ETTG | European Think Tanks Group

The European Think Tanks Group (ETTG) is a network of European independent think tanks working on EU international cooperation for global sustainable development

www.ettg.eu

EU-AU cyber cooperation: From patchwork to partnership

ETTG Policy Brief 6/2024

Author:
Félix Arteaga
(Real Instituto Elcano)

Reviewers:
Melody Musoni (ECDPM),
Niels Keijzer (IDOS)
and Dora Meredith (ODI)

KEY MESSAGES

1. The EU should continue providing cybersecurity assistance to African countries under a needs-based approach and on equal footing.

2. EU delegations in Africa should consult on assistance priorities with local partners while acknowledging local challenges to cyber capacity building.

3. The EU should continue mainstreaming cybersecurity assistance to wider African digitalisation goals including infrastructures and connectivity.

4. The lack of a developed African cybersecurity ecosystem at the continental level prevents the EU from providing the African Union with its direct expertise on enabling a regional and multilateral system.

5. The EU should make additional strategic communication efforts to highlight the scope and impact of its cybersecurity cooperation programmes with Africa.

TABLE OF CONTENTS

INTRODUCTION

This policy brief aims to analyse the state of European Union–Africa cooperation on cybersecurity and its instruments and priorities, to assess whether its objectives should be maintained or modified. The paper is based on a review of open-source literature, including official documents from Africa and Europe, think-tank analysis and African media reports. The results of this preliminary review were cross-checked at a workshop in Accra, Ghana. The paper provides a general background to European external cooperation on cybersecurity, the African cybersecurity context and recommendations for the development of EU-Africa cooperation in the future.

BACKGROUND

With the rapid digital transformation and interconnectedness of society, cyberspace has become a central part of everyday life. This development has led to a broadening of the cyber threat landscape, including disinformation, cyber-attacks and artificial intelligence, posing a risk to digital and economic growth everywhere including Africa (Interpol, 2024; SAT Reporter, 2024).

According to the European Commission (2021), 'Cybersecurity is an integral part of Europeans' security. Whether it is connected devices, electricity grids, or banks, aircraft, public administrations or hospitals they use or frequent, people deserve to do so within the assurance that they will be shielded from cyber threats. The EU's economy, democracy and society depend more than ever on secure and reliable digital tools and connectivity. Cybersecurity is therefore essential for building a resilient, green and digital Europe.' For the EU, cybersecurity is about the protection of networks, information systems and data from cyber threats. The EU aims to ensure the security, integrity and availability of digital infrastructures and the protection of citizens, businesses and public institutions against cyber attacks.

Cybersecurity is a prerequisite for economic development in general and for the digital economy in particular. The nexus between cybersecurity and development is that cyber capacity building (CCB) increases the resilience of critical infrastructures and the resilience of information and communication technologies to risks and threats in cyberspace. Likewise, the implementation of confidence-building measures (CBM) increases the interaction among stakeholders and end-users for the digital economy to flourish (Collet, 2021).

In the EU ecosystem, cybersecurity strategies and policies contribute to the development of the Digital Single Market, a strategic goal of the EU integration process (European Commission, 2015).[1] Meanwhile,

[1] The Digital Single Market is an EU strategy to break down regulatory barriers and move from 27 national markets to a single market, allowing the EU to better compete globally, create jobs and boost economic growth. It encompasses a wide range of legislative and non-legislative measures aimed at unlocking the full potential of the digital economy in Europe.

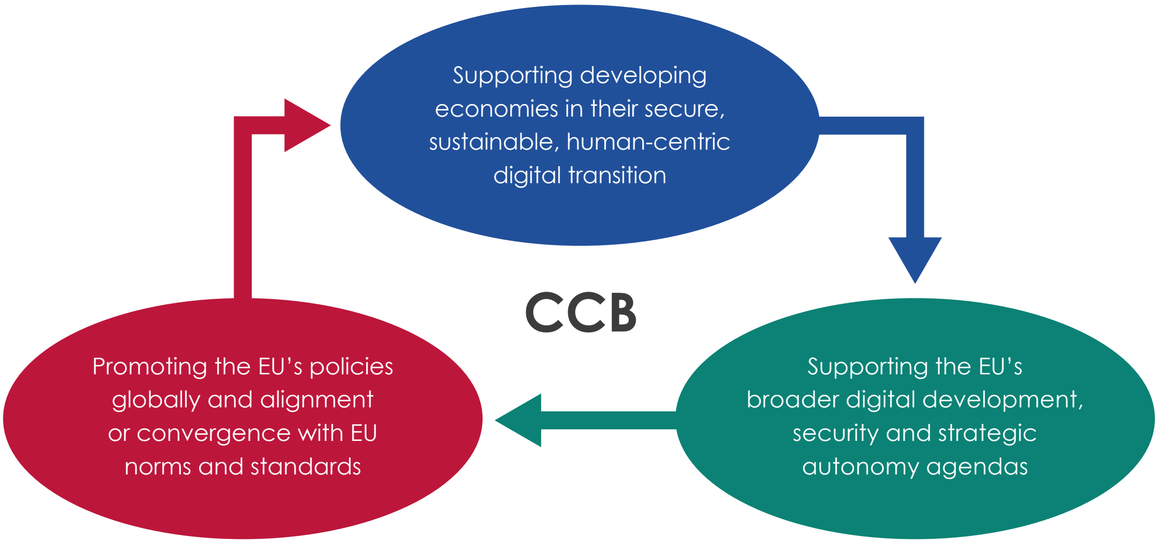
the EU has so far gone through a long learning curve, helping its member states to converge their strategies, policies and rules into a resilient and highly shared continental cybersecurity ecosystem.

Over more than a decade, the EU through the lead of the Directorate-General for Communications Networks, Content and Technology (DG CONNECT) of the European Commission has developed a comprehensive set of strategies, policies, procedures and institutions to address the growing challenges of cyberspace. The supranational nature of the EU has helped to overcome the reluctance of member states to converge into the Digital Single Market, but the European Commission has developed effective CCB and confidence-building practices to foster the convergence. As a spin-off of this process, the EU has developed expertise and tools to provide cybersecurity assistance to third countries and organisations with the CCB goals shown in Figure 1.

Since the EU Cybersecurity Strategy of 2013, the EU has integrated cybersecurity as an instrument of its external action in many official documents (European Commission, 2013; European Council, 2015, 2018, 2022; High Representative & European Commission, 2017, 2020). Cybersecurity is a cross-cutting tool for the EU to implement its foreign, security and development cooperation policies. The EU understands that CCB is an enabler for achieving the Sustainable Development Goals (SDGs) and that EU interventions should go beyond achieving cyber resilience (silo approach) to create synergies between different programmes on cybersecurity, development cooperation, digitalisation and security, rather than isolating CCB from the wider development goals (mainstreaming approach), according to Sheriff et al. (2024). In this way the European Council agreed to develop "an effective EU model for cyber capacity building" integrating all aspects of development and security in its conclusions on cyber diplomacy (European Council, 2015, p. 9).

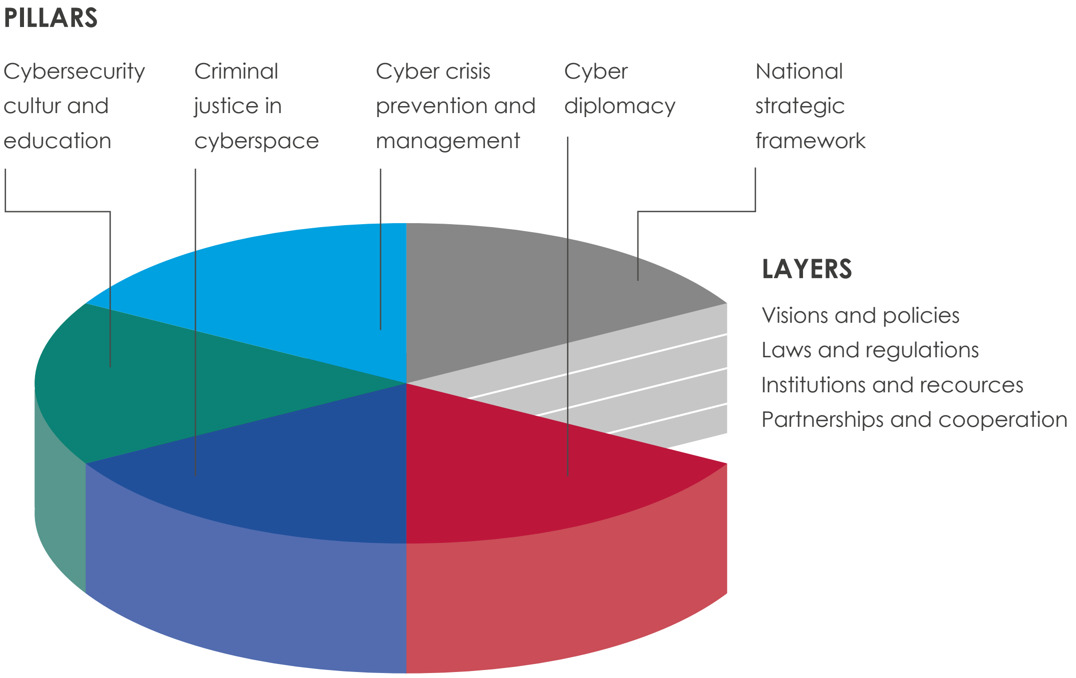
> "The EU should continue providing cybersecurity assistance to African countries under a needs-based approach and on equal footing."

Figure 1. Goals of the EU's cyber capacity building (CCB) engagement


Supporting developing economies in their secure, sustainable, human-centric digital transition
CCB
Supporting the EU's broader digital development, security and strategic autonomy agendas
Promoting the EU's policies globally and alignment or convergence with EU norms and standards

Source: European Commission (2023)

Figure 2. Pillars and Layers of the EU's Cyber Capacity Building


PILLARS
Cybersecurity cultur and education
Criminal justice in cyberspace
Cyber crisis prevention and management
Cyber diplomacy
National strategic framework
LAYERS
Visions and policies
Laws and regulations
Institutions and recources
Partnerships and cooperation

Source: EU's Operational Guidance (p. 30)

The EU has continued to integrate cybersecurity into all dimensions of its external action (cyber-security mainstreaming) so that cybersecurity can be incorporated by design into wider areas of the development such as infrastructures or digital connectivity of the EU's Global Gateway (Fanni et al., 2022). On the other hand, the EU's operational guidelines on cyber capacity building define the elements for which decentralised assistance is planned, like the pillars and layers of Figure 2. According to the traditional donor-recipient model, the parties select the areas for cooperation according to the priorities of the recipients, without defining the outcome of the cooperation.

> "The EU should continue mainstreaming cybersecurity assistance to wider African digitalisation goals including infrastructures and connectivity."

Pillars and layers intertwine at national, regional, and global levels in a coherent way to strike the right balance between ends, means and local contexts in EU cybersecurity assistance projects.

MODEL AND PROGRAMMES OF THE EU-AFRICA CYBERSECURITY COOPERATION SO FAR

Relations between Africa and Europe seek to move from a development approach towards a partnership of equals. The EU and the African Union (AU) share values and principles regarding digitalisation, cybersecurity and responsible state behaviour in cyberspace (African Union, 2015; European Council, 2017). EU tools support cyber security capacity-building measures, resilience of networks and information systems, and data and privacy protection, in line with the principles and values of the EU's external action, and contribute to achieving the goals set out in the UN 2030 and Africa 2063 agendas. In addition, the EU has been working with public and private actors such as the EU-African Union Digital Economy Task Force (EU-AU DETF), the Global Forum on Cyber Expertise and the D4D Initiative for Digital Government and Cybersecurity or with international organisations such as the Council of Europe or the United Nations to build cybersecurity capacity in Africa (EUISS, 2021). These and other interventions are presented in Table 1.

However, the main comparative advantage for the EU's cybersecurity assistance abroad is its own experience in developing its continental cyber ecosystem (the Digital Single Market). Many other cyber practitioners, public or private, can provide cybersecurity technical assistance, but only European Commission officials can add the value of their direct experience in integration processes at a continental level. For EU-Africa assistance focused on the integration of different national ecosystems into a continent-wide one, Commission officials have a comparative advantage and ad-hoc tools (ESDC, 2023).[2]

European cooperation with Africa has so far developed in a decentralised way through national (EU-African countries), regional (EU-African organisations) and continental (EU-AU) frameworks. Table 1 (left column) shows projects funded by the EU, alone or together with other multinational

Table 1. EU-Africa cybersecurity cooperation

EU-funded projects	**CJ**	**NSF**	**ICM**	**VP**	**LR**	**IR**	**deadline**
Regional Integration Support COMESA			🟥			🟥	2022
Promoting Peace Stability Horn of Africa (IPPSHAR)	🟥					🟥	2023
Policy Regulation Initiative for Digital Africa (PRIDA)		🟩			🟩		2022
OCWAR-C	🟥	🟥	🟥	🟥			2024
HIPSSA	🟩	🟩			🟩		active
GLACY+	🟦				🟦	🟦	2023
EU-Africa Infrastructure Trust Fund		🟩				🟩	2019
ENACT	🟩	🟩				🟩	2017
Digital Economy Task Force (DETF)		🟩		🟩			2019
D4D Platform		🟩		🟩		🟩	2023
CyberSouth	🟦				🟦	🟦	active
Cyber4Dev		🟦	🟦	🟦		🟦	2024
Africa Connect 1,2,3		🟥				🟥	2023

🟩 EU is funding AU objectives

🟦 EU funds objectives set by individual African states

🟥 EU funds objectives set by African sub-regional organisations

Source: Adaptation from "Africa as a Cyber Player" (Van Raemdonck, 2021)

[2] A precedent to follow could be the EU training courses where the main stakeholders of the European cyber ecosystem like the European Parliament, the European Commission, the European External Action Service or the European Cybersecurity Agency (ENISA) among many others exchange direct experiences with regional counterparts.

frameworks, but implemented through third parties, be they African or European, but not by EU officials. The projects have the objectives indicated in the following columns, the last one indicating the known date of closure. The projects are spread across several objectives: Criminal Justice (CJ), National Strategic Frameworks (NSF), Incident and Crisis Management (ICM), Vision and Policies (VP), Laws and Regulations (LR) and Institutions and Resources (IR) without clear priority. The green colour distinguishes projects where the EU is funding AU objectives from projects where the EU funds objectives set by individual African states (blue) or by African sub-regional organisations (red).

Table 1 also shows a division of labour between the design, conducted by EU institutions and funds, and the implementation, which mainly involves non-EU experts and resources. From a regional convergence perspective, projects related to National Strategic Frameworks (NSF), Vision and Policies (VP) or Laws and Regulations (LR) contribute more to the development of an AU cyber ecosystem than those related to Criminal Justice (CJ), Institutions and Resources (IR) or Incident and Crisis Management (ICM). While the latter are focused on cyber resilience, the former look for transformational changes in strategies, regulations and governance. As Table 1 (light blue) shows, a great part of the EU cooperation is already transformation-oriented but at the national level. Therefore, if African countries and the AU call for a deepening of African convergence, the EU should prioritise its future cooperation with fewer objectives but with greater transformational ambition.

The EU's cyber cooperative projects have been implemented on a decentralised basis like most of the development cooperation projects: the EU provides the financial means, and the beneficiaries implement their CCB and CBM projects. However, this decentralised approach does not seem to be adequate when it comes to framing the different objectives into a regional integration process. Regardless of the concrete outcome of each project, the diversity of approaches and objectives does not facilitate structural changes in ecosystems. Decentralised cooperation, without a comprehensive strategy for action, favours a concentration of projects and an imbalance among beneficiaries (European Commission, 2021). In order to promote convergence, European assistance should focus on the one hand, on supporting the AU's integration strategy and, on the other hand, on increasing the direct involvement of European institutions such as the European Commission, the European Union Network and Information Security Agency (ENISA), the European Cybercrime Centre within Europol and the EU Institute for Security Studies (EUISS).

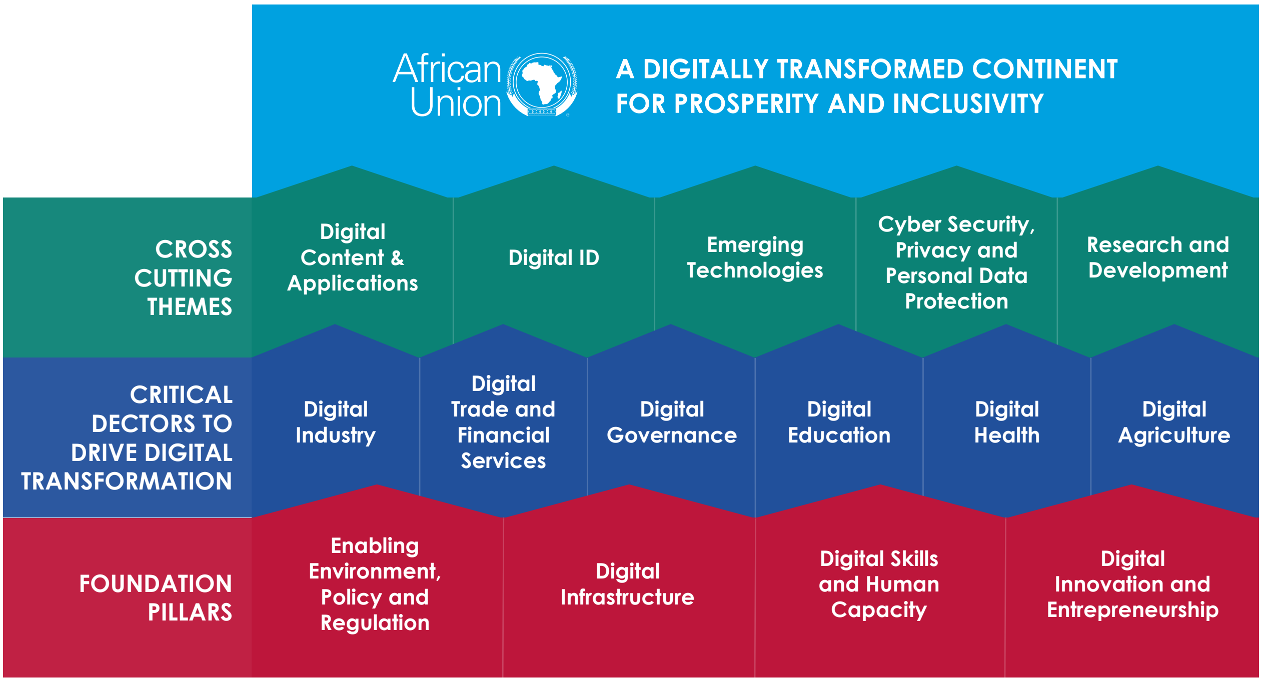
THE AFRICAN CYBERSECURITY CONTEXT

Africa has various mechanisms to promote convergence among African countries such as the AU Agenda 2063, the Convention on Cybersecurity and Personal Data Protection (Malabo Convention), the AU Cybersecurity Expert Group (AUCSEG), the Policy and Regulations Initiative for Digital Africa (PRIDA), the Programme for Infrastructure Development for Africa (PIDA), the Digital Transformation Strategy for Africa 2020-2030 (2020), the Smart Africa Alliance or the ECOWAS Cybersecurity Strategy (2021), among others. However, these mechanisms have not yet produced the expected results for the reasons explained below.

The Information Society Division of the African Union is driving the implementation of the Digital Transformation Strategy for Africa (2020–2030), including the formulation of cybersecurity governance and the contribution of its Group of Governmental Experts to promoting responsible state behaviour in cyberspace in the context of international security (cyber diplomacy). As a result, the E-Government Development Index of the United Nations (2024) shows an upward trend in e-government development in Africa, with 28 African countries showing steady growth in digital integration, while seven remain stagnant due to their security situation.

Cybersecurity is one of the objectives of the African Union in its Digital Transformation Strategy for Africa 2020–2030. As Figure 3 reveals, it is one of the five cross-cutting themes for the digital transformation. Digitalisation is supported by key countries and progress has been made on e-governance indicators and internet penetration. However, analysis by the EUISS suggests that the 'lack of coordination structures among the AU member states and a single pan-African digital ID system have been the main reasons for the low levels of digital governance'

Figure 3. Digital Transformation Strategy for Africa (2020–2030)



African Union

A DIGITALLY TRANSFORMED CONTINENT FOR PROSPERITY AND INCLUSIVITY

CROSS CUTTING THEMES: Digital Content & Applications; Digital ID; Emerging Technologies; Cyber Security, Privacy and Personal Data Protection; Research and Development

CRITICAL DECTORS TO DRIVE DIGITAL TRANSFORMATION: Digital Industry; Digital Trade and Financial Services; Digital Governance; Digital Education; Digital Health; Digital Agriculture

FOUNDATION PILLARS: Enabling Environment, Policy and Regulation; Digital Infrastructure; Digital Skills and Human Capacity; Digital Innovation and Entrepreneurship

Source: African Union Digital Transformation Strategy for Africa (2020)

(2021, p. 32). Similarly, according to the EU-AU Digital Economy Task Force's assessment (2019), the main obstacle for achieving the digital economy in Africa is the lack of an enabling e-governance environment entailing harmonised national, regional and continental digitalisation policies.[3]

Makumane (2023) states that regional convergence is hampered by asymmetries within African countries and the confidence-building measures implemented to date have failed to overcome national resistance. The continental cybersecurity agenda remains stagnant in Africa despite progress on several national or sub-regional agendas. One third of countries lack legislation on cybercrime, electronic transactions, consumer protection, privacy and data protection, according to the data for Africa from the UNCTAD Global Cyberlaw Tracker (2024), or have not ratified the Malabo Convention (African Union, 2014). The World Economic Forum (2024) estimates that there are around 20,000 certified security professionals in a continent of 1.4 billion people, an insufficient number to meet the demand in Africa. Only a third of countries have cybersecurity strategies according to the database of the International Communication Union (2024), and nationalist agendas are holding back African convergence (Ifeanyi-Ajufo, 2022).

According to the Global Cybersecurity Index (2021), just 19 African countries are signatories to multilateral cybersecurity agreements, in contrast to 41 European countries, while only ten African countries have entered into bilateral cybersecurity agreements. The same index reveals the disparity on cyber maturity between African countries and how far Africa lags behind other regional ecosystems. Few countries conduct threat assessments, making it difficult for them to strategically anticipate and prepare for cyberattacks (see Ajyola & Allen, 2022).

The AU's Digital Transformation Strategy of 2020 proposed the strengthening of regional and continental governance to guide, develop and harmonise digital and cybersecurity

[3] The EU-AU DETF is an independent platform of partnership sponsored by the EU and the AU for the private sector, donors, international organisations, financial institutions and civil society based on a shared understanding of how an already rapidly evolving African digital transformation can achieve cross-border integration and bring benefits to all citizens.

strategies, policies and standards. This convergence process is not progressing at the desired pace for the structural reasons outlined above, and as national and sub-regional convergence processes consolidate, it will become increasingly difficult to harmonise them within a continental framework. The gap between desired goals and outcomes, together with the deteriorated cybersecurity situation, called the AU's Peace and Security Council to make cybersecurity a key agenda point in the AU Summit of Addis Ababa in February 2024. African leaders agreed to develop a Continental Cybersecurity Strategy, and the first-ever Common African Position on the application of international law in cyberspace, among other significant developments (Ifeanyi-Ajufo, 2024).

The African Union's decision to develop an African Cyber Security Strategy could change the pattern of EU-Africa cyber security cooperation. If the decision is implemented, the AU would need specific support to align all the transformation processes underway in African countries and sub-regions to converge into an Africa-wide ecosystem in line with the new strategy. A greater role for the AU in the development of African cybersecurity would imply a shift from a cooperation model focused on cyber resilience to one focused on digital transformation, and from one aimed at addressing specific, short-term needs (patchwork) to one that broadens and deepens long-term strategic cooperation (partnership).

The AU's cybersecurity strategy would complement the AU's Digital Transformation Strategy and could be the first step in articulating a regional cybersecurity ecosystem, comprising a set of actors and procedures that would allow the AU to lead the convergence of national and sub-regional ecosystems. If the African Union decides at some point to speed up the regional convergence, and given Europe's experience in building its own continental ecosystem, the EU could seize the opportunity to support the AU at this transformative moment. Long-term, structural and peer-to-peer cooperation would enable a strategic partnership between the EU and the AU to accelerate and transform the cyber convergence process of African countries.

To date, EU-AU cyber cooperation lacks guiding strategies and institutional mechanisms for political dialogue to foster and consolidate cybersecurity integration processes. There is neither an AU strategy to create an African cyber ecosystem, nor a supporting EU strategy to set in motion a long-term strategic partnership between the EU and the AU.[4] Without such guidance, EU-AU cybersecurity cooperation would never evolve into a strategic partnership, be it on cybersecurity or digitalisation. The absence of a direct EU-AU assistance does not underestimate the contribution of the current decentralised cooperation, but it does not help the AU to transform the African ecosystem. In the absence of a stronger EU institutional presence, the European cybersecurity assistance remains unnoticed by the media and the public and its relevance is diluted into the wider digitalisation process.

The EU's operational guidelines stress the need for coordination and coherence among bilateral and regional cooperation programmes according to the cyber maturity of countries, neighbours and regions. Developing bilateral cybersecurity projects in isolation from regional initiatives could hinder further interoperability and harmonisation at the regional and multilateral level if decision-making cycles for regional and bilateral programmes are not aligned. In the same vein, EU delegations in Africa should make sure that programmes are adapted to the local context of partners to avoid mirroring EU solutions.

The lessons learnt by the EU during this integration process, as a driver for the convergence of its member states towards a continental ecosystem, could add more value to the AU-EU cybersecurity cooperation than the scattered technical assistance and advisory actions currently offered by the EU. However, and given the limitations of the African regional ecosystem as expressed by the available indicators and the reservations shown by local actors on its priority for the short- and medium-term EU-Africa cybersecurity assistance, the EU should continue to provide technical and financial assistance as it has done so far, rather than offering a bilateral long-term strategic framework for cooperation with the African Union. Should the African Union at any point request European support for the development and implementation of a regional cybersecurity ecosystem (see Annex), the EU Cybersecurity Agency (ENISA) could be instrumental for a regional-to-regional cooperation. It has the proper expertise, instruments and competence, but this objective is outside its medium-term plans because its assistance in policy development is limited to the EU and Member States (ENISA, 2023, p. 38).

[4] For example, EU CyberNet is an e-learning platform that has conducted CCB courses in Africa to enhance the resilience of local ecosystems and to socialise decision-makers with EU values, strategies, policies, procedures and standards, but it does not pursue any concrete regional transformation.

RECOMMENDATIONS FOR EU-AFRICA CYBER COOPERATION

Cybersecurity is a cross-cutting issue that affects not only the security of networks and information systems, but also the development of democracy, governance and digitalisation in Africa. It creates mistrust in electoral processes, in the regulation of rights and freedoms, and in access to the benefits of the digital economy. As a result, African end-users prefer EU-Africa cybersecurity cooperation to cope with the concrete problems they detect in their home localities.

The current model of EU-Africa decentralised cooperation meets these needs by allowing projects to be focused on local priorities. In particular, African end-users recognise the usefulness of cooperation projects on criminal justice, incident and crisis management, data protection and cybersecurity regulation, which are tailored to help local authorities address local and regional problems.

Nevertheless, African actors missed the existence of cooperation projects that included infrastructure and equipment rather than just training and technical assistance. They were also concerned about their limited resources, digital skills, literacy and awareness to address cybersecurity challenges. The impact of the new infrastructures like 5G or 6G on collecting criminal e-evidence was among their concerns as well. The European Commission is now addressing these issues through new EU frameworks such as the last investments in the Global Gateway initiative (European Commission, 2024) or Safe Digital Boost Africa (see Domingo et al., 2024).

Another important issue for the future is the involvement of civil society in the design and monitoring of EU-African cooperation. The participation of civil society in cyber politics to elaborate policies or to protect fundamental rights and freedoms was also addressed in the workshop. The European interlocutors explained best practices for public-private and private-private cooperation to increase the inclusiveness of cyber politics. Greater participation of civil society could improve current levels of efficiency, transparency and accountability. It would also increase the African population's perception of EU-Africa cooperation projects, which currently barely extends beyond the limited circle of participants.

The AU's decision to develop a regional cybersecurity strategy is a milestone in the development of an African cyber ecosystem, but there are many doubts about the timeliness and maturity of the African Union to align national and sub-regional strategies and policies into an Africa-wide cyber ecosystem. Accordingly, there is little expectation that the African Union Commission and the European Union Commission will transform the traditional donor-recipient model into a partnership of equals. The workshop did not question the potential value of developing a continental cybersecurity strategy, as agreed by the AU in Addis Ababa, but local actors underestimated the timeliness and maturity required to align national and sub-regional strategies and policies into an Africa-wide cyber ecosystem. Neither did they question that greater and more direct protagonism by the African Union Commission and the European Union Commission could help transform the traditional donor-recipient model into a partnership of equals. In any case, the EU should be ready to support the AU as a potential enabler for intra-African cybersecurity cooperation.

As conclusion, the main recommendations for the future of EU-Africa Cybersecurity Cooperation can be summarised as follows:

> “The EU should be ready to support the AU as a potential enabler for intra-African cybersecurity cooperation.”

1 The EU should continue to **PROVIDE CYBERSECURITY ASSISTANCE** to African countries and organisations on a needs-based and equal basis.

2 EU delegations in Africa should **CONSULT WITH LOCAL PARTNERS ON ASSISTANCE PRIORITIES**, while recognising local challenges to cyber capacity building.

3 The EU should continue to **INTEGRATE CYBERSECURITY ASSISTANCE INTO BROADER AFRICAN DIGITALISATION OBJECTIVES**, including infrastructure and connectivity.

4 The lack of a developed African cybersecurity ecosystem prevents the EU from **PROVIDING ITS DIRECT EXPERTISE TO THE AFRICAN UNION** to enable a regional framework for aligning national and sub-regional developments.

5 The EU should make **ADDITIONAL STRATEGIC COMMUNICATION EFFORTS TO HIGHLIGHT THE SCOPE AND IMPACT OF ITS CYBERSECURITY COOPERATION PROGRAMMES** with Africa.

ANNEX

Basic components for the development of an African regional ecosystem according to the EU model: ENISA (2023), the High Representative and the European Commission (2020).

- A regional agreement setting out measures for achieving a high common level of security of network and information systems within the African Union to improve the functioning of the African internal market (Network and Information Systems Directive, NIS, in the case of the EU).
- Guidelines for developing and harmonising national cybersecurity strategies (as done by the National Cybersecurity Strategies Guidelines & Tools from the European Network and Information Systems Agency, ENISA, for the European Commission).
- Creation of an ad-hoc inter-ministerial working group to manage convergence and build trust between member states. Over time, the management of the group could be shared with a cybersecurity agency under the AU (the roles of the Cooperation Group and ENISA, respectively in the EU).
- Establish incident notification procedures and cybersecurity authorities for member states' operators of essential services and digital service providers, including incident response teams and incident response centres (CSIRTs and CSIRTs network in the EU).
- Identify cybersecurity authorities and national contact points in African countries to channel notifications, manage crises, elaborate and evaluate norms and policies, raise public awareness, build public-private cooperation and so forth.
- Establish mechanisms for data protection, promotion of public-private cooperation and international cooperation: from self-regulation codes to more binding commitments, from the protection of critical infrastructures to a more strategic involvement of private stakeholders, and from sub-regional cooperation schemes to regional and transnational networks.

REFERENCES

African Union. (2014). Convention on cybersecurity and personal data protection. https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection

African Union. (2015). Agenda 2063: The Africa we want. https://au.int/sites/default/files/documents/36204-doc-agenda2063_popular_version_en.pdf

African Union. (2020). The digital transformation strategy for Africa (2020–2030), 5. https://au.int/en/documents/20200518/digital-transformation-strategy-africa-2020-2030

Ajyola, A., & Allen, N. (2022, March 8). African lessons in cyber strategy. Africa Center for Strategic Studies (ACSS). https://africacenter.org/spotlight/african-lessons-in-cyber-strategy

Collet, R. (2021). Understanding cybersecurity capacity building and its relationship to norms and confidence building measures. *Journal of Cyber Policy*, pp. 298–317. https://www.researchgate.net/publication/363354000_Understanding_cybersecurity_capacity_building_and_its_relationship_to_norms_and_confidence_building_measures

Domingo, E., Muscat, S., Arnold, S., Satzinger, M., & Chetty, P. (2024, June). The geopolitics of digital literacy and skills cooperation with Africa. European Centre for Development Policy Management (ECDPM), Discussion Paper 369.

ECOWAS. (2021). ECOWAS regional cybersecurity and cybercrime strategy. https://parl.ecowas.int/information-and-communication-technology-ecowas-adopts-a-regional-strategy-for-cybersecurity-and-the-fight-against-cybercrime/

ENISA. (2023). Single Programming Document 2023-2025, January, 38. https://www.enisa.europa.eu/publications/corporate-documents/enisa-single-programming-document-2024-2026-condensed-version.

ENISA (2023). A governance Framework to National Cybersecurity Strategies. https://www.enisa.europa.eu/publications/a-governance-framework-for-national-cybersecurity-strategies

ESDC. (2023). The role of the EU cyber ecosystem in global security stability. European Security and Defence College. https://esdc.europa.eu/enlistapi/Invitation%20Letter%20The%20Role%20of%20the%20EU%20Cyber%20Ecosystem.pdf

EU-AU Digital Economy Task Force. (2019). New Africa-Europe digital economy partnership, 47. https://digital-strategy.ec.europa.eu/en/library/new-africa-europe-digital-economy-partnership-report-eu-au-digital-economy-task-forceue-africa-final.pdf

EUISS. (2021). International cyber capacity building: Global trends and scenarios. European Institute for Security Studies. https://www.iss.europa.eu/sites/default/files/EUISSFiles/CCB%20Report%20Final.pdf

European Commission. (2013). EU cybersecurity strategy. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52013JC0001

European Commission. (2015). EU digital single market strategy. Available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52015DC0192

European Commission. (2021). The EU`s international cooperation on cyber capability building. EU CyberNet. https://op.europa.eu/en/publication-detail/-/publication/a90640f1-a423-11e8-99ee-01aa75ed71a1/language-en

European Commission. (2023). International cyber capacity building, 18. https://www.iss.europa.eu/sites/default/files/EUISSFiles/CCB%20Report%20Final.pdf

European Commission. (2024). EU-Africa: Global Gateway investment package. https://international-partnerships.ec.europa.eu/policies/global-gateway/initiatives-region/initiatives-sub-saharan-africa/eu-africa-global-gateway-investment-package_en

European Council. (2015). Conclusions on Cyber Diplomacy. https://data.consilium.europa.eu/doc/document/ST-6122-2015-INIT/en/pdf

European Council. (2017). The new European consensus on development. https://international-partnerships.ec.europa.eu/policies/european-development-policy/european-consensus-development_en

European Council. (2018). EU external cyber capacity building guidelines. https://data.consilium.europa.eu/doc/document/ST-10496-2018-INIT/en/pdf

European Council. (2022). Conclusions on the development of the European Union's cyber posture. https://www.consilium.europa.eu/media/56358/st09364-en22.pdf

Fanni, R., Ford, C., Nitschekter, M., Perarnaud, C., Renda, A., & Rico, M. (2022, December 19). A digital connectivity masterplan for Global Gateway. Center European Policy Studies (CEPS), 25. https://cdn.ceps.eu/wp-content/uploads/2023/03/INTRA_Digital-Connectivity-Masterplan.pdf

High Representative & European Commission. (2017). Resilience, deterrence and defence: Building strong cybersecurity for the EU. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017JC0450

High Representative & European Commission. (2020). The EU's cybersecurity strategy for the digital decade. https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0

Ifeanyi-Ajufo, N. (2022, January 13). Net politics in Africa. EU cyber direct comments. https://directionsblog.eu/net-politics-in-africa

Ifeanyi-Ajufo, N. (2024, February 26). The AU took important actions on cybersecurity at its 2024 summit, but more is needed. Expert Comment, Chatham House. https://www.chathamhouse.org/2024/02/au-took-important-action-cybersecurity-its-2024-summit-more-needed

International Communication Union. (2021). Global cybersecurity index 2020, 32-53. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf

International Communication Union. (2024). National cybersecurity strategies repository as of September 27. https://www.itu.int/en/ITU-D/Cybersecurity/Pages/National-Strategies-repository.aspx

Interpol. (2024). African cyberthreat assessment report 2024. https://www.interpol.int/en/Search-Page?search=AFRICA&limit=12&page=2

Makumane, M. (2023, June 14). Pathways towards confidence: Priorities and perspectives. on African confidence-building measures in cyberspace. EU Cyber Direct. https://eucyberdirect.eu/research/pathways-towards-confidence

SAT Reporter. (2024, July 6). Top 10 African countries affected by data breaches in 2024. The Southern African Times. https://southernafricantimes.com/top-10-african-countries-affected-by-data-breaches-in-2024

Sheriff, P., Sanders, J., & Waisser Harris, C. (2024). Evaluating the impact of cybersecurity capacity building. Oxford University-Royal Holloway University, 2.c https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4821426

UNCTAD Global Cyberlaw Tracker. (2024, September 27 data). https://unctad.org/topic/ecommerce-and-digital-economy/ecommerce-law-reform/summary-adoption-e-commerce-legislation-worldwide

United Nations. (2024). E-Government survey 2024. Department of Economic and Social Affairs, 92-97. https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2024

Van Raemdonck, N. (2021, January). Africa as a cyber player. EU Cyber Direct, 45. https://eucd.s3.eu-central-1.amazonaws.com/eucd/assets/FgLaEKYp/digital-dialogue-africa-final.pdf

World Economic Forum. (2024, April). Strategic cybersecurity talent framework, 4. https://www3.weforum.org/docs/WEF_Strategic_Cybersecurity_Talent_Framework_2024.pdf

The Policy Brief was realised with the support of the Mercator Foundation

STIFTUNG
MERCATOR

ETTG | European Think Tanks Group

The views presented in this publication are those of the authors and do not necessarily represent the views of the organisations that make up the European Think Tanks Group.

ISSN 2984-0457

ecdpm | REAL INSTITUTO elcano ROYAL INSTITUTE | IAI Istituto Affari Internazionali | IDDRI SUSTAINABLE DEVELOPMENT & INTERNATIONAL RELATIONS | IDOS German Institute of Development and Sustainability | ODI Think Change