FRIEDRICH NAUMANN STIFTUNG Für die Freiheit.

CYBER-KAPAZITÄTS-AUFBAU UND STRATEGISCHES ENGAGEMENT IN AFRIKA

Eine neue Mission für Deutschland und Europa

von Kaan Sahin

ANALYSE

Impressum

Herausgeberin
Friedrich-Naumann-Stiftung für die Freiheit
Truman-Haus
Karl-Marx-Straße 2
14482 Potsdam-Babelsberg

/freiheit.org
/FriedrichNaumannStiftungFreiheit
/FNFreiheit
/stiftungfuerdiefreiheit

Autor
Kaan Sahin

Redaktion
Ann Cathrin Riedel, Themenmanagerin Digitalisierung & Innovation,
Referat Globale Themen im Fachbereich Internationales

Kontakt
Telefon +49 30 220126-34
Telefax +49 30 690881-02
E-Mail service@freiheit.org

Stand
April 2022

Inhalt

Zusammenfassung

Während die Digitalisierung für moderne Gesellschaften transformative Effekte und Vorteile mit sich bringt, setzt sie andererseits Länder, Unternehmen und Einzelpersonen immer mehr Cyberangriffen aus. Diese haben potenziell verheerende Auswirkungen auf wirtschaftlichen Wohlstand, den Schutz von Daten und soziale Sicherheit. Insbesondere Länder des Globalen Südens wie etwa in Afrika verfügen noch nicht über die nötige Cyber Maturity und werden in den kommenden Jahren aufgrund der zunehmenden Einführung digitaler Technologie höchstwahrscheinlich mehr und mehr Opfer von böswilligen Cyberaktivitäten sein.

Daher ist die Verbesserung der Cybersicherheit in afrikanischen Ländern unerlässlich, und immer mehr internationale Akteure haben nach und nach damit begonnen, in Projekte zum Cyber-Kapazitätsaufbau in Afrika zu investieren und diese zu unterstützen. Da diese Engagements jedoch politische und wertebasierte Auswirkungen haben – insbesondere im Kontext des wachsenden Trends des Digitalen Autoritarismus –, ist der Cyber-Kapazitätsaufbau nicht nur eine rein technische oder wirtschaftliche Angelegenheit, sondern beinhaltet auch die Vermittlung grundlegender Ideen und Werte zum Umgang von Regierungen und Gesellschaften mit der Digitalisierung und dem Cyberbereich. Daher beleuchtet das vorliegende Papier die aktuellen Trends beim Cyber-Kapazitätsaufbau und die Auswirkungen in Afrika und darüber hinaus sowie die Auswirkungen auf die Akteure. Es legt dar, dass Deutschland und Europa beim Cyber-Kapazitätsaufbau strategisch stärker mit afrikanischen Ländern zusammenarbeiten sollten, um zu verhindern, dass diese Länder in das Lager des ‚digitalen Autoritarismus' abrutschen, und ihnen helfen sollten, die Vorteile einer digitalisierten Wirtschaft, flankiert von angemessener Cybersicherheit, zu nutzen.

1. Einführung

Während die digitale Transformation modernen Gesellschaften große Chancen in Bezug auf Wirtschaftswachstum und soziale Sicherheit bieten kann, sind Bürgerinnen und Bürger, Unternehmen und Regierungen gleichzeitig immer häufiger böswilligen Cyberaktivitäten ausgesetzt. Cyberangriffe nehmen an Häufigkeit, Umfang, Raffinesse und verursachtem Schaden zu. Staatliche und nichtstaatliche Akteure, einschließlich Proxys, oder Cyberkriminelle haben ihre Cyberaktivitäten verstärkt, die sich in Umfang, Dauer, Intensität und Komplexität unterscheiden. Darüber hinaus können solche Angriffe verschiedene Zwecke verfolgen. Darunter böswillige Cyberaktivitäten (z. B. Ransomware- oder Wiper-Malware-Attacken) gegen kritische Infrastrukturen, Cyberspionage, Diebstahl geistigen Eigentums, sowie die Verbreitung von Desinformation und hybride Aktivitäten. Mit zunehmender Vernetzung können Abhängigkeiten und Schwachstellen in einem Land zu Risiken für andere Regionen führen. Mit dem Aufkommen technologischer Innovationen wie Künstlicher Intelligenz, Cloud Computing oder dem Internet der Dinge und der gesamten digitalen Durchdringung unseres Alltags- und Geschäftslebens steigen sowohl Chancen als auch Risiken aufgrund neuer Vernetzungsstrukturen und erweiterter Angriffsmöglichkeiten und -oberflächen rasant an.

Regierungen und Unternehmen sind daher auf der ganzen Welt mit der Herausforderung einer ständig wachsenden Zahl böswilliger Cyberaktivitäten konfrontiert, was durch die Zunahme von Angriffen während der weltweiten COVID-19-Pandemie noch deutlicher geworden. Dies gilt auch für Länder des Globalen Südens, die ihre Verwaltungen und Unternehmen digitalisieren, gleichzeitig aber durch „the absence of local expertise and limited resources" (Pawlak 2016: 88) auch zunehmend anfällig für Cyberangriffe sind. Daher müssen Cyberfähigkeiten sowohl staatlicher, als auch weiterer Akteure gestärkt werden, um ihre Resilienz gegen diese Angriffe zu erhöhen und ihre Anfälligkeit zu verringern. Dies gilt insbesondere für Entwicklungsländer, die in Bezug auf Cybersicherheit noch sehr viel Aufholbedarf haben.

Daher ist der Cyber-Kapazitätsaufbau in diesem Zusammenhang von größter Bedeutung. Denn der digitale Transformationsprozess schreitet immer weiter foran und die Nationalstaaten werden immer stärker miteinander vernetzt. **Grob gesagt umfasst der Begriff Cyber-Kapazitätsaufbau unter anderem technische, politische, strategische, rechtliche und soziokulturelle Maßnahmen zur Entwicklung und Stärkung von Cyberfähigkeiten, um den Risiken aus dem Cyberraum begegnen zu können und die Resilienz des öffentlichen und privaten Sektors zu erhöhen.** Dies können beispielsweise rein technische Maßnahmen wie die Einrichtung von CERTs (Computer Emergency Response Teams) oder strategische Maßnahmen wie die Entwicklung nationaler Cybersicherheitsstrategien für Regierungen sein. Aufgrund der zunehmenden Digitalisierung und der ständigen Zunahme von Cyberangriffen sowie der damit verbundenen wachsenden Anforderungen an die Länder, ihre Resilienz zu verbessern, wurde der Cyber-Kapazitätsaufbau von mehreren Geberländern, internationalen Organisationen wie der EU (Europäische Union), der Weltbank oder dem GFCE (Global Forum on Cyber Expertise) sowie NGOs und Forschungsinstituten verstärkt.

Der Cyber-Kapazitätsaufbau ist insbesondere für den Globalen Süden von entscheidender Bedeutung, da er die Rahmen-

bedingungen für Entwicklungsländer schafft, die wirtschaftlichen Vorteile der digitalen Transformation voll auszuschöpfen und ‚to reap the digital dividends', indem sie ihre Infrastrukturen und Netzwerke sichern. Während der Bedarf am Cyber-Kapazitätsaufbau wächst, intensivieren auch immer mehr Staaten, internationale Organisationen und NGOs ihre Bemühungen um den Cyber-Kapazitätsaufbau als Mittel, bestimmte außenpolitische Ziele zu erreichen und Ideen und Normen zur Gestaltung des Internets und des Cyberraums zu vermitteln.

Angesichts der zunehmenden Aktivitäten autoritärer Staaten und internationaler Akteure in diesem Kontext **ist es von entscheidender Bedeutung, dass die politischen Entscheidungsträger in der Europäischen Union und ihren Mitgliedstaaten die Bedeutung des Aufbaus von Cyberkapazitäten als strategisches Instrument im Umgang mit dem Globalen Süden und mit afrikanischen Ländern im Besonderen erkennen.** Gerade der afrikanische Kontinent wird in den Debatten um den Zusammenhang von Geopolitik und Technologie sowie im Diskurs um die Digitale Souveränität Europas und seine Beziehungen zu anderen Weltregionen noch zu oft übergangen. Allerdings könnten einige afrikanische Länder mit ihrem hohen Wachstumspotenzial Opfer der zunehmenden Geopolitisierung der cyber- und technologiebezogenen Entwicklungen werden.

Es wäre irreführend zu glauben, dass der Cyber-Kapazitätsaufbau rein technischer Natur ist. **Durch Cyber-Kapazitätsaufbau können die EU und Mitgliedsstaaten wie Deutschland weltweit demokratische und humanistische Ziele und Ideale verfolgen und fördern, Selbstschutz betreiben, Einfluss in einem international wachsenden Bereich erhalten und ausbauen sowie potenzielle Empfängerländer vor problematischen Abhängigkeiten und in erster Linie vor böswilligen Cyberaktivitäten schützen.** In ihrer im Dezember 2020 angenommenen Cybersicherheitsstrategie kündigte die EU an, dass sie diesem aufkommenden Problem mit der Einrichtung einer EU External Cyber Capacity Building Agenda und eines EU Cyber Capacity Building Board mehr Aufmerksamkeit widmen wird. Gleiches gilt für die Bundesregierung, die sich in ihrer aktuellen Cybersicherheitsstrategie ab 2021 mit dem Cyber-Kapazitätsaufbau befassen will. Zuletzt hat auch das Auswärtige Amt erklärt, dass Projekte für den Cyber-Kapazitätsaufbau in ausgewählten Partnerländern während der deutschen G7-Präsidentschaft im Jahr 2022 einen hohen Stellenwert einnehmen werden.

Ziel des vorliegenden Papiers ist es, die aktuellen Hintergründe, Akteure und Herausforderungen des Aufbaus von Cyberkapazitäten im internationalen Kontext aufzuzeigen. Darauf aufbauend werden Positionen und Maßnahmen für einen aktiveren und kohärenteren Ansatz der Europäischen Union und Deutschlands zum Cyber-Kapazitätsaufbau gegenüber dem afrikanischen Kontinent vorgeschlagen, die auch als Blaupause für das Engagement in anderen Regionen wie Lateinamerika oder Südostasien dienen können. Darüber hinaus soll die Analyse einen Beitrag zur noch begrenzten Literatur zum Cyber-Kapazitätsaufbau leisten.

Zunächst wird der Cyber-Kapazitätsaufbau als Feld der internationalen Politik mit den damit verbundenen Herausforderungen beschrieben. Zweitens wird ein Überblick der digitalen Transformation und insbesondere der Cybersicherheit in Afrika dargestellt. Drittens werden kurz aktuelle Trends und Initiativen im EU- und deutschen Kontext sowie darüber hinaus skizziert, auf die im Anhang näher eingegangen wird. Abschließend werden Empfehlungen gegeben, wie sich die EU und Deutschland beim Cyber-Kapazitätsaufbau strategisch engagieren sollten und welche Maßnahmen ergriffen werden sollten.

2. Was ist Cyber-Kapazitätsaufbau?

Die Digitalisierung hat weitreichende und anhaltende transformative und disruptive Auswirkungen auf Regierungen, Volkswirtschaften, Gesellschaften und jeden Einzelnen. Mit dem Aufkommen des Internets und der zunehmenden globalen Vernetzung sowie mit IKT (Informations- und Kommunikationstechnologien) und neu aufkommenden Innovationen wie Künstlicher Intelligenz, Cloud Computing oder dem Internet der Dinge versuchen mehrere Akteure – wie Staaten und Unternehmen – von den Vorteilen dieser Entwicklungen zu profitieren. Eine weitere Verbreitung der Digitalisierung führt jedoch auch zu mehr Cybersicherheitsrisiken und einer Vergrößerung der Angriffsfläche. Die zunehmende Digitalisierung von Verwaltungen und Unternehmen geht idealerweise Hand in Hand mit der Steigerung von Cyber-Resilienz und Cyberfähigkeiten sowie der allgemeinen Stärkung der Cybersicherheit. Der letztgenannte Begriff beschreibt technisch den Übergang von der ‚Computersicherheit' zum Zeitalter der weit verbreiteten Nutzung des Internets und der wachsenden Vernetzung.

Der Cyber-Kapazitätsaufbau hat sich daher ab Ende der 1990er Jahre entsprechend der zunehmenden Verbreitung des Internets und der damit verbundenen Anwendungen von IKT entwickelt. In den letzten zehn bis fünfzehn Jahren wurde der Cyber-Kapazitätsaufbau als Konzept weiter spezifiziert, wobei sich Länder und internationale Organisationen

mit speziellen Programmen, Initiativen und Strategien darauf konzentrierten und spezielle Organisationen für Cyber-Kapazitätsaufbau, etwa das GFCE, gegründet wurden.

Dennoch gibt es keine allgemein anerkannte Definition, was angesichts verschiedenster Aspekte bei diesem Themenfeld nicht verwundert. Erstens wurde, wie von Collett/Barmpaliou (2021a) dargelegt, Cybersicherheit und in der Folge der Cyber-Kapazitätsaufbau von verschiedenen parent communities der Praxis wahrgenommen und angegangen, darunter die „criminal justice community", die „CSIRT (Computer Security Incident Response) and technical community", die „foreign policy community", die „development community", die „human rights online community", die „defence community" und die „private sector community". Jede dieser Gemeinschaften hat ihre eigenen Mandate und Traditionen, was zu einer fragmentierten und inkohärenten Architektur der internationalen Cyberpolitik und dem Fehlen „[of] an overarching global public policy narrative that connects the different communities' interests and elevates cyber policy to a strategic, cross-cutting issue for global policy-makers" führt. (Collett/Barmpaliou 2021a: 34)

Zweitens, und ebenfalls verbunden mit dem Bestehen unterschiedlicher parent communities, **sind Maßnahmen zum Cyber-Kapazitätsaufbau vielfältig und können strategischer, politischer, regulatorischer, organisatorischer, kultureller oder technischer Natur sein.** Dies ist wichtig festzuhalten, da Cybersicherheit und der Cyber-Kapazitätsaufbau immer noch zu oft fälschlicherweise als rein technische Angelegenheit wahrgenommen werden. Eine solche Perspektive führt jedoch zu einem unvollständigen Ansatz bei der Verbesserung der Cyber Maturity, da Cyberangriffe unter anderem auch gesellschaftliche, organisatorische oder individuelle Schwächen ausnutzen. Der Cyber-Kapazitätsaufbau kann vor diesem Hintergrund Maßnahmen umfassen[1] wie z. B.[2]

→ Unterstützung und Austausch zur Entwicklung und Umsetzung von Cybersicherheitskonzepten und -strategien;

→ Hilfe und Austausch zur Schaffung und Verabschiedung rechtlicher, normenbasierter Regulierungs- und Verwaltungsrahmen in Bereichen wie Cyberdiplomatie, Cyberkriminalität oder Cyberkriegsführung, die die Umsetzung von UN-Resolutionen oder internationalen Konventionen zur Cyberkriminalität wie der Budapester Konvention beinhalten;

→ technische Maßnahmen wie die Installation und Verbesserung von CERTs (Computer Emergency Response Teams) oder CSIRTs (Cyber Security Incident Response Teams);

→ kulturelle Maßnahmen wie die Steigerung des Cyberbewusstseins und die Schaffung von Vertrauen, Normen und Praktiken in Bezug auf die Cybersicherheit, da das Verhalten von Endnutzerinnenn und -nutzern sowie die Art und Weise, wie Menschen Technologie- und Sicherheitspraktiken entwerfen und nutzen, entscheidende Auswirkungen auf die gesamte Cybersicherheit haben;

→ Trainingsmaßnahmen, die darauf abzielen, Wissen und Fähigkeiten zu entwickeln und das *Cyber Awareness* zu erhöhen, beispielsweise in Form von Schulungen;

→ organisatorische Maßnahmen wie die Strukturierung nationaler Kompetenzen im Bereich Cybersicherheit, etwa im Hinblick auf die Klärung von Verantwortlichkeiten und technische und politische Prozessen.

Die Bevorzugung oder der Ausschluss bestimmter Instrumente führt jedoch zu unterschiedlichen Vorstellungen und Akzentuierungen dessen, was den Cyber-Kapazitätsaufbau ausmacht, und zu „differences in focus result in fragmented coverage" (Muller 2015: 7) des Kapazitätsaufbaus im Cyberbereich. Dementsprechend haben einige Projekte oder Programme zum Cyber-Kapazitätsaufbau einen eher ganzheitlichen Ansatz, der mehrere Maßnahmen umfasst, während andere sich nur auf ausgewählte Maßnahmen konzentrieren. Bemerkenswert ist zudem, dass die Entwicklung dieser Kapazitäten eng mit „sensitive issues of national sovereignty, including the functioning of a state and relations between governments and their citizens" (Pawlak 2016: 84) verbunden ist, was die Umsetzung dieser Maßnahmen behindern könnte (siehe nächstes Kapitel).

Schließlich gibt es unterschiedliche Rahmenbedingungen, welche Akteure beteiligt werden sollen und wie die Beziehung zwischen diesen Akteuren gestaltet wird. Dabei wird zunächst zwischen der Einbindung ausschließlich staatlicher Akteure oder auch der Hinzuziehung nichtstaatlicher Akteure unterschieden. So haben Stiftungen oder NGOs wie ICT-4Peace, wissenschaftliche Einrichtungen wie das GCSCC (Oxford Global Cyber Security Capacity Centre) oder private Unternehmen wie Microsoft, Symantec oder Kaspersky ihre Aktivitäten und Initiativen im Laufe der Jahre immer stärker investiert. Eine weitere Unterscheidung ergibt sich aus der Frage, wie das Verhältnis zwischen ‚entwickelten' und ‚sich entwickelnden' Ländern bzw. zwischen dem Globalen Norden und dem Globalen Süden gestaltet wird. Traditionell wurde die Beziehung in einem Rahmen wahrgenommen und umgesetzt, in dem ein staatlicher Geber in Form eines entwickelten Landes aus dem Globalen Norden einem staatlichen Nehmer in Form eines Entwicklungslandes aus dem Globalen Süden Hilfe leistet.

Diese Perspektive ist jedoch, wie von Collett (2021) beschrieben, von einer verengten Sichtweise geprägt und teilweise fehlerhaft. Die Gleichsetzung zwischen wirtschaftlicher Entwicklung und Cyber Maturity ist nicht immer gerechtfertigt. Letztere ist zudem schwer abzuschätzen und es gibt kein allgemein akzeptiertes Instrument oder System, das den Stand der Cyber Maturity von Ländern genau bestimmt. Darüber hi-

1 Basierend auf Dutton et al. (2019) und eigener Forschung.
2 Eine andere Kategorisierung für den Cyber-Kapazitätsaufbau unterscheidet drei Hauptbereiche: „[…] (1) addressing the vulnerabilities of devices and services (primarily the role of security practitioners), (2) the security practices that should be followed by end users; and (3) what can be done about these two things who should be doing it (the role of governance)." (Dutton et al. 2019: 281-282).

naus spiegelt die staatszentrierte Sichtweise des traditionellen Ansatzes nicht die entscheidende Rolle wider, die der private Sektor und die Zivilgesellschaft bei der Cybersicherheit im Allgemeinen spielen und auch nicht ihre wachsende Rolle beim Cyber-Kapazitätsaufbau . Zudem liegt der Fokus durch die Annahme eines herkömmlichen Geber-Nehmer-Rahmens automatisch auf der Erreichung von Entwicklungszielen. Wie oben dargestellt, ist der Cyber-Kapazitätsaufbau jedoch in vielen übergeordneten parent communities verwurzelt, nicht nur im Kontext der Entwicklungszusammenarbeit.

Vor diesem Hintergrund sollte der Cyber-Kapazitätsaufbau als Multi-Stakeholder- und sektorübergreifende Anstrengung sowie als Konzept verstanden werden, in dem die Arbeitsbeziehung staatliche und nichtstaatliche Akteure einbezieht. Darüber hinaus **sollte der Schwerpunkt auf Zusammenarbeit und den Austausch von Ideen, Wissen, Ressourcen und Fähigkeiten gelegt werden und nicht auf das traditionelle und staatszentrierte Geber-Nehmer-Konzept.** Daher ist die vorgeschlagene Definition von Collett (2021: 8) hilfreich: *„International cybersecurity capacity building is an umbrella concept for all types of activity in which individuals, organizations or governments collaborate across borders to develop capabilities that mitigate risks to the safe, secure and open use of, and relationship with, the digital environment."* Der Vorteil dieser Definition besteht darin, dass Risikominderung ein ausreichend breiter Begriff ist, der mehrere potenziell unterschiedliche Motivationen und Ziele für den Cyber-Kapazitätsaufbau zulässt.[3] Darüber hinaus schließt es bestimmte Instrumente nicht aus.

Bei dieser breitangelegten Betrachtungsweise wird deutlich, dass es für einen nachhaltigen und wirksamen Erfolg beim Cyber-Kapazitätsaufbau bestenfalls einer Vielzahl von Ressourcen und einer strukturierten und ganzheitlichen Vorgehensweise bedarf. In einer idealen Welt würden alle Länder auch die Unterstützung für Cyberkapazitäten entsprechend ihren genauen Bedürfnissen erhalten. Das neue Gebiet des Aufbaus von Cyberkapazitäten birgt jedoch mehrere Herausforderungen, die im nächsten Kapitel skizziert werden.

2.1 Herausforderungen des globalen Cyber-Kapazitätsaufbaus

Es gibt noch viel Raum für Verbesserungen in Bezug auf den Aufbau globaler Cyberkapazitäten und dessen effektive Gestaltung und Umsetzung sowie die internationale Gesamtkoordination. **Eine grundlegende Herausforderung für Geber- und Empfängerländer besteht darin, dass die Entwicklungen im Cyberraums, wie etwa die Angriffsfläche und Methoden, sowie technologische Entwicklungen rasant fortschreiten und daher Wissen, Maßnahmen und Vorgehensweisen ständig aktualisiert werden müssen.** Dieses sich schnell verändernde Umfeld im Cyberraum führt auch zu der fast unvermeidlichen Situation, dass institutionelle und rechtliche Rahmenbedingungen immer hinterherhinken und der Cyber-Kapazitätsaufbau eine kontinuierliche Aufgabe in einem zeitkritischen Kontext ist. Diese Bedingungen wirken sich auf alle anderen Herausforderungen in Bezug auf den Cyber-Kapazitätsaufbau aus. Es würde den Rahmen dieses Papiers sprengen, alle möglichen Risiken von Projekten zum Cyber-Kapazitätsaufbau aufzuzählen und zu diskutieren. Um jedoch einen Eindruck davon zu vermitteln, werden einige große Bereiche der Herausforderungen beim Cyber-Kapazitätsaufbau auf globaler Ebene im Folgenden benannt.

So stellen beispielsweise die **Identifizierung und Auswahl der Empfängerländer und ihrer tatsächlichen Bedürfnisse** sehr hohe Anforderungen an die potentiellen Geber. Eine Voraussetzung für die Auswahl der Empfängerländer und das anschließende Projektdesign ist evidenz- und datenbasierte Forschung. Die Auswahl der Partnerländer und die Gestaltung von Projekten zum Cyber-Kapazitätsaufbau basieren jedoch immer noch zu oft auf „logical reasoning, limited case studies, anecdotal evidence, and expert option rather than systematic empirical evidence". (Dutton et al. 2019: 280) Die Forschung zum Stand der Cyber Maturity von Ländern, beispielsweise durch die Cybil-Portal-Initiative des GFCE oder des GCSCC (Global Cyber Security Capacity Centre)[4], hat sich in den letzten Jahren verbessert. Darüber hinaus hat das GFCE im Jahr 2020 eine Forschungsagenda aufgestellt, um auf die zunehmenden Forschungsanfragen der Mitgliedstaaten zu reagieren, und die World Bank Digital Development Unit hat ein Global Analytics Department eingerichtet, welches mehr Forschung in diesem Bereich leistet. (Collett/ Barmpaliou 2021a: 54) Auch der kürzlich gestartete Cybersecurity Multi-Donor Trust Fund der Weltbank sieht einen starken Fokus auf Forschung und die Bestimmung der Reife und Bedürfnisse der jeweiligen Länder vor, was als Grundlage dienen sollte, um Projekte und Programme besser zu gestalten. Darüber hinaus haben einige Projektanbieter damit begonnen, im Vorfeld der Projektkonzeption und -implementierung nationale Bewertungen und Erhebungen hinsichtlich der Cyberkapazitäten durchzuführen.

Doch trotz dieser positiven Trends besteht in vielen Kontexten noch immer ein großer Mangel an zuverlässigen Daten und Informationen, insbesondere in Entwicklungsländern. Aufgrund der sicherheitsbezogenen Natur von Cyberfähigkeiten sind viele Regierungen auch nicht geneigt, einzelne Informationen, geschweige denn große Datensätze, an Geberakteure weiterzugeben, insbesondere bezüglich vergangener Datenschutzverletzungen oder Netzwerkschwachstellen. Da Cyberkapazitäten mit den eigenen, inländischen Stärken und Schwächen im Cyberbereich sowie einer externen Bedrohungswahrnehmung verknüpft sind, behandeln Regierungen diese Informationen als „proprietary information to be guarded, rather than a resource that is shared with other stakeholders". (Dutton et al. 2019: 288) Und selbst wenn staatliche Behörden bereit sind, entsprechende Informationen bereitzustellen, haben einige Länder nicht immer den Überblick über die tatsächlich vorhandenen Kapazitäten. (Muller 2015: 14) Dies behindert oft eine bedarfsgerechte und nachhaltige Gestaltung und Umsetzung von Projekten zum Cyber-Kapazitätsaufbau . Gründlichere Kapazitätsbewertungen und Analysen der poli-

3 Man könnte jedoch argumentieren, dass der Verweis auf die „offene Nutzung […] der digitalen Umgebung" selbst ein Ziel ist, das nicht alle Länder (hier autoritäre Regierungen) unterstützen würden.

4 Weitere Quellen sind das EUISS (European Union Institute for Security Studies) oder das ASPI (Australian Strategic Policy Institute).

tischen Kontexte zusammen mit den nationalen Interessengruppen sind notwendig, um die tatsächlichen Prioritäten und Kapazitätslücken in den jeweiligen Ländern zu ermitteln. Auf dieser Basis können die richtigen Prioritäten und Erwartungen gesetzt werden.

In diesem Zusammenhang ist es nicht immer einfach, Partner zu finden oder zu überzeugen sowie das Bewusstsein in den Empfängerländern zu schärfen, um mit ihnen bei Projekten zum Cyber-Kapazitätsaufbau zusammenzuarbeiten. Darüber hinaus ist aufgrund der entscheidenden Rolle des privaten Sektors bei der Verbesserung der allgemeinen Cybersicherheit die Zusammenarbeit zwischen Unternehmen und dem öffentlichen Sektor unerlässlich. Aber „donor countries need to work through the government of the country it is assisting through development aid" (ebd.: 15), und die Beziehung zwischen ‚beiden Bereichen' ist in bestimmten Empfängerländern nicht immer überschaubar und eng verwoben.

Auch bei der Ermittlung und Bewertung der Wirksamkeit von Projekten zur Cyberkapazität gibt es noch Verbesserungsbedarf. Es besteht tatsächlich Bedarf an „cyber-specific capacity frameworks" (Collett/Barmpaliou 2021a: 52) und einer besseren Verknüpfung von Leistungsindikatoren und Methoden. Darüber hinaus macht es der Mangel an „publicly available projects' evaluations and end-of-project assessments" (Barbero/Berglund 2021: 13) den Gebern schwer, Best Practices für zukünftige Interventionen zu etablieren. Außerdem ist es manchmal schwierig, Empfängerländer davon zu überzeugen, Folgeprojekte durchzuführen oder sich an neuen Projekten zu beteiligen, da Investitionen in Cyberkapazitäten, beispielsweise in Bereichen wie Cyber Awareness oder strukturelle Veränderungen, oft Zeit brauchen, um ihre Wirkung zu zeigen.

Eine weitere bekannte Herausforderung betrifft **die effektive Koordinierung zwischen verschiedenen Gebern und das Risiko von Duplikationen.** Aufgrund des wachsenden, aber immer noch unübersichtlichen Bereichs des internationalen Aufbaus von Cyberkapazitäten sowie des Fehlens einer ausführlichen Erfassung relevanter Akteure auf Geberseite führt eine begrenzte Koordinierung zwischen nationalen Ministerien, internationalen Organisationen und NGOs zu Duplikationen bei Projekten. Daher führen ein Mangel an Kommunikation und geeigneten Kanälen zwischen verschiedenen Geberländern und -organisationen sowie zwischen Geber- und Empfängerakteuren zu einer potenziellen Verschwendung finanzieller Ressourcen. Das hat zum Beispiel zur Folge, dass in Afrika das „darling and orphan"-Phänomen auftritt, was bedeutet, dass eine kleine Anzahl von Ländern eine breite Palette von Projekten erhält, während die Mehrheit der Länder des Kontinents meist übersehen wird. (Collett/Barmpaliou 2021a: 22)

Ein zusätzliches potenzielles Hindernis, das häufig bei der Konzeption von Projekten auf Geberseite auftritt, ist die **fehlende oder begrenzte Verfügbarkeit von Expertinnen und Experten,** hauptsächlich von solchen mit technischer Expertise. Der Markt der Cybersicherheitsexpertinnen und -experten ist bereits hart umkämpft und für heimische Zwecke ‚leergekauft'. Einer Schätzung zufolge übersteigt die Gesamtzahl der zusätzlich benötigten Cybersicherheitsexpertinnen im Jahr 2019 in elf großen Volkswirtschaften weltweit 4 Millionen. ((ISC)² 2019:8) Dieses düstere Szenario führt häufig dazu, dass potentielle Experten entweder nicht für Projekte rekrutiert werden können oder nur in Form von ‚Fly-In Fly-Out'-Schulungen, bei denen sie ihr Wissen im Cyberbereich nur kurze Zeit zur Verfügung stellen. Der nur kurzzeitige Einsatz von Expertinnen und Experten hat oft den nachteiligen Effekt, dass der Aufbau zwischenmenschlicher Beziehungen und das Verständnis des lokalen Kontextes behindert werden. (Collett/Barmpaliou 2021a: 56)

In diesem Zusammenhang sind die **Finanzierung von Projekten zum Cyber-Kapazitätsaufbau und die Investition in damit verbundene Fähigkeiten eine Herausforderung für Geber und Empfänger gleichermaßen,** und das insbesondere unter den Bedingungen der COVID-19-Pandemie, wodurch *„more competing priorities limit the financial, human and time capacities that can be devoted to cyber capacity building."* (Barbero/Berglund 2021: 6) Um ihre Cyber-Resilienz und -kapazitäten zu erhöhen, müssten Regierungen auf der Empfängerseite dauerhaft und erheblich in Hardware, Software, Personalschulung oder Wartung investieren. Für Entwicklungsländer liegt der Fokus jedoch oft darauf, in digitale Technologien per se zu investieren und nicht in Cybersicherheit, auch wenn die Welle von Cyberangriffen inmitten der Pandemie die diesbezügliche Prioritätensetzung verändert haben könnte.

3. Der Stand der Cybersicherheit in Afrika

Der digitale Raum und neue Technologien entwickeln sich in einem extrem schnellen Tempo. Entwicklungsländer haben ein enormes Wachstumspotenzial, da immer noch viele Benutzerinnen und Benutzer erst in diesem Jahrzehnt zum allerersten Mal online gehen und digitale Dienste nutzen. Die Nutzung digitaler Technologien und deren Einführung für den wirtschaftlichen und gesellschaftlichen Fortschritt wird zu einem entscheidenden Faktor für Entwicklungsländer. Dazu gehören auch Möglichkeiten zum *Leapfrogging.* Im Allgemeinen haben sich Entwicklungsländer in den letzten Jahren zunehmend auf diese Chancen konzentriert, ohne jedoch auf die Gefahren, die sich aus den Cyberrisiken und -schwachstellen ergeben, zu achten.

Vor allem viele afrikanische Länder sind derzeit mit diesen Herausforderungen konfrontiert. Viele internationale Akteure haben nach und nach mit einem (strategischen) Engagement mit afrikanischen Partnern begonnen, welches geopolitische und wirtschaftliche Auswirkungen hat. Vor diesem Hintergrund ist **ein genauerer Blick auf das digitale und cyberbezogene Umfeld auch für Europa und Deutschland von großer Bedeutung und sollte nicht außer Acht gelassen werden,** zumal der technologie- und cyberbezogene Fortschritt in afrikanischen Ländern nicht vom geopolitischen und dem technologischen Wettbewerb zwischen den USA, China und anderen Mächten ausgenommen ist.

Im digitalen Bereich ist insbesondere Subsahara-Afrika eine der am wenigsten entwickelten Regionen der Welt. **Laut dem Digital Acceleration Index der Boston Consulting Group weist der afrikanische Kontinent bei der digitalen Reife den niedrigsten Durchschnittswert auf.** (Dannouni et al. 2020) **Gleichzeitig ist das Wachstumspotenzial immens.** Im Jahr 2019 lag die Verbreitung des mobilen Internets in Subsahara-Afrika bei gerade einmal 26 Prozent. (GSMA 2020: 1)[5] Schätzungen zufolge müssten 1,1 Milliarden Menschen Anschlüsse erhalten, damit alle afrikanischen Bürgerinnen und Bürger, Unternehmen und Regierungen bis 2030 digital arbeiten können. Dies erfordert rund 100 Milliarden US-Dollar und die Einrichtung von fast 250.000 neuen 4G-Basisstationen sowie mindestens 250.000 Kilometer Glasfaserkabel auf dem gesamten Kontinent. (United Nations Broadband Commission for Sustainable Development 2019: 16) Angesichts des Bedarfs an neuerer digitaler Infrastruktur kann der Schluss gezogen werden, dass mehrere Systeme und Netzwerke in entscheidenden Bereichen auf veralteter Ausrüstung basieren.

Mit der zunehmenden Einführung und Nutzung von IKT leiden auch afrikanische Länder immer mehr unter böswilligen Cyberaktivitäten, auch wenn konkrete Analysen noch sehr selten zu finden sind. **Im Jahr 2017 kosteten Angriffe von Cyberkriminellen die afrikanischen Volkswirtschaften 3,5 Milliarden US-Dollar, eine Steigerung von 75 % gegenüber dem Vorjahr und mehr als 95 % der Institutionen aus dem öffentlichen und privaten Sektor haben nicht mehr als 1500 US-Dollar in ihre Cybersicherheit investiert.** (Europäische Investitionsbank 2021: 82) Im selben Jahr wurden die durch Cyberkriminalität verursachten Verluste für Nigeria auf 649 Millionen US-Dollar und für Kenia auf 210 Millionen US-Dollar geschätzt. (Kshetri 2019: 77) Die geringe Reife bringt auch mit sich, dass afrikanische Länder zwar meist nicht wirklich an staatlich geförderten böswilligen Cyberaktivitäten beteiligt sind, *„[but] they are simply at potential risk from the attacks of more developed countries."* (Calandro/Berglund 2019: 4)

Angesichts dieser Zahlen hat Afrika einen großen Nachholbedarf in Bezug auf seine Cybersicherheit, und die Mehrheit der afrikanischen Länder hat Cybersicherheit nicht als regionale oder nationale Priorität wahrgenommen (ebd.: 2). Auch wenn offizielle Zahlen zur Cyber Maturity auf dem afrikanischen Kontinent eher spärlich sind, bestätigen verschiedene Indikatoren dieses niedrige Niveau. Beispielsweise haben laut ITU (International Telecommunication Union) nur 14 afrikanische Länder nationale Cybersicherheitsstrategien. Drei Länder sind derzeit dabei, welche zu entwerfen. (International Telecommunication Union 2022) Nur elf afrikanische Länder verfügen derzeit über Gesetze zur Bekämpfung von Cyberkriminalität (African Union Commission/ OECD 2021: 30) und im Allgemeinen sind *„governmental institutional capacity and awareness of the threat […] often limited".* (Müller 2015: 6)

Dazu passt auch, dass die „African Union Convention on Cyber Security and Personal Data Protection" von 2014 – auch bekannt als *Malabo-Konvention* – erst von 14 der 55 Mitgliedsstaaten unterzeichnet und von 8 ratifiziert wurde (Stand: Juni 2020). (African Union 2020a) Fünf afrikanische Länder (Kap Verde, Ghana, Mauritius, Marokko, Senegal) sind Vertragsparteien und weitere sechs (Benin, Burkina Faso, Nigeria, Niger, Südafrika, Tunesien) haben einen Beobachterstatus bei der Convention on Cybercrime of the Council of Europe, auch bekannt als Budapest Convention (Stand November 2021). (Council of Europe 2022) Auch ist das internationale Engagement in der Diskussion über Cybernormen begrenzt, da nur neun afrikanische Länder einmal Mitglied der UN GGE (UN Group of Governmental Experts on Advancing Responsible State Behavior in Cyberspace in the Context of International Security) waren und keines davon länger als insgesamt fünf Jahre. (Calandro/Berglund 2019: 2-3)

Was das Humankapital angeht, so wurde geschätzt, dass dem afrikanischen Kontinent bis 2020 100.000 Cybersicherheitsexpertinnen und -experten fehlen würden. Laut ITU Global Cybersecurity Index (GCI) rangieren nur 19 Länder unter den Top 100. (ITU 2021: 25-26). Auch bei anderen Daten wird die vergleichsweise Schwäche afrikanischer Staaten bei der Cybersicherheit deutlich: Beispielsweise haben nur 19 Länder auf dem Kontinent ein nationales CERT, zehn haben nationale Cybersicherheitsüberprüfungen durchgeführt und sechs verfügen über Metriken zur Bewertung des mit dem Cy-

5 Anderen Schätzungen zufolge „konsumieren [nur] 26 % der Landbewohner des Kontinents das Internet regelmäßig, im Vergleich zu 47 % der Stadtbewohner." (Kommission der Afrikanischen Union/ OECD 2021: 19)

berraum verbundenen Risikos auf nationaler Ebene.[6] Im März 2019 verfügten nur 13 afrikanische Länder über ein nationales CSIRT. (Collett 2021: 4)

Angesichts des weitgehenden Mangels an strategischen, rechtlichen und technischen Rahmenbedingungen und Maßnahmen zur Cybersicherheit hat die AU (Afrikanische Union) die dringende Notwendigkeit des Aufbaus von Cyberkapazitäten in afrikanischen Ländern aufgegriffen und in ihrer „Digital Transformation Strategy (2020–2030)" Ziele gesetzt. (African Union 2020b) Hier decken die vorgeschlagenen Maßnahmen zur Verbesserung der cyberbezogenen Fähigkeiten ein breites Spektrum von Bereichen ab, darunter strategische, rechtliche, kulturelle, institutionelle und technische Bereiche (siehe Kasten 1), was den weitreichenden Bedarf an Projekten und Hilfestellung in dieser Hinsicht aufzeigt.

6 Alle Daten basieren auf dem ITU Global Cyber Security Index.

Kasten 1: Ausgewählte Policy und Handlungsempfehlungen zu Cybersicherheit und Datenschutz der „Digital Transformation Strategy (2020–2030)" der AU

Support interventions to strengthen cybersecurity at national level:

- → Develop and adopt national cybersecurity strategies and legal and regulatory framework for personal data protection/privacy, cybersecurity standards and governance, and cybercrime;
- → Establish national cyber-security governance structures under multi-stakeholder structures;
- → Promote human and institution capacity building (public awareness campaign, professional training, R&D, Computer Emergency Response Teams, CERTs, etc.);
- → Conduct capacity building of policy makers and law enforcement to strengthen cyber security;
- → Support the development and implementation of strong encryption to help keep Internet users safe online by protecting the integrity and confidentiality of their data and communications;
- → Make the Malabo Convention consistent with standards such as the modernized convention 108, the GDPR to promote competitiveness of African companies outside the continent;
- → Adopt a law on the localization of data with respect for the privacy of African citizens and residents;
- → Adopt legislation to regulate social networks;

Support interventions to strengthen cybersecurity at regional and continental level:

- → Support the signing and ratification of the Malabo Convention;
- → Develop incident reporting and information sharing frameworks among National CERTS in Member States;
- → Establish regional CERT and forensic labs;
- → Set up regional centers of excellence for training and research;
- → Ensure commercial rights of the use of personal data of Africa's citizens staying in Africa or provide a fair commercial share to Africa;
- → Support the UN-led process for the establishment of the Global Cybersecurity Framework under the UN;
- → Steer innovations at continental level that seek to address challenges related to cybersecurity, interoperability of systems, and persistency of information;

Mögliche Projekte zur Cyberkapazität hätten in diesem Zusammenhang einen entscheidenden Einfluss auf diese gesetzten Ziele und sind zu deren Erfüllung sogar notwendig. Aus Geber- und Empfängerperspektive ist die Stärkung der Cyberkapazitäten auf dem afrikanischen Kontinent aus mehreren Gründen von entscheidender Bedeutung und wird mehrdimensionale Auswirkungen haben. Mehrere internationale und regionale Akteure haben dies bereits anerkannt, und laut dem Cybil-Portal gibt es derzeit über 200 cyberbezogene Projekte in Subsahara-Afrika, an denen über hundert internationale und regionale Akteure beteiligt sind. Darunter umsetzende Akteure wie CTO (Commonwealth Telecommunications Organisation), ITU, Weltbank, Europarat, Global Cyber Security Capacity Center und UN-Agenturen sowie Nationalstaaten wie Estland, die Niederlande, Südkorea oder das Vereinigte Königreich. (Cyber Portil 2022) Als einer der ganz wenigen regionalen Akteure hat auch das C3SA (Cybersecurity Capacity Centre for Southern Africa) seine diesbezüglichen Aktivitäten verstärkt. Dennoch ist nach dem oben beschriebenen aktuellen Stand der Cyber Maturity das Potenzial für den Cyber-Kapazitätsaufbau auf dem afrikanischen Kontinent noch recht hoch.

3.1 Der Cyber-Kapazitätsaufbau als Basis für Innovation und Wachstum

Wie bereits angedeutet, gehen die Wirkungen von Projekten zum Cyber-Kapazitätsaufbau über technische Ergebnisse hinaus und haben sowohl für Geber als auch für Empfänger eine wirtschaftliche, wertebasierte und politische Bedeutung, die von den deutschen und europäischen Entscheidungsträgern berücksichtigt werden muss. **Der Cyber-Kapazitätsaufbau ist für Innovation und nachhaltiges digitales Wachstum unverzichtbar.** Cybersicherheit sorgt für Vertrauen in digitale Technologien und den digitalen Transformationsprozess und fördert die individuelle Akzeptanz. Aus entwicklungspolitischer Sicht können digitale Technologien Gesellschaften in Entwicklungskontexten mehrere Vorteile bringen, darunter die Bereitstellung von mehr Wissen und Bildung (E-Learning), soziale und politische Teilhabe (E-Partizipation), Gesundheitsdienste auch in abgelegenen Gebieten (E-Health, Telemedizin) oder Zugang zu Finanzdienstleistungen (Digital Finance). Nutzerinnen und Nutzer müssen jedoch darauf vertrauen können, dass ihre sensiblen Daten sicher sind. Daher spielt Cybersicherheit für Länder in Entwicklungsregionen eine entscheidende Rolle, um das Potenzial der digitalen Transformation voll auszuschöpfen. Allerdings haben Geber- und Empfängerländer auf dem afrikanischen Kontinent in den vergangenen Jahren die Cyberkomponenten in ihren digitalen Entwicklungsprojekten stark vernachlässigt. Dennoch hat der erwähnte starke Anstieg von Cyberangriffen inmitten der COVID-19-Pandemie die Bedeutung des Aufbaus von Cyberkapazitäten in den Augen der Regierungen, insbesondere in Schwellen- und Entwicklungsländern, gesteigert und deutlich gemacht. **Wenn die wachsende digitale Wirtschaft Afrikas (siehe Kasten 2) nicht von angemessenen Maßnahmen zur Cybersicherheit begleitet wird, kann sie sich nicht optimal entfalten und Cyberangriffe werden den potenziellen wirtschaftlichen Nutzen zunichte machen.** Dies kann auch zu *spill-over*-Effekten auf andere Länder in der gesamten vernetzten Welt führen, wie andere Cyberangriffe, zum Beispiel WannaCry oder NotPetya, in der Vergangenheit gezeigt haben. Darüber hinaus müssen Cyberkapazitäten entwickelt werden, damit afrikanische Länder globale Cybernormen ordnungsgemäß umsetzen können, einschließlich UN-basierter Normen wie etwa *„the reporting of ICT vulnerabilities and the sharing of information on available remedies as well as cooperation and assistance in order to prosecute the criminal use of ICTs."* (Homburger 2019: 231)

Kasten 2: Ausgewählte Zahlen über Afrikas wachsende digitale Wirtschaft

- → Afrikas Internetwirtschaft besitzt das Potenzial, bis 2025 180 Milliarden US-Dollar zu erreichen, was 5,2 % des Bruttoinlandsprodukts (BIP) des Kontinents entspricht. Bis 2050 könnte der Beitrag 712 Milliarden US-Dollar erreichen, 8,5 % des BIP des Kontinents; (Google/ International Finance Corporation 2020: 17)
- → Bis 2025 wird sich die 4G-Einführung in Subsahara-Afrika auf 28 % verdoppeln; (GSMA 2021: 11)
- → Bis 2025 wird es etwa 120 Millionen neue Mobilfunkteilnehmer geben, was die Gesamtzahl der Teilnehmer auf 615 Millionen (50 % der Bevölkerung der Region) erhöht; (ebd. 10)
- → Bis 2025 hat der E-Commerce-Markt in Afrika das Potenzial, einen Wert von über 46,1 Milliarden US-Dollar zu erreichen (2020: 27,97 Milliarden US-Dollar). (Statista 2022)

3.2 Cyber-Kapazitätsaufbau zum Schutz und zur Förderung eines sicheren, stabilen, offenen und freien Cyberraums

Es wäre kurzsichtig, den Cyber-Kapazitätsaufbau als rein apolitisches Instrument zu verstehen[7]. Direkt oder indirekt werden Ideen zur rechtlichen und wertebasierten Gestaltung des Cyberraum und des Internets sowie zur Regulierung und Standardisierung von Informations- und Kommunikationstechnologien vermittelt, etwa durch die Verbreitung bestimmter rechtlicher, regulatorischer und administrativer Rahmenbedingungen. Wie Homburger (2019: 224–225) formuliert: *„[the] debate on norms of state behaviour in cyberspace is far from being consensual. […] The positions of China, Russia on the one side and the US and European Union (EU) member states on the other side are often pointed out as a major divide in the debate. Their approaches towards cybersecurity governance can be exported to other countries through cybersecurity capacity building as the latter implies a transfer of values and world views from the donor countries."* Entgegen der ursprünglichen Idee und dem Geist der Zusammenarbeit ist der Cyberraum zunehmend zu einem Bereich konkurrierender Interessen, Normen und Werte und der strategischen Rivalität geworden. Daher **könne der Cyber-Kapazitätsaufbau auch „[a] form of political instrument, oriented around the advancement of foreign policy interests" sein.** (Barbero/ Berglund 2021: 6)

7 So erklärt beispielsweise der jüngste Konsensbericht der UN-Gruppe von Regierungsexperten zur Förderung verantwortungsvollen staatlichen Verhaltens im Cyberraum im Kontext der internationalen Sicherheit die „politisch neutrale Natur des Aufbaus von Kapazitäten". Allerdings gibt es, wie im Text beschrieben, Beispiele, die dieser Aussage widersprechen.

Diese Feststellung ist besonders angesichts der Tatsache wichtig, dass gerade autoritäre Staaten zunehmend versuchen, ihre Ideen – etwa im Hinblick auf Überwachungstechnologien oder Einschränkungen der Internetfreiheit – an andere Staaten weltweit weiterzugeben. **Vor diesem Hintergrund ist der Cyber-Kapazitätsaufbau auch nicht ausgenommen von der sich abzeichnenden Dichotomie im digitalen Bereich zwischen ‚digitalem Autoritarismus' oder ‚autoritärer Technologie' und einer starken Betonung von ‚staatlicher Souveränität' auf der einen Seite (vorangetrieben z. B. von China oder Russland) und Demokratien – wie die Europäische Union und ihre Mitglieder –, die das Konzept eines ‚sicheren, stabilen und offenen und freien Cyberraums' in einem Kontext mit vielen Interessengruppen schützen und fördern wollen.**

Viele Projekte beispielsweise des Europarates und der EU geben als Voraussetzung für die Empfängerstaaten an, dass sie die Ideen und Richtlinien der Budapester Konvention unterstützen und ein Interesse daran haben sollten, dem verbindlichen internationalen Instrument zur Bekämpfung von Cyberkriminalität beizutreten. Länder der Shanghai Cooperation Organization hingegen beziehen sich auf ihren International Code of Conduct for Information Security von 2015 als Leitlinie für Projekte zum Cyber-Kapazitätsaufbau, der eine stärkere Betonung auf Souveränität und nationale Sicherheit in Bezug auf die Nutzung von Informations- und Kommunikationstechnologien legt und impliziert, dass auch Inhalte per se als Bedrohung betrachtet werden könnte. Beispielsweise legt China in seiner Internationalen Strategie zur Zusammenarbeit im Cyberraum Wert auf die Förderung des Internationalen Verhaltenskodex, und sein Versuch, *„to gain support for their vision of cyberspace governance coupled with actual cooperative action with Asian countries points towards the use of such cooperation for advancing Chinese interests."* (Homburger 2019: 235) Im Fokus stehen dabei auch fragile Demokratien (‚digitale Entscheider'), die nicht eindeutig dem ‚demokratischen' oder ‚autoritären' Lager zuzuordnen sind.[8] Gerade viele dieser Länder befinden sich auf dem afrikanischen Kontinent. Angesichts der sehr starken Präsenz Chinas im IKT-Sektor Afrikas und seines Interesses, Investitionen im Rahmen seiner Initiative ‚Digitale Seidenstraße' auszuweiten, könnte dies aus europäischer und deutscher Sicht eine kritische Entwicklung sein, zumal beide versuchen, einen freien und offenen Cyberraum mit Multi-Stakeholder-Ansatz zu fördern und den zunehmenden Einschränkungen der Internetfreiheit im Sinne der ‚nationalen Souveränität' entgegenzuwirken. Insgesamt besteht auch die Gefahr, dass es zu einer Fragmentierung von Standards kommt, da verschiedene Geberländer unterschiedliche Werte vermitteln.

3.3 Cyber-Kapazitätsaufbau als Instrument zur internationalen Koalitionsbildung

Drittens und basierend auf dem vorherigen Punkt und einer dezidierten außenpolitischen Perspektive könnte der Cyber-Kapazitätsaufbau auch als Instrument zur Bildung von Koalitionen in Normsetzungsprozessen in internationalen Organisationen eingesetzt werden. Da in diesem Jahrzehnt Milliarden neue Internetnutzer aus Afrika und Lateinamerika hinzukommen werden, werden die jeweiligen Heimatländer dieser Nutzerinnen und Nutzer stärker ihren Anspruch geltend machen, Normen und Prinzipien zu verantwortungsvollem staatlichem Verhalten im Cyberraum ebenfalls mitzugestalten und sich darin stärker diplomatisch engagieren. Mit anderen Worten: Der derzeitige Trend, dass *„African stakeholders have remained largely absent from the evolving norms debate of the last decades"* (Calandro/Berglund 2019: 2) wird sich höchstwahrscheinlich in den kommenden Jahren ändern und afrikanische politische Entscheidungsträger werden zunehmend globale Normen für den Cyberraum prägen, die sie umgesetzt haben.

Angesichts der aktuellen kontroversen Debatten um Cybernormen im UN-Kontext, der Förderung eines neuen UN-basierten globalen Abkommens zur Cyberkriminalität durch Russland, um die westlich orientierte Budapester Konvention zu ersetzen, oder des allgemeinen Trends des ‚digitalen Autoritarismus' oder der ‚autoritären Technologie' (siehe Kasten 3) kann der **Cyber-Kapazitätsaufbau als strategisches Instrument eingesetzt werden, um Länder für das ‚eigene Lager' zu gewinnen,** insbesondere im Hinblick auf Prozesse, für die das Prinzip ‚ein Mitglied, eine Stimme' gilt. Dass der Cyber-Kapazitätsaufbau in den kommenden Jahren höchstwahrscheinlich stärker als außenpolitisches Instrument genutzt wird, ist aufgrund der immer neuen Akteure und der zunehmenden Geopolitisierung dieses Feldes sehr wahrscheinlich.

8 Wie Homburger (2019: 236) formuliert: „Staaten, die als Swing States im Bereich der Internet-Governance identifiziert werden, könnten für die Debatte von besonderem Interesse sein. Denn Swing States können als Staaten definiert werden, die eine gemischte politische Ausrichtung haben und daher keinem der beiden Lager zugeordnet werden und über die notwendigen Ressourcen verfügen, um den Verlauf eines internationalen Prozesses zu beeinflussen. Der Aufbau von Cybersicherheitskapazitäten könnte eine Form der Beeinflussung dieser Swing States sein."

Kasten 3: Beispiele für Entwicklungen im Cyberbereich in internationalen Organisationen

- Im Rahmen des UN Cybercrime Ad Hoc Committee werden im Laufe der nächsten zwei Jahre die Ziele und die Struktur eines potenziellen ersten UN-Abkommens zur Cyberkriminalität erörtert, das die Budapester Konvention des Europarates langfristig ersetzen könnte; der ursprüngliche Vorschlag für einen solchen UN-Vertrag stammt von Russland, das sich – obwohl es Mitglied des Europarates ist – weigert, der Budapester Convention beizutreten. Auf westlicher Seite gibt es allerdings Bedenken, dass eine solche neue UN-Konvention dazu genutzt wird, Cyberkriminalität so weit zu fassen, dass sie beispielsweise auch regierungskritische Inhalte umfasst.
- Bisher gab es zwei UN-Cyberdiplomatie-Prozesse, die sich auf die Festlegung von Regeln für verantwortungsvolles staatliches Verhalten im Cyberraum konzentrieren: Die jahrzehntealte und von den USA geförderte „UN GGE", die aus einer Arbeitsgruppe von Ländervertretern aus 25 UN-Mitgliedstaaten besteht, und die von Russland initiierte UN OEWG (Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security), die für alle UN-Mitglieder offen ist. Beide Gruppen veröffentlichten 2021 Abschlussberichte, in denen sie die Bedeutung des Aufbaus von Cyberkapazitäten betonten (siehe Anhang). Die Dualität der beiden Gruppen und das derzeit diskutierte Aktionsprogramm (POA), das von Frankreich und Ägypten vorgeschlagen wurde, um beide Gruppen zu vereinen, ist jedoch immer noch in einer offenen Debatte und spiegelt die tiefen Meinungsverschiedenheiten zwischen den Ländern über den Prozess und den Inhalt der internationalen Regeln für den Cyberbereich wider.
- Mit der Vorlage eines neuen Internetprotokolls („New IP") in der UN-Sonderorganisation ITU im Jahr 2019 hat China vorgeschlagen, die technischen Strukturen des Internets zu ändern, was zu einer differenzierteren Betonung der „nationalen Souveränität" und größeren Zugangsrechten für Nationalstaaten führt.

Dabei ist die Machtdynamik zwischen Gebern und Empfängern anzuerkennen, denn *„when states or regional organization support other countries, the understanding of risks as well as values and infrastructure which need protection will form an essential part of the cooperative effort"* und die Geberländer *„might be in a more convincing position to frame expected risks"*. (Homburger 2019: 228). Daher sollten und können all diese vorgeschlagenen Ansätze nicht aufgezwungen werden; mit anderen Worten, sie müssen in einem Multi-Stakeholder-Kontext und jenseits des herkömmlichen Geber-Empfänger-Verständnisses durchgeführt werden (siehe vorgeschlagene Definition für den Cyber-Kapazitätsaufbau von Collett). So kann Länder zu ‚gewinnen' nicht bedeuten, sie zu zwingen, sondern ihnen bessere Alternativen anzubieten und gleichzeitig die Regierungen zu befähigen, sich beispielsweise auch effektiver in Normsetzungsprozessen im UN-Kontext zu engagieren. Auch Maßnahmen müssen in erster Linie darauf ausgerichtet sein, die lokale Eigenverantwortung der Akteure vor Ort zu stärken. In Entwicklungskontexten gibt es auch *„[the] increasing skepticism to the measures needed to protect and secure the digital realm, seeing them as 'Western imposition' on their governance."* (Muller 2015: 6) Daher sollte **die klare Botschaft lauten, dass die Zusammenarbeit beim Cyber-Kapazitätsaufbau nicht dazu führen sollte, wirtschaftliche und technologische Abhängigkeiten zu schaffen und Entwicklungsländer an bestimmte Geberländer zu ‚binden', sondern die lokalen Kapazitäten in einer selbstbestimmten und nachhaltigen Weise zu unterstützen.** Auch gegenüber dem Vorgehen autoritärer Staaten ist dieses Vorgehen ein klarer Vorteil.

4. Akteure (Positionen und Aktivitäten)

Während die Zahl der Geber und Umsetzer beim internationalen Cyber-Kapazitätsaufbau rasant wächst, wird auch die Akteurslandschaft immer komplexer und unübersichtlicher. Das Ökosystem der Akteure wurde in den letzten Jahren erweitert, da Aktivitäten zur Cyberkapazität zunehmend über technische Angelegenheiten hinaus definiert werden und mehr *parent communities* begonnen haben, sich diesbezüglich zu engagieren. Zu den Interessengruppen gehören internationale Organisationen, Regierungen, Organisationen der Zivilgesellschaft, Privatunternehmen, akademische Einrichtungen oder einzelne Beraterinnen und Berater. Fast alle Länder sind in irgendeiner Weise an mindestens einem Projekt zum Cyber-Kapazitätsaufbau beteiligt. (Collett/Barmpaliou 2021a: 5) Die vielfältige Akteurslandschaft aus verschiedenen parent communities könnte jedoch zu *„competing and overlapping frameworks that can cause fragmentation in program implementation and impact effectiveness"* führen. (Csenkey/Perron 2020: 2)

Aus einer anderen Perspektive kann die Akteurslandschaft auch wie folgt differenziert werden: „(1) security practitioners to advance technical designs to reduce the vulnerabilities of digital devices and services, (2) end users, such as Internet users, to follow security practices and norms, and (3) managers, policy-makers, and regulators to govern these two areas and who should be doing what in order to enhance cybersecurity." (Dutton et al. 2019: 284).

Im deutschen, EU- und multilateralen Kontext haben mehrere Länder und internationale Organisationen in den letzten Jahren damit begonnen, verschiedene Initiativen, Programme und Projekte auf den Weg zu bringen. Das hebt die allmählich zunehmende strategische Bedeutung hervor, die diese Akteure dem Cyber-Kapazitätsaufbau beimessen.

So betont die deutsche Cybersicherheitsstrategie 2021 die Bedeutung des Aufbaus von Cyberkapazitäten als Instrument zur Förderung „[d]emokratische und normative Werte und Ideale" und für eine Erhöhung der „Cybersicherheit in den Partnerstaaten". (Bundesministerium des Innern 2021) Die Strategie gibt im Wesentlichen die (sehr) groben Linien für ein (wertebasiertes) stärkeres Engagement Deutschlands für den Cyber-Kapazitätsaufbau vor. Die konkrete Ausgestaltung und Strukturierung dieser Ideen und eine mögliche strategische Ausrichtung stehen damit aber noch nicht fest. Angesichts der zunehmenden Aktivitäten des Auswärtigen Amtes (AA) und des Bundesministeriums für wirtschaftliche Zusammenarbeit und Entwicklung (BMZ) bleibt auch abzuwarten, wie die digitale Entwicklung und die außenpolitischen Ansätze sowie die übergeordneten Gemeinschaften im deutschen Kontext zusammengeführt werden können.

In diesem Zusammenhang hat das Auswärtige Amt sein strategisches Engagement im Bereich Cyber-Kapazitätsaufbau durch die Bereitstellung von Mitteln für Projekte und Programmierer (z. B. für die Weltbank und das GFCE) und seine Beteiligung am EU-CyberNet-Projekt (siehe Anhang) zunehmend verstärkt. Zuletzt hat es im Rahmen der deutschen G7-Präsidentschaft angekündigt, *„to put projects aimed at ensuring better cyber security in selected partner countries outside the G7 and future investments in joint global infrastructure on the agenda"*. (Auswärtiges Amt 2022) Darüber hinaus hat auch das BMZ (Bundesministerium für wirtschaftliche Zusammenarbeit und Entwicklung) damit begonnen, Projekte mit Cybersicherheitskomponenten zu beauftragen.

Der Cyber-Kapazitätsaufbau wurde von der EU schrittweise aufgegriffen, mit dem Ziel, dessen strategische Bedeutung zu erhöhen und damit verbundene Projekte des Blocks und seiner Mitgliedstaaten wirksam zu gestalten und umzusetzen. Bereits 2018 hat die EU zwei Nachschlagewerke ausgearbeitet, die *„Council Conclusions on EU External Cyber Capacity Building Guidelines" und die „Operational Guidance for the EU's international cooperation on cyber capacity building"*, die die grundlegenden Konzepte, Ansätze, Methoden und Ziele skizzieren. Die EU-Cybersicherheitsstrategie vom Dezember 2020 (Europäische Union 2020) geht noch einen Schritt weiter und fordert die Entwicklung einer EU External Cyber Capacity Building Agenda. Die Agenda soll das Fachwissen der Mitgliedstaaten und der einschlägigen EU-Organe, -Einrichtungen, -Agenturen und -Initiativen im Einklang mit ihren jeweiligen Mandaten nutzen. Darüber hinaus sollte ein EU Cyber Capacity Building Board eingerichtet werden, dem relevante institutionelle EU-Akteure angehören, um Fortschritte aufzuzeichnen und weitere Synergien und potenzielle Lücken zu ermitteln. Hauptsächlich über ihre Generaldirektion für internationale Partnerschaften (GD INTPA) hat die Europäische Kommission mehrere Projekte zum Cyber-Kapazitätsaufbau mit Schwerpunkt auf ihrer unmittelbaren Nachbarschaft (z. B. Westbalkan), aber auch darüber hinaus, unterstützt.

Auf globaler Ebene betonen die 2021 veröffentlichten Abschluss- und Konsensberichte der UN GGE und der UN OEWG die Bedeutung des Aufbaus von Cyberkapazitäten im Allgemeinen und für Entwicklungsländer im Besonderen. Darüber hinaus haben große internationale Organisationen wie die Weltbank begonnen, ihre Aktivitäten in diesem Bereich zu intensivieren.

Im Anhang wird eine Auswahl relevanter Akteure mit Fokus auf Deutschland und der EU – aber nicht nur – weiter detailliert ausgeführt und diskutiert. Die folgende Tabelle soll einen Einblick in die Vielfalt und die unterschiedlichen Rollen der Akteure geben, die am Aufbau globaler Cyberkapazitäten beteiligt sind.

Akteure	Rolle(n)	Beispiele
Cybersicherheits-expertinnen und -experten	Einzelpersonen und Teams mit Fachkenntnissen in den Bereichen Computing, IT-Netzwerke und IT-Sicherheit	Computer Emergency Response Teams (CERTs); IT-Experten in Organisationszentren
Forscher, Ausbildungen	Akademische Kompetenzzentren für Praktiken und Richtlinien beim Aufbau von Cybersicherheitskapazitäten in Universitäten und Denkfabriken	Oxford Global Cyber Security Capacity Centre (GCSCC), Oceania Cybersecurity Centre, Chatham House, Brookings, Rand Corporation, Europäisches Institut für Sicherheitsstudien (EUISS)
Ausbilder	Einzelpersonen und Teams, die Schulungen und Sensibilisierungskampagnen entwerfen und durchführen und Sicherheit fördern	Die Geneva Internet Platform (GIP) Digital Watch Observatorium, ICT4Peace
Netzwerker und Koordinatoren	Bereitstellung von Online-Portalen, Konferenzen und Foren zum Cyber-Koordinationsaufbau	Das Global Forum on Cyber Expertise (GFCE), Weltwirtschaftsforum (WEF)
Spender	Einzelpersonen und Organisationen, die Initiativen zum Aufbau von Kapazitäten finanziell und organisatorisch unterstützen	Regierungen (Außen-, Entwicklungs-, Innenministerien etc.), philanthropische Stiftungen, internationale Organisationen wie Weltbank, Europarat
Politische Entscheidungsträger und Regelungen	Internet Governance und Cybersicherheitsnormen und -praktiken	Internet Governance Forum (IGF)

Basierend auf: Dutton et al. (2019: 284–285) und eigene Recherchen

5. Policy-Empfehlungen

Relevante Akteure in der EU und in der Bundesregierung haben begonnen, die Bedeutung eines konzertierten und strategischen Ansatzes für den Cyber-Kapazitätsaufbau zu erkennen. Dies ist angesichts des steigenden Bedarfs an Cyberfähigkeiten in Afrika eine willkommene und notwendige Entwicklung. Dennoch ist es wichtig, dass die Bundesregierung eine Strategie zum Cyber-Kapazitätsaufbau entwickelt, die im Einklang mit den großen Initiativen auf EU- und UN-Ebene steht. Hier kann die Bundesregierung die Bereitstellung organisatorischer, personeller und finanzieller Ressourcen aufgrund der zunehmenden Bedeutung, die dem Cyber-Kapazitätsaufbau durch diese multilateralen Organisationen und Foren beigemessen wird, immer rechtfertigen.

Die strategische Schwerpunktsetzung des Auswärtigen Amtes während der deutschen G7-Präsidentschaft 2022 zu Entwicklungsländern sollte als Impuls für das weitere Engagement in afrikanischen Ländern und darüber hinaus genutzt werden. **Aufgrund des zunehmenden Trends zum ‚digitalen Autoritarismus' und der wachsenden Bedeutung von Ländern des Globalen Südens für die Gestaltung der Debatten über globale Cybernormen sollten die Bundesregierung und die Europäische Union darauf abzielen, den Cyber-Kapazitätsaufbau als strategisches Instrument zu nutzen und außerdem zu versuchen, die Mandate und Ziele der Entwicklungszusammenarbeit, der Außenpolitik und der inneren Sicherheitscommunity im Kampf gegen die Cyberkriminalität zusammenzuführen.** Vor diesem Hintergrund ist es wichtig, den Aufbau externer Cyberkapazitäten und das strategische Engagement in Ländern des Globalen Südens als Teil der Stärkung der eigenen digitalen Souveränität in Europa zu gestalten. Mit anderen Worten, digitale Souveränität[9] sollte nicht nur bedeuten, die eigene Technologiebranche zu stärken und aufkommende Innovationen und digitale Dienste in der eigenen Gerichtsbarkeit zu regulieren, sondern auch Standards und Normen im Einklang mit europäischen Werten wie Menschenrechten, Menschenwürde, Rechtsstaatlichkeit oder Datenschutz international zu fördern – beispielsweise durch Cyber-Kapazitätsaufbau . Dadurch sollten die EU und ihre Mitgliedstaaten im Hinblick auf den Cyber-Kapazitätsaufbau die oben genannten Risiken und Herausforderungen bei ihrem Aufbau angehen. Daher werden folgende Empfehlungen vorgeschlagen:

5.1 Die deutsche Bundesregierung

→ **Bereitstellung von Mitteln zur Unterstützung von Think Tanks, NGOs und Universitäten, die an diesem Thema arbeiten:** Der Cyber-Kapazitätsaufbau sowie der Stand der Digitalisierung und Cybersicherheit in Afrika werden als Forschungsfeld in deutschen und europäischen Thinktanks und Forschungsinstituten noch nicht ausreichend abgedeckt. Im Allgemeinen besteht die Literatur zum Cyber-Kapazitätsaufbau hauptsächlich aus Grundsatzpapieren und nicht aus etablierten, von Expertinnen und Experten begutachteten qualitativen oder quantitativen Studien, die die Cyber Maturity von Ländern und Regionen bestimmen. (Collett/Barmpaliou 2021a: 12) Daher sollte die Bundesregierung Think Tanks und Forschungseinrichtungen ermutigen und unterstützen, sich stärker mit diesem Thema zu befassen, um die operative Politik mit Forschungsergebnissen und Empfehlungen zu unterstützen. Dies wird dazu beitragen, die tatsächlichen Bedürfnisse dieser Länder und die Lücken in ihrer Cyber Maturity besser einzuschätzen und zu ermitteln.

→ **Nutzung und Einbindung deutscher Expertise für bilaterale/EU-Programme:** Neben der Förderung von Projekten und konzeptionellen Arbeiten ist es für Deutschlands glaubwürdiges Eintreten für den Cyber-Kapazitätsaufbau wichtig, dass sich deutsche Expertinnen und Experten in bilateralen Projekten und EU-Programmen engagieren. In diesem Zusammenhang sind insbesondere das BSI (Bundesamt für Sicherheit in der Informationstechnik) aufgrund seiner Expertise im Bereich Cybersicherheit, aber auch die Privatwirtschaft und die wissenschaftlichen Einrichtungen wichtige Ansprechpartner. Die Bundesregierung sollte daher die Zivilgesellschaft und private Unternehmen dafür sensibilisieren.

→ **Bereitstellung von Mitteln zur Unterstützung bilateraler/multilateraler Projekte zum Aufbau von Kapazitäten:** Die Bundesregierung sollte vertrauenswürdige internationale Akteure, etwa die Weltbank oder das GFCE, weiter unterstützen. Daneben sollten mit den Mitteln auch Organisationen gestärkt werden, die Projekte professionell, nachhaltig und nach europäischen Maßstäben und Werten anbieten und umsetzen können. Dabei sollte die Bundesregierung den Fokus auch auf Länder des afrikanischen Kontinents richten, die in der Vergangenheit vernachlässigt wurden und als ‚*digital deciders*' gelten könnten.

→ **Erstellen einer Arbeitsgruppe aus Vertreterinnen und Vertretern verschiedener Ministerien:** Um die verschiedenen *parent communities* (foreign policy community, development community, cybercrime community) zusammenzuführen und die unterschiedlichen Positionen

9 Grob gesagt könnte eine mögliche Definition von digitaler Souveränität folgende drei Aspekte beinhalten: (1) die Fähigkeit, Schlüsseltechnologien zu besitzen, eigene Innovationen hervorzubringen und strategisch wichtige Positionen in globalen Wertschöpfungsketten im digitalen und technologischen Bereich zu besetzen; (2) die Fähigkeit, die Resilienz kritischer Infrastrukturen und Netzwerke zu stärken und unsere freien und demokratischen Gesellschaften vor böswilligen Cyberaktivitäten zu schützen; und (3) die Fähigkeit, neue Technologien sowie digitale Dienste und Plattformen zu regulieren und internationale Standards und Normen im Einklang mit europäischen Werten wie Menschenrechten, Menschenwürde, Rechtsstaatlichkeit oder Datenschutz festzulegen.

in einer konzertierten Strategie zum Cyber-Kapazitätsaufbau zusammenzufassen, sollte eine Regierungsarbeitsgruppe eingerichtet werden. Dies sollte auch dazu beitragen, einen ganzheitlichen Ansatz für den Cyber-Kapazitätsaufbau zu schaffen und das Bewusstsein der Ministerien in der Regierung zu schärfen.

→ **Verankerung von Cybersicherheit als fester Bestandteil von Entwicklungsprogrammen:** Cybersicherheit ist eine wichtige Grundlage für die Digitalisierung von Wirtschaft und Gesellschaft und die Nutzung der damit verbundenen Potenziale. Das BMZ (und die GIZ) sollten Cybersicherheit als integralen Bestandteil von Entwicklungsprogrammen im Digitalbereich verankern. Internationale Akteure wie die Weltbank sind hier gute Beispiele; sie haben ihre ‚digitalen Portfolios' sukzessive erweitert.

5.2 Die Europäische Union und ihre Mitgliedstaaten

→ **Die EU und ihre Mitgliedstaaten sollten die angekündigte EU External Cyber Capacity Building Agenda und das EU Cyber Capacity Building Board für ein strategisches und koordiniertes Vorgehen nutzen:** Aufgrund der wachsenden Bedeutung afrikanischer Länder in Governance-Debatten zum Cyberbereich sollten die EU und ihre Mitgliedstaaten die EU External Cyber Capacity Building Agenda nutzen, um klare Prinzipien und Ziele für Zusammenarbeit und Umgang mit Ländern auf dem afrikanischen Kontinent zu entwickeln. In diesem Zusammenhang sollten sie sich auch auf afrikanische Länder konzentrieren und diese priorisieren, die bei Projekten zum Cyber-Kapazitätsaufbau übersehen wurden und die als ‚digitale Entscheider' in der wachsenden Dichotomie ‚digitale Demokraten vs. Autokraten' betrachtet werden könnten. Darüber hinaus sollte die Agenda auch für eine bessere Koordinierung zwischen verschiedenen EU-Institutionen genutzt werden und versuchen, deren Mandate und Ziele zusammenzuführen, auch um Duplikationen zu vermeiden. Dies würde auch dazu beitragen, eine bessere Finanzierungsstrategie im Lichte des aktuellen Mehrjährigen Finanzrahmens (2021–2027) zu entwickeln.

→ **Die EU sollte bestehende Initiativen und Foren zur Zusammenarbeit zwischen der EU und Afrika nutzen, um die Zusammenarbeit beim Cyber-Kapazitätsaufbau zu intensivieren:** Die Einrichtung eines AU-EU Digital-4Development (D4D) Hubs ist ein wichtiger Schritt, der um das Thema Cybersicherheit erweitert werden sollte. Dies könnte auch dazu beitragen, dass sich die Agenturen für Entwicklungszusammenarbeit der EU-Mitgliedstaaten stärker für den Cyber-Kapazitätsaufbau engagieren.

→ **Die EU und ihre Mitgliedstaaten sollten die Rolle das EU CyberNet als zentrale Drehscheibe für Expertinnen und Experten für den Cyber-Kapazitätsaufbau, den Austausch bewährter Verfahren und die Koordinierung stärken:** Die EU, Deutschland und andere Mitgliedsstaaten sollten den weiteren Aufbau des EU CyberNet als zentrale Drehscheibe für Expertise und Koordination von EU-geführten Projekten aktiv unterstützen, um eine Anlaufstelle für EU-Institutionen und Mitgliedsstaaten zu haben. Die Mitgliedstaaten sollten ihre eigenen nationalen Expertinnen und Experten in ihren Ländern ermuntern, sich am Rahmen des EU Cybernet zu beteiligen, und sie ermutigen, ihr Fachwissen für Projekte zur Verfügung zu stellen.

→ **Förderung eines Multi-Stakeholder-Ansatzes in afrikanischen Ländern:** Um dem sich abzeichnenden Trend des ‚digitalen Autoritarismus' entgegenzuwirken und aufgrund der Mehrdimensionalität und Beteiligung einer Vielzahl von Akteuren an der Cybersicherheit sollten die Bundesregierung und die EU gemeinsam mit Organisationen der Privatwirtschaft und der Zivilgesellschaft Projekte zur Cyberkapazität fördern und sodann konzipieren und eine Interaktion nur zwischen Regierungen vermeiden. Im partnerschaftlichen Geist sollte stark auf lokale Eigenverantwortung und Kompetenzentwicklung gesetzt werden, auch um aus Sicht der Entwicklungsländer langfristige Abhängigkeiten zu vermeiden.

→ **Konzentration darauf, die politische Entscheidungsfindung in Afrika im Sinne der Cyberdiplomatie zu ermöglichen:** Entscheidend ist, dass die fortschreitende Digitalisierung und die Stärkung der Cybersicherheit in diesen Ländern mit einer verstärkten Einbindung afrikanischer Diplomatinnen und Diplomaten in globale Normsetzungsdiskussionen rund um den Cyberraum einhergehen. Daher sollte die EU und Ministerien der Mitgliedstaaten wie das Auswärtige Amt Fachleute für Cyberdiplomatie beauftragen, mit afrikanischen Diplomatinnen und Diplomaten, sowie Angehörigen von Think Tanks zusammenzuarbeiten, um ihnen die Teilnahme und Gestaltung von Cyber-Governance-Debatten und -Prozessen zu ermöglichen.

Literatur

African Union (2020a): African Union Convention on Cyber Security and Personal Data Protection, https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection

African Union (2020b): The Digital Transformation Strategy for Africa (2020–2030), May 18, 2020, https://au.int/sites/default/files/documents/38507-doc-dts-english.pdf

African Union Commission and OECD (2021): Africa's Development Dynamics 2021, January 19, 2021 https://www.oecd-ilibrary.org/docserver/0a5c9314-en.pdf?expires=1640539352&id=id&accname=guest&checksum=B7D88B751EC6411ABD8A51A1FF6BFFA3

Barbero, Fabio/Berglund, Nils (2021): Cyber Capacity Building and Donor Coordination in the Western Balkans, in: DCAF- Geneva Centre for the Democratic Control of Armed Forces, May 7, 2021, https://www.dcaf.ch/sites/default/files/publications/documents/CybersecurityCapacityBuilding_DonorCoordination_inWB_mar2021.pdf

Calandro, Enrico/ Berglund, Nils (2019): Bridging the cyber norms debate with evidence, in: Research ICT Africa, December 4, 2019, https://www.un.org/disarmament/wp-content/uploads/2019/12/Discussion-Paper-OEWG-Intersessional-Meeting.pdf

Collett, Robert (2021): Understanding cybersecurity capacity building and its relationship to norms and confidence building measures, in: Journal of Cyber Policy, 2021, Vol 6, No. 3, 298–317

Collett, Robert/Barmpaliou, Nayia (2021a): International Cybercapacity Building: Global Trends and Scenarios, in: European Union Institute Security Studies, 23.September 2021, https://www.iss.europa.eu/sites/default/files/EUISSFiles/CCB%20Annex%203%20Final_0.pdf

Collet, Robert/ Barmpaliou, Nayia (2021b): International Cyber Capacity Building: Global Trends and Scenarios, Annex 3, Notes on Cyber Capacity Building Funders, in European Union Institute Security Studies, 23.September 2021, https://www.iss.europa.eu/sites/default/files/EUISSFiles/CCB%20Annex%203%20Final_0.pdf

Council of Europe (2022): Parties/Observers to the Budapest Convention and Observer Organisations to the T-CY, https://www.coe.int/en/web/cybercrime/parties-observers

Csenkey, Kristin/ Perron, Maj. Bruno (2020): Cyber Capacity Building in the Canadian Arctic and the North, in: NAADSN, October 27, 2020, https://www.naadsn.ca/wp-content/uploads/2020/10/Csenkey-and-Perron_Cyber-Capacity-Building-in-the-Canadian-Arctic-and-the-North.pdf

Cyber Portal (2022): https://cybilportal.org/actors-advanced?_sft_region=sub-saharan-africa

Dannouni, Amane et al. (2020): The Race for Digital Advantage in Africa, in: Boston Consulting Group, https://www.bcg.com/de-de/publications/2020/race-digital-advantage-in-africa

Dutton et al. (2019): Cybersecurity Capacity: Does It Matter?, in: Journal of International Policy, Vol. 9 (2019), pp. 280–306

European Investment Bank (2021): The rise of Africa's digital econom – The European Investment Bank's activities to support Africa's transition to a digital economy February 2021, https://www.eib.org/attachments/thematic/study_the_rise_of_africa_s_digital_economy_en.pdf

European Union (2020): The EU's Cybersecurity Strategy for the Digital Decade, December 16, 2020, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020JC0018&from=EN

Federal Foreign Office (2022): Acting resolutely instead of merely reacting – Germany's G7 Presidency in 2022, January 1, 2022, https://www.auswaertiges-amt.de/en/aussenpolitik/internationale-organisationen/g8-g20/g7-presidency/2504680

Federal Ministry of Interior (2021): Cyber Security Strategy for Germany, https://www.cio.bund.de/SharedDocs/Publikationen/DE/Strategische-Themen/css_engl_download.pdf?__blob=publicationFile

Google/ International Finance Corporation (2020): e-Conomy Africa 2020. Africa's $180 billion Internet economy future, https://www.ifc.org/wps/wcm/connect/e358c23f-afe3-49c5-a509-034257688580/e-Conomy-Africa-2020.pdf?MOD=AJPERES&CVID=nmuGYF2

GSMA (2021): The Mobile Economy Sub-Saharan Africa 2021, https://www.gsma.com/mobileeconomy/wp-content/uploads/2021/09/GSMA_ME_SSA_2021_English_Web_Singles.pdf

GSMA (2020): Mobile Internet Connectivity 2020. Sub-Saharan Africa Factsheet, https://www.gsma.com/r/wp-content/uploads/2020/09/Mobile-Internet-Connectivity-SSA-Fact-Sheet.pdf

Homburger, Zine (2019): The Necessity and Pitfall of Cybersecurity Capacity Building for Norm Development in: Cyberspace, Global Society, 33:2, pp. 224–242

International Telecommunication Union (2022): National Cybersecurity Strategies Repository, https://www.itu.int/en/ITU-D/Cybersecurity/Pages/National-Strategies-repository.aspx

International Telecommunication Union (2021): Global Cybersecurity Index 2020. Measuring commitment to cybersecurity, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf

(ISC)² (2019): Strategies for Building and Growing Strong Cybersecurity Teams, (ISC)² Cybersecurity Workforce Study, 2019, https://www.isc2.org/-/media/ISC2/Research/2019-Cybersecurity-Workforce-Study/ISC2-Cybersecurity-Workforce-Study-2019.ashx?la=en&hash=1827084508A24DD75C60655E243EAC59ECDD4482

Kshetri, Nir (2019): Cybercrime and Cybersecurity in Africa, in: Journal of Global Information Technology Management, 2019, Vol. 22, No. 2, pp. 77-81

Muller, Pijnenburg Lilly (2015): Cyber Security Capacity Building in Developing Countries: Challenges and Opportunities, in: Nowegian Institute of International Affairs

Pawlak, Patryk (2016): Capacity Building in Cyberraum as an Instrument of Foreign Policy, in: Global Policy, Vol. 7, Issue 1, February 2016, 83–92

Statista (2022): E-commerce revenue in Africa in 2017 to 2025, https://www.statista.com/statistics/1190541/e-commerce-revenue-in-africa/

United Nations Broadband Commission for Sustainable Development (2019): Connecting Africa Through Broadband: A strategy for doubling connectivity by 2021 and reaching universal access by 2030, October 17, 2019, https://www.broadbandcommission.org/publication/connecting-africa-through-broadband/

Liste der Abkürzungen

ASPI (Australian Strategic Policy Institute)

AU (Afrikanische Union)

BMZ (Bundesministerium für wirtschaftliche Zusammenarbeit und Entwicklung)

BSI (Bundesamt für Sicherheit in der Informationstechnik)

C3SA (Cybersecurity Capacity Centre for Southern Africa)

CERT (Computer Emergency Response)

CSIRT (Cyber Security Incident Response Team)

CTO (Cyber Security Incident Response Team)

EU (Europäische Union)

EUISS (European Union Institute for Security Studies)

GCSCC (Oxford Global Cyber Security Capacity Centre)

DSGVO (EU-Datenschutzgrundverordnung)

GFCE (Global Forum on Cyber Expertise)

GIZ (Deutsche Gesellschaft für Internationale Zusammenarbeit)

IKT (Informations- und Kommunikationstechnologien)

ITU (International Telecommunication Union)

NGO (Nichtregierungsorganisation)

UN GGE (UN Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security)

UN OEWG (UN Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security)

Anhang

National

Wie in anderen Nationalstaaten ist auch in Deutschland der Aufbau von externen Cyberkapazitäten ein vergleichsweise junges Feld. Es ist jedoch festzuhalten, dass sich verschiedene Akteure der Bundesregierung in letzter Zeit mit dem Thema auseinandergesetzt und diesbezüglich Maßnahmen ergriffen haben.[1]

Das Auswärtige Amt hat bereits in der Vergangenheit Projekte zum Cyber-Kapazitätsaufbau unterstützt und wird sein Engagement und seine Aktivitäten in diesem Bereich weiter ausbauen. Der „Koordinierungsstab für internationale Cyber-Außenpolitik und Cybersicherheit" des Auswärtigen Amtes hat sich finanziell am Digital Development Trust der Weltbank beteiligt, der als eine seiner sechs Säulen Cybersicherheit hat, und gehörte zu den ersten Geldgebern, die den neu gegründeten Cybersecurity Multi-Donor Trust Fund unterstützten. Darüber hinaus hat er Projekte des GFCE unterstützt. In der Vergangenheit hat er Projekte zum Cyber-Kapazitätsaufbau für mehrere Interessengruppen mit Schwerpunkt auf der Anwendung des Völkerrechts auf den Cyberraum finanziert, mit Umsetzung durch die ICT4Peace Foundation. (Collett/Barmpaliou 2021b: 14-15) Als eines der drei Mitglieder des Beirats hat das Auswärtige Amt eine tragende Rolle bei der Einrichtung des EU CyberNet gespielt (siehe nächstes Kapitel). Darüber hinaus hat das Auswärtige Amt angekündigt, dass Cybersicherheit ein Schwerpunkt seines Programms während der deutschen G7-Präsidentschaft im Jahr 2022 sein wird und „to put projects aimed at ensuring better cyber security in selected partner countries outside the G7 and future investments in joint global infrastructure on the agenda." (Auswärtiges Amt 2022)

In jüngster Zeit haben das BMZ (Bundesministerium für wirtschaftliche Zusammenarbeit und Entwicklung) und seine Durchführungsorganisation GIZ (Deutsche Gesellschaft für Internationale Zusammenarbeit) ihre Anstrengungen verstärkt und ihre Aktivitäten zur digitalen Entwicklung ausgebaut. Dies spiegelte sich vor allem in der Digitalstrategie 2019 des BMZ und der Einrichtung eines eigenen Referats ‚Digitalisierung in der Entwicklungszusammenarbeit' wider. Die Strategie umfasst jedoch nicht ausdrücklich den Cyber-Kapazitätsaufbau oder Cybersicherheit. Darüber hinaus sind vom BMZ geförderte und von der GIZ durchgeführte Projekte mit Cybersicherheits-Elementen zahlenmäßig noch begrenzt, es gibt jedoch einige Entwicklungen in diese Richtung. So umfasst beispielsweise das vom BMZ beauftragte und von der GIZ geleitete Projekt „Digitalzentrum Tunesien" die Sicherung der digitalen Infrastruktur und den Ausbau von Cybersicherheitskompetenzen. (GIZ 2022a) Darüber hinaus führt die deutsche Tech-Denkfabrik Stiftung Neue Verantwortung im Auftrag des BMZ und finanziert von der GIZ Übungen zur Cyberpolitik in mehreren Ländern durch, darunter Ruanda, Kenia, Südafrika, Ghana und der Elfenbeinküste (Stiftung Neue Verantwortung 2021). Auch das von der EU und dem Auswärtigen Amt in Auftrag gegebene GIZ-Projekt „Enhancing Security Cooperation in and with Asia" besteht aus Hilfestellungen in Sachen Cybersicherheit. (GIZ 2022b)

Auch die Bundesregierung bezieht sich in ihrer im September 2021 veröffentlichten neuesten Cybersicherheitsstrategie (Bundesministerium des Innern (2021)) auf den Cyber-Kapazitätsaufbau als „wichtiges Instrument, um die Chancen der Digitalisierung zu nutzen und den damit verbundenen Risiken entgegenzuwirken", und zwar im Besonderen an Orten, „wo Menschen den Erstzugang zum Cyberraum" erhalten. Außerdem heißt es dort auch, dass „Cybersicherheit wird daher als Komponente in allen digitalen Projekten der Entwicklungszusammenarbeit mitgedacht".[2] Darüber hinaus erkennt sie an, dass das Thema international weiter an Bedeutung gewonnen hat und strebt eine stärkere Integration der Cybersicherheit in Programme zur Förderung der digitalen Wirtschaft und in Stabilisierungsmaßnahmen an. Mit dem Cyber-Kapazitätsaufbau, so die Strategie, soll auch der Effekt auftreten, dass „[d]emokratische und normative Werte und Ideal" verankert werden können und eine allgemeine Erhöhung der Cybersicherheit in den Partnerstaaten erfolgt. Um diese Ziele zu erreichen, gibt es zwei Maßnahmenkriterien: 1. „Der Cyberkapazitätsaufbau ist in internationalen Gremien als Thema etabliert und wurde in relevanten Policy-Dokumenten verankert."; 2. „Deutschland beteiligt sich an der Durchführung und/oder Unterstützung von Maßnahmen zum Cyberkapazitätsaufbau im nationalen, EU-, NATO- oder internationalen Kontext."

Die Cybersicherheitsstrategie gibt grundsätzlich die (sehr) groben Linien für ein (wertebasiertes) stärkeres Engagement Deutschlands für den Cyber-Kapazitätsaufbau vor. Die konkrete Ausgestaltung und Strukturierung dieser Ideen und eine mögliche strategische Ausrichtung stehen damit aber noch nicht fest. Angesichts der zunehmenden Aktivitäten des Auswärtigen Amtes und des BMZ bleibt zudem abzuwarten, wie die digitale Entwicklung und die außenpolitischen Ansätze sowie die übergeordneten Gemeinschaften im deutschen Kontext zusammengeführt werden können.

1 Der folgende Abschnitt basiert auf eigenen Informationen des Autors und Open-Source-Referenzen.

2 Betrachtet man die von der Bundesregierung geförderten Digitalprojekte, ist dies jedoch nicht immer der Fall.

International

Europa: EU und Europarat

Der Cyber-Kapazitätsaufbau wurde schrittweise von der EU (Europäische Union) aufgegriffen, mit dem Ziel, dessen strategische Bedeutung zu erhöhen und damit verbundene Projekte des Blocks und seiner Mitgliedstaaten effektiv zu gestalten und umzusetzen. Bereits 2018 hat die EU zwei Nachschlagewerke ausgearbeitet, die „Council Conclusions on EU External Cyber Capacity Building Guidelines" und die „Operational Guidance for the EU's international cooperation on cyber capacity building", die die grundlegenden Konzepte, Ansätze, Methoden und Ziele skizzieren. In ihrem Gesamtdiskurs betont die EU die Bedeutung des Aufbaus von Cyberkapazitäten als strategischen Baustein für die europäische Cyberdiplomatie, der zur Förderung und zum Schutz der Menschenrechte, der digitalen Gleichstellung der Geschlechter, der Rechtsstaatlichkeit, der Sicherheit, des inklusiven Wachstums und der nachhaltigen Entwicklung sowie zu einem sicheren, stabilen, freien und offenen Cyberraum beitragen sollte. Auch das „Non-Paper on EU Cyber Diplomacy", das Deutschland, Estland, Frankreich, Polen, Portugal und Slowenien im Rahmen der deutschen EU-Ratspräsidentschaft im November 2020 herausgegeben haben, unterstreicht diese Ziele. (Auswärtiges Amt 2020)

In den Schlussfolgerungen des Rates von 2018 heißt es, dass der Cyber-Kapazitätsaufbau verschiedenen Zielen dient, darunter die Stärkung nationaler, institutioneller und organisatorischer Kapazitäten, die die Resilienz kritischer digitaler Dienste und Netzwerke und den Schutz kritischer Informationsinfrastrukturen verbessern; Unterstützung von Reformen der Strafjustiz zur Bekämpfung der Cyberkriminalität; Bekämpfung der Nutzung des Internets für terroristische Zwecke; Verbesserung der Cybersicherheitsfähigkeiten und -kompetenzen von Einzelpersonen; und Förderung der Sensibilisierung sowie wirksamer Zusammenarbeit zu diesen Themen auf nationaler, regionaler und internationaler Ebene.

Die EU-Cybersicherheitsstrategie vom Dezember 2020 (Europäische Union 2020) geht noch einen Schritt weiter und fordert die Entwicklung einer EU-Agenda zum Aufbau externer Cyberkapazitäten. Die Agenda soll das Fachwissen der Mitgliedstaaten und der einschlägigen EU-Organe, -Einrichtungen, -Agenturen und -Initiativen im Einklang mit ihren jeweiligen Mandaten nutzen. Darüber hinaus sollte ein EU-Ausschuss für den Cyber-Kapazitätsaufbau eingerichtet werden, dem relevante institutionelle EU-Akteure angehören, um Fortschritte aufzuzeichnen und weitere Synergien und potenzielle Lücken zu ermitteln. Beide Vorschläge sind Anzeichen dafür, dass die EU dem Cyber-Kapazitätsaufbau eine höhere strategische Bedeutung beimessen und einen stärker koordinierten Ansatz verfolgen wird.

Hauptsächlich über ihre GD INTPA (Generaldirektion für Internationale Partnerschaften) hat die Europäische Kommission mehrere Projekte zum Cyber-Kapazitätsaufbau mit Schwerpunkt auf ihrer unmittelbaren Nachbarschaft (z. B. Westbalkan), aber auch darüber hinaus, unterstützt. Über ihre verschiedenen externen Finanzierungsinstrumente wie IcSP (Instrument Contributing to Stability and Peace), EDF (European Development Fund) oder das PI (Partnership Instrument) hat sie im Laufe der Jahre globale, regionale und bilaterale Projekte im Cyberbereich finanziert, z. B. auch das Projekt OCWAR-C (West African Response on Cybersecurity and Fight against Cybercrime) in Zusammenarbeit mit der Kommission der ECOWAS (Wirtschaftsgemeinschaft Westafrikanischer Staaten). Laut Collett/Barmpaliou (2021b: 6) hat die EU hauptsächlich Projekte zu drei großen Bereichen unterstützt: *„the development or reform of appropriate legal frameworks in the fight against cybercrime on the basis of international standards (Budapest Convention on Cybercrime)" and "enhancing the capacities of criminal justice authorities"; "the development of a comprehensive set of organizational, technical and cooperation frameworks and mechanisms that increase third countries' cyber resilience and preparedness"; and the strengthening of "international cyber policy coordination"*. (Collett/Barmpaliou 2021b: 6) Es bleibt abzuwarten, inwieweit das aktuelle EU-Budget (Multi-Annual Financial Framework, MFF) für Projekte zum Cyber-Kapazitätsaufbau bereitgestellt wird.

Allerdings fehlt oft der Überblick über diese Projekte und den jeweiligen Bedarf in den Empfängerländern, was zu Duplikationen und einem unzureichenden Gleichgewicht zwischen Angebot und Nachfrage führen kann. Darüber hinaus ist die Bereitstellung von Expertinnen und Experten aus den EU-Mitgliedstaaten nach wie vor eine Herausforderung. Das von der EU geförderte Projekt EU CyberNet[3] soll hier Abhilfe schaffen. Ziel des Projekts ist es, einen EU-weiten Expertenpool für Projekte zum Cyber-Kapazitätsaufbau zu schaffen und eine europäische Stakeholder-Community zu diesem Themenfeld aufzubauen. Das Projekt soll bewirken, dass die EU kohärenter und koordinierter vorgeht. Das Projekt wird von der RIA (Estonian Information Security Authority) durchgeführt, in Zusammenarbeit mit den beiden Beiratsmitgliedern, dem Auswärtigen Amt der Bundesrepublik Deutschland und dem C3 Cybersecurity Competence Center Luxembourg. Es wird von der Europäischen Kommission bis 2025 gefördert.

Die EU arbeitet auch aktiv mit dem Europarat zusammen, der selbst Projekte umsetzt und vor allem auf der Grundlage der Förderung seiner eigenen Budapester Konvention gestaltet. In diesem Zusammenhang zielen das gemeinsam vom Europarat und der Europäischen Kommission finanzierte Vorzeigeprojekt GLACY (Global Action on Cybercrime) und das Nachfolgeprojekt GLACY+ (Global Action on Cybercrime Extended) darauf ab, unter anderem die Gesetzgebung zur Cyberkriminalität, Policies und Strategien sowie die Kapazitäten der Justiz und Polizeibehörden zur Untersuchung von Cyberkriminalität in asiatischen und afrikanischen Staaten zu fördern und zu stärken[4]. Das Octopus-Projekt ist ein weiteres laufendes Projekt des Europarates mit dem Ziel, die Umsetzung der *Budapest Convention* über Computerkriminalität auf globaler Ebene zu unterstützen.

3 Der Verfasser dieses Beitrags war in seiner Funktion als Strategic Advisor for Cyber Diplomacy/EU Presidency des Internationalen Koordinierungsstabs für Cyber-Außenpolitik und Cybersicherheit des Auswärtigen Amts Mitglied des Beirats von EU Cyber Net.
4 GLACY+ konzentriert sich derzeit auf folgende Schwerpunkt- und Hub-Länder in Afrika: Benin, Burkina Faso, Cabo Verde, Ghana, Mauritius, Marokko, Nigeria und Senegal.

Im Rahmen der deutschen EU-Ratspräsidentschaft in der zweiten Jahreshälfte 2020 (begleitet durch das BMZ) wurde im Dezember 2020 zudem der AU-EU Digital4Development (D4D) Hub – ein Netzwerk von bislang elf EU-Mitgliedstaaten in Kooperation mit der DG INTPA – gegründet. Er zielt darauf ab, eine Vielzahl digitaler Initiativen europäischer Akteure in einem strategischen und koordinierten Ansatz zusammenzuführen und umzusetzen. Der Hub ist dem ‚Team Europe'-Konzept nachempfunden und bündelt die Ressourcen der EU, ihrer Mitgliedstaaten und Finanzinstitute, insbesondere der Europäischen Investitionsbank und der Europäischen Bank für Wiederaufbau und Entwicklung. Weitere Initiativen in diesem Rahmen sind die ‚African-European Innovation Bridge', die darauf abzielt, ein panafrikanisches Netzwerk von Digital Innovation Hubs aufzubauen, und das ‚EU-AU Data Flagship', dessen Ziel ist, die Investitionen in die afrikanische Dateninfrastruktur anzukurbeln und den Datenschutz zu verbessern. Cybersicherheit wird in diesen Zusammenhängen bisher jedoch nicht explizit genannt.

Außerdem haben einzelne Mitgliedsstaaten, wie im Fall Deutschlands, ihre eigene Cyberkapazitätsagenda und investieren und unterstützen entsprechende Projekte, beispielsweise die digitalaffinen Länder Estland und die Niederlande. Ersteres spielt im EU-Kontext eine zentrale Rolle, da die Estonian Information System Authority, die für die Verwaltung der landesweiten Informationssysteme zuständig ist, die Leitung der Umsetzung von EU CyberNet und von mehreren anderen EU-finanzierten Projekten übernimmt. Die Niederlande haben auch bereits eine Tradition darin, die Gesamtentwicklung der internationalen Agenda zum Cyber-Kapazitätsaufbau zu unterstützen, beispielsweise durch die Ausrichtung der vierten GCCS (Global Conference on Cyber Space), die als „launchpad for the Global Forum on Cyber Expertise (GFCE)" diente (Collett/ Barmpaliou 2021b: 20–21), und durch die Finanzierung des GFCE-Sekretariats mit Sitz in Den Haag. Das niederländische Außenministerium finanziert auch das Sekretariat der Freedom Online Coalition und unterstützt mehrere andere Projekte, auch als Konsortialpartner im Rahmen des EU-geführten Programms ‚Cyber Resilience for Development' (Cyber-4Dev) zusammen mit Großbritannien und Estland.

Es bleibt abzuwarten, wie der Cyber-Kapazitätsaufbau in diese Entwicklungen integriert wird, die hauptsächlich aus Überlegungen zur digitalen Entwicklung stammen, und wie die von der EU-Cybersicherheitsstrategie vorgeschlagenen Initiativen entwickelt werden, die eine stärkere Ausrichtung auf den Bereich der Cyber-Diplomatie haben. Die aktuelle europäische Debatte um digitale Souveränität und Cyber-Resilienz ist jedoch weitgehend nach innen gerichtet und der afrikanische Kontinent spielt in den Diskussionen in diesen Kontexten noch eine eher untergeordnete Rolle. Selbst zentrale EU-Initiativen wie der KI-Rechtsrahmen der Europäischen Kommission gehen nur am Rande auf die potenzielle Bedeutung des Gesetzesvorschlags für entwicklungsschwache Staaten ein.

Kasten 1: OEWG-Prinzipien zum Cyber-Kapazitätsaufbau:

Process and Purpose

- → Capacity-building should be a sustainable process, comprising specific activities by and for different actors.
- → Specific activities should have a clear purpose and be results focused, while supporting the shared objective of an open, secure, stable, accessible and peaceful ICT environment.
- → Capacity-building activities should be evidence-based, politically neutral, transparent, accountable, and without conditions.
- → Capacity-building should be undertaken with full respect for the principle of State sovereignty.
- → Access to relevant technologies may need to be facilitated.

Partnerships

- → Capacity-building should be based on mutual trust, demand-driven, correspond to nationally.
- → identified needs and priorities, and be undertaken in full recognition of national ownership. Partners in capacity-building participate voluntarily.
- → As capacity-building activities should be tailored to specific needs and contexts, all parties are active partners with shared but differentiated responsibilities, including to collaborate in the design, execution and monitoring and evaluation of capacity-building activities.
- → The confidentiality of national policies and plans should be protected and respected by all partners.

People

- → Capacity-building should respect human rights and fundamental freedoms, be gender sensitive and inclusive, universal and non-discriminatory.
- → The confidentiality of sensitive information should be ensured.

Andere internationale Organisationen

Die Normsetzungsprozesse in der UN GGE (UN Group of Governmental Experts on Advancing Responsible State Behavior in Cyberraum in the Context of International Security) und in der UN OEWG (UN Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security), die die Hauptgruppen für die Festlegung von Regeln für verantwortungsvolles staatliches Verhalten im Cyberraum sind, bieten eine Grundlage für Projekte zum Cyber-Kapazitätsaufbau, und ihre Abschluss-/Konsensberichte haben wiederholt ihre Bedeutung für die Stärkung der Cybersicherheit über die Jahre gesteigert.

Im jüngsten inhaltlichen Abschlussbericht vom März 2021 (UN 2021a) stellt die OEWG klar fest, dass Cyber-Kapazitätsaufbau „is of particular relevance to developing States, in order to facilitate their genuine participation in discussions on ICTs in the context of international security and their ability to address vulnerabilities in their critical infrastructure" sowie „for promoting adherence to international law and the implementation of norms of responsible State behaviour". Darüber hinaus legt sie bestimmte Grundsätze fest, die Projekte zum Cyber-Kapazitätsaufbau leiten sollten (siehe Kasten 1), und hebt hervor, dass der Aufbau von Kapazitäten eine „two-way street" ist, was bedeutet, dass „participants learn from each other" in Form von „South–South, South–North, triangular, and regionally focused cooperation" Insbesondere wird die Bedeutung des Aufbaus von Kapazitäten für „[the] genuine involvement of developing countries in relevant discussions and fora and strengthening the resilience of developing countries in the ICT environment." betont.

In gleicher Weise hebt der jüngste UN GGE-Bericht (UN 2021b), der im Juli 2021 angenommen wurde, den Aufbau von Cyberkapazitäten hervor und betont, dass die internationale Zusammenarbeit in dieser Hinsicht dazu führen sollte, dass Länder in Bereichen wie *„developing and implementing national ICT policies, strategies and programmes", „creating and enhancing the capacity of CERTs/CSIRTs and strengthening arrangements for CERT/CSIRT-to-CERT/CSIRT cooperation"* oder *„'implementing agreed voluntary, non-binding norms of responsible State behaviour"* unterstützt werden. Darüber hinaus heißt es in dem Bericht, dass Nationalstaaten *„should consider approaching cooperation in ICT security and capacity-building in a manner that is multi-disciplinary, multi-stakeholder, modular and measurable."*

Das 2015 gegründete GFCE (Global Forum on Cyber Expertise) mit Sitz in Den Haag hat sich zu einer internationalen Anlaufstelle für den Cyber-Kapazitätsaufbau entwickelt und ist *„the only international, multistakeholder forum with the primary purpose of strengthening global cyber capacity by supporting international coordination and cooperation."* (Collett/Barmpaliou 2021: 5) Es hat mehr als 140 Mitgliedstaaten und Partnerorganisationen und engagiert sich in mehreren Bereichen, vor allem durch seine Arbeitsgruppen. Die Bereiche umfassen die Koordination regionaler und globaler Projekte und Initiativen, den Wissensaustausch durch Empfehlungen von Tools und Publikationen sowie die Ermittlung des individuellen Bedarfs an Cyberkapazitäten mit Unterstützungsangeboten. Deutschland engagiert sich im GFCE als Beitragszahler und im Vorstand sowie in der Projektförderung. Die Wirksamkeit seiner koordinierenden Rolle wird jedoch immer noch durch die Freiwilligkeit der Beiträge seiner Mitglieder behindert. (ebd. 5)

Mit ihren beiden Treuhandfonds – dem *umbrella trust fund* Digital Development Partnership und dem nachgeordneten Cyber Security Multi-Donor Trust Fund – sowie mit dem Global Cyber Security Capacity Program will die Weltbankgruppe ihre Arbeit an der digitalen Entwicklung mit mehr Aktivitäten zum Aufbau von Cybersicherheitskapazitäten ausbauen. Insbesondere der Multi-Donor Trust Fund sieht einen konzertierteren und strategischeren Ansatz vor – beispielsweise die Konzeption von Projekten auf der Grundlage evidenzbasierter Forschung – auch mit Schwerpunkt auf dem afrikanischen Kontinent.

Die SCO (Shanghai Cooperation Organization) ist ein weiterer Akteur, der sich mit dem Cyber-Kapazitätsaufbau beschäftigt. Eine besondere Rolle in diesem thematischen Schwerpunkt kommt der SCO durch die Mitgliedschaft Chinas und Russlands und deren Vorstellungen zur Regulierung des Cyberraum zu. Die auf staatliche Souveränität und nationale Sicherheit ausgerichteten Ideen spiegeln sich vor allem in dem von der Organisation herausgegebenen Internationalen Verhaltenskodex für Informationssicherheit wider. Damit einher geht der Trend, dass beispielsweise BRICS-Staaten nicht mehr nur Nutzer und Importeure von Cyberfähigkeiten sind, sondern diese aktiv bereitstellen. Insbesondere China „emphasizes its commitment to cybersecurity capacity building in developing economies and mentions Asian Regional Forum and Forum on China–Africa Cooperation as fora for cooperation." (Homburger 2019: 234–235)

Auch die ITU (International Telecommunication Union) ist in diesem Bereich zunehmend aktiv, bietet beispielsweise sogenannte „model laws" zur Regulierung der Cybersicherheit an und führt selbst Projekte zum Cyber-Kapazitätsaufbau in Entwicklungsländern durch (Homburger 2019: 230). Vor diesem Hintergrund ist es bemerkenswert, dass *„[c]ountries like China and Russia – together with some developing countries – openly suggest that the ITU should play a more active role in Internet governance, which would result in more governmental control".* (Pawlak 2016: 89)

Auch andere regionale Organisationen engagieren sich zunehmend: Die OAS (Organization of American States) bietet eine Reihe von Maßnahmen an (z. B. National Cyber Security Strategy Development, Crisis Management Exercises etc.) und hat das OAS Cybersecurity Program und ein interamerikanisches Portal zur Cyberkriminalität eingerichtet. Die ASEAN (Association of Southeast Asian Nations) verfügt über groß angelegte Initiativen für ihre Region, darunter den Brunei Action Plan Enhancing ICT Competitiveness: Capacity Building, das ASEAN Cyber Capacity Program (ACCP) oder das ASEAN-Japan Cybersecurity Capacity Building Center.

Neben staatlichen Akteuren und internationalen Organisationen engagieren sich zunehmend mehrere Stiftungen und zivilgesellschaftliche Akteure (z. B. ICT4Peace, Asia Foundation, Bill and Melinda Gates Foundation, Hewlett Foundation), akademische Institutionen und Thinktanks (z. B. DCAF – Geneva Centre for Security Sector Governance) sowie private Unternehmen (z. B. Microsoft, Kaspersky, Symantec) beim Aufbau internationaler Cyberkapazitäten.

Abkürzungen

ASEAN (Association of Southeast Asian Nations)

BMZ (Bundesministerium für wirtschaftliche Zusammenarbeit und Entwicklung)

EDF (Europäischer Entwicklungsfonds)

EU (Europäische Union)

GCCS (Global Conference on Cyber Space)

GFCE (Global Forum on Cyber Expertise)

IcSP (Instrument Contributing to Stability and Peace)

ITU (International Telecommunication Union)

RIA (Estonian Information Security Authority)

OAS (Organization of American States)

SCO (Shanghai Cooperation Organization)

UN GGE (UN Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security)

UN OEWG (UN Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security)

Literatur

Collett, Robert/Barmpaliou, Nayia (2021a): International Cybercapacity Building: Global Trends and Scenarios, in: European Union Institute Security Studies, 23.September 2021, https://www.iss.europa.eu/sites/default/files/EUISSFiles/CCB%20Report%20Final.pdf

Collet, Robert/ Barmpaliou, Nayia (2021b): International Cyber Capacity Building: Global Trends and Scenarios, Annex 3, Notes on Cyber Capacity Building Funders, in European Union Institute Security Studies, 23.September 2021, https://www.iss.europa.eu/sites/default/files/EUISSFiles/CCB%20Annex%203%20Final_0.pdf

European Union (2020): The EU's Cybersecurity Strategy for the Digital Decade, December 16, 2020, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020JC0018&from=EN

Federal Foreign Office (2022): Acting resolutely instead of merely reacting – Germany's G7 Presidency in 2022, January 1, 2022, https://www.auswaertiges-amt.de/en/aussenpolitik/internationale-organisationen/g8-g20/g7-presidency/2504680

Federal Foreign Office (2020): Non-Paper on EU Cyber Diplomacy by Estonia, France, Germany, Poland, Portugal and Slovenia, November 19, 2020, https://www.auswaertiges-amt.de/en/aussenpolitik/themen/eu-cyber-non-paper/2418984

Federal Ministry of Interior (2021): Cyber Security Strategy for Germany, https://www.cio.bund.de/SharedDocs/Publikationen/DE/Strategische-Themen/css_engl_download.pdf?__blob=publicationFile

GIZ (2022a): Shaping Tunisia's digital transformation and creating jobs, https://www.giz.de/en/downloads/giz2020-en-digitalzentrum-tunesien.pdf

GIZ (2022b): Enhancing Security Cooperation in and with Asia, https://www.giz.de/en/worldwide/87412.html

Stiftung Neue Verantwortung (2021): https://www.stiftung-nv.de/en/publication/cybersecurity-policy-exercises

UN (2021a): Final Substantive Report, March 10, 2021 https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf

UN (2021b): Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, July 14, 2021, https://front.un-arm.org/wp-content/uploads/2021/08/A_76_135-2104030E-1.pdf

Über den Autor

Kaan Sahin ist Berater für internationale Politik mit Schwerpunkt auf Technologie- und Cyberfragen. Er war Technology Fellow im Planungsstab im Auswärtigen Amt. Zuvor war er Research Fellow für Technologie und Außenpolitik bei der Deutschen Gesellschaft für Auswärtige Politik (DGAP). Während dieser Zeit nahm er eine Auszeit, um als Strategischer Berater für Cyberdiplomatie/EU-Präsidentschaft im Auswärtigen Amt zu arbeiten. In dieser Funktion entwickelte er ein Konzept und einen Aktionsplan zum Cyber-Kapazitätsaufbau und war Mitglied des Beirats von EU CyberNet.

Zuvor arbeitete Herr Sahin bei Deloitte als Cyber Risk Consultant und Projektleiter. Davor erhielt er ein Mercator Fellowship für internationale Aufgaben und spezialisierte sich auf Strategien zur Bekämpfung hybrider Bedrohungen. In dieser Eigenschaft arbeitete er beim International Institute for Strategic Studies (IISS), dem Sonderbeauftragten der OSZE für den Südkaukasus, Carnegie Europe und in der Emerging Security Challenges Division im NATO-Hauptquartier.

Herr Sahin studierte Politikwissenschaft an der Universität Duisburg-Essen sowie internationale Politik und Friedensforschung an der Universität Tübingen, der University of Connecticut und der Koç University in Istanbul.