FRIEDRICH NAUMANN FOUNDATION For Freedom.

CYBER CAPACITY BUILDING AND STRATEGIC ENGAGEMENT WITH AFRICA

A new mission for Germany and Europe

by Kaan Sahin

ANALYSIS

Imprint

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

/freiheit.org
/FriedrichNaumannStiftungFreiheit
/FNFreiheit
/stiftungfuerdiefreiheit

Authors
Kaan Sahin

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

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

Date
April 2022

Notes on using this publication
This publication is an information offer of the Friedrich Naumann Foundation for Freedom.
It is available free of charge and not intended for sale. It may not be used by parties or election workers for the purpose of election advertising during election campaigns (federal, state or local government elections, or European Parliament elections).

Table of Content

Executive Summary

While the digitalization entails transformative effects and benefits for modern societies, it also exposes countries, companies and individuals to more and more cyberattacks, with potential devastating impact on economic prosperity, data privacy and social well-being. Especially countries in the Global South such as in Africa have still a limited cyber maturity and will most likely suffer increasingly from malicious cyber activities in the years to come due to their growing digital adoption.

Thus, the enhancement of cyber security in African countries is imperative and more and more international actors have gradually started to invest and support in cyber capacity building projects in Africa and beyond. However, since these engagements have political and value-based implications – in particular in the context of the growing trend of digital authoritarianism –, cyber capacity building is not only a sheer technical or economic matter, but entails also the transfer of basic ideas and values concerning on how governments and societies deal with digitalization and the cyber domain. Hence, the present paper sheds light on the current trends of cyber capacity building and its implications in Africa and beyond as well as on its actor landscape. It argues that Germany and Europe should strategically engage more with African countries in terms of cyber capacity building to avoid that these countries slide into the camp of 'digital authoritarianism' and help them to embrace the benefits of digitalized economy flanked by proper cyber security.

1. Introduction

While the digital transformation can bring great opportunities to modern societies in terms of economic growth and social well-being, citizens, businesses, and governments are exposed to malicious cyber activities at an ever-increasing rate at the same time. Cyber attacks are expanding in form of frequency, scope, sophistication and the caused damage. Certain state and non-state actors, including proxies, or cyber criminals have ramped up their malicious cyber activities, which are differing in scale, duration, intensity, and complexity. In addition, these attacks can take various purposes, including malicious cyber activities (e.g., ransomware or wiper malware) against critical infrastructure, cyber-espionage, intellectual property theft or to serve criminal and political purposes in form of disinformation or hybrid activities. As interconnectedness increases, dependencies and vulnerabilities in one country can cause risks to other regions. With the emergence of new technological innovations such as artificial intelligence, cloud computing or the Internet of Things and the overall digital adoption in our daily and business lives, opportunities as well as risks increase rapidly due to new networking structures and expanded attack possibilities and surfaces.

Thus, governments and businesses around the world are confronted with the challenge of an ever-increasing number of malicious cyber activities, which has become even more obvious by the surge of these attacks during the COVID-19 pandemic. This is also true for countries in the Global South, which are digitizing their administrations and companies, but are also increasingly vulnerable to cyber attacks due "the absence of local expertise and limited resources" (Pawlak 2016: 88) at the same. Therefore, the cyber capabilities of state actors and beyond need to be strengthened to increase their resilience against these attacks and to reduce their vulnerabilities, especially in developing countries where cyber maturity is comparatively low.

Thus, cyber capacity building is of paramount importance in this context as the digital transformation process continues and nation states become more and more interconnected with each other. **Roughly speaking, cyber capacity building refers to technical, policy, strategic, legal, sociocultural, among others, measures to develop and strengthen cyber capabilities to confront the risks from cyberspace and increase the resilience of the public and private sector.** This could, for instance, just include technical measures such as the set-up of CERTs (Computer Emergency Response Teams) or strategic ones such as the development of national cyber security strategies for governments. Due to the increasing digitalization and the perpetual surge of cyber attacks as well as the related growing needs by countries to improve their

resilience, cyber capacity building has been levelled up by several donor countries, international organizations such as the EU (European Union), World Bank or the GFCE (Global Forum on Cyber Expertise) as well as NGOs and research institutes.

In particular, cyber capacity building is key for the Global South as it sets the framework for developing countries to harness the full economic benefits of digital transformation and 'to reap the digital dividends' by securing their infrastructures and networks. While the need for cyber capacity building is growing, more and more states, international organizations and NGOs are also intensifying their cyber capacity building efforts as instruments to achieve certain foreign policy goals and to communicate ideas and norms regarding the design of the Internet and cyberspace.

Given the increasing activity of authoritarian states and international actors in this regard, **it is crucial that policy makers in the EU and its member states recognize the importance of cyber capacity building as strategic instrument in its dealings with the Global South and in particular with African countries.** Especially the African continent is still too often overlooked in the debates surrounding the interface of 'geopolitics and technology' as well as in terms of the discourse regarding Europe's digital sovereignty and its relationships with other world regions. However, several African countries with its high growth potential might fell victim to the increasing geopolitization of the cyber- and tech-related developments.

It would be misleading to believe that cyber capacity building is purely technical. **Through cyber capacity building, the EU and member states such as Germany can pursue and promote democratic and humanistic goals and ideals worldwide, engage in self-protection, maintain and expand influence in an internationally growing field, protect potential recipient countries from problematic dependencies and, first and foremost, from malicious cyber activities.** In its Cyber Security Strategy adopted in December 2020, the EU announced that it will devote more attention to this emerging issue with the establishment of an EU External Cyber Capacity Building Agenda and an EU Cyber Capacity Building Board. The same applies for the German government which has addressed cyber capacity building in its recent Cyber Security Strategy from 2021. Most recently, the Federal Foreign Office of Germany has also declared that cyber capacity building projects in selected partner countries will be a high priority during Germany's G7 presidency in 2022.

The purpose of the present paper is to highlight the current background, actors and challenges of cyber capacity building in the international context. Based on this, positions and measures are proposed for a more active and coherent cyber capacity building approach of the EU and Germany towards the African continent which can also serve as a blueprint for the engagement with other regions such as Latin America or South East Asia. Furthermore, the analysis should contribute to the literature of cyber capacity building which is still limited.

2. What is Cyber Capacity Building?

Digitalization has far-reaching and ongoing transformative and disruptive effects for governments, economies, societies and for the individual. With the advent of the Internet and increasing global connectivity as well as with ICTs (information and communication technologies) and always new emerging innovations such as artificial intelligence, cloud computing or the Internet of Things, several actors such as states and companies seek to reap the benefits of these developments. More digital adoption, however, also leads to more cyber security risks and the expansion of the attack surface. The increasing digitalization of administrations and companies go ideally hand in hand with the enhancement of cyber resilience and cyber capabilities and the overall strengthening of cyber security. The latter term technically describes the transition from 'computer security' to the era of the wide-use of the Internet and the growing interconnectivities.

Thus, cyber capacity building has started to emerge as a field in the late 1990s in line with the growing adoption of the Internet and the applications of ICTs connected to it. In the last ten up to fifteen years, cyber capacity building has been further specified as a concept, with countries and international organizations focusing on it with dedicated programs, initiatives and strategies as well as special organizations on cyber capacity building such as the GFCE have even been established.

Nevertheless, there is no generally accepted definition, which is not surprising in view of various aspects. First, as put by Collett/Barmpaliou (2021a), cyber security and, subsequently, cyber capacity building has been perceived and tackled by different 'parent communities of practice', among them the 'criminal justice community', the 'Computer Security Indicent Response (CSIRT) and technical community', the 'human rights online community', the 'defence community', and the 'private sector community'. Each of these communities have their own mandates and cultures, leading to a fragmented and incoherent international cyber policy architecture and the lack 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."

(Collett/Barmpaliou 2021a: 34)

Second, and also linked to the existence of different parent communities, **cyber capacity building measures are diverse and can be of a strategic, political, regulatory, organizational, cultural or technical nature.** This is important to note since cyber security and cyber capacity building are still too often incorrectly perceived as a sheer technical matter. Such a perspective, however, lead to an incomplete approach towards increasing cyber maturity since cyber attacks exploit, among others, also societal, organizational or individual weaknesses. Against this backdrop, cyber capacity building can encompass measures[1] such as[2]

→ the support and exchange on the development and implementation of cyber security concepts and strategies;

→ the help and exchange for creating and adopting legal, norms-based regulatory and administrative frameworks in fields such as cyber diplomacy, cybercrime or cyber warfare, which include the implementation of UN resolutions or international cybercrime conventions such as the Budapest Convention;

→ technical measures such as the installation and improvement of CERTs (Computer Emergency Response Teams) or CSIRTs (Cyber Security Incident Response Teams);

→ cultural measures such as increasing cyber awareness and establishing trust, norms, practices concerning cyber security since the behavior of end users as well as how humans design and utilize technological and security practices have critical implications on overall cyber security;

→ educational initiatives aiming at developing knowledge, skill development and increasing cyber awareness, for instance in form of trainings;

→ organizational measures such as structuring national cyber security competencies, for instance in terms of clarification of responsibilities and technical and political processes.

However, the emphasis on or exclusion of certain instruments lead to different notions and accentuations what constitutes cyber capacity building and the "differences in focus result in fragmented coverage" (Muller 2015: 7) of capacity building in the cyber realm. Accordingly, some cyber capacity building projects or programs possess a rather holistic approach covering several measures, while yet others concentrate solely on selected measures. Furthermore, it is noteworthy that the development of these capacities is closely tied to "sensitive issues of national sovereignty, including the functioning of a state and relations between governments and their citizens" (Pawlak 2016: 84), which might impede the implementation of these measures (see next chapter).

Finally, there are different frameworks on which actors are to be involved and on how the relationship between these actors are formed. The first differentiation is between the involvement of only state actors or also the addition of non-state actors. For instance, foundations or NGOs such as ICT4Peace, academic institutions such as GCSCC (Oxford Global Cyber Security Capacity Centre), or private companies such as Microsoft, Symantec or Kaspersky have increasingly geared up their activities and initiatives over the years. Another distinction is derived from the question on how the relationship between 'developed' and 'developing' countries or between the Global North and Global South is shaped. Traditionally, the relationship has been perceived and implemented in a framework in which a state donor in form of a developed country from the Global North provides assistance to a state beneficiary in form of a developing country from the Global South.

However, as described by Collett (2021), this perspective is characterized by a narrow view and is defective in part. The equation between economic development and cyber maturity is not always given. The latter is also still difficult to estimate and there is no generally accepted tool or system pinpointing the cyber maturity level of countries. Furthermore, the state-centric view of the traditional approach does not reflect the crucial role of the private sector and civil society in cyber security in general and its growing role in cyber capacity building. Furthermore, by adopting a conventional donor-beneficiary framework, the focus is automatically on achieving development goals. However, as depicted above, cyber capacity building is rooted in many parent communities, not only in the context of development work.

Having this in mind, cyber capacity building should be understood as a multi-stakeholder and cross-sectoral effort as well as a concept in which the working relationship include state and non-state actors. Furthermore, **the emphasis should be put on collaboration and the exchange of ideas, knowledge, resources and skills, and not on the traditional and state-centric donor-beneficiary concept.** Therefore, the proposed definition of Collett (2021: 8) is helpful: *"International cyber security 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."* The advantage of that definition is that risk mitigation is a broad enough term which allows the several potential different motivations and objectives for cyber capacity building.[3] Furthermore, it does not exclude certain instruments.

1 Based on Dutton et al. (2019) and own research.

2 Another categorization for cyber capacity building differentiate three main domains: "[…] (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).

3 One might argue, however, that the reference to the "open use of […] the digital environment" is a goal itself which not all countries (here authoritarian government) would support.

By sticking to this broad perspective, it becomes clear that in order to have sustainable and effective success in building cyber capacities, a large number of resources and a structured and holistic approach is needed at best. In an ideal world, all the countries would also receive cyber capacity assistance according to their exact needs. However, the emerging field of cyber capacity building contains several challenges which is outlined in the next chapter.

2.1 Challenges of Global Cyber Capacity Building

There is still much room for improvement in terms of global cyber capacity building and its effective design and implementation as well as overall international coordination. **A fundamental challenge for donors and beneficiaries is that since developments in cyberspace, for instance the attack surface and attack methods, and technological advancements are evolving at a fast pace, knowledge, measures and approaches have to be updated steadily.** This rapidly changing environment in cyberspace also leads to the almost inevitable situation that institutional setting and legal frameworks are always lagging behind and the building of cyber capacities is a continuous task in a time-sensitive context. These conditions impact all other challenges with regard to cyber capacity building. It would go beyond the scope of the present paper to list and discuss all of possible risks of cyber capacity building projects. Nevertheless, in order to give a glimpse of it, some broad areas can be identified of cyber capacity building challenges on a global scale.

For instance, the **identification and selection of the beneficiary countries and their actual needs** are very demanding for assistance providers. An actual precondition for choosing beneficiary countries and the subsequent project design is evidence- and data-based research. However, the selection of partner countries and the design of cyber capacity building projects are still too often based on "logical reasoning, limited case studies, anecdotal evidence, and expert option rather than systematic empirical evidence." (Dutton et al. 2019: 280) The research on the cyber maturity level of countries, for instance through the Cybil Portal initiative by the GFCE or the GCSCC (Global Cyber Security Capacity Centre)[4] have improved in recent years. Furthermore, in 2020, the GFCE established a research agenda in order to respond to increasing research requests by member states and the World Bank Digital Development unit launched a Global Analytics Department providing more research in this regard. (Collett/ Barmpaliou 2021a: 54) Also, the recently launched Cyber security Multi-Donor Trust Fund of the World Bank envisions a strong focus on research and determining the maturity and needs of respective countries which should serve as a basis to help to better design projects and programs. In addition, some project providers have also started to conduct national cyber capacity assessments and surveys in advance of the project design and implementation.

However, despite these positive trends, there is still a huge lack of reliable data and information in many contexts, especially in developing countries. Due to the security-related nature of cyber capabilities, many governments are also not inclined to share data to donor actors, in particular data breaches or network vulnerabilities. Since cyber capacities are linked to domestic cyber strengths and weaknesses as well as an external threat perception, governments might treat these related information as "proprietary information to be guarded, rather than a resource that is shared with other stakeholders." (Dutton et al. 2019: 288) Even if state authorities are willing to provide relevant information, some countries do not always have the overview about the capacities that they really possess. (Muller 2015: 14) This often impedes a needs-based and sustainable design and implementation of cyber capacity building projects. More thorough capacity assessments and analysis of the policy contexts together with the national stakeholders are necessary to pinpoint the actual priorities and capability gaps in the respective countries. On this basis, the right priorities and expectations can be set.

In that context, locating and persuading partners as well as raising awareness in beneficiary countries in order to cooperate with them in cyber capacity building projects is not always an easy task. Additionally, due to the crucial role of the private sector in enhancing overall cyber security, cooperation between companies and the public sector is essential. But "donor countries need to work through the government of the country it is assisting through development aid" (ibid: 15) and the relationship between 'both domains' is not always manageable and close enough in certain beneficiary countries.

Similar to that, there is still a room for enhancement with regard to the determination and evaluation of the effectiveness of cyber capacity projects. There is actually a need for more cyber-specific capacity frameworks (Collett/Barmpaliou 2021a: 52) and better relating performance indicators and methodologies. In addition, the shortage of "publicly available projects' evaluations and end-of-project assessments" (Barbero/Berglund 2021: 13) makes it difficult for donors to establish best practices for future interventions. Furthermore, it is at times difficult to persuade beneficiary countries to conduct follow-up projects or engage in new ones since cyber capacity investments, for instance in areas such as cultural awareness or structural changes, often need time to demonstrate its effects.

Another well-known challenge concerns **the effective coordination among different donors and the risk of duplication.** Due to the growing, but still convoluted field of international cyber capacity building as well as the lack of a comprehensive mapping of relevant stakeholders on the donor side, limited coordination between national ministries, international organizations and NGOs lead to duplications of projects. Thus, a lack of communication and appropriate channels among different donor countries and organizations as well as between donor and beneficiary actors cause potential waste of financial resources. A result of that is that, for instance, the 'dar-

4 Other sources include the EUISS (European Union Institute for Security Studies) or the ASPI (Australian Strategic Policy Institute).

ling and orphan phenomena' occurs in Africa, meaning that a small number of countries receive a wide range of projects while the majority of countries on the continent are mostly overlooked. (Collett/Barmpaliou 2021a: 22)

An extra potential obstacle that often arises in the conception of projects on the donor side is the **missing or limited availability of experts,** mostly with technical knowledge. The market of cyber security experts is already highly competitive and 'bought empty' for domestic purposes. According to one estimation in 2019, the total number of additionally needed cyber security professionals in eleven major global economies exceeds 4 million. ((ISC)² 2019: 8) This grim picture often leads to the situation that either potential experts cannot be recruited for projects or only in the form of 'fly-in fly-out' training, when experts provide their cyber-related knowledge only on a short-term basis. The short-lived deployment of experts often has the detrimental effect of hampering the building of interpersonal relationships and gaining understanding of the knowledge of local context. (Collett/Barmpaliou 2021a: 56)

Related to that, **financing cyber capacity building projects and investing in related capabilities are challenging for donors and beneficiaries alike** and that especially under the COVID-19 pandemic conditions where "more competing priorities limit the financial, human and time capacities that can be devoted to cyber capacity building." (Barbero/Berglund 2021: 6) In order to increase its cyber resilience and capacities, governments on the receiving end would have to make constant and substantial investments in hardware, software, training of personnel or maintenance. For developing countries, the focus is often, however, to invest in digital technologies per se and not in cyber security, even though the surge of cyber attacks in the midst of the pandemic might have changed the setting of priorities in this regard.

3. The State of Cyber Security in Africa

Cyberspace and emerging technologies are expanding at an extremely fast pace and developing countries have a huge growth potential, with many users still getting online and using digital services the first time in the current decade. Harnessing digital technologies and adoption for economic and societal progress is becoming a crucial factor for developing countries, including the possibility of leapfrogging. Generally, developing countries have increasingly focused on these digital opportunities in recent years, without, however, giving close and thoughtful attention to the risks stemming from the cyber risks and vulnerabilities.

Especially many African countries are currently confronted with these challenges, and many international actors have gradually started its (strategic) engagement with its African counterparts, with geopolitical and economic implications. Against this backdrop, **a closer look to the digital and cyber-related environment is also of great importance for Europe and Germany and should not be ignored,** especially since the tech- and cyber-related progress in African countries is not exempt from geopolitical bickering and the tech competition between the USA, China and other international powers.

In the digital sector, Sub-Saharan Africa in particular is one of the world's least developed regions. **According to the BCG's Digital Acceleration Index, the African continent has the lowest average digital maturity score. (Dannouni et al. 2020) At the same time, the growth potential is immense.** In 2019, the mobile internet adoption in Sub-Saharan Africa was just at 26 percent. (GSMA 2020: 1)[5] It is estimated that 1.1 billion new users will need to be connected to enable every African citizen, business and government to operate digitally by 2030. This will require around $100 billion and the deployment of nearly 250,000 new 4G base stations and at least 250,000 kilometers of fiber optic cable across the continent. (United Nations Broadband Commission for Sustainable Development 2019: 16) In light of the need for more newer digital infrastructure, it can be concluded that several systems and networks in crucial areas are based on outdated equipment.

With the increasing adoption and use of ICTs and the Internet, African countries have also suffered more and more from malicious cyber activities, even if concrete assessments are still very rare to find. **In 2017, cybercrime attacks costed African economies $3.5 billion, a 75 % increase from the previous year, and more than 95 % of institutions from the public and private sector have not invested more than $1500 on their cyber security postures.** (European Investment Bank 2021: 82) In the same year, losses inflicted by cybercrime attacks were estimated for Nigeria at $649 million, and Kenya at $210 million. (Kshetri 2019: 77) The low maturity also entails that while African countries are mostly not really engaged in state-sponsored malicious cyber activities, "they are simply at potential risk from the attacks of more developed countries." (Calandro/Berglund 2019: 4)

In light of these numbers, Africa has a great deal of catching up to do in terms of their cyber postures and the majority of African countries have not perceived cyber security as a regional or national priority. (ibid: 2) Even though official figures for cyber maturity on the African continent are rather scarce, there are certain indications for the low level of readiness. For instance, according to the ITU (International Telecommunication Union), only 14 African countries have national cyber security strategies in place, while three countries are currently

5 According to other estimations, "[o]nly 26% of the continent's rural dwellers use the Internet regularly, compared to 47% of its urban inhabitants." (African Union Commission/ OECD 2021: 19)

in the process of drafting one. (International Telecommunication Union 2022) Only eleven African countries currently have substantive laws in place to combat cybercrime (African Union Commission/ OECD 2021: 30) and in general "the governmental institutional capacity and awareness of the threat is often limited". (Muller 2015: 6)

Related to this is also that the 2014 "African Union Convention on Cyber Security and Personal Data Protection" – also known as *Malabo Convention* – has only been signed by 14 and ratified by 8 out of 55 member states (as of June 2020). (African Union 2020a) Five African countries (Cabo Verde, Ghana, Mauritius, Morocco, Senegal) are parties and further six (Benin, Burkina Faso, Nigeria, Niger, South Africa, Tunisia) have an observer status to the Convention on Cybercrime of the Council of Europe, known as the *Budapest Convention* (as of November 2021). (Council of Europe 2022) Also, the international engagement in cyber norms discussion is limited since only nine African countries were once a member of the UN GGE (UN Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security) and none of them have had a membership longer than a total of five years. (Calandro/Berglund 2019: 2–3)

In terms of human capital, it was estimated that the African continent would lack 100,000 cyber security experts by 2020. According to the ITU Global Cyber security Index (GCI), only 19 countries rank among the top 100. (ITU 2021: 25–26). Concerning other data, too, the comparative weakness of African states in cyber security becomes apparent: For instance, only 19 countries on the continent have a national CERT, ten have national cyber security audits performed and six have metrics for assessing cyberspace associated risk at the national level.[6] As of March 2019, only 13 African countries possessed a national CSIRT. (Collett 2021: 4)

Given the wide-ranging lack of strategic, legal and technical cyber security frameworks and measures, the AU (African Union) has taken up the urgent need for building cyber capacities among African countries and set goals in its "Digital Transformation Strategy (2020–2030)". (African Union 2020b) Here, the proposed measures to enhance cyber-related capabilities cover a wide range of areas, including strategic, legal, human, institutional and technical ones (see box 1), which demonstrates the far-reaching need for projects and assistance in this regard.

6 All data is based on the ITU Global Cyber Security Index.

Box 1: Selected "Policy Recommendations and Proposed Action" on Cyber Security and Data Protection by the AU "Digital Transformation Strategy (2020-2030)"

Support interventions to strengthen cyber security at national level:

- → Develop and adopt national cyber security strategies and legal and regulatory framework for personal data protection/privacy, cyber security 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 cyber security 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 Cyber security Framework under the UN;
- → Steer innovations at continental level that seek to address challenges related to cyber security, interoperability of systems, and persistency of information;

In this context, **potential cyber capacity projects would have a crucial impact on these set goals and are in fact necessary to fulfill them.** From a donor- and recipient-based perspective, strengthening cyber capacities on the African continent is crucial for several reasons and will have multi-dimensional implications. Several international and regional actors have already acknowledged this and according to the Cybil Portal, there are currently over 200 cyber-related projects in Sub-Saharan Africa with over 100 international and regional actors involved. Among them implementers such as the CTO (Commonwealth Telecommunications Organisation), ITU, World Bank, Council of Europe, Global Cyber Security Capacity Centre and UN agencies as well as nation states such as Estonia, the Netherlands, South Korea or United Kingdom. (Cybil Portil 2022) As one of the very few regional actors, the C3SA (Cyber security Capacity Centre for Southern Africa) has also increased its activities in this regard. Nevertheless, according to the above-described current state of play in terms cyber maturity, the potential for cyber capacity building on the African continent is still quite high.

3.1 Cyber Capacity Building as a Basis for Innovation and Growth

As already indicated, the impact of cyber capacity building projects goes beyond technical effects and have economic, value-based and political significance for donors and beneficiaries alike, which has to be considered by the German and European decision-makers. **Cyber capacity building is indispensable for innovation and sustainable digital growth.** Cyber security ensures trust in digital technologies and the digital transformation process as well as spurs individual adoption. From a development perspective, digital technologies can bring several benefits to societies in developing contexts, including providing better knowledge and education (e-learning), social and political participation (e-participation), health services even in remote areas (e-health, telemedicine), or access to financial services (digital finance). However, new users need to trust that their sensitive data is secure. Thus, cyber security plays a crucial part for countries in developing regions to fully harness the potential of digital transformation. However, donors and beneficiary countries on the African continent have neglected the cyber components in their digital development projects to a great extent in previous years. Yet, the mentioned sharped surge of cyber attacks in the midst of the COVID-19 pandemic has heighten and displayed the importance of cyber capacity building in the eyes of governments, especially in emerging and developing countries. **If Africa's growing digital economy (see box 2) is not accompanied by adequate cyber security measures, it cannot flourish and cyber attacks will comprise the potential economic benefits.** This can also lead to spill-over effects to other countries all over the connected world, demonstrated by other cyber attacks in the past such as WannaCry or NotPetya. Furthermore, cyber capacities have to be developed so that African countries can implement properly global cyber norms, including UN-based norms such as "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)

Box 2: Selected numbers about Africa's growing digital economy

- → Africa's Internet economy possess the potential to reach $180 billion by 2025, accounting for 5.2% of the continent's gross domestic product (GDP). By 2050, the contribution could reach $712 billion, 8.5% of the continent's GDP; (Google/ International Finance Corporation 2020: 17)
- → By 2025, 4G adoption in Sub-Saharan Africa will double to 28%; (GSMA 2021: 11)
- → By 2025, there will be approximately 120 million new mobile subscribers, taking the total number of subscribers to 615 million (50% of the region's population); (ibid. 10)
- → By 2025, the e-commerce market in Africa has the potential to reach a value of over 46.1 billion U.S. dollars (2020: 27.97 billion U.S dollars). (Statista 2022)

3.2 Cyber Capacity Building to Safeguard and Promote a Secure, Stable, Open and Free Cyberspace

It would be too short-sighted to understand cyber capacity building as a purely non-political instrument[7]. Directly or indirectly, ideas are conveyed about the legal and value-based design of cyberspace and the Internet as well as about the regulation and standard-setting of ICTs, for instance through the dissemination of certain legal, regulatory and administrative frameworks. As put by Homburger (2019: 224–225), 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 cyber security governance can be exported to other countries through cyber security capacity building as the latter implies a transfer of values and world views from the donor countries." Contrary to the initial idea and spirit of cooperation, cyberspace has increasingly become an area of competing interests, norms and values and strategic rivalry. Thus, cyber capacity building might be also a "form of political instrument, oriented around the advancement of foreign policy interests." (Barbero/Berglund 2021: 6)

This diagnosis is particularly important in light of the fact that authoritarian states in particular are increasingly attempting to pass on their ideas – for example, with regard to surveillan-

7 For instance, the latest consensus report of the UN Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security states the 'politically neutral nature of capacity-building'. However, there are examples as described in the text which contradict this statement.

ce technologies or restrictions on Internet freedom – to other states around the world. **Against this backdrop, cyber capacity building is also not exempt from the emerging dichotomy between 'digital authoritarianism' or 'authoritarian tech' and a strong emphasis on 'state sovereignty' on the one side (e.g., pushed by China or Russia) and democracies in the digital realm – such as the European Union and its members –, which aims at to safeguard and promote the idea of a 'secure, stable and open and free cyberspace' in a multi-stakeholder context.**

For instance, many projects of the Council of Europe and the EU, for example, state as a prerequisite for recipient states that they should support the ideas and guidelines of the Budapest Convention and have an interest to join the binding international instrument concerning the fight of cybercrime. Countries of the Shanghai Cooperation Organization, however, refer to their 2015 International Code of Conduct for Information Security as a guideline for cyber capacity building projects, which places greater emphasis on sovereignty and national security in relation to the use of information and communications technology and implies that the context of information might be also considered as a threat. For example, China emphasizes promoting the International Code of Conduct in its International Strategy of Cooperation on Cyberspace and its attempt "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) In this context, the focus is also on fragile democracies ('digital deciders') that cannot be clearly assigned to the 'democratic' or 'authoritarian' camp.[8] Precisely many of these countries are located on the African continent. Given the very strong Chinese presence in Africa's ICT sector and its interest to expand investments in the framework of its 'Digital Silk Road' initiative, this might be a critical development from a European and German perspective, especially since both are trying to promote a free and open cyberspace, multi-stakeholder approach and counter the increasing restrictions on Internet freedom for the sake of 'national sovereignty'. Overall, there is also a risk that there may also be a fragmentation of standards, as different donor countries convey different values.

3.3 Cyber Capacity Building as an Instrument for International Coalition-Building

Third, and based on the previous point and on a dedicated foreign policy perspective, cyber capacity building might also be used as a tool for building coalitions in norm-setting processes in international organizations. Since billion of new Internet users will stem from Africa and Latin America in this decade, the respective host countries of these users will stronger stake out their claims to also shape norms and principles on responsible state behavior in cyberspace and devote more diplomatic engagement to it. In other words, the current trend that "African stakeholders have remained largely absent from the evolving norms debate of the last decades" (Calandro/Berglund 2019: 2) will most likely change in the upcoming years and African political decision-makers will finally more and more shape global norms concerning cyberspace, which they have been implementing.

Box 3: Examples of cyber-related developments in international organizations

- → The UN Cybercrime Ad Hoc Committee will discuss in in the course of the next two years the objectives and structure of an UN's potential first treaty on cybercrime, which might replace the Council on Europe's Budapest Convention long-term; the initial proposal for such an UN treaty has been made by Russia, which – despite being a member of the Council of Europe – refuses to join the Budapest Convention. There are concerns on the Western side, however that such a new UN convention will be used to define cybercrime so broadly that it will also include, for example, content critical of the government.
- → So far, there have been two UN cyber diplomacy processes focused on establishing rules of responsible state behavior in cyberspace: The decades-old and US-sponsored 'UN GGE, which comprises a working group of country representatives from 25 UN member states; and the Russia-initiated UN OEWG (Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security), which is open for all UN members. Both Groups published final reports in 2021, emphasizing the importance of cyber capacity building (see appendix). However, the duality of the two groups and the currently discussed Programme of Action (POA), proposed by France and Egypt, in order to combine both groups, is still an open debate and reflect the deep disagreements among the countries about the process and content of international cyber-related rules.
- → By proposing a new Internet Protocol ("New IP") in the UN-specialized agency ITU in 2019, China has suggested to change the technical structures of the Internet, leading to a more nuanced emphasis on 'national sovereignty' and greater rights of access by nation states.

In light of the current controversial debates concerning cyber norms in the UN context, the promotion of a new UN-based global cybercrime treaty by Russia in order to replace the Western-linked Budapest Convention, or the general trend of 'digital authoritarianism' or 'authoritarian tech' (see box 3), **cyber capacity building can be used as a strategic instrument to win over countries to its 'own camp',** especially

8 As put by Homburger (2019: 236), "[S]tates which are identified as swing states in the realm of internet governance might be of special interests to the debate. This is because swing states can be defined as states with mixed political orientation and therefore not being associated with one of the two camps and having the necessary resources to influence the trajectory of an international process. Cyber security capacity building might be one form of influencing these swing states."

with view to 'one member, one vote'-processes. That cyber capacity building will be most probably more harnessed as a foreign policy tool in the upcoming years is due to the ever-increasing new players in and the increasing geopolitisation of the field very likely.

In that context, the power dynamics between donors and beneficiaries have to be acknowledged since "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" and the donor countries "might be in a more convincing position to frame expected risks." (Homburger 2019: 228). Hence, all these proposed approaches should and cannot be imposed; in other words, they have to be conducted in a multi-stakeholder context and beyond the conventional donor-beneficiary understanding (see proposed definition for cyber capacity building by Collett 2021). For instance, 'winning-over' countries cannot mean to force them, but to offering them better alternatives and at the same time, empowering the governments to also engage, for instance, more effectively in norm-setting processes in the UN context. First and foremost, also measures must be focused on strengthening the local ownership of the stakeholders on-site. In developing contexts, there is also 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) Therefore, **the clear message should be that cyber capacity building cooperation should not result in creating economic and technological dependencies and to 'lock in' developing countries with specific donor countries, but to support the local capacities in a self-reliant and sustainable fashion.** This approach is also a clear advantage over the way of proceeding of authoritarian states.

4. Actors (Positions and Activities)

While the number of donors and implementers in the cyber capacity building field is growing in a rapid pace, the actor landscape also gets more and more complex and difficult to keep track of. The ecosystem of actors has been broadened in the recent years since cyber capacity activities are increasingly defined beyond just technical matters and more parent communities have started its engagement in this regard. Stakeholders include international organizations, governments, civil society organizations, private companies, academic institutions or individual consultants. Almost all countries are somehow involved in at least one cyber capacity building project. (Collett/Barmpaliou 2021a: 5) However, the diverse actor landscape from different parent communities might lead to "competing and overlapping frameworks that can cause fragmentation in program implementation and impact effectiveness." (Csenkey/Perron 2020: 2)

From another perspective, the actor landscape can also be differentiated as following: "(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 cyber security." (Dutton et al. 2019: 284).

In the German, EU and multilateral context, several countries and international organizations have started to kick off various initiatives, programs and projects in recent years, indicating the gradual increased strategic importance that these actors are dedicating to cyber capacity building.

The 2021 Cyber Security Strategy of Germany, for instance, emphasizes the importance of cyber capacity building as an instrument to promote 'democratic and normative values and ideals' and for 'an overall increase of cyber security in partner states'. (Federal Ministry of Interior 2021) The Strategy basically provides the (very) broad lines for a (value-based) stronger engagement of the Germany towards cyber capacity building. However, the concrete design and structuring of these ideas and a possible strategic direction is thus not yet determined. In light of the increasing activities by the Federal Ministry for Foreign Affairs (Auswärtigens Amt, AA) and the BMZ (Federal Ministry for Economic Cooperation and Development/Bundesministerium für wirtschaftliche Zusammenarbeit und Entwicklung), it also remains to be seen how to bridge the digital development and the foreign policy approaches and parent communities in the German context.

In that context, the Federal Foreign Office has increasingly heightened its strategic engagement with cyber capacity building by providing funds to projects and programmers (e.g., for instance to the World Bank and GFCE) and its involvement in the EU CyberNet project (see appendix). Most recently, it has announced in the context of Germany's G7 Presidency "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." (Federal Foreign Office 2022) In addition, the BMZ has also started to commission projects with cyber security components.

Cyber capacity building has been gradually taken up by the European Union with the aim of heighten its strategic importance and effectively design and implement related projects from the bloc and its member states. Already in 2018, the EU has formulated two reference works, the 'Council Conclusions on EU External Cyber Capacity Building Guidelines' and the 'Operational Guidance for the EU's international cooperation on cyber capacity building', which outline the basic ideas, approaches, methods and goals. The EU Cyber Security Strategy of December 2020 (European Union 2020) is taking this a step further, which calls for the development of an EU Exter-

nal Cyber Capacity Building Agenda. The agenda is intended to leverage the expertise of member states and relevant EU institutions, bodies, agencies, and initiatives in line with their respective mandates. Furthermore, an EU Cyber Capacity Building Board should be established, including relevant EU institutional actors, to map progress and identify further synergies and potential gaps. Mainly through its Directorate-General for International Partnerships (DG INTPA), the European Commission has supported several cyber capacity building projects with a focus on its immediate neighborhood (e.g., Western Balkans), but also beyond.

On the global level, the final and consensus reports of the UN GGE and UN OEWG published in 2021 emphasizes the importance of cyber capacity building in general and in particular for developing countries. Furthermore, major international organizations such as the World Bank have started to intensify its activities in this area.

In the appendix, a selection of relevant actors will be further detailed and discussed with a focus on the Germany and the EU, but not limited to it. The table below should give a glimpse about the diversity and different roles of actors involved in global cyber capacity building.

Actor	Role(s)	Examples
Cyber security practitioners	Individuals and teams with expertise in computing, networking, and security	Computer Emergency Response Teams (CERTs); IT experts in organizational centers
Researchers, educations	Academic centers of expertise in cyber security capacity-building practices and policy in universities and think tanks	Oxford Global Cyber Security Capacity Centre (GCSCC), Oceania Cyber security Centre, Chatham House, Brookings, Rand Corporation, European Institute for Security Studies (EUISS)
Trainers and advocates	Teams and individuals designing and delivering training, awareness campaigns, and promoting security	The Geneva Internet Platform (GIP) Digital Watch observatory, ICT4Peace
Networkers and coordinators	Provisions of online portals, conferences, and forums on capacity building	The Global Forum on Cyber Expertise (GFCE), World Economic Forum (WEF)
Donors	Individuals and organizations financially and organizationally supporting capacity-building initiatives	Governments (Foreign, Development, Interior Ministries, etc.), philanthropic foundations, international organizations such as the World Bank, Council of Europe
Policy-makers and regulations	Governance of the Internet and cyber security norms and practices	Internet Governance Forum (IGF)

Based on: Dutton et al. (2019: 284-285) and own research

5. Policy Recommendations

Relevant actors in the EU and in the German government have started to recognize the importance of a concerted and strategic approach towards cyber capacity building. This is in light of the increasing need for increasing cyber capabilities in Africa a welcome and necessary development. Nevertheless, it is important that the German government develops a cyber capacity building strategy which is in line with the major initiatives on EU and UN level. Here, the German government can always justify the allocation of organizational, personal and financial resources due to the increasing importance that has been attached to cyber capacity building by these multilateral organizations and fora. The strategic prioritization of the Federal Foreign Office during Germany's G7 2022 Presidency on developing countries should be used as a momentum for further engagement with African countries and beyond. **Due to the increasing trend of 'digital authoritarianism' and the growing importance of countries in the Global South in shaping global cyber norm debates, the German government and the European Union should aim to use cyber capacity building as a strategic instrument, while also trying to bridge the mandates and goals of different parent communities such as the digital development, foreign policy and cybercrime communities.** Against this backdrop, it is of importance to frame external cyber capacity building and its strategic engagement with countries of the Global South as part of Europe's strengthening of its digital sovereignty. In other words, digital sovereignty[9] should not only mean to strengthen its own tech industry and to regulate emerging innovations and digital services in the own jurisdiction, but also to promote standards and norms – for instance via cyber capacity building – in line with European values such as human rights, human dignity, rule of law or data privacy internationally. By doing so with regard to cyber capacity building, the EU and its member states such as Germany should tackle the afore-mentioned risks and challenges of cyber capacity building. Hence, following recommendations are proposed:

5.1 The Federal Government of Germany

→ **Provide funds to support think tanks, NGOs, universities working on this topic:** Cyber capacity building as well as the state of play of digitalization and cyber security in Africa are still not sufficiently covered as a research field in German and European think tanks and research institutes. In general, the literature on cyber capacity building consists mainly of policy papers and not established peer reviewed qualitative or quantitative studies determining the cyber maturity of countries and regions. (Collett/Barmpaliou 2021a: 12) Therefore, the German government should encourage and support think tanks and research institutions to focus more on this topic in order to support operational policy with research results and recommendations. This will help to better assess and pinpoint the actual needs of these countries and the gaps in their cyber maturity.

→ **Use and integration of German expertise for bilateral/EU programs:** In addition to funding projects and conceptual work, it is important for Germany's credible advocacy of cyber capacity building that German experts are involved in bilateral projects and EU programs. In this context, the BSI (Federal Office for Information Security) in particular is a key point of contact due to their expertise in cyber security, but also the private sector and the academic institutions. Thus, the German government should raise awareness in the civil society and in private companies for this purpose.

→ **Provide funding to support bilateral/multilateral capacity building projects:** The German government should further support trusted international actors, for instance the World Bank or the GFCE (Global Forum on Cyber Expertise). Besides that, the funds should also be used to strengthen organizations that can offer and implement projects professionally, sustainably and according to European standards and values. Here, the German government should also turn the focus on countries on the African continent, which have been overlooked in the past and might be considered as 'digital deciders'.

→ **Create a working group between ministries:** In order to bridge the different parent communities (foreign policy community, development community, cybercrime community, etc.) and to synthesize the different position in to a concerted cyber capacity building strategy, a governmental working group should be established. This also should help to create a holistic approach towards cyber capacity building and raise awareness among ministries in the government.

→ **Anchor cyber security as a permanent component of development programs:** Cyber security is an important basis for the digitalization of the economy and society and for exploiting the associated potential. The BMZ (and the GIZ) should anchor cyber security as an integral part of development programs in the digital sector. International actors such as the World Bank are good examples here, which have gradually expanded their 'digital portfolios'.

9 Roughly speaking, a possible definition of digital sovereignty might contain following three aspects: (1) the ability to possess key technologies, to produce its own innovations and to occupy strategically important positions in global value chains in the digital and technological domain; (2) the ability to strengthen the resilience of critical infrastructures and networks and to protect our free and democratic societies against malicious cyber activities; and (3) the ability to regulate emerging technologies as well as digital services and platforms and to set international standards and norms in line with European values such as human rights, human dignity, rule of law or data privacy.

5.2 The European Union and its Member States

→ **The EU and its member states should use the announced EU External Cyber Capacity Building Agenda and the EU Cyber Capacity Building Board for a strategic and coordinated approach:** Due to the growing importance of African countries in cyber-related governance debates, the EU and its member states should use the EU External Cyber Capacity Building Agenda to develop clear principles and objectives on how to cooperate with and approach countries on the African continent. In that context, it should also focus on and prioritize African countries which have been overlooked concerning cyber capacity building projects and which might be considered as 'digital deciders' in the growing dichotomy of 'digital democrats vs. digital autocrats.' Furthermore, it should also be leveraged for better coordination among different EU institutions and try to synthesize their mandates and objectives, also to avoid duplications. This would also help to develop a better funding strategy in light of the current Multi-Annual Financial Framework (2021–2027).

→ **The EU and should use existing initiatives and fora on EU-Africa cooperation for intensifying cyber capacity building cooperation:** The installation of an AU-EU Digital4Development (D4D) Hub is an important step which should be expanded with cyber security as a topic. This might also help that EU member states' development cooperation agencies will stronger engage in terms of cyber capacity building.

→ **The EU and its member states should strengthen the role of EU CyberNet as central hub for cyber capacity building experts, exchange of best practice and coordination:** The EU, Germany and other member states should actively support the further build-up of EU CyberNet as a central hub for expertise and coordination of EU-led projects in order to become a go-to-place for EU institutions and member states. Member states should encourage their own local experts in their countries to participate in the framework of EU Cybernet and to encourage them to make their expertise available for projects.

→ **Promote a multi-stakeholder approach in African countries:** In order to counterbalance the emerging trend of digital authoritarianism and due to the multi-dimensional and multi-actor nature of cyber security, the German government and the EU should promote and subsequently design cyber capacity projects together with private sector and civil society organizations and avoid solely government-to-government interaction. In a partnership spirit, a strong emphasis should be put on local ownership and expertise development in order to also avoid long-term dependencies from the perspective of the developing countries.

→ **Focus on enabling African political decision-making in terms of cyber diplomacy:** It is crucial that the progressive digitalization and the strengthening of cyber security in these countries go hand in hand with an increased involvement of African diplomats in global norm-setting discussions surrounding cyberspace. Therefore, the EU and member states' ministries such as the Federal Foreign Office of Germany should commissioned cyber diplomacy experts to cooperate with African diplomats and think tankers in order to enable them to participate in and shape cyber governance debates and processes.

Literature

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/Cyber securityCapacityBuilding_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 cyber security 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%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

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

Cybil Portal (2022): https://cybilportal.org

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, William H. et al. (2019): Cyber security 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 Cyber security 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 Cyber security Capacity Building for Norm Development in: Cyberspace, Global Society, 33:2, pp. 224–242

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

International Telecommunication Union (2021): Global Cyber security Index 2020. Measuring commitment to cyber security, 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 Cyber security Teams, (ISC)² Cyber security Workforce Study, 2019, https://www.isc2.org/-/media/ISC2/Research/2019-Cyber security-Workforce-Study/ISC2-Cyber security-Workforce-Study-2019.ashx?la=en&hash=1827084508A24DD75C60655E243EAC59ECDD4482

Kshetri, Nir (2019): Cybercrime and Cyber security 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 Cyberspace 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/

List of Abbreviations

ASPI (Australian Strategic Policy Institute)

AU (African Union)

BMZ (Federal Ministry for Economic Cooperation and Development)

BSI (Federal Office for Information Security)

C3SA (Cyber security Capacity Centre for Southern Africa)

CERT (Computer Emergency Response)

CSIRT (Cyber Security Incident Response Team)

CTO (Commonwealth Telecommunications Organisation)

EU (European Union)

EUISS (European Union Institute for Security Studies)

GCSCC (Oxford Global Cyber Security Capacity Centre)

GDPR (EU General Data Protection Regulation)

GFCE (Global Forum on Cyber Expertise)

GIZ (Deutsche Gesellschaft für Internationale Zusammenarbeit)

ICT (Information and communication technologies)

ITU (International Telecommunication Union)

NGO (Non-Governmental Organisation)

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)

Appendix: Selected National and International Actors in Global Cyber Capacity Building

National

As in other nation states, external cyber capacity building is still a comparatively emerging field in the German context. However, it can be noted that various actors in the Federal Government have recently turned their attention to the issue and have taken action in this regard.[1]

The Federal Foreign Office of Germany has already supported cyber capacity building projects in the past and is about to further increase its engagement and activities in this field. The 'International Cyber Foreign Policy and Cyber Security Coordination Staff' of the Federal Foreign Office has financially contributed to the World Bank's Digital Development Trust, which has cyber security as one of its six pillars, and was among the first donors supporting the newly set up Cyber security Multi-Donor Trust Fund. In addition, it has supported projects of the Global Forum on Cyber Expertise. In the past, it has financed cyber capacity building projects for several stakeholders with a focus on the application of the international law to cyberspace, with the ICT4Peace Foundation as an implementer. (Collett/Barmpaliou 2021b: 14–15) Being one of the three members of the Advisory Board, the Federal Foreign Office has had a contributing role in the establishment of EU CyberNet (see next chapter). Furthermore, the Federal Foreign Office have announced that cyber security is a key priority of its programme during Germany's G7 Presidency in 2022 and that it wants "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." (Federal Foreign Office 2022)

In recent times, the BMZ (Federal Ministry for Economic Cooperation and Development) together with its implementing agency GIZ (Deutsche Gesellschaft für Internationale Zusammenarbeit) have increased its efforts and expanded its activities regarding digital development. This was most notably reflected in the 2019 Digital Strategy by the BMZ and the set-up of a dedicated unit for 'Digitalization in Development Cooperation.' However, the Strategy does not encompass cyber capacity building or cyber security explicitly. Furthermore, projects with cyber security elements supported by the BMZ and implemented by the GIZ are still limited in number, but there are some developments in this direction. For instance, the BMZ-commissioned and GIZ-led project 'Digital Transformation Center Tunisia' includes securing the digital infrastructure and the enhancement of cyber security skills. (GIZ 2022a) Furthermore, commissioned by the BMZ and financed by the GIZ, the German tech think tank Stiftung Neue Verantwortung is implementing cyber policy exercises in several countries, among them Rwanda, Kenya, South Africa, Ghana, and Ivory Coast (Stiftung Neue Verantwortung 2021). Also, the GIZ-project 'Enhancing Security Cooperation in and with Asia', commissioned by the EU and the Federal Foreign Office, consists of assistance in terms of cyber security. (GIZ 2022b)

In its newest Cyber Security Strategy (Federal Ministry of Interior 2021) published in September 2021, the Federal Government also touches upon cyber capacity building as an 'important instrument for utilizing the opportunities of digitization and counteracting the associated risks', and that in particular in places 'where people are given initial access to cyberspace.' Furthermore, it also states that 'cyber security is perceived as a component in all digital development cooperation projects.'[2] In addition, it recognizes that the issue has continued to gain importance internationally and aims at integrating cyber security stronger in programs to promote the digital economy and of stabilization measures. Through cyber capacity building, the strategy states that the expected impact should include that 'democratic and normative values and ideals can be anchored worldwide' and 'an overall increase of cyber security in partner states.' In order to achieve these goals, there are two measurement criteria: 1) 'cyber capacity building is established as an issue in international bodies and has been anchored in relevant policy documents'; 2) 'Germany participates in the implementation and/or support of measures for the cyber capacity building measures in national, EU, NATO or international contexts.'

The Cyber Security Strategy basically provides the (very) broad lines for a (value-based) stronger engagement of the Germany towards cyber capacity building. However, the concrete design and structuring of these ideas and a possible strategic direction is thus not yet determined. In light of the increasing activities by the Federal Foreign Office and the BMZ, it also remains to be seen how to bridge the foreign policy and the digital development approaches and parent communities in the German context.

International

Europe: EU and Council of Europe

Cyber capacity building has been gradually taken up by the EU (European Union) with the aim of heighten its strategic importance and effectively design and implement related projects from the bloc and its member states. Already in 2018, the EU has formulated two reference works, the 'Council Conclusions on EU External Cyber Capacity Building Guidelines' and the 'Operational Guidance for the EU's international cooperation on cyber capacity building', which outline the basic ideas, approaches, methods and goals. In its overall discourse, the

1 The following paragraph is based on the author's own information and open-source references.

2 However, by considering the digital projects supported by the Federal Government, this is not always the case.

EU emphasizes the importance of cyber capacity building as a strategic building block for European cyber diplomacy, which should contribute to the promotion and protection of human rights, digital gender equality, the rule of law, security, inclusive growth and sustainable development as well as for a secure, stable, free and open cyberspace. The 'Non-Paper on EU Cyber Diplomacy' issued by Germany, Estonia, France, Poland, Portugal and Slovenia in the course of the German EU Council Presidency in November 2020 also highlights these objectives. (Federal Foreign Office 2020)

The 2018 Council Conclusions state that cyber capacity building serves different objectives, including strengthening national, institutional, and organizational capacities that enhance the resilience of critical digital services and networks and the protection of critical information infrastructures; supporting criminal justice reforms to combat cybercrime; combating the use of the Internet for terrorist purposes; enhancing the cyber security skills and competencies of individuals; and facilitating awareness-raising as well as effective cooperation on these issues at the national, regional, and international levels.

The EU Cyber Security Strategy of December 2020 (European Union 2020) is taking this a step further, which calls for the development of an EU External Cyber Capacity Building Agenda. The agenda is intended to leverage the expertise of member states and relevant EU institutions, bodies, agencies, and initiatives in line with their respective mandates. Furthermore, an EU Cyber Capacity Building Board should be established, including relevant EU institutional actors, to map progress and identify further synergies and potential gaps. Both proposals are indicators that the EU will attach higher strategic importance to cyber capacity building and intend to pursue a more coordinated approach.

Mainly through its DG INTPA (Directorate-General for International Partnerships), the European Commission has supported several cyber capacity building projects with a focus on its immediate neighborhood (e.g., Western Balkans), but also beyond. Via its various external financing instruments such as the IcSP (Instrument Contributing to Stability and Peace), EDF (European Development Fund) or the PI (Partnership Instrument), it has financed global, regional and bilateral cyber-related projects over the years, for instance also the OCWAR-C ('West African Response on Cyber security and Fight against Cybercrime' project) in cooperation with Commission of the ECOWAS (Economic Community of West African States). According to Collett/Barmpaliou (2021b: 6), the EU has mainly supported projects concerning three broad areas: "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) It remains to be seen how the current EU budget (Multi-Annual Financial Framework, MFF) will be allocated to cyber capacity building projects.

However, there is often a lack of overview of these projects and the respective needs in the recipient countries, which can lead to duplication and an ineffective balance between supply and demand. Furthermore, the provision of experts from EU member states is still a challenge. The EU CyberNet[3] project funded by the EU aims to remedy this situation. The aim of the project is to create an EU-wide expert pool for cyber capacity building projects and to build a European stakeholder community on this topic area. The project should serve to ensure that the EU applies a more coherent and coordinated approach. The project is implemented by the RIA (Estonian Information Security Authority), which is in cooperation with the two Advisory Board members the Federal Foreign Office of Germany and the C3 Cyber security Competence Center Luxembourg. It is funded by the European Commission until 2025.

The EU also actively cooperates with the Council of Europe, which itself implements projects and designs them mainly based on the promotion of its own Budapest Convention. In this context, the flagship project GLACY (Global Action on Cybercrime) and the successor GLACY+ (Global Action on Cybercrime Extended), jointly funded by the Council of Europe and the European Commission, aim at to promote and strengthen, among others, cybercrime legislation, policies and strategies as well as the capacity of judicial police authorities to investigate cybercrime in Asian and African states[4]. The Octopus Project is another ongoing project from the Council of Europe, with the aim of supporting the implementation of the Budapest Convention on Cybercrime on a global scale.,

In the context of the German EU Presidency in the second half of 2020 (accompanied by the BMZ), the AU-EU Digital4Development (D4D) Hub – a network of so far eleven EU member states in cooperation with DG INTPA was also established in December 2020, which aims to bring together and implement a variety of digital initiatives of European actors in a strategic and coordinated approach. The Hub is modeled on the 'Team Europe' concept, pooling the resources of the EU, its member states and financial institutions, in particular the European Investment Bank and the European Bank for Reconstruction and Development. Other initiatives under this framework include the 'African-European Innovation Bridge', which aims to establish a pan-African network of Digital Innovation Hubs, and the 'EU-AU Data Flagship', which aims to boost investment in African data infrastructure and increase data protection. Cyber security is, however, not an explicitly named in these contexts so far.

Also, as in the German case, individual member states have their own cyber capacity agenda and invest und support respective projects, for instance, the digital-savvy countries Estonia and the Netherlands. The former has a pivoted role in the EU context since its Estonian Information System Authority, which is responsible for the administration of the country-wide information systems, is the implementing lead

3 The author of paper was in his function as Strategic Advisor for Cyber Diplomacy/EU Presidency to the Cyber Foreign Policy and Cyber Security Coordination Staff of the Federal Foreign Office of Germany a member of EU Cyber Net's Advisory Board.
4 CLACY+ currently focuses on following priority and hub countries in Africa: Benin, Burkina Faso, Cabo Verde, Ghana, Mauritius, Morocco, Nigeria, and Senegal.

of EU CyberNet and of several other EU-funded projects. The Netherlands has also already a tradition of supporting the overall development of the international cyber capacity building agenda, for instance by hosting the fourth GCCS (Global Conference on Cyber Space), which served as a "launchpad for the Global Forum on Cyber Expertise (GFCE)" (Collett/ Barmpaliou 2021b: 20-21) and by funding the GFCE Secetariat based in The Hague. Its Ministry of Foreign Affairs also funds the secretariat of the Freedom Online Coalition and supports several other projects, among them as a consortium partner in the framework of the EU-led 'Cyber Resilience for Development' (Cyber-4Dev) programme together with the UK and Estonia.

It remained to be seen how cyber capacity building will be integrated into these developments which are mainly stemming from a digital development thinking and how to develop the initiatives proposed by the EU Cyber Security Strategy, which have a closer leaning towards the cyber diplomacy realm. However, the current European debate on digital sovereignty and cyber resilience is largely inward-looking and the African continent still plays a rather subordinate role in the discussions in these contexts. Even key EU initiatives such as the European Commission's AI legal framework only marginally address the potential importance of the legislative proposal for developing states.

Other International Organizations

The norms-setting processes in the UN GGE (UN Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security) and in the UN OEWG (UN (Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security), which are the main groups for setting rules of responsible state behavior in cyberspace, serve as overall guidance for cyber capacity building projects and their final/consensus reports have repeatedly heightened their importance for strengthening cyber security over the years.

The latest Final Substantive Report from March 2021 (UN 2021a), the OEWG clearly states that cyber capacity building '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' and 'for promoting adherence to international law and the implementation of norms of responsible State behaviour'. Furthermore, it lays out certain principles which should guide cyber capacity building projects (see Box 1) and highlights that capacity building is a 'two-way street', meaning that 'participants learn from each other' in form of 'South–South, South–North, triangular, and regionally focused cooperation.' In particular, it stresses the significance of capacity building for 'genuine involvement of developing countries in relevant discussions and fora and strengthening the resilience of developing countries in the ICT environment.'

Box1: OEWG Cyber Capacity Building Principles:

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.

In the same vein, the latest UN GGE report (UN 2021b) adopted in July 2021 highlights cyber capacity building and that international cooperation in this regard should lead to support countries in areas such as '[d]eveloping 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' or concerning 'implementing agreed voluntary, non-binding norms of responsible State behaviour'. Additionally, the report states that countries 'should consider approaching cooperation in ICT security and capacity-building in a manner that is multi-disciplinary, multi-stakeholder, modular and measurable.'

Evolved into an international go-to-place for cyber capacity building, the GFCE (Global Forum on Cyber Expertise), based in The Hague and founded in 2015, is "the only international, multistakeholder forum with the primary purpose of strengthening global cyber capacity by supporting international coordination and cooperation." (Collett/Barmpaliou 2021: 5) It has more than 140 member states and partner organizations and is involved in several areas, most notably through their working groups. The areas include the coordination of regional and global projects and initiatives, the exchange of knowledge through recommendations of tools and publications as well as the identification of individual cyber capacity needs with offers of support. Germany is actively involved in GFCE as a contributor and on the Board as well as in project funding. However, the effectiveness of its coordinating role is still impeded due to the voluntary nature of contribution by its members. (ibid. 5)

With its two trust funds – the umbrella trust fund Digital Development Partnership and the subordinated Cyber Security Multi-Donor Trust Fund – as well as with Global Cyber Security Capacity Program, the World Bank Group aims at extending its work on digital development with more cyber security capacity building activities. Especially the Multi-Donor Trust Fund foresees a more concerted and strategic approach – for instance, the design of projects on the basis of evidence-based research –, also with an emphasis on the African continent.

The SCO (Shanghai Cooperation Organization) is another player engaged in cyber capacity building. The SCO has a special role in this thematic focus due to the membership of China and Russia and their ideas on how to regulate cyberspace. The ideas, which have a focus on state sovereignty and national security, are most notably reflected in the International Code of Conduct for Information Security issued by the organization. This goes hand in hand with the trend that BRICS countries, for example, are no longer just users and importers of cyber capabilities, but are now actively providing them. Especially "China emphasizes its commitment to cyber security capacity building in developing economies and mentions Asian Regional Forum and Forum on China–Africa Cooperation as fora for cooperation." (Homburger 2019: 234-235)

The ITU (International Telecommunication Union) is also increasingly active in this area, offering, for example, so-called 'model laws' relating to cyber security regulation and implements itself cyber capacity building projects in developing countries (Homburger 2019: 230). Against this backdrop, it is noteworthy that "[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)

Other regional organizations are also becoming increasingly involved: the OAS (Organization of American States) offers a range of measures (e.g., National Cyber Security Strategy Development, Crisis Management Exercises, etc.) and has set up the OAS Cyber Security Program and an Inter-American Portal on Cybercrime. The ASEAN (Association of Southeast Asian Nations) has large-scale initiatives for its region, including the Brunei Action Plan Enhancing ICT Competitiveness: Capacity Building, the ASEAN Cyber Capacity Programme (ACCP) or the ASEAN-Japan Cyber security Capacity Building Centre

Beyond state actors and international organizations, several foundations and civil society actors (e.g., ICT4Peace, Asia Foundation, Bill and Melinda Gates Foundation, Hewlett Foundation), academic institutions and think tanks (e.g., DCAF – Geneva Centre for Security Sector Governance) and private companies (e.g., Microsoft, Kaspersky, Symantec) have engaged more and more in international cyber capacity building.

Abbreviations

ASEAN (Association of Southeast Asian Nations)

BMZ (Federal Ministry for Economic Cooperation and Development)

EDF (European Development Fund)

EU (European 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)

Literature

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 Cyber security 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/cyber security-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

About the Author

Kaan Sahin is an International Policy Advisor with a focus on technology and cyber issues. He was Technology Fellow at the Policy Planning Unit in Germany's Federal Foreign Office. Prior to that, he was a Research Fellow for Technology and Foreign Policy at the German Council on Foreign Relations (DGAP). During that time, he took a hiatus to serve as Strategic Advisor for Cyber Diplomacy/EU Presidency at Germany's Federal Foreign Office. In this capacity, he developed a concept and action plan on cyber capacity building and was an advisory board member of EU CyberNet.

Previously, Mr. Sahin worked with Deloitte as a Cyber Risk Consultant and Project Lead. Prior to that, he received a Mercator Fellowship on International Affairs and specialized in strategies to combat hybrid threats. In this capacity, he was based with the International Institute for Strategic Studies (IISS), the Special Representative of the OSCE for the Southern Caucasus, Carnegie Europe, and the Emerging Security Challenges Division at NATO Headquarters.

Mr. Sahin studied political science at the University of Duisburg-Essen and international politics and peace research at the University of Tübingen, the University of Connecticut, and Koç University in Istanbul.