatisch zu.

Eingebunden in das NATO-Rahmenwerk, das von seinen Mitgliedstaaten die Umsetzung der MDO-Doktrin verlangt, muss sich die Bundeswehr im veränderten Kriegs- und Krisenfeld anpassen. Das erfordert eine massive Steigerung der Rolle neuer Technologien wie der Quantentechnologie zur Orchestrierung der verschiedenen Domänen, Einheiten und Partnerstaaten entlang der kritischen Determinante Information.

Das Bundesministerium der Verteidigung beauftragte daher im Jahr 2022 das Planungsamt der

Bundeswehr mit der Ausarbeitung einer konzeptionellen Erschließung von MDO für die Bundeswehr, die bis März 2024 abgeschlossen sein sollte.

Bis heute ist jedoch keine frei zugängliche Ausarbeitung dieser Erschließung verfügbar, was sich möglicherweise mit der neuen Bundesregierung ändern wird. Selbst wenn diese Ausarbeitung intern bereits vorliegt, hinkt die Bundeswehr den Trends und Ausarbeitungen anderer Armeen weit hinterher.

Die mangelnde Digitalisierung und die damit verbundenen Schwächen in der MDO-Fähigkeit der Bundeswehr sind besonders problematisch in NATO-Kontexten, in denen sichere und leistungsfähige Kommunikationskanäle vorhanden sein müssen, um eine reibungslos vernetzte Operationsführung nicht nur über Domänen hinweg, sondern auch zwischen multinationalen Einheiten zu gewährleisten. Die Entsendung und dauerhafte Stationierung deutscher Soldatinnen und Soldaten nach Litauen an die Ostflanke des Bündnisgebietes sowie die deutsche Operationsführung des NATO-Kontingents machen dies umso notwendiger.

Das Kommando Cyber- und Informationsraum (CIR) soll diese Fähigkeitslücke schließen und skizziert damit den Trend der Bundeswehr hin zu einer vernetzten Streitkraft des 21. Jahrhunderts. Auch wenn das Kommando 2024 zur Teilstreitkraft erhoben wurde und größer ist als die Marine, hat es dennoch vor allem rechtliche Herausforderungen zu bewältigen, die die schnelle Handlungsfähigkeit mitunter einschränken. So können zwar im Rahmen der Landes- und Bündnisverteidigung oder mandatierten Auslandseinsätze feindliche Systeme gehackt oder lahmgelegt werden, doch unterliegen diese Einsätze strengen rechtlichen Richtlinien, was die notwendige Schnelligkeit beeinflusst. Ein Musterbeispiel dafür ist Afghanistan: Hier waren die Angst der Entscheidungsträger vor rechtlichen Schwierigkeiten und die Notwendigkeit hoher Ränge entscheidend dafür, dass eine dynamische und vernetzte Kriegsführung nicht funktionierte.

Auch wenn Entwicklungen in der Quantentechnologie oder anderen EDTs die Fähigkeiten der Bundeswehr im Informationsraum erhöhen, muss die gesamte Doktrin der Bundeswehr einschließlich der rechtlichen Rahmenbedingungen angepasst werden, um diese Fähigkeiten nutzen zu können.

Ein weiteres Problem ist die Informationsgewinnung. Zwar gewinnt sie durch die Diskussion über deutsche oder europäische Weltraumfähigkeit immer mehr an Wichtigkeit, dennoch weist sie Lücken beziehungsweise Abhängigkeiten zu anderen Staaten, vor allem zu den USA, auf. Ein Beispiel hierfür ist die Verwendung des US-amerikanischen GPS-Systems zur Navigation, da das europäische Pendant Galileo strengen Bedingungen für die militärische Nutzung unterliegt und nur für europäische Einsätze im Rahmen der GSVP verwendet werden darf.

Mit dem Voranschreiten der Entwicklungen in der Quantentechnologie und der Beschleunigung im Informationssektor werden die hier aufgeführten Herausforderungen zunehmen. Dies ist ein großes sicherheitspolitisches Problem, da die Bundeswehr gegenüber feindlichen Akteuren, die über Quantentechnologien verfügen, nicht bestehen kann, sollte sie selbst nicht über diese Technologien verfügen.

Abschließend kann das hohe Potenzial einer frühzeitigen Beschäftigung mit Quantentechnologie durch die Bundeswehr hervorgehoben werden. Wie gezeigt wurde, können im Bereich der Quantensensorik Navigationssysteme ohne orbitale Infrastruktur etabliert werden. Dies schmälert den nur schwer aufzuholenden Fortschritt anderer Länder im Weltraum zumindest in diesem Bereich und stellt eine Einsatzbereitschaft unter allen Umständen sicher.

Anders als beispielsweise in der Weltraumtechnologie oder bei autonomen Systemen steht die Bundeswehr im Bereich der Quantentechnologie noch nicht vor geschaffenen Fakten. Sie kann sich daher noch proaktiv mit der Entwicklung und Adaption dieser Technologien beschäftigen, ohne sich auf eine Aufholjagd begeben zu müssen. Die Beschäftigung mit quantentechnologisch-militärischen Applikationen ist für die Bundeswehr nach Auflistung der Umwälzungen eine Notwendigkeit, aber auch eine Chance zur Fähigkeitssicherung auf dem Schlachtfeld des 21. Jahrhunderts. Ziel muss es sein, die Informationshoheit und die digitale Souveränität Deutschlands und der Bundeswehr zu gewährleisten. In beiden Bereichen – sowohl dem

zivilen als auch dem militärischen – sind wir schon heute gefährlich abhängig von anderen Staaten. Diese Abhängigkeit wird sich durch Entwicklungen in der Quantentechnologie noch weiter verstärken, sollte man nicht frühzeitig handeln.

Die Bundeswehr befasst sich bereits im Rahmen verschiedenster Projekte und Initiativen mit Quantentechnologie. So gibt es seit 2018 das zentrale Labor Q-Lab am Forschungsinstitut CODE, das Zugang zur IBM-Quantencomputer-Infrastruktur bietet. Mittelfristig ist auch die Beschaffung eines Quantencomputers geplant. Derzeit ist allerdings nur der Einsatz im Personalmanagement vorgesehen. An der Universität der Bundeswehr in München wird im Münchner Quantennetzwerk außerdem an Anwendungen der Quantentechnologie zur Informationsverbreitung geforscht.

Seit 2023 gibt es zudem das Competence Center Quantum Enabled Technologies im BWI, das sich mit den strategischen Herausforderungen der Quantentechnologie beschäftigt. Eine solche Auseinandersetzung wird auch in der Ausrichtung von Symposien wie dem „Symposium für Quantentechnologien in Defence: Quo Vadis“ gebündelt.

Dieser Überblick über ausgewählte Beispiele des öffentlichen Engagements der Bundeswehr zeigt, dass das Interesse und Engagement der Bundeswehr im Quantenbereich gestiegen ist, wenngleich die Beschäftigung mit diesem Thema und der Reifegrad dieser Projekte im internationalen Vergleich hinsichtlich der militärischen Erschließung und Analyse zurückfallen.

Gesellschaftliche Sicherheit

Wie bei allen von der NATO als Dual Use betrachteten Technologien gehen von der Quantentechnologie im zivilen Sektor sowohl positive Auswirkungen als auch Risiken aus. Dies zeigt sich insbesondere mit Blick auf die innere Sicherheit, wobei in Zeiten hybrider Kriegsführung die Grenze zwischen innerer und äußerer Sicherheit sowie zwischen Kriegs- und Friedenszeiten verschwimmt.

Cybersicherheit

Der Bereich des Cyberspace ist laut Festlegung der NATO seit 2016 eine Domäne der Kriegsführung und wird mit zunehmender Digitalisierung immer verwundbarer. Die Angreifer sind dabei sowohl Staaten als auch kriminelle Organisationen. Die Bandbreite der Angriffsziele erstreckt sich von staatlichen Organen über Unternehmen jeglicher Größe bis hin zu Privatpersonen. Auch der Grund für die Angriffe variiert dabei sehr stark und kann im Falle krimineller Organisationen rein monetäre Aspekte sowie im Falle staatlich orchestrierter Angriffe geopolitische Ziele verfolgen.

Eine grobe Einordnung kann allerdings durch zwei Kategorien erfolgen: Entweder geht es um Informationsgewinnung oder um die Disruption digitaler Prozesse in einem Land. Beispiele für solche Angriffe gibt es in Deutschland und überall auf der Welt genügend. Im militärischen Kontext wurden bereits die Gefahren durch Fortschritte in der Quantentechnologie aufgezeigt. Die Fähigkeit, alle gängigen Verschlüsselungen digitaler Kommunikation durch Quantencomputing zu brechen, ist jedoch sowohl gesellschaftlich als auch wirtschaftlich prekär. Hinzuzufügen ist, dass nicht nur der Austausch von Informationen zwischen Individuen, sondern auch die Interaktion mit Cloud-Applikationen und die in solchen Clouds gespeicherten Inhalte bedroht sind.

Dies ist heutzutage ein besonders kritischer Bereich für Unternehmen und Privatpersonen. Für Unternehmen ist das ein besonderes Problem, da der Trend aus Effizienzgründen und aufgrund der zunehmenden Homeoffice-Nutzung immer stärker zur Nutzung von Cloud-Computing geht. Deutsche Unternehmen haben zunehmend damit zu kämpfen, Cyberangriffe aufgrund ihrer hohen Zahl und des schnellen technologischen Fortschritts abzuwehren und ihre unternehmensinternen Informationen zu schützen. Die deutsche Wirtschaft ist also verwundbar. Wenn man sich nun einem Quantencomputer gegenübersieht, der jede heute gängige Verschlüsselung brechen kann, öffnet dies eine enorme Sicherheitslücke. Anfangs werden aufgrund des hohen technologischen Know-hows und des notwendigen Zugangs zu einem Quantencomputer vor allem staatliche Akteure die ausführende Instanz sein. Doch die Verknüpfung von semiautonomen kri-

minellen Organisationen und staatlichen Instanzen ist in Cybersicherheitskreisen kein Geheimnis mehr, seit es die russische Dancing-Bear-Gruppe gibt.

Wenn also ein Staat oder ein Unternehmen einen Quantencomputer entwickeln würde, der gängige Verschlüsselungen brechen kann, hätte diese Instanz Zugang zu sensiblen staatlichen und wirtschaftlichen Geheimnissen. Zudem hätte sie die Möglichkeit, kritische Infrastruktur zu infiltrieren und/oder zu stören. Diese Verwundbarkeit und die Auswirkungen einer Disruption kritischer Infrastruktur wurden in der Vergangenheit immer deutlicher – sei es durch Hacks von Windkraftwerken oder der Blackout in Spanien und Portugal, der nach heutigen Erkenntnissen zwar nicht auf Fremdeinwirkung zurückging, aber die drastischen Folgen gut darstellte. Dies und die Taktik, Daten vorzuhalten, bis sie entschlüsselt werden können, macht die Umstellung gängiger Verschlüsselungen auf im ersten Moment vermutlich für Quantencomputer nicht entschlüsselbare Verschlüsselungen heute schon notwendig. Von staatlicher Seite aus sollte daher im Dachgesetz zum Schutz kritischer Infrastrukturen (KRITIS) eben diese Bedingung in die sektorübergreifenden Resilienzmaßnahmen aufgenommen werden.

Aus der Perspektive der Vorteile kann die Quantentechnologie allerdings wie bereits angesprochen auch eine Lösung für die negativen Auswirkungen darstellen. So kann beispielsweise durch die Quantum Key Distribution (QKD) eine sichere digitale Kommunikation selbst im Angesicht eines Quantencomputers gewährleistet werden. Doch auch diese Entwicklung birgt Risiken für die innere Sicherheit eines Staates, da sie die Arbeit der Strafverfolgungsbehörden deutlich erschwert. So können Kriminelle QKD ebenfalls nutzen, um ihre Kommunikation zu schützen und den Sicherheitsapparat wortwörtlich auszuschließen. Die Frage ist, welche Technologie schneller einsatzbereit ist. So bildet sich ein Wettrennen zwischen der Entwicklung eines Quantencomputers und der breit angelegten Verwendung von QKD.

Schutz personenbezogener Daten

Die Möglichkeit der Entschlüsselung hat auch Auswirkungen auf den Schutz der Privatsphäre, da sie dazu führen könnte, dass personenbezogene Daten öffentlich zugänglich werden. Quantencomputer können somit auch eine Gefahr für die Persönlichkeitsrechte darstellen, indem sie durch Datenanalyse neue Verbindungen zwischen Datensätzen herstellen und diese zur Kategorisierung von Personen nutzen. Eine wichtige Frage ist, ob Quantenalgorithmen größere Überwachungsrisiken bergen als aktuelle KI-Systeme. Die Arbeit der KI wird in jedem Fall verbessert. Diese Sorge zeigt sich auch bei der Quantensensorik. Die neuen Sensoren können genauer messen und an Stellen „blicken“, die derzeit verborgen sind. So setzen Strafverfolgungsbehörden beispielsweise bereits Infrarotkameras ein, um Cannabisplantagen aufzuspüren, ohne irgendwo eindringen zu müssen. Mit der Quantensensorik werden noch bessere Möglichkeiten für einen Blick ins Innere erwartet. Die Frage ist, wer dies tun darf und unter welchen Umständen dies wünschenswert wäre. Die neuen Möglichkeiten der Sensorik und Datenverarbeitung stellen somit die bestehenden Grenzen des Datenschutzes infrage.

Es besteht die Sorge, dass Regierungen und Unternehmen mithilfe der Quantentechnologie ihre Kontrolle über Bürger und Verbraucher verstärken werden. Das ist im chinesischen Fall ein enormes Risiko für die Bevölkerung, da der Staat bereits heute über ein digitales Überwachungsnetz verfügt, um sein autoritäres System zu schützen. Aber auch im Falle westlicher Staaten, in denen heute vor allem Digitalkonzerne über große Macht verfügen, besteht dieses Risiko. Ein weiteres Problem ist die Fähigkeit von Quantencomputing, komplexe Zusammenhänge zu simulieren. Seit den US-Wahlen 2016 und der Cambridge-Analytica-Affäre, aber auch den Bundestagswahlen 2020 und 2024, ist die schädliche Nutzung von Desinformationen und Fake News zur Beeinflussung der Bevölkerung eines anderen Staates und zur Destabilisierung des politischen Systems eine immense Bedrohung. In Verbindung mit der Möglichkeit, eine gesamte Bevölkerung durch erbeutete private Informationen zu analysieren und auf sie zugeschnittene Desinformationskampagnen vor Wahlen zu modellieren, tritt diese Gefahr vor allem für Demokratien wie Deutschland deutlich hervor. Dies alles erfordert, dass man sich sorgfältig mit der Regulierung der neuen Beobachtungs- und Analysemethoden durch Quantentechnologie auseinandersetzt und bei deren Entwicklung nicht zurückfällt, sofern man die Wahrung der digitalen Souveränität ernst nimmt.

Strategische Autonomie

Die strategische Autonomie wird sowohl aus wirtschaftlicher als auch aus sicherheitspolitischer Sicht für Deutschland von entscheidender Bedeutung sein. Derzeit gibt es zwei Trends, die dem Trend in der KI folgen: Entweder dominieren große privatwirtschaftliche Unternehmen wie IBM, Google und Microsoft oder stark mit einem Staat verknüpfte Unternehmen und Universitäten wie Alibaba oder die USTC den Bereich des Quantencomputings.

Wer die Quantensupremacy als Erster erreicht und damit einen voll einsatzfähigen und für alle Anwendungen nutzbaren Quantencomputer entwickelt, wird über ungeahnte politische, wirtschaftliche und militärische Macht verfügen. Da in Fachkreisen feststeht, dass die ersten Quantencomputer ihre Rechenleistung durch Cloud-Computing einer großen Anzahl von Nutzerinnen und Nutzern zur Verfügung stellen werden, entstehen dadurch enorme Abhängigkeiten. Dieser Zugang wird sowohl für Forschende als auch für Unternehmen und Regierungen von essenzieller Bedeutung sein. In Zeiten einer immer volatiler werdenden Welt ist das gefährlich.

Der Nicht-Zugang zu dieser Rechenleistung wird massive Wettbewerbsnachteile in allen Bereichen nach sich ziehen. Deshalb wird es für jeden Staat wichtig sein, einen eigenen Quantencomputer zu besitzen, über den er souverän verfügen kann, um die wirtschaftlichen, politischen und militärischen Vorteile zu nutzen und nicht ins Hintertreffen zu geraten. Das macht es für Deutschland unabdingbar, in diese Entwicklung zu investieren. Dasselbe gilt für Entwicklungen in der Quantensensorik und -kommunikation, da sie mit ziemlicher Sicherheit Exportrestriktionen unterliegen und ebenfalls einen entscheidenden Beitrag zu den oben genannten Bereichen leisten werden.

Deutschland im geopolitischen Wettbewerb

Technologiefähigkeit

Deutschland sieht sich international mit einer Vielzahl höchst volatiler Spannungsfelder konfrontiert: Einerseits gibt es den Wettbewerb zwischen den USA und China, in dem sich Deutschland und die EU positionieren beziehungsweise durch den sie manövrieren müssen. Andererseits gibt es die Bedrohung des Friedens durch Russland auf dem europäischen Kontinent.

Hier haben die hybriden Kriegsführungsarten der Russischen Föderation, die sich unter anderem gegen Deutschland richten, sowie der Angriff auf die Ukraine selbst direkte Auswirkungen auf die Sicherheitspolitik Deutschlands. Aber auch das Aufkommen anderer Staaten wie Indien und die zunehmende Multipolarisierung der Welt stellen Deutschland, das sich vor allem an der Bipolarität des Kalten Krieges ausgerichtet hat, vor Herausforderungen.

Hinzu kommt, dass Technologie und Vorherrschaft historisch schon immer eng miteinander verbunden waren, sich dieser Trend im 21. Jahrhundert jedoch nochmals deutlich verstärkt hat. Während im Kalten Krieg die Anzahl an Atomsprengköpfen und die militärische Stärke über die globale Vorherrschaft entschieden haben, ist heute der technologische Fortschritt ein Gradmesser der Macht eines Staates.

Großmächte nutzen Technologien, um ihre Macht auszuüben beziehungsweise zu beeinflussen und somit die Geopolitik zu formen. Zusätzlich steigern sie das Niveau von Waffen und die ökonomische Kraft. Forschung und Entwicklung zeigen darüber hinaus, wie leistungsfähig ein Staat ist und welchen globalen Einfluss er hat.

Der technologische Fortschritt hat sich also von einem eher symbolbehafteten Faktor im Kalten Krieg zu einem entscheidenden Gradmesser für die Macht eines Staates in der heutigen Zeit verändert. Ein Beispiel hierfür ist die Quantentechnologie: 2024 beliefen sich die Investitionen von 20 Staaten in diesem Bereich auf circa 40 Milliarden US-Dollar.

Diese Dynamiken haben dabei Implikationen, die weit über die sicherheitspolitische Dimension hinausreichen, und beeinflussen sowohl den Wirtschaftsstandort Deutschland als auch die Prägungskraft über die Grenzen hinweg. Aktuelle Entwicklungen in den USA haben dabei wohl den größten Einfluss auf die EU und besonders auf Deutschland, da man sich sowohl sicherheitspolitisch als auch wirtschaftlich auf die USA verließ und sich somit auf beiden Seiten verwundbar machte.

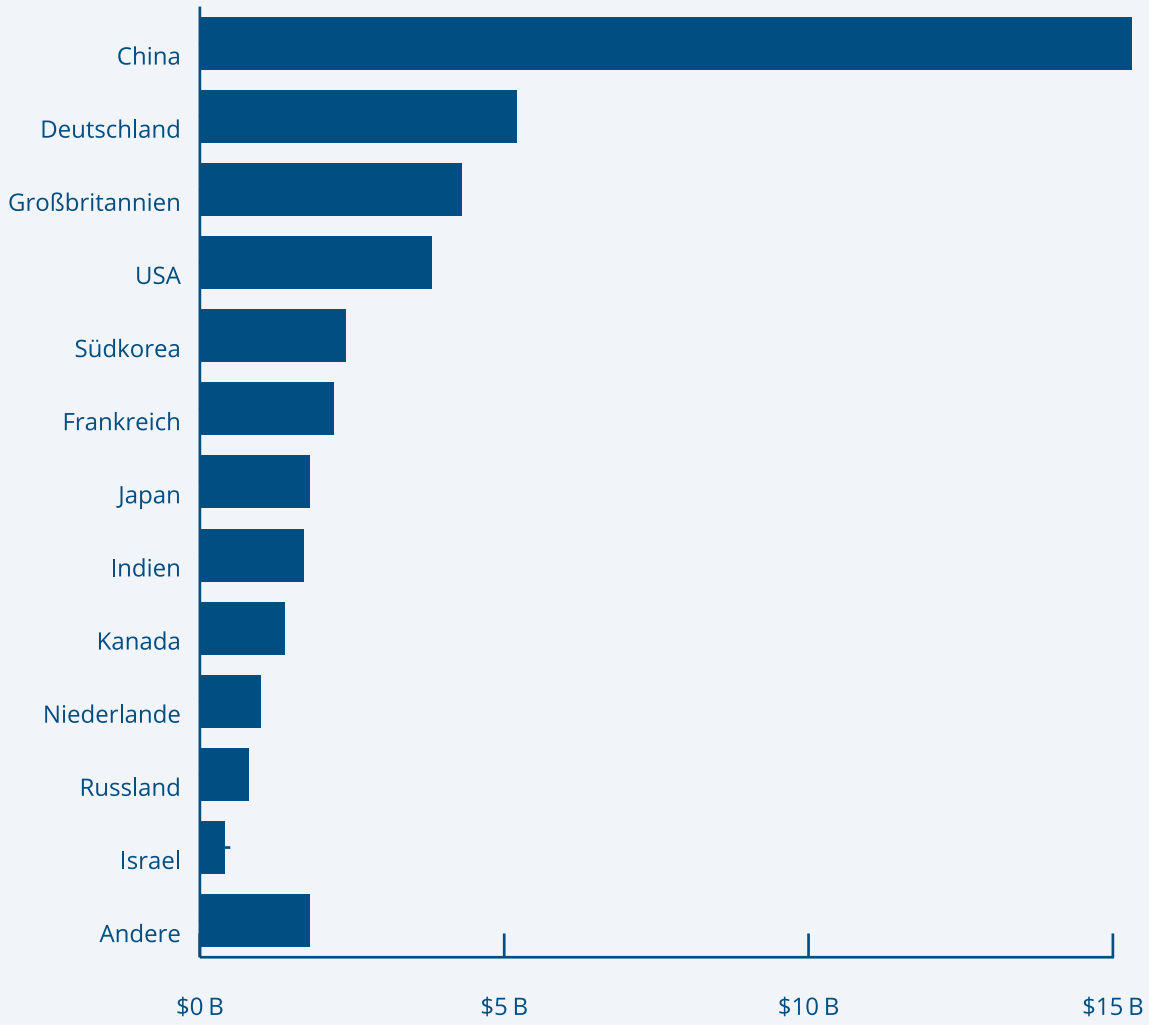
Trumps neu definierter Isolationismus, seine unklare Außen- und Sicherheitspolitik und die Hinterfragung von Bündnissen zwischen gleichgesinnten, freiheitlich-demokratischen Systemen führen zu sehr hohen Unsicherheiten. Gleichzeitig ist die EU in ihrer heutigen Aufstellung bei Weitem kein so homogener Raum, dass sie eine klare Außen- und Sicherheitspolitik gegenüber Russland, China oder den USA nach außen vertreten kann.

USA und China

Die geopolitische Auseinandersetzung im Technologiesektor zeichnet sich vor allem zwischen den USA und China ab. Sie ist heute vor allem im Bereich der KI, im Wettbewerb um kritische Ressourcen sowie in der Chipherstellung und -entwicklung sichtbar. Hin-

Investitionsvolumen Quantentechnologie nach Staaten

(in Billionen US-Dollar)



Quelle: Quantum Technology Monitor, McKinsey Digital, April 2024

Abbildung 2: Investitionsvolumen Quantentechnologie nach Staaten (Stand: 2024)

ter diesem Wettbewerb bahnt sich jedoch bereits der Wettbewerb im Bereich der Quantentechnologie an.

China begann bereits 2016, eine Quantenstrategie zu formulieren, und legte 15,3 Milliarden in einem Fünfjahresplan fest. Die USA folgten 2018 mit einer ungebundenen Förderung von 3,7 Milliarden. Dabei verknüpfen beide Staaten die technologischen Errungenschaften direkt mit der Erschließung neuer militärischer Technologien im Sinne der sogenannten informationsbasierten Kriegsführung (Intelligentized Warfare). Im US-amerikanischen Diskurs wird diese Art der Kriegsführung im MDO/MDB berücksichtigt, und beide Staaten formulieren in ihren Militärdoktrinen, dass die Informationshoheit im Kriegsfall für zukünftige Kriege entscheidend ist.

Als Ausdruck dieser zunehmenden Bedeutung von Informationen gründete China bereits 2015 die sogenannte People's Liberation Army Strategic Support

Force (PLASSF), die sich damals vor allem auf den Weltraum und den Cyberspace fokussierte. 2024 wurde sie in PLA-Information Support Force (PLAISF) umbenannt und damit noch breiter aufgestellt. Das Ziel dieser Einheit ist es, EDTs schnell in militärische Fähigkeiten zu integrieren und den Fokus stärker auf den Informationsbereich zu legen. Diese Einheit koordiniert auch den Forschungsbereich rund um die Universitäten (USTC und CAS) sowie die Staatsunternehmen in China.

Auch das Flaggschiff der US-amerikanischen Forschung und Entwicklung im militärischen Sektor, die DARPA, legt einen stärkeren Fokus auf Technologien zur Erreichung der Informationsvorherrschaft. Ähnlich wie im Weltraumsektor (Stichwort: New Space) profitieren die USA von einem starken privatwirtschaftlichen Engagement und diversen Start-ups, die sich mit Quantentechnologien beschäftigen. In diesem Bereich agiert DARPA zumeist eher als Richtschnur denn als von oben geleitetes Investitionsorgan für die Privatwirtschaft. In China fließen dagegen vor allem noch massive staatliche Förderungen in Forschung und Entwicklung. Das erklärt auch den Unterschied im Investitionsvolumen der beiden Staaten. So beträgt das Volumen in China 15,3 Milliarden und in den USA 3,8 Milliarden (Stand: 2024). Die Art der Förderung führt Expertinnen und Experten jedoch zu dem Schluss, dass die chinesischen Investitionen nur einen Wirkungsgrad von 60 Prozent haben.

Im Bereich der Quantentechnologie liefern sich beide Staaten ein Kopf-an-Kopf-Rennen. Laut dem von ASPI ins Leben gerufenen „Critical Technology Tracker“ liegen die USA im Bereich des Quantencomputings vorne, während China vor allem im Bereich der Kommunikation, Sensorik und in der quantengestützten Satellitenkommunikation führend ist. Bereits im Jahr 2016 brachte China mit dem Satelliten Micius das erste Quantenkommunikationssystem ins All. Dabei gelang nicht nur die verschlüsselte Schlüsselübertragung zwischen Satelliten und Bodenstation, sondern sogar die Quanten-Teleportation von Photonen. Es folgten spektakuläre Tests, darunter ein abhörsicheres Videotelefonat zwischen Wien und Peking sowie eine sichere Kommunikationsverbindung mit Russland, die einen Meilenstein in der internationalen Vernetzung durch Quantentechnologie darstellen. 2022 startete China mit Jinan-1 die nächste Generation von Quanten-Satelliten, die kleiner, effizienter und schneller sind. Das langfristige Ziel ist ein weltumspannendes, abhörsicheres Kommunikationsnetz für staatliche, militärische und wirtschaftliche Zwecke.

Auch die USA stellen sich im Wettbewerb um die Quantentechnologie international auf: 2019 schlossen sie eine entsprechende Kooperation mit Japan, welche 2023 nochmals vertieft wurde. 2024 wurde schließlich eine multilaterale Quantum Development Group ins Leben gerufen und auch die Einbindung von Quantentechnologien und deren Erforschung in die Bündnisse AUKUS und QUAD diskutiert. Auch die Kooperation zwischen den USA und der EU in diesem Bereich soll durch das US-EU Trade and Technology Council vertieft werden.

Im Bereich der formalen Forschungskooperation zu Quantentechnologie ist China weniger international aufgestellt. Es gibt allerdings Kooperationen zwischen deutschen Forschenden und China im Bereich der Quanten-Grundlagenforschung. Abseits der viel beachteten Belt-and-Road-Initiative verfügt China auch über eine sogenannte Digital Silk Road, die häufig weniger Beachtung findet. Sie wird einerseits zur Investition in ausländische digitale Infrastruktur und andererseits zur Etablierung von Kooperationen im technologischen Bereich genutzt. Problematisch ist insbesondere die Einbindung eines voll einsatzfähigen chinesischen Quantencomputers in die Digital Silk Road und die damit geschaffenen Abhängigkeiten von Staaten vom von China gewährten Zugang. Abgesehen davon hätte China vollen Zugang zu allen in seinem Quantencomputer verarbeiteten Daten, was ein extremes Risiko für die Datensicherheit darstellt.

Deutschland nimmt im Rennen um Quantentechnologie einen wichtigen Platz ein und landet im Bereich der Investitionen mit einem Volumen von 5,2 Milliarden auf Platz 2. Gerade im Forschungssektor ist Deutschland ein wichtiger Akteur. Die Umsetzung der Forschung in konkrete Anwendungen gelingt hier allerdings weniger gut als beispielsweise in China und den USA. Darüber hinaus ist die Verwendung von Forschungs- und Entwicklungsergebnissen für militärische Anwendungen in Deutschland stark reglementiert und lange nicht so einfach möglich wie in den USA und China.

Insgesamt zeigt sich, dass alle drei Bereiche der Quantentechnologie hart umkämpft sind und sich weder die USA noch China eine klare Führungsposition erarbeiten konnten. Das Rennen ist also noch offen, und Deutschland ist zumindest mit Blick auf seine entsprechenden Forschungskapazitäten gut aufgestellt. Für Fachkreise und zahlreiche Regierungen steht jedoch fest, dass die Quantentechnologie im Wettbewerb um die globale Vorherrschaft von entscheidender Bedeutung ist und möglicherweise Entwicklungen in den Bereichen KI, Weltraumtechnologie und andere EDTs in den Schatten stellen könnte.

Strategische Allianz zwischen Russland und China

Russland stellt für Deutschland und Europa eine sicherheitspolitische Bedrohung dar, hat aber Probleme mit allen von der NATO definierten EDTs – mit Ausnahme der Hyperschalltechnologie. Diese Probleme existieren nicht erst seit Beginn des Angriffskrieges auf die Ukraine und den westlichen Sanktionen. Der fehlende freie Markt, mangelnde Innovations- und Arbeitseffizienz, Korruption in Wirtschaft und staatlicher Verwaltung sowie das Abwandern von Fachkräften verstärken diesen Trend seit Langem und führen dazu, dass beispielsweise im KI-Sektor nur wenige russische Akteure globales Gewicht einbringen oder mithalten können.

Ähnlich verhält es sich im Bereich der Quantentechnologie. Gerade noch rechtzeitig erfüllte die Moscow State University die von der Regierung im Jahr 2020 gesteckte Wegmarke, indem sie Ende 2024 erfolgreich einen Quantencomputer mit 50 Qubits testete. Zum Vergleich: Die USA verfügen über Quantencomputer mit über 1000 Qubits und China mit 504 Qubits. Auch bei den öffentlichen Investitionen im Quantenbereich fällt Russland mit nur 800 Millionen Dollar deutlich zurück und belegt global den elften Platz.

Insbesondere in Kooperation mit China stellt Russland für Deutschland und die EU im Bereich der Quantentechnologie dennoch ein Sicherheitsproblem dar. Seit 2022 arbeiten die beiden Staaten im Bereich der Quantenkommunikation eng zusammen und verfügen durch den chinesischen Satelliten Micius und zwei Bodenstationen über das weltweit erste QKD-Kommunikationsnetzwerk zwischen zwei Staaten. Dies zeigt, dass China und Russland vor allem im Bereich der Quantenkommunikation sehr eng zusammenarbeiten und ihre Kommunikation in Friedens- wie auch in Konfliktzeiten absichern. Russland ist in dieser Kooperation der Juniorpartner, da das technologische Know-how und der Satellit selbst aus chinesischer Produktion stammen. Dies stellt eine seit Langem erkennbare Trendwende in den bilateralen Beziehungen zwischen der Volksrepublik China und Russland im Bereich neuer Technologien dar. Die Spannungen zwischen dem Westen und Staaten wie Russland und China, die nicht erst seit dem Angriff auf die Ukraine bestehen, machen eine solche Kooperation zum Sicherheitsrisiko für die NATO, die USA, die EU und Deutschland. Einerseits gibt es auf dieser Seite keine QKD-Kommunikation, andererseits existieren nicht kompromittierbare Kommunikationskanäle zwischen China und Russland.

NATO

Die NATO spielt eine entscheidende Rolle in der europäischen und der deutschen Sicherheitsarchitektur. Dies gilt auch für den Bereich der EDTs, die Organisation der Applikation und deren Einbindung in die militärischen Strukturen der NATO. Die NATO fungiert hierbei als Bündelungs- und Organisationspunkt unter ihren Mitgliedern. Die Entwicklung und Produktion von Rüstungsprodukten und militärisch relevanten Gütern bleibt jedoch Aufgabe der Nationalstaaten. Der russische Angriffskrieg hat diesen Trend, die Produktion und Entwicklung von Rüstungsgütern über das Verteidigungsbündnis hinweg besser zu koordinieren und somit für jedes Mitglied zu optimieren, noch einmal vorangetrieben.

So startete im Rahmen des NATO-Programms „Science for Peace and Security“ im Jahr 2020 ein multinationales Forschungsprojekt mit deutscher Beteiligung zur Entwicklung spintronik-basierter Quantensensoren, das bis 2024 lief. Dabei arbeiteten Forschende aus Deutschland, Griechenland, Frankreich, Spanien, Ungarn und der Ukraine an neuartigen Spintronik-Mikrowellendetektoren für Anwendungen wie Radar, Magnetfeldmessung und energieeffiziente Sensorik. Dieses Projekt ist eines von vielen multinationalen Programmen, die unter

der Schirmherrschaft der NATO durchgeführt werden und alle Bereiche der Quantentechnologie abdecken. So wurden auch QKD-Applikationen getestet und Quantensensoren zur Detektion von biologischen oder chemischen Waffen und deren Einsatz entwickelt (LiGAIert). Solche Sensoren sind sicherheitspolitisch von großer Bedeutung, da sie für die Einhaltung der internationalen Verträge zum Verbot von chemischen und biologischen Waffen sowie für die Überprüfung ersterer durch die Organisation for the Prohibition of Chemical Weapons (OPCW) relevant sein werden.

Im Rahmen der Anfang 2024 verabschiedeten NATO-Quantentechnologie-Strategie soll die Zusammenarbeit innerhalb der Allianz bei der militärischen Anwendung von Quantencomputing, -sensorik und -kommunikation weiter intensiviert werden. Viele dieser multilateralen und bilateralen Kooperationen sind dabei nicht direkt im NATO-Rahmen verwurzelt, deren Erkenntnisse werden jedoch direkt in die NATO-Strukturen und Militärplanung übernommen. Die Hauptaufgabe der NATO besteht demnach vor allem darin, die sicherheitspolitischen Implikationen zu analysieren und die militärische Applikation und Integration in das Bündnis zu prüfen.

EU

Im Jahr 2022 startete unter dem Dach des EU-Verteidigungsfonds das Großprojekt ADEQUATE mit 31 Partnern aus Wirtschaft und Forschung. Zu den deutschen Vertretern zählen beispielsweise Rheinmetall, Diehl Defence und das Fraunhofer-Institut. Das Projekt hat ein Gesamtvolumen von 27 Millionen Euro und fokussiert sich auf satellitenunabhängige Navigation durch Quantentechnologie sowie auf Quanten-Radiofrequenz- und Quanten-Optronik-Sensoren. Die beiden letztgenannten Bereiche sollen die Erkennung, Identifikation und Klassifizierung von Objekten jeglicher Art, wie beispielsweise Raketen oder Drohnen, deutlich verbessern. Das gesamte Projekt kann somit der Kategorie der Quantensensorik zugeordnet werden und greift die in diesem Bereich behandelten Anwendungsfelder auf. Dennoch kann gesagt werden, dass das Investitionsvolumen in dieses Projekt angesichts der Bedeutung der Entwicklung als gering angesehen wird.

Im Bereich der Kommunikation wurde im Jahr 2018 das von der ESA unterstützte Konsortium QUARTZ gegründet. Zu den Mitgliedern zählen die DLR, die LMU München, das MPI für die Physik des Lichts und Tesat-Spacecom aus Deutschland. Das Bündnis entwickelt ein satellitengestütztes QKD-System für hochsichere Kommunikationsdienste, die beispielsweise von Regierungsstellen, dem Militär und kritischen Infrastrukturen genutzt werden können. Das Projekt soll im Rahmen der im Jahr 2019 verabschiedeten Initiative EuroQCI zum Aufbau einer EU-weiten Quantenkommunikationsinfrastruktur führen. Ziel dieser Initiative, der alle 27 Mitgliedstaaten beigetreten sind, ist es, eine sowohl terrestrische als auch orbitale Infrastruktur zu schaffen. Diese soll kritische Kommunikationskanäle durch QKD und Quantenkommunikation sicherer und schneller über das Gebiet der EU ermöglichen und damit auch einen sicherheitspolitischen und militärischen Nutzen haben. Letzteres wird in den Papieren allerdings nicht direkt erwähnt. Die Initiative baut auf den Forschungserkenntnissen der im Jahr 2018 gestarteten Leitinitiative Quantentechnologie der EU auf. Diese unterstützt EU-weite Forschungen in allen Bereichen der Quantentechnologie mit einem Volumen von einer Milliarde Euro.

Die erste terrestrische Umsetzungsphase begann im Jahr 2023. Der Satellit Eagle-1, die orbitale Infrastruktur, soll Ende 2025 oder Anfang 2026 gestartet werden. Darüber hinaus wurde im Januar 2024 ein vierjähriges Projekt mit dem Namen NOSTRADAMUS von der Europäischen Kommission gestartet. Ziel ist es, eine Test- und Evaluierungsinfrastruktur einzurichten. Diese soll es ermöglichen, QKD-basierte Technologien und Dienste im Hinblick auf eine Zertifizierung zu bewerten und zu validieren.

Zusammengefasst lässt sich festhalten, dass die EU und damit auch Deutschland zwar hinter den Schwergewichten USA und China zurückliegen, auf EU-Ebene jedoch in den letzten Jahren viel unternommen wird, um aufzuholen. Das liegt vermutlich an der wirtschaftlichen Relevanz der Quantentechnologie, denn obwohl es Kooperationen mit dem Rüstungssektor und unter dem Europäischen Verteidigungsfonds gibt, wird bei den anderen Projekten die militärische Anwendung nicht direkt genannt. Dies ist der generellen Natur der EU als vorwiegend wirtschaftlicher und weniger militärischer Institution geschuldet. Dennoch

werden die auf wirtschaftlichen Ebenen gewonnenen Erkenntnisse und Entwicklungen aufgrund des Dual-Use-Charakters der Quantentechnologie auch den militärischen Strukturen innerhalb der EU und damit auch der NATO dienen.

Außerhalb des EU-Rahmens ist noch das bilaterale Projekt zur Quanten-Kryptografie von Frankreich und Deutschland hervorzuheben, in dem das deutsche Rüstungsunternehmen Hensoldt und die französische Firma Secure-IC neue Post-Quanten-Kryptografie-Technologien für militärische Datenlinks entwickeln.

Außereuropäische Kooperation

Die außereuropäische Kooperation beschränkt sich vor allem auf nicht vordergründig militärische Anwendungen. Im Sinne der Dual-Use-Regelung soll dieses Thema jedoch kurz aufgegriffen werden. Die Kooperationen sind zumeist bilateraler Natur und finden im deutschen Fall vor allem mit Südkorea, Japan und den USA statt. So eröffnete Südkorea in Brüssel das Korea-Europe Quantum Technology Cooperation Center, um die Zusammenarbeit zwischen Forschungseinrichtungen und der Industrie im Bereich der Quantentechnologie zu intensivieren. In diesem Rahmen arbeitet auch das Fraunhofer-Institut an diversen Projekten mit.

Im Falle Japans gibt es seit 2024 eine Vertiefung der bilateralen Kooperation durch einen gemeinsamen Förderaufruf. Dabei werden deutsch-japanische Teams vor allem im Bereich des Quantencomputings und der Quantensensorik unterstützt. Ein konkretes Projekt ist DIAMONDQTECH, das 2025 startet und die Entwicklung von Quantensensoren zur Magnetfeldmessung zum Ziel hat. Diese sind für eine nicht orbital gebundene Navigation notwendig und somit von sicherheitspolitischer Bedeutung.

Mit den USA hat Deutschland die wohl größte Bandbreite an bilateralen Kooperationen im Quantenbereich. So gab es beispielsweise im Jahr 2024 eine gemeinsame Erklärung zur Quantenkooperation sowie diverse andere staatliche Kooperationen in Form von Forschungsaufrufen oder gemeinsam organisierten Forschungen des DLR und der NASA. Auch im Industriesektor gibt es diverse Kooperationen, beispielsweise zwischen IBM und Bosch oder Infineon und Quantinuum. All diese Projekte sind jedoch nicht explizit zur Entwicklung militärischer Anwendungen ausgelegt.

Technologie und Industrie

Der kritische Pfad in die Zukunft

Angesichts des immer komplexer werdenden Schlachtfelds und der massiven Bedeutung neuer Technologien wie der Quantentechnologie verändert sich die globale Struktur der Verteidigungsindustrie seit einigen Jahren. Der durch diese Entwicklungen notwendige Fokus auf Dual-Use-Technologien zur Absicherung der militärischen Vormachtstellung erforderte ein Umdenken. Am deutlichsten zeigt sich diese Veränderung am US-Modell „New Space".

Im Weltraumsektor gab es seit den 2010er-Jahren einen Wandel von hochfinanzierten, monopolistisch agierenden staatlichen Organisationen wie der NASA hin zu einer Öffnung dieses Feldes für die Privatwirtschaft. Diese Öffnung bezieht auch kleine Start-ups ein, die mit gezielten Ausschreibungen und anderen finanziellen Anreizen unterstützt werden. So warb beispielsweise Ashton Carter (US-Verteidigungsminister a. D.) im Jahr 2015 für tiefgreifende Kooperationen zwischen dem Silicon Valley und dem Pentagon.

In den USA spielt die DARPA eine entscheidende Rolle. Sie hat durch dieses Vorgehen eine bemerkenswerte Rolle bei der Entwicklung neuer, umwälzender Technologien gespielt. Sie hat die Verteidigung mit Drohnen und präzisionsgelenkter Munition revolutioniert und das zivile Leben mit tragbaren GPS-Empfängern, Spracherkennungssoftware, selbstfahrenden Autos und unbemannten Luftfahrzeugen verändert. Sie fördert gezielt den New-Space-Sektor und ist geprägt von Innovation, Miniaturisierung, Dual-Use-Fähigkeit und wirtschaftlicher Dynamik.

Das Militär – besonders in den USA, aber zunehmend auch in Europa – nutzt diesen Wandel gezielt, um seine Raumfahrtfähigkeiten flexibler, schneller und widerstandsfähiger zu machen. Organisationen wie die DARPA spielen dabei eine Schlüsselrolle als Innovationsmotor zwischen Militär, Industrie und Forschung. Sie ermöglichten es beispielsweise SpaceX, Blue Origin und vielen kleineren Start-ups, die Effizienz und die Entwicklungsgeschwindigkeit neuer Technologien zu steigern. Im Weltraumsektor bilden sich kleinere Unternehmen, die sich beispielsweise nur auf die Entwicklung von Treibstoffen konzentrieren. Durch die Aufteilung des Baus einer neuen Rakete in verschiedene Bereiche kann dieser im Vergleich zu einem vollständig von der NASA kontrollierten Bau deutlich beschleunigt werden. Dieser Markt, der vom Staat und von der Finanzbranche durch Risikokapital-Investitionen (engl. *venture capital*) finanziert wird, funktioniert im Bereich der EDT-Entwicklung so gut, dass selbst das staatszentrierte China dies (mit deutlichen Begrenzungen) nachbildet. Anders als klassische Forschungsförderer setzt DARPA dabei stark auf visionäre, risikoreiche Projekte mit disruptivem Potenzial – oft lange vor deren kommerzieller Reife.

Das US-Modell und damit DARPA fördert auf diese Weise alle EDTs und deren militärische Applikation. So auch im Bereich der Quantentechnologie, in dem DARPA der Motor und Wegbereiter der militärischen Quantentechnologie in den USA ist. Der Fokus liegt dabei stets auf Technologien, die das militärisch-strategische Gleichgewicht zugunsten der USA verändern könnten. Die Programme decken die gesamte Innovationskette ab: von theoretischer Grundlagenforschung über experimentelle Plattformen bis hin zu anwendungsreifen Prototypen der Quantentechnologie.

Industrielle Basis

Der dynamische und effiziente Prozess, wie er beispielsweise im New-Space-Sektor zu beobachten ist, ist vor allem bei der Entwicklung neuer Quantentechnologien und deren militärischer Adaption notwendig. Ähnlich wie in der Weltraumwirtschaft sind sowohl der Forschungs- als auch der Entwicklungsprozess lang, komplex und erfordern ein breites Spektrum an Fachbereichen. Nur mit einem gut funktionierenden Steuerungsorgan für öffentliche Investitionen und einem florierenden freien Markt mit kleinen Start-ups ist dies in der notwendigen Schnelligkeit möglich.

Die Bundeswehr und das Bundesministerium der Verteidigung stehen allerdings seit Langem dafür, dass Förderungen zu ineffizient, zu bürokratisch und zu zeitaufwendig erfolgen. Mit der Etablierung des Cyber Innovation Hub (CIH) der Bundeswehr soll dies behoben werden. Doch derzeit verfügt das CIH über keine eigenständige Vergabestelle mit einem eigenen Budget. Hinzu kommt, dass es teilweise keine klare Koordination mit anderen Institutionen wie der Agentur für Innovation in der Cybersicherheit oder dem Forschungsinstitut CODE gibt. Gerade im Rahmen der Zeitenwende und der massiven Investitionen in die Bundeswehr bildet die Impulsgebung für die Industrie und speziell für die Start-up-Branche daher einen sehr geringen Anteil, während der Großteil der Investitionen weiterhin an die großen Akteure der Rüstungsindustrie wie Rheinmetall wandert. Das mag neben den langen bürokratischen Prozessen innerhalb der Bundeswehr auch am Problem des Risikokapitals und dessen gesetzlicher Regulierung liegen. Die Europäische Investitionsbank beispielsweise legt fest, dass mindestens 50 Prozent der Einnahmen eines Unternehmens, das Risikokapital erhält, aus dem zivilen Bereich kommen müssen. Entfallen mehr als 50 Prozent der Gewinne eines Start-ups auf militärische oder auch nur militärisch nahe Verkäufe, so darf keine Risikokapitalinvestition stattfinden.

Auch auf nationaler Ebene unterliegen Investitionen in Rüstungsgüter oder rüstungsnahe Güter – hierzu zählen oftmals Dual-Use-Technologien – diversen Regulierungen und Gesetzen. Darüber hinaus muss jede Investition, die 25 Millionen Euro übersteigt, vom Bundestag bestätigt werden. Von einer Technologieförderung – wie sie die DARPA in den USA betreibt – und deren sowohl militärischen als auch wirtschaftlichen Nutzen sind wir, darin sind sich alle Expertinnen und Experten einig, weit entfernt. Zwar wurden in den letzten Jahren diverse Strategien für die Rüstungsindustrie veröffentlicht, ihre Umsetzung in der Realität fehlt jedoch. All dies erschwert die Förderung von Unternehmen, die an Dual-Use-Technologien wie im Quantenbereich arbeiten, erheblich und gefährdet damit die Souveränität Deutschlands in der Quantentechnologie maßgeblich – nicht nur im militärischen, sondern auch im zivilen und damit wirtschaftlichen Bereich.

In den USA hat man in der Vergangenheit gesehen, dass die staatliche Förderung von Forschung und Entwicklung für militärische Anwendungen häufig große Vorteile für die zivile Wirtschaft mit sich brachte. Die unterstützten Firmen wurden nach der Förderung durch die DARPA oft zu Pionieren und Marktführern, wenn nicht gar Weltmarktführern in nicht-militärischen Bereichen.

Ein Blick auf die Start-up- und Risikokapitalbranche in Deutschland macht das Problem der wenig agilen deutschen Innovationsförderung deutlich. Project A ist eine der wenigen deutschen Risikokapitalfirmen, die in Dual Use investieren. Zu ihrem Portfolio gehören die Drohnenunternehmen Quantum Systems und ARX Robotics, die bei mehreren Projekten eng mit dem CIH zusammengearbeitet haben. Diese Zusammenarbeit und Förderung der Start-ups geht jedoch häufig nicht weit genug. Ein weiteres deutsches Start-up im Bereich der Verteidigungstechnologie ist das KI- und Drohnen-Unternehmen Helsing. Dieses wird hauptsächlich vom US-amerikanischen Risikokapitalanleger General Catalyst unterstützt, was die Schwächen des deutschen industriell-technologischen Ökosystems aufzeigt. Das größte Problem bleibt die monetäre und ideelle Förderung von Start-ups in der Verteidigungsbranche, damit diese von der Forschung und Entwicklung zur Produktion geführt werden. Die Gründung von Palladion an der Universität der Bundeswehr in München als Plattform und ideeller Begleiter für Rüstungs-Start-ups ist ein erster Schritt. Da es sich dabei aber um die einzige solche Institution in Deutschland handelt, bleibt weiterhin viel Potenzial ungenutzt.

Schlussfolgerungen und Empfehlungen

Das Thema „Quantentechnologie und Sicherheitspolitik“ wirft für jeden Staat ein komplexes Bild aus Vorteilen und Risiken auf. Für Deutschland und die Bundeswehr muss die Förderung der Forschung und Entwicklung in diesem Bereich jedoch besonders priorisiert werden. Als eine der führenden Industrienationen sichert dies nicht nur unsere militärische Stärke, sondern auch unsere wirtschaftliche Entwicklung. Der Dual-Use-Gedanke ist bei allen Entwicklungen, seien sie auch zuerst militärischer Natur, nicht wegzudenken.

Die Welt wird sich wandeln, und Deutschland sowie die neue Bundesregierung müssen sich an diesen Wandel anpassen, um auch in Zukunft eine gewichtige Rolle einzunehmen und die Werte und Normen der internationalen regelbasierten Ordnung zu vertreten. Im Folgenden werden die größten Probleme und Herausforderungen noch einmal dargestellt, gefolgt von Handlungsempfehlungen an die Bundesregierung und die Bundeswehr. Ziel ist es, Deutschland „quantum-ready“ zu machen. Nun ist die Zeit, zu handeln.

Strategische Herausforderungen für Deutschland

- Die Ausarbeitung einer neuen Doktrin für die Bundeswehr für das Schlachtfeld des 21. Jahrhunderts mit Fokus auf die Determinante Information weist deutliche Lücken auf, zudem geht die Umsetzung zu schleppend voran.
- Die Bundeswehr ist bislang unzureichend in die Entwicklung quantentechnologischer Anwendungen eingebunden (mangelnde Förderstruktur).
- Die Verankerung von Quantentechnologie als sicherheitspolitische Querschnittsaufgabe findet kaum statt. Die Zuständigkeiten sind zersplittert und sicherheitsrelevante Anwendungsfälle werden meist zivil adressiert.
- Die derzeitige Innovationsarchitektur (z. B. Cyber Innovation Hub ohne eigenes Vergaberecht) und das restriktive Vergaberecht hemmen die Förderung von Start-ups mit Dual-Use-Fokus.
- Die strategische Autonomie ist gefährdet, denn ohne eigene Quantenrechenkapazitäten und Kommunikationsnetzwerke drohen sicherheitskritische Abhängigkeiten von Drittstaaten und großen Tech-Konzernen.

Empfehlungen für Entscheidende

- Quantentechnologien müssen systematisch in die Sicherheitsstrategie und die Bundeswehrplanung integriert werden.
- Quantentechnologien müssen als sicherheitspolitisch relevante Zukunftstechnologien in die Nationale Sicherheitsstrategie, das Verteidigungsweißbuch und die Rüstungsplanungen aufgenommen werden.
- Etablierung einer kontinuierlichen Szenarienbildung und Analyse des Einsatzes durch feindliche Akteure sowie der Verschiebungen auf dem Gefechtsfeld durch die verschiedenen Entwicklungsschritte in der Quantentechnologie.
- Die Bundeswehr sollte zeitnah ein eigenes Quantentechnologie-Programm aufsetzen, das den Forschungsbedarf, die Applikationsszenarien und die internationalen Kooperationen definiert.
- Entwicklung und Test quantensicherer Kommunikation (QKD) für militärische Führungsinfrastrukturen forcieren, auch im Rahmen von NATO- oder EU-Projekten (z. B. EuroQCI).
- Aufbau eigener quantensensorischer Fähigkeiten zur satellitenunabhängigen Navigation und Hyperschallabwehr (z. B. Gradiometrie, Quanten-LiDAR).
- Förderung simulationsfähiger Quantencomputer zur taktisch-strategischen Operationsplanung (z. B. Gefechtsfeldoptimierung, Logistik) einleiten.

Innere Sicherheit gewährleisten – Analysen durchführen und Handlungsleitfaden erstellen

- Etablierung einer kontinuierlichen Szenarienbildung und Analyse für Gefahren der inneren Sicherheit durch Entwicklungsschritte in der Quantentechnologie.
- Anpassung des Schutzes für sensible staatliche Informationskanäle und Datenspeicher an die Veränderungen durch Quantentechnologien.
- Im Bereich der Cybersicherheit muss die Bundesregierung für wirtschaftliche wie auch zivile Akteure einen Leitfaden im Umgang mit neuen Quantentechnologien erstellen und früh neue Cybersicherheitsstandards setzen.

Förderarchitektur reformieren – Agilität durch gezielte Dual-Use-Investitionen schaffen

- Einrichtung einer vergabefähigen Agentur nach Vorbild von DARPA zur Förderung sicherheitsrelevanter Quantentechnologien und Start-ups.
- Aufhebung oder Anpassung hinderlicher Förderrestriktionen (z. B. 50%-Zivilklausel bei Investitionsfonds).
- Risikokapital und Public-Private-Partnerships bereitstellen, um Forschung schneller in die Anwendung zu überführen.

Internationale Kooperation strategisch nutzen – Souveränität sichern

- Deutsche Beteiligung an NATO-, EU- und bilateralen Quantenprogrammen stärken; militärische Anwendungsperspektiven systematisch einbringen.
- Partnerschaften mit technologisch führenden Staaten wie den USA, Japan oder Südkorea im Bereich der militärischen Quantenforschung vertiefen – unter Wahrung von Sicherheitsinteressen.
- Deutschland sollte innerhalb der EU eine Führungsrolle bei der Entwicklung einer Quanteninfrastruktur (Kommunikation, Sensorik, Computing) anstreben.

Prägungsmacht nutzen und Normen exportieren

- Die Auswirkungen von Quantentechnologien auf die Sicherheitspolitik, aber auch die Gesellschaft müssen weiter erforscht und thematisiert werden.

Literatur

A Araya, Daniel / Mavinkurve, Maithili (2022): Emerging Technologies, Game Changers and the Impact on National Security. Waterloo: Centre for International Governance Innovation.

B Burrows, Mathew / Mueller-Kaler, Julian / Kaisa, Oksanen / Piironen, Ossi (2022): Unpacking the Geopolitics of Technology. New York City: Atlantic Council.

C Chou, Charina / Manyika, James / Neven, Hartmut (2025): The Race to Lead the Quantum Future. In: Foreign Affairs, https://www.foreignaffairs.com/united-states/race-lead-quantum-future-chou-manyika-neven (letzter Abruf: 10.05.2025).

Clegg, Brian (2021): Quantum Computing. The Transformative Technology of the Qubit Revolution. London: Icon Books Ltd.

E Ertan, A. / Floyd, K. / Pernik, P. / Stevens, T. (2020): Cyber Threats and NATO 2030: Horizon Scanning and Analysis. Tallinn: NATO CCDCOE Publications.

G Gamberini, Sarah Jacobs / Lawrence, Rubin (2021): Quantum Sensing's Potential Impacts on Strategic Deterrence and Modern Warfare. In: Orbis, Jahrgang 65, Heft 2, S. 354–368.

I International Institute for Strategic Studies: Cyber Capabilities and National Power, https://www.iiss.org/globalassets/media-library---content--migration/files/research-papers/2023/09/cyber-capabilities-and-national-power-vol-2/cyber-capabilities-and-national-power_volume-2.pdf (letzter Abruf: 26.05.2023).

K Kaku, Michio (2023): Quantum Supremacy: How the Quantum Computer Revolution will Change Everything. New York City: Doubleday.

Krelina, Michael (2021): Quantum technology for military applications. In: EPJ Quantum Technology, Heft 8, Nr. 24, S. 1– 53.

Krelina, Michal / Dúbravčík, Denis (2023): Quantum Technology for Defence. What to Expect for the Air and Space Domain. In: The Journal of the JAPCC, Heft 35, S. 39–36.

L Lele, Ajey (2021): Quantum Technologies and Military Strategy. Neu-Delhi: Springer.

M Mölling, Christian / Schütz, Torben / Hellmonds, Sören (2023): German Defense Spending. A Repeat of the Past Instead of a New Era. In: DGAP Policy Briefing, Nr. 19.

N Neitzel, Sönke (2024): Kriegstüchtig? Zur Zeitenwende in Politik, Gesellschaft und Truppe. In: ApuZ, 47, S. 4–10.

Neugebauer, Reimund (2022): Quantum Technologies. München: Fraunhofer ZV.

S Soare, Simona R. / Burton, Joe / Reuben, Steff (2022): Emerging Technologies and International Security. London und New York City: Routledge.

Spencer, Joe (2023): Quantum Sensing: Enhancing Situational Awareness in Defence and Military Operation, https://www.karveinternational.com/insights/quantum-sensing-enhancing-situational-awareness-in-defence-military-operations#:~:text=The%20applicability%20of%20quantum%20sensing,of%20navigation%2C%20communication%2C%20and%20cybersecurity (letzter Abruf: 10.06.2025).

W Weizenegger, Sven (2024): Defense Technology and Innovation in Germany, https://www.atlantik-bruecke.org/defense-technology-and-innovation-in-germany/#:~:text=As%20the%20demands%20on%20German,will%20provide%20on%20the%20battlefield (letzter Abruf: 10.06.2025).

Der Autor

Manuel Steudle ist Politikwissenschaftler und promoviert seit 2024 an der TU Chemnitz zum Thema „Nationale Sicherheit und Quantenphysik – Eine strategische Vorausschau“. Zuvor absolvierte er seinen M.A. in Demokratiewissenschaft (Schwerpunkt: Internationale Politik, EDTs & Sicherheitspolitik) sowie einen B.A. in Politikwissenschaft, Germanistik und Medieninformatik an der Universität Regensburg. Das Thema der Masterarbeit beschäftigte sich mit Abschreckungsstrategien für den Weltraum.

Seine Forschung konzentriert sich auf internationale Sicherheitspolitik, den Konnex zwischen neuen Technologien und Sicherheitspolitik und strategische Vorausschau. Zu seinen Publikationen zählen *Chinas Weltraumpolitik – Zwischen wirtschaftlichem Nutzen und militärischer Notwendigkeit* (Springer, 2024) sowie *Vor und während der Ukraine-Invasion: Russlands Einsatz von Desinformation* (Hanns-Seidel-Stiftung, 2022). Er ist Mitglied der Gesellschaft für Sicherheitspolitik e. V. und der Deutschen Nachwuchsgesellschaft für Politik- und Sozialwissenschaft.

Kontakt in der Konrad-Adenauer-Stiftung:

Dr. Christian Hübner
Agenda 2030
Analyse und Beratung
christian.huebner@kas.de
T +49 30 26996-3264

Dr. Jan Cernicky
Wirtschaft und Innovation
Analyse und Beratung
jan.cernicky@kas.de
T +49 30 26996-3516

Impressum

Herausgeberin: Konrad-Adenauer-Stiftung e. V., 2025, Berlin

Gestaltung und Satz: KALUZA + SCHMID Studio, Berlin

Hergestellt mit finanzieller Unterstützung der Bundesrepublik Deutschland.

ISBN 978-3-98574-306-3