SPECIAL REPORT

Feb 2025

Global Gateway

BETWEEN AMBITION AND PRAGMATISM

The future of cyber capacity-building in a fragmented world

by
Nayia Barmpaliou
and
Patryk Pawlak

euiss
European Union Institute for Security Studies

The EUISS is an agency of the European Union

CATALOGUE NUMBER QN-01-25-026-EN-N
ISBN 978-92-9462-422-2
DOI 10.2815/6691818
Cover image: Batyrkhan Shalgimbekov/Unsplash

CONTENTS

This paper has been commissioned by the European Union Institute for Security Studies (EUISS) with the financial assistance of the European Union (EU) as a contribution to the side-event "The future of responsible state behaviour in a fragmented cyber capacity ecosystem" that took place on 13 May 2024 in the context of the intersessional meetings of the Open-ended working group on security of and in the use of information and communication technologies 2021-2025. The side-event was co-hosted by the EU, the EUISS, the Global Forum on Cyber Expertise (GFCE), and the United Nations Institute for Disarmament Research (UNIDIR). The contents of this paper are the sole responsibility of the authors and can under no circumstances be regarded as reflecting the position of the European Union or any of the side-event co-hosts.

INTRODUCTION

Cyber capacity-building (CCB) has gained increasing prominence in international cyber policy discussions over the past decade. It is viewed as a key mechanism for international cooperation, supporting countries in developing their cyber resilience and fostering partnerships on cyber-related issues. However, while there is broad consensus globally on the need for CCB, this agreement has not fully translated into a unified approach for scaling up, coordinating, and enhancing the efficiency and effectiveness of these efforts.

Although CCB cooperation has grown, with more funders, implementers, and partner countries engaging bilaterally, regionally, or through multilateral organizations, the cybersecurity capability gap is also widening, set against the backdrop of a rapidly evolving and complex threat landscape. The demands and costs associated with developing the expertise and skills needed to address the strategic, institutional, regulatory, and security challenges for a successful and sustainable digital transition place a disproportionate burden on low- and middle-income countries. As a result, there is a significant divergence in cyber equity between cyber-mature countries and those beginning their cybersecurity journey.[1]

Despite the interconnectedness of cyber-related issues, many debates to date have not captured the whole CCB ecosystem as it has organically grown within the confines of different communities, such as international security, criminal justice, and information and communication technologies (ICTs). The siloed discussions on CCB have fostered a high potential for gaps and inefficiencies by not systematically combining the different communities' respective know-how and resources. The result has been a progressing operational fragmentation of cyber capacity-building efforts.

As investments in digital infrastructure, systems, and services continue to increase worldwide, the need for a more holistic understanding of capacity development for cyber resilience has become even more critical. An increasing number of development actors are now integrating cyber resilience into broader development financing and programming, beyond the initial first movers of the 2010s. Collective initiatives such as the Accra Call for Cyber Resilient Development aim to "stimulate action and voluntary commitments to elevate cyber resilience across international and national development agendas" and to promote cyber capacity-building that is responsive to the needs and priorities of developing countries while supporting broader development goals. Similarly, discussions within the current mandate of the "Open-ended Working Group on security of and in the use of information and communications technologies 2021-2025"[2] (OEWG) under the United Nations First Committee have begun to consider CCB more broadly, beyond the context of international security and the Framework for Responsible State Behaviour (FRSB), recognizing the connection to sustainable development. However, debates in such policy forums, as well as CCB practices to date, point to a persistent

divergence in conceptual understandings and approaches to cooperation that are crucial in shaping global CCB efforts.

This paper aims to provide a structured overview of the complex international CCB ecosystem, deepen the reflection on how the ideological and operational fragmentation within it influences the effectiveness of ongoing efforts, and explore how these challenges may impact the CCB community moving forward.[3]

SLICING THE ELEPHANT: UNDERSTANDING THE CCB ECOSYSTEM

To understand the evolution of the international cyber capacity-building ecosystem, we must consider the actors shaping it and the different roles they play.[4] Taking a birds-eye view, a functional categorization serves as the starting point to identify the main groups of CCB actors involved in partnerships formed through the financing, receiving, or implementation of CCB-related assistance.[5]

Funders

Funders primarily include donor governments and their agencies, as well as development banks, philanthropic organisations, and private sector entities that finance CCB actions in partner countries and regions.[6] In a global environment characterized by multiple development and cooperation priorities, numerous cascading crises, and budgetary pressures, funders face both the pressure and responsibility to support capacity development that delivers results aligned with national priorities. Reflecting on the OEWG principles for cyber capacity-building,[7] funders are uniquely positioned to prioritize actions that are demand-driven, based on their partner countries' priorities, ownership, and sovereignty.

Donor governments

Donor governments play a critical role in supporting international cyber cooperation through technical assistance, capacity-building, and financing programmes for partner countries and regions in order to "leave no one behind". The financing streams for CCB in national governments rarely originate from a single institution or authority, but there is often a leading actor with either the majority of available funds or the institutional mandate to coordinate – ranging from the Ministry of Foreign Affairs, the Ministry of Finance, the Ministry of ICT, the national development agency, the cybersecurity authority, to the national law enforcement or crime agency. For partner countries and regions, it is useful to understand which part(s) of the donor governments finance CCB actions as these most often inform the funders' objectives, thematic and geographical priorities, and delivery approaches.

Box 1: Examples of Donor Government Authorities Financing CCB

The respective Ministries of Foreign Affairs of Australia, Brazil, Canada, France, Germany, the Netherlands, New Zealand, Norway, Switzerland, the United Kingdom and the United States are in the lead of financing international CCB through their foreign assistance funds, or in combination with development cooperation envelopes when they are in charge of both mandates.[8] These ministries are also responsible for coordinating CCB efforts across all government agencies engaged in this field.

Another model includes national cybersecurity authorities and Computer Emergency Response Teams (CERTs) or Computer Security Incidence Response Team (CSIRTs) as the leading financing and/or implementing CCB government actor. Indicative cases include the Cybersecurity Authority of Singapore (CSA), the Korea Internet and Security Agency (KISA), and India's Computer Emergency Response Team (CERT-In) within the Ministry of Electronics and Information Technology (MeitY).

There are also cases where development agencies and institutions play a key role in donor countries' international CCB initiatives by utilizing development aid flows. Examples include the Directorate-General for International Partnerships (INTPA) of the European Commission, the Japan International Cooperation Agency (JICA), and the United States Agency for International Development (USAID).

A different approach involves Ministries of Economy and/or Finance engaging with International Financial Institutions (IFIs) for CCB actions through grants or contributions to trust funds. Since 2016, Israel's Ministry of Finance has identified cybersecurity as a strategic priority in its partnerships with IFIs, and in coordination with the Israel National Cyber Directorate (INCD), it has provided cyber-specific grants to the Inter-American Development Bank (IADB), the European Bank for Reconstruction and Development (EBRD), and the World Bank. Similarly, South Korea's Ministry of Economy and Finance has partnered with the World Bank under the Korea-World Bank Group Partnership Facility (KWPF) Trust Fund in setting up the Global Cybersecurity Capacity Program, creating the Combating Cybercrime Toolkit and Assessment Tool, and establishing the Asia-Pacific Cybercrime Hub (APC-HUB).

The increasing importance of CCB as part of donor governments' international cyber engagement is also demonstrated by the creation of dedicated CCB programmes, centres, and/or funds, for example:

- The **European Union**[9] has defined since 2013 a dedicated cyber-specific financing envelope under its Instrument for Stability, and by now has dedicated cyber programmes under the thematic and geographic envelopes of its current external financing instruments.[10] In 2019, the EU created the Digital for Development (D4D) Hub as a strategic, multi-stakeholder platform to coordinate support for human-centric digital transformation in EU partner countries and leverage the expertise, resources and strengths of the private sector, civil society organisations, financial institutions, and other stakeholders. The global D4D Hub has a thematic working group on cybersecurity and by now has regional branches for Africa, the Asia-Pacific, Latin America and the Caribbean, the Western Balkans, and the EU's Eastern Neighbourhood. Moreover, in 2022, the EU funded the establishment of the Latin America and Caribbean Cyber Competence Centre (LAC4), with a physical training facility in the Dominican Republic to provide cybersecurity and cybercrime expertise in support of LAC countries' digital transformation.
- The **United States** State Department has been tapping into different financial envelopes to finance CCB actions globally. As early as 2004, it created its Cybercrime Program, which sits within the Bureau of International Narcotics and Law Enforcement Affairs (INL) and is implemented in close cooperation with the Department of Justice. In 2014, the State Department launched the Cybersecurity Capacity Building Program, initially managed by the Office of the Coordinator for Cyber Issues (S/CCI), which, following a 2022 reorganisation, transitioned to the Bureau of Cyberspace and Digital Policy (CDP). Both programmes are centrally managed and are separate to additional funds earmarked by regional bureaus within the Department for specific countries and regions. Moreover, the U.S. Government launched the Digital Connectivity and Cybersecurity Partnership (DCCP) in 2018, a whole-of-government programme co-chaired by the State Department and USAID, with the participation of ten other Departments and Agencies, to support the development of open communications infrastructure, transparent regulatory policies, and partners' cybersecurity capacity. In addition, a new Cyberspace, Digital Connectivity and Related Technologies (CDT) Fund was created by Congress in December 2023 under the State Department to finance strategic foreign assistance programmes that enable long-term capacity and resilience building, as well as to support swift and effective rapid incident response and cyber aid.

- **The Netherlands**' Ministry of Foreign Affairs (MFA) spearheaded the establishment of both the Freedom Online Coalition (FOC) in 2011 and the Global Forum on Cyber Expertise (GFCE) in 2015, committing to multi-year financing for their respective secretariats. It is also one of the donors behind the launch of the World Bank's Cybersecurity Multi-Donor Trust Fund. Its cyber capacity-building programme includes financing actions across several areas, such as support to CSIRT maturity, critical information infrastructure protection, internet freedom, and human rights online, in alignment with the CCB priorities set in its successive International Cyber Strategies of 2017 and 2023.
- The **United Kingdom** began funding its international CCB initiatives in 2012 under the international envelope of the National Cyber Security Programme (NCSP-I). Since then, it diversified its financing sources, leveraging the cross-government ODA-eligible Prosperity Fund for the Digital Access Programme (DAP), and mobilising the UK's Conflict, Stability and Security Fund (CSSF) to establish the Cyber and Tech Programme in 2018.
- The **Korea** Internet & Security Agency (KISA), under the remit of the Ministry of Science and ICT, established in 2015 the Global Cybersecurity Center for Development (GCCD) as its primary vehicle for financing and delivering CCB actions in developing countries. Additionally, KISA provides grant-making support to IFIs, such as the World Bank and the IADB. In 2023, using the Korea-ASEAN cooperation fund, KISA also launched the ASEAN Cyber Shield initiative to nurture cybersecurity experts across the region.
- **Australia**'s Department of Foreign Affairs & Trade (DFAT) established its Cyber and Critical Tech Cooperation Program (CCTCP) in 2016 as the main vehicle for financing CCB efforts aimed at strengthening cyber and critical technology resilience across the Indo-Pacific. Australia has also collaborated with the Pacific Islands Forum and its Member States to establish the Pacific Fusion Centre in Vanuatu in 2021. The Centre provides Pacific countries with strategic analysis, information sharing, and capacity building support on security issues, including cyber threats. In 2023, Australia also announced the creation of Pacific 'Cyber Rapid Assistance for Pacific Incidents and Disasters' (RAPID) teams to respond to cyber crises as they occur in the Pacific, when governments in the region request assistance.
- **Singapore** launched the ASEAN Cyber Capacity Programme (ACCP) in 2016 to enhance the cybersecurity capacities of ASEAN Member States. In 2019, the ACCP was extended with the inauguration of the ASEAN-Singapore Cybersecurity Centre of Excellence (ASCCE), a multi-disciplinary research and training facility.
- Utilising the Japan – ASEAN Integration Fund (JAIF 2.0), **Japan** set up the ASEAN-Japan Cybersecurity Capacity Building Centre (AJCCBC) in 2018. Established in Bangkok under the management of the National Cyber Security Agency (NCSA) of Thailand and the Japan International Cooperation Agency (JICA), the Centre offers training and services to enhance the cybersecurity expertise of public sector staff and critical information infrastructure operators across the region. Under its Digital for Development Global Agenda, JICA has also developed a dedicated technical cooperation programme to support partner countries strengthen their cybersecurity response capabilities, in line with its 'Cluster Strategy for Cybersecurity' and the priorities set in the Government's 2021 'Basic Policy on Cybersecurity Capacity Building Support for Developing Countries'.
- **New Zealand**'s Ministry of Foreign Affairs and Trade (MFAT) established the Cyber Security Capacity Building in the Pacific Programme in 2019, supported in its implementation by CERT NZ, the Department of Internal Affairs, and the Cabinet Office.
- **France** established the Cyber National School with Regional Vocation in Dakar in 2021, in partnership with Senegal, to deliver cyber training primarily to public officials from Central and Western Africa, as well as from other African sub-regions requesting support. Similarly, in 2023, France and Slovenia launched the Western Balkans Cyber Capacity Center (WB3C) in partnership with

Montenegro to reinforce the institutional and operational capacities in the region.

- **Germany**'s Federal Foreign Office created the Partnership for Strengthening Cybersecurity in 2023 as a key vehicle to advance cyber capacity-building and cooperation internationally. The programme started with a regional focus in the Western Balkans, Eastern Europe, West Africa (ECOWAS), and continental Africa (African Union). Germany is also one of the founding donors of the World Bank's Cybersecurity Multi-Donor Trust Fund, established in 2021.
- **Qatar** has financed the establishment of the UNODC Regional Centre for Combatting Cybercrime (UNRCCC) in Doha which was launched in 2023 to support Member States' capacity development in the identification, prevention, investigation, prosecution, and adjudication of cybercrimes.

Key Take-Away: Donor Governments

To date, government donors primarily use grants and technical assistance for their international cyber capacity-building actions. These implementation modalities are commonly employed to provide advice in the development of cyber-related national strategies, regulations and legislation; to finance policy fellowships and study trips; and support the establishment or strengthening of operational capacities on cybersecurity (e.g., Computer Security Incident Response Teams, CERTs/CSIRTs) and cybercrime (e.g., high-tech crime units). However, these approaches have certain limitations in terms of the impact, scalability, and sustainability of results the can achieve.

At the same time, there is a growing focus on financing digital infrastructure and connectivity projects, including through donor government instruments, such as the European Fund for Sustainable Development Plus EFSD+, USAID's Digital Invest. These mechanisms leverage guarantees, loan subsidies, and blended finance to improve the mobilisation of private sector financial resources for digital development projects in partner countries. With cyber capacity needs increasing globally and digital governance issues becoming increasingly complex, donor governments could expand the use of implementation modalities for cyber projects, for example through the use of sector budget support and blended finance to improve partner countries' cybersecurity capacities, governance, and service delivery.

Donors could also pursue locally led development in their cyber cooperation both as a principle, in order to increase the use of local implementing partners, but also as an objective, to support local cybersecurity ecosystems and markets, and nurture home-grown cybersecurity talent and services. Moreover, donors should fully incorporate cyber resilience as a (sub-)priority within any digitally-enabled investment. Systematising such measures can help CCB transition from rather niche foreign assistance funds to more mainstream development financing. In turn, this shift can enable an ecosystem-wide approach to cyber resilience cooperation and meaningfully support local cyber development.

Development Banks

While ad hoc technical cooperation initiatives around cybersecurity strategy development and critical information infrastructure protection by IFIs can be traced back to the 2000s, a more systematic engagement and investment in CCB actions is more evident after 2015. This period saw an uptake in cybersecurity-related long-term loans, advisory services, grants, and equity investments by multilateral development banks (MDBs). Notable cases include:

- The **World Bank:** The Bank's work on CCB entails both lending operations, with loans to partner countries aimed at improving their cybersecurity posture, and grant-based

activities designed to help countries strengthening their ability to absorb cybersecurity-specific lending or incorporate cyber resilience in digital investment projects. Under the second category, the Bank's Global Cybersecurity Capacity Program ran between 2016 and 2021 (phases 1 and 2), financed by the Korea-World Bank Group Partnership (KWPF) with KISA and Oxford University's Global Cyber Security Capacity Centre (GCSCC) as key implementers. Concurrently, the Bank established the Digital Development Partnership (DDP) umbrella programme with a dedicated cybersecurity window. In response to growing demand for cybersecurity support, the Bank launched a dedicated Cybersecurity Multi-Donor Trust Fund (MDTF) in 2021 to assist low- and middle-income countries. Funded by Estonia, Germany, Japan and the Netherlands, the MDTF includes country-based and sector-based programmes, with a focus on knowledge building.

- The **Inter-American Development Bank (IADB)**: In 2017, the IADB developed a strategic plan for supporting cyber capacity-building in Latin America and the Caribbean. This includes combining a lending programme, which enables government-owned multi-year development plans for enhancing cyber resilience, with donor-funded grants for technical cooperation projects in support of the loan operations. In 2018, the IADB approved its first purely cybersecurity-focused lending operation with a loan to Uruguay to enhance the country's capacity to prevent, detect, and respond to cyberattacks. Other countries have followed suit. In parallel, the IADB has been mainstreaming cybersecurity across its vertical sectors especially on infrastructure-focused industries, such as energy and transportation. These efforts are mainly co-financed from the Bank's national and sectorial envelopes, along with in-kind contributions in expertise from its cybersecurity team.
- The **European Bank for Reconstruction and Development (EBRD):** The EBRD has committed to leveraging digital transition as a driver of sustainable economic growth through its financial instruments and technical cooperation. Its 2021 Digital Approach emphasised the importance of building cybersecurity capacity for digital projects across its sectors of activity. The EBRD Digital Hub, established in 2022, leads this effort with a dedicated advisory programme to enhance the cybersecurity resilience of its clients, especially critical infrastructure operators and those undergoing significant digital transformation. Additionally, through its financial investments portfolio, the EBRD also invests in the private sector of partner countries to foster the growth of local cybersecurity industries and contribute to locally sustained change.
- The **African Development Bank (AfDB):** The AfDB has focused to date primarily on strengthening the cyber resilience of the fintech sector. A key initiative includes a grant to establish the African Cybersecurity Resource Center (ACRC) for Financial Inclusion in Dakar, Senegal. The ACRC aims at bolstering the resilience of digital financial ecosystems across Africa. It is mobilising the blended finance instrument Africa Digital Financial Inclusion Facility which is expected to run until 2030 in order to accelerate digital financial inclusion throughout the continent. Initial donors and partners in this effort include the Agence Francaise de Développement (AfD), the French Ministry of Economy and Finance, the Ministry of Finance of the Grand Duchy of Luxembourg, and the Bill and Melinda Gates Foundation.
- The **Asian Development Bank (ADB):** The ADB's Digital Technology for Development approach recognises cybersecurity as a critical safeguard for unlocking the potential of digital transformation. The Bank promotes the incorporation of cybersecurity regulations and standards through its lending operations with targeted technical assistance. For example, it has supported efforts to strengthen sub-national level cybersecurity ecosystems across selected states in India as part of the digitalisation of government services.

Key Take-Away: Development Banks

To date, IFIs engaging on cyber-specific actions and investments are primarily Multilateral Development Banks, which finance relevant activities for both the public or the private sectors in low- and middle-income countries. In contrast, numerous bilateral Development Finance Institutions (DFIs) – often majority-owned by national governments – invest primarily in private sector development to spur job creation and sustainable economic growth.

However, there is limited reporting on their engagement in the cybersecurity field, even though digital transformation is an emerging priority. Integrating cybersecurity into their portfolios, either as a cross-cutting issue or as a stand-alone sector, could contribute to a more holistic financing architecture for cyber resilience in developing countries. When combined with the investments of MDBs and the assistance of government donors – that often focus on technical assistance for the analogue foundations of strategic, regulatory, and institutional capacities and reforms – it can enhance support for comprehensive cyber resilience.

Philanthropy

Several philanthropic organisations are also engaging as cyber capacity-building funders most often focusing on research, the creation of scalable knowledge resources and toolkits, training courses, and fellowships. While substantive information on the interaction of local philanthropy with CCB is limited, foundations with a global footprint that address digital and internet issues, in recent years have expanded their activities to CCB. The positioning of philanthropic organisations often allows them to build trust among partners and provide alternative sources of financing. Some notable examples of CCB investment by international foundations include:

- The **Asia Pacific Network Information Centre (APNIC):** The Internet address registry for the Asia-Pacific region allocates a significant portion of its budget towards CCB initiatives, such as the APNIC Academy. Its affiliated APNIC Foundation, established in 2016, facilitates fundraising to support technical assistance and grants for actions in the region. The Information Society Innovation Fund (ISIF Asia) serves as the Foundation's main grants and awards mechanism, supporting infrastructure, inclusion and knowledge projects in the region. ISIF Asia was originally set up as a partnership among APNIC, the Internet Society (ISOC), and the International Development Research Centre (IDRC).
- The **Bill and Melinda Gates Foundation:** The Foundation has financed cybersecurity-related actions under its Inclusive Financial Systems programme, which aims to expand access to digital financial services for lowest-income communities worldwide. It has partnered with CREST International, the standards certification organisation, to support local markets address the growing cyber risks in digital financial services. Additionally, it has collaborated with MITRE Engenuity to develop a comprehensive cyber threat model for mobile financial services in developing countries. The Foundation has also provided a grant to the GFCE to develop training modules for the Member States of the African Union and to enhance CCB coordination in the region through the establishment of the Africa CCB Coordination Committee.
- The **Citi Foundation** addresses cybersecurity through its institutional priorities on youth unemployment and innovation. Indicatively, it has partnered with the Organization of American States' Cybersecurity Program to finance cyber skills-building projects such as the Creating a Career Path in Digital Security during 2017-2023, as well as training courses for the Young Americas Business Trust to support Latin America's low-income urban youth pursue careers in cybersecurity.[11] The Citi Foundation has also financed the OAS

Cybersecurity Innovation Fund together with Cisco.

- **Google.org**, serving as Google's philanthropic arm, is financing the APAC Cybersecurity Fund that aims to reinforce the local cybersecurity ecosystems and communities by focusing on equipping underserved micro and small businesses, non-profits, and social enterprises with cybersecurity skills across 13 countries in the Asia-Pacific region. In addition, the project has a regulatory reform strand that focuses on supporting policy dialogues and localised research, as well as the piloting of two university-based cyber clinics in Pakistan and Singapore – similarly to the Consortium of Cybersecurity Clinics for the public good it has been financing in the United States. This initiative is implemented by the Asia Foundation in partnership with the CyberPeace Institute and the Global Cyber Alliance.
- The **Hewlett Foundation's** ten-year Cyber initiative (2014-2023) provided numerous grants aimed at building a more robust and multidisciplinary cyber policy field to help guide decision-makers through a rapidly evolving problem area. Some of its funding addressed international CCB, notably grants to the Carnegie Endowment for International Peace's Cyber Policy Initiative, the Global Cyber Alliance, and the Centre for Internet and Society (CIS) in India.
- The **Mastercard Center for Inclusive Growth** advances sustainable and equitable economic growth and financial inclusion around the world, often tackling cyber resilience as a horizontal aspect. Examples include its financing of training, certification and job placement programmes on cybersecurity skills with partners in-country, as well as the funding international civil society organisations with a cybersecurity mission, such as the Global Cyber Alliance and its Cybersecurity Toolkit for Small Business, the Cyber Peace Institute, and the Cyber Readiness Institute.

Key Take-Away: Philanthropy

In general, large philanthropic organisations engaged in traditional development and humanitarian sectors, as documented in the OECD's Development Co-operation Profiles, have not yet made any or significant investments in CCB. However, the use cases above highlight a significant opportunity to promote to integrate cyber resilience as a horizontal priority in digital economy initiatives. This could involve promoting the responsible and secure use of digital technologies and the creation of the relevant enabling analogue foundations, or mainstreaming cybersecurity skills within digital literacy and workforce programmes.

Furthermore, given that only a few philanthropic institutions have cybersecurity as a priority area, such as the Hewlett Foundation (until 2023) and Craig Newmark Philanthropies (e.g., its Cyber Civil Defense initiative), there is potential to explore how to leverage the resources, products, and tools they have financed domestically and adapt them for use by partner countries and organisations in the Global South.

Private Sector

The private sector plays multiple roles within the international CCB ecosystem, and acting as a funder in CCB activities is one of them. Prominent industry partners that finance CCB initiatives typically include technology-focused companies central in shaping cyberspace, such as those in the ICTs, cybersecurity, and telecommunications sectors, as well as entities from the financial and banking sector. Their motivation for financing CCB stems from corporate social responsibility but is also driven by priorities such as cybersecurity talent development, regulatory advocacy, and government relations.[12] In these efforts, the private sector often collaborates with others, primarily governments and multilateral

organisations. The **main types of CCB activities** financed by the private sector in low- and middle- income countries to date include:

> developing cybersecurity toolkits (e.g., for small and medium enterprises),

> establishing in-person cybersecurity training academies,[13]

> delivering training courses for a wide range of stakeholders (e.g., national, and regional authorities, schools and universities, vulnerable groups, civil society), including capture-the-flag competitions,

> offering tailored programmes and fellowships for women to increase their participation in the cybersecurity workforce,[14]

> conducting awareness raising campaigns for the general public or specific groups,

> providing equipment and software for training, instructional, or exercise platforms (e.g., Cyber Ranges),

> supporting actions aimed at fostering local cybersecurity innovation ecosystems.[15]

In addition to direct funding, the private sector also contributes to strengthening cyber resilience in the broader ecosystem through **indirect contributions**:

> Several technology companies have set up their own free online cybersecurity training platforms and programmes that are open to any individual,[16] as well as public-private tech hubs in partner countries that include specific cybersecurity components.

> Industry associations and alliances offer cybersecurity policy resources, technical advisory guides, and training courses[17] that are either available to everyone, or tailored to their membership base, including small and medium enterprises.

> Several private sector companies provide in-kind contributions, such as pro bono capacity-building programmes for government and academic entities, which include evaluating product security and integrating cybersecurity courses into degree programmes at no cost.

> Some multinational companies finance research products, guides, and compendia that serve as thought leadership resources for the global community,[18] while also enhancing the evidence base on the cybersecurity landscape and needs in developing countries and regions[19].

Key Take-Away: Private Sector

CCB initiatives in low- and middle-income countries financed by corporate entities most often are connected to their corporate social responsibility portfolio or cyber workforce development programmes, or they are ad hoc grants to key CCB actors. Given that the private sector is a driver of job creation and economic growth, untapped potential remains for sustainable partnerships on CCB between the private sector, governments, and other development actors. Businesses can bring access to new financing and partnership opportunities that could scale up cybersecurity solutions.

In fact, the slow but steady uptake of cybersecurity in development cooperation presents an opportunity for more cyber-related or cyber-adjacent investments by the private sector, particularly as it plays a pivotal role in **blended finance mechanisms**. This involves leveraging the strategic use of development finance to mobilise additional investments, including commercial capital from the private sector for digitalisation projects that contribute to sustainable development in developing countries.[20] This modality is relevant to CCB given that critical connectivity and digital infrastructure initiatives[21] must integrate cybersecurity-by-design.

Partner countries and regions ('recipients')

The partner nations and regions that engage in bilateral or regional cyber cooperation interventions are the key players in building effective CCB partnerships.[22] A significant

amount of work is undertaken by **nations within their own ecosystems and with their own resources**, either through initiatives with a digital focus (e.g., digital literacy, and STEM education) that incorporate cybersecurity elements, or through actions directly targeting cyber issues (e.g., cyber hygiene and national cybersecurity strategies).

Therefore, it is critical to ensure that external CCB initiatives align to national efforts and respond to the capacity needs of partners. Ideally, CCB should be integrated into national development processes and dialogue, though this is not always the case. One reason for this shortcoming is the slow connection of the international cyber capacity-building efforts with broader sustainable development goals. Many donors and implementers in this field originated from diplomatic, international security, ICT security, and law enforcement communities. As a result, linking up with the national development authorities in partner countries, or leveraging the expertise and implementation know-how of development cooperation partners has often been neglected.[23] However, this is gradually changing on the ground. Digital transition is becoming a strategic national development priority for many low- and middle-income countries, thus increasing the awareness of governments about the cross-cutting role of cyber resilience. At the same time, the rapid growth of digital development investments and initiatives is bringing the development and cyber capacity-building communities of practice closer together, particularly when operating within the ecosystem of a partner country.

In general, most CCB actions to date have focused on institutional capacity development within the national and regional contexts in which they operate. Consequently, the main actors engaging in and benefiting from international CCB in partner countries are competent **national Ministries and Agencies within central governments** across a range of issues such as cybercrime, cybersecurity, cyber diplomacy, among others. These are notably the Ministries of ICT/Digitalisation, Ministries of Interior/Security, Ministries of Justice, Ministries of Foreign Affairs, Ministries of Defence, National Cybersecurity Authorities, National CERTs/CSIRTs, ICT regulators, and Law Enforcement Agencies.

In practice, the linkages between cyber issues necessitate broad support across government. The adoption of a **whole-of-government approach** that brings together ministries and services is optimal for achieving meaningful CCB outcomes. Equally, the interconnected nature of cyberspace – where the private sector, the technical community, cybersecurity experts, civil society and academia have distinct and vital roles in its technical management and governance – makes multi-stakeholder perspectives invaluable. Their perspectives bring diverse insights from different angles and expertise on cyber issues, threats, policies, and their impact. As such, **multistakeholder involvement and collaboration** across the national ecosystem in the planning, design, and implementation of CCB are essential for shaping initiatives, fostering an enabling environment for cyber resilience, and achieving sustainable results. When donors support the partner government in pursuing and leading a **whole-of-society approach**, multiple benefits arise. It enhances accountability, creates space for valuable insights and adaptations in the CCB process, and lays the groundwork for engaging the multi-stakeholder community in implementing CCB activities.[24]

> **The local private sector** (e.g., tech companies, network operators, critical infrastructure providers, among others) and **technical community** (e.g., existing sectorial and organisational CERTs/CSIRTs beyond the national one, and national or regional internet registries) provide essential knowledge in supporting countries assess their overall level of cyber resilience, inform on emerging cyber threats, share information on cyber incidents, and build partnerships for cybersecurity workforce development. Similarly, in-country **civil society and academia** are crucial partners, not only for the expertise they bring to the ecosystem but also in promoting transparency and strengthening trust. Finally, **parliamentarians** play a key role in shaping national policy and legislation, while **local authorities** often have large service-delivery responsibilities to citizens. However, to date, few CCB actions have applied concrete strategies or developed workstreams to engage these two groups systematically and effectively.

Key Take-Away: Partner Countries

Understanding the global CCB landscape should be complemented by an appreciation of the **national and regional CCB ecosystems**. These ecosystems require strengthened engagement from funders and partner governments with the multistakeholder community to ensure that CCB initiatives are inclusive and responsive to the needs of all stakeholders. Achieving this requires **sustained leadership from partner governments**, supported by both donors and implementers, to create a space for inclusive dialogue and meaningful CCB coordination that leverages local knowledge, capacity, and expertise.[25] Partner countries can connect such processes with their existing development coordination structures, and enhance efficiencies by **mainstreaming cyber resilience into their national development agenda**. This approach allows externally funded CCB actions to contribute strategically rather than being carried out as ad hoc actions. In the same vein, donors and implementers have the responsibility to ensure that CCB actions align with national priorities and that their outcomes are captured within national systems.

To further bolster sustainable financing for cyber resilient development, partner countries should collaborate with development partners and experts to meaningfully include cybersecurity into the design, implementation, and review of their Integrated National Financing Frameworks (INFFs).

Implementers

Entities responsible for or contributing to the implementation of cyber capacity-building range from government agencies and bodies in the public sector, the private sector, the technical community, and civil society organisations.

Government Agencies

Many donor governments utilise authorities within their ranks as implementing partners, especially when they bring thematic expertise from national cybersecurity authorities, regulators, criminal justice bodies, and national research institutes. On one hand, this approach facilitates peer-to-peer learning with a strong public sector focus, fostering peer networks and long-term relationships between implementing and beneficiary authorities. On the other hand, while more specialised cyber entities possess unique thematic expertise, they often lack in-depth experience in international cooperation management and methodology. Examples of government agencies serving as CCB implementers include:

- The Australian Department of Foreign Affairs and Trade (DFAT) partnered with the Australian Federal Police (AFP) to implement the Cyber Safety Asia Programme which aims to develop cybercrime investigations skills and enhance capabilities within ASEANAPOL agencies, in collaboration with the Singapore Police Force (SPF). The Australian Attorney-General's Department leads the implementation of technical assistance for Pacific countries in revising domestic legislative frameworks to combat cybercrime, in line with the Council of Europe Convention on Cybercrime.[26]
- The Estonian Ministry of Foreign Affairs runs the Tallinn Summer School of Cyber Diplomacy.
- The EU engages national cybersecurity authorities from its Member States such as the Estonian Information System Authority (RIA), which implements the EU Cyber Capacity Building Network (EU CyberNet).[27]
- India leverages its National Security Council Secretariat to deliver exercises and training sessions in multilateral settings, such as the Group of 20 (G20) and the Shanghai Cooperation Organisation (SCO).
- JICA combines its own cybersecurity experts with the deployment of Japanese and locally hired experts and companies to deliver

cybersecurity technical cooperation programmes in partner countries.

- The Netherlands implements a training programme promoting CSIRT maturity and Critical Information Infrastructure Protection (CIIP) through its National Cyber Security Centre (NCSC-NL) across different regions, namely in Southern Africa, Western Balkans and the Indo-Pacific.
- The Republic of Korea places the Korea Internet & Security Agency (KISA) at the centre of its CCB implementation and coordination efforts. However, for cybercrime training courses it relies on the Supreme Prosecutors' Office and the Korean National Police Agency which also implements a Fellowship Programme funded by the Korea International Cooperation Agency (KOICA).
- Through the 'U.S. Transnational and High-Tech Crime Global Law Enforcement Network (GLEN) program', the Department of Justice deploys experienced U.S. law enforcement experts abroad as long-term mentors to deliver sustained training to partner countries. The Department of State utilises institutions such as the George C. Marshall European Center for Security Studies to deliver cyber policy training courses to officials from all over the world. Additionally, the U.S. State Department manages several cyber-related interagency agreements to leverage U.S. Government expertise in the implementation of technical assistance and training activities in partner countries (e.g., Departments of Commerce, Homeland Security, and Defence).[28]

International Organisations

International organisations have direct access to governments and are traditional implementing partners. While they primarily rely on extra-budgetary donor funding for CCB actions, their established relationships with governments allow them to champion country priorities and support the development of country-owned policies and initiatives. Several UN agencies and other international organisations play a key role in this context, notably:

- The **International Telecommunication Union (ITU)**, as the UN's specialized agency for ICTs, has been at the forefront of capacity-building activities, with origins in the World Summit on the Information Society (WSIS) held in 2003 and 2005. One of the action lines agreed upon at WSIS was building confidence and security in the use of ICTs. This led to the launch of the ITU Global Cybersecurity Agenda in 2007, which identified capacity building as one of its five pillars. ITU began implementing CCB activities in 2010, funded through a combination of donor contributions and its regular budget. The pursued CCB actions relate to ITU's core mandate to support its Member States, and particularly developing countries, strengthen their national cybersecurity capabilities. ITU also receives extra-budgetary resources for specific donor-funded projects. Its cybersecurity programme primarily focuses on: strengthening national incident response capacities; supporting national cybersecurity strategy and policy development; cyber skills development; online safety initiatives; and data and advocacy activities, such as the Global Cybersecurity Index which aims to enhance the cybersecurity evidence base and be a globally trusted resource.
- **The United Nations Institute for Disarmament Research (UNIDIR)** pursues capacity-building activities in the context of international ICT security through its Security and Technology Programme (SecTec). This entails three core areas: research on cyber policy, norms, international law and threats, and capacity building; participatory learning activities, including the annual Cyber Stability Conference, ad hoc thematic seminars, clinics, training modules, table-top exercises and scenario-based simulations; and facilitated access to information, primarily through the continued update of UNIDIR's Cyber Policy Portal.
- **The United Nations Development Programme (UNDP)** integrates cybersecurity into its broader digital programmes, which mainly entail digital infrastructure, digital literacy, and e-governance. UNDP tries to ensure that capacity building initiatives in the digital domain indirectly support cybersecurity by promoting secure and

resilient digital solutions. For instance, it introduced the Digital Readiness Assessment (DRA) to help partner countries assess their digital landscape and prioritise interventions in their digital transformation. It also supports digital literacy and safety skills development programmes and training courses, awareness raising campaigns, innovation, and digital entrepreneurship, as well as the development of regulatory and institutional cybersecurity frameworks.

- **The United Nations Office on Drugs and Crime (UNODC)** established its Global Programme on Cybercrime in 2013, under a mandate provided by the General Assembly resolution 65/230 and the Economic and Social Council's Commission on Crime Prevention and Criminal Justice resolutions 22/7 and 22/8. UNODC's programme provides technical assistance and training to Member States to prevent and respond to cybercrime and technology-enabled crimes. It takes a holistic approach to capacity building, addressing the full circle of cybercrime prevention, detection, investigation, prosecution and sentencing or adjudication.
- **The International Criminal Police Organization (INTERPOL)** has been implementing capacity building projects that address cybercrime challenges since the 2010s. In 2015, INTERPOL inaugurated its Global Complex for Innovation in Singapore, which serves as a key platform for their capacity building actions globally.
- The **Commonwealth Telecommunications Organisation (CTO)** assists its Member States in developing and implementing national cybersecurity strategies, protecting critical information infrastructure, and establishing national incident response teams.

Regional Organisations

The importance of the regional context in fostering meaningful and effective international cooperation is well established. The same holds true for CCB, where regional organisations to date have played a critical role. There is an unparalleled value in sharing regional experiences, learning from each other, and fostering policy and operational cooperation. As a result, many CCB funders rely on regional organisations as implementers, and these organisations, in turn, have developed internal capacities and structures to deliver CCB programmes.

It is important to note that while all regional organisations have the convening power to bring together their Member States and address cyber issues through policy dialogue, workshops, and exercises, such activities relate to their respective core mandate. As such, it is distinct from their role as implementers of extra-budgetarily funded CCB actions. Below are examples of regional organisations that lead the implementation of CCB programmes:

- The **African Union (AU)** has leveraged its mandate to convene relevant stakeholders for CCB and to create platforms for knowledge exchange and coordination at the continental level. Several donors and development actors have partnered with the AU to deliver CCB activities, notably through its Commission, including its Departments of Infrastructure and Energy and Political Affairs, Peace and Security, as well as affiliated bodies such as the African Union Development Agency-NEPAD (AUDA-NEPAD) and expert groups. Numerous events and workshops covering a wide range of cyber issues are undertaken by the AU in partnership with key donors. Examples of supported projects include the Policy and Regulation Initiative for Digital Africa (PRIDA) – a joint initiative of the AU, the EU, and the ITU; the AU-GFCE Cyber Capacity Building project funded by the Bill and Melinda Gates Foundation which led to the creation of the Africa Cyber Capacity Building (CCB) Coordination Committee in 2021; and the Partnership for Strengthening Cybersecurity implemented by GIZ on behalf of the German Federal Foreign Office that has seconded a principal cyber diplomacy officer to the AUC's Political Affairs, Peace and Security Department in 2024.
- The **Association of Southeast Asian Nations (ASEAN)** plays a critical role as a convener of its Members States and its Dialogue Partners, facilitating regional CCB initiatives. The 2021-2025 ASEAN Cybersecurity Cooperation Strategy identifies regional cyber capacity-building as a key priority, with a focus on "multi-disciplinary, modular, multi-

stakeholder and measurable programmes". ASEAN leverages regional centres that have been specifically established to support the implementation of capacity building efforts in a coordinated and complementary manner. These include the ASEAN–Japan Cybersecurity Capacity Building Centre (AJCCBC) set up in Bangkok, Thailand in 2018, and the ASEAN–Singapore Cybersecurity Centre of Excellence (ASCCE) established in Singapore in 2019, while a more recent addition is the ADMM Cybersecurity and Information Centre of Excellence (ACICE), created in 2021 to focus on cyber confidence-building measures, enhancing information-sharing, and capacity building among ASEAN defence establishments, following approval by the ASEAN Defence Ministers.

- The **Council of Europe (CoE)** has been implementing CCB projects since the early 2000s. It has a dedicated Cybercrime Programme Office (C-PROC) in Bucharest, Romania to assist countries worldwide in strengthening their criminal justice capacities on cybercrime and electronic evidence. This includes support for enhancing legislation on cybercrime and electronic evidence in line with the rule of law and human rights (including data protection) standards; training judges, prosecutors, and law enforcement officers; establishing specialised cybercrime and forensic units and improving inter-agency cooperation; promoting public/private cooperation; protecting children against sexual violence online; enhancing the effectiveness of international cooperation. C-PROC became operational in April 2014 and has since supported well over 2200 activities for more than 130 countries globally. The CoE depends on extra-budgetary resources to implement projects and has mobilised more than EUR 60 million external funds until the end of 2023, mainly from the European Union,[29] and voluntary contributions by the USA, the United Kingdom, Japan, Canada, the Netherlands, Estonia, and others.
- The **Organization of American States (OAS)** has an active Cybersecurity Program under the Inter-American Committee against Terrorism (CICTE/OAS) since 2003. It has developed various initiatives and support programmes for Member States to build technical, political, and diplomatic capacities to prevent, identify, respond to, and recover from cyber incidents, as well as to promote responsible behaviour by States in cyberspace. Its work focuses on supporting the development, updating and implementation of national cybersecurity strategies; establishing national CERTs/CSIRTs; fostering collaboration through the CSIRT Americas Hemispheric Network; and providing tailored technical assistance and training opportunities, as well as the OAS/CICTE Cyber Diplomacy Training Program, which offers specialised courses for officials in charge of cyberspace issues in the OAS Member States.
- The **Organization for Security and Co-operation in Europe (OSCE)** has a key focus on the development of confidence building measures (CBMs) between participating States to reduce the risks of conflict stemming from the use of ICTs. With a regional scope that covers South-Eastern Europe, Eastern Europe, the South Caucasus, and Central Asia, the OSCE participating States have adopted sixteen such measures since 2013. When implemented these constitute concrete tools to enhance interstate transparency, communication, and cooperation in cyberspace. The cyber capacity-building activities of the OSCE led by the Transnational Threats Department are intrinsically tied to its CBMs mandate, and focus on strengthening the participating States' institutional and operational capabilities to implement the CBMs through technical assistance, training courses, table-top exercises, and e-learning. The OSCE also supports the development of national cybersecurity strategies and implements programmes to enhance the capacities of police officers and prosecutors on cybercrime and digital evidence, as well as on cyber diplomacy to support national delegates meaningfully engage in and contribute to UN and OSCE processes on international cyber policy.

Development Banks

While the primary function of most development banks with cybersecurity as a practice area is financing through lending operations (e.g., AfDB, IADB, World Bank – see *funders section*), some also serve as administrators and implementers of donor-funded grants. They often use such grants for CCB activities to provide technical assistance in support of their loan operations (e.g., conducting maturity assessments), to create knowledge tools and resources (e.g., cybersecurity strategy development guides), to finance developing countries' participation in international cyber-related convenings, and to implement other tailored activities.

Private Sector

Private sector entities are among the leading implementers of CBC projects financed by others. The diversity of companies engaged reflects the wide range of expertise within the private sector, from general consultancy firms with project management expertise, to specialised companies on different cyber technical or regulatory issues. In an attempt to categorise them, the main groupings include:

- Professional services companies (e.g., Deloitte, EY, KPMG).
- Consultancies with a niche expertise on a specific cyber dimension (e.g., Cyber Law International).
- Cybersecurity companies, ranging from multinationals to small and medium-sized enterprises with international CCB experience (e.g., NRD Cybersecurity, PGI, CyberCX).
- Security and defence companies (e.g., BAE Systems).
- Development consultancies and service providers for international cooperation (e.g., DAI, GIZ, Stantec).

Technical Community

A diverse technical community forms the backbone of the Internet's functioning and governance. This community comprises of technical entities and experts (e.g., network engineers, designers, developers, researchers, and incident responders) who play a critical role in maintaining the structural integrity and security of the Internet. This broad community includes network operators, Internet registries, Internet standards development organisations,[30] and cybersecurity incident management response teams (CERTs/CSIRTs) and their networks.

Since the early days of international cyber cooperation, the development of national incident response capacities has been a CCB priority, with significant engagement from CERTs/CSIRTs and their networks in the implementation of CCB actions. The Forum of Incident Response and Security Teams (FIRST) is a leading organisation in this community, with a global network of almost 600 national and organisational CSIRTs. FIRST facilitates collaboration and capacity building of its members through informal exchanges, conferences, as well as training, mentorship, and fellowship programmes. Regional CERT/CSIRT networks also play a crucial role in delivering CCB activities, particularly technical training sessions and cybersecurity exercises. Notable examples include the Asia Pacific Computer Emergency Response Team (APCERT), the Task Force on Computer Security Incident Response Teams (TF-CSIRT) in Europe, the Pacific Cyber Security Operational Network (PaCSON), the Oman-ITU Arab Regional Cyber Security Center (ARCC), and the Organisation of the Islamic Cooperation Computer Emergency Response Team (OIC-CERT). Additionally, many donor governments leverage their national CERTS/CSIRTs as implementers of their CCB activities (see earlier section).

Crucially, the collaborative culture of the technical community, rooted in shared technical knowledge and trust, has enabled it to navigate geopolitical tensions rather effectively and contribute meaningfully to advancing international cooperation on cybersecurity.[31]

Civil Society, Academia, Think Tanks

Civil society, academia and think tanks bring significant expertise and are uniquely positioned to implement impactful projects across a broad range of themes.

- Examples of **think tanks** working on CCB focusing on research, project implementation, or both, include: the Australian Strategic Policy Institute (ASPI),

the Royal Institute of International Affairs (Chatham House), the EU Institute for Security Studies (EUISS), the Norwegian Institute of International Affairs (NUPI), Research ICT Africa (RIA), RAND, the Royal United Services Institute (RUSI), the Observer Research Foundation (ORF), among others.

- Examples of **universities** engaging in CCB actions include: Carnegie Mellon University's Software Engineering Institute (SEI), the Australian National University (ANU), Monash University, the Rajaratnam School of International Studies (RSIS), Oxford University's Global Cyber Security Capacity Centre (GCSCC), and the University of Exeter, among others.
- Examples of **civil society organisations** implementing CCB actions include: the Association for Progressive Communications (APC), DCAF – Geneva Centre for Security Sector Governance, the Diplo Foundation, the e-Governance Academy (eGA), the Global Cyber Alliance (GCA), Global Partners Digital (GPD), and the ICT4Peace Foundation, among others.

Key Take-Away: Implementers

It is evident that most of non-government implementers financed to lead the delivery of CCB are of Western representation which fosters North-South power asymmetries. CCB actions anchored in development practice (often within digital access programmes) frequently incorporate local NGOs and private sector entities as project partners or subcontractors. However, there is no consistent trend to date indicating that CCB initiatives systematically support local stakeholders in developing their own capacity to deliver CCB. There is a big opportunity for CCB donors to promote a **'localisation agenda in CCB'**[32] particularly given the existing constraints in the available cyber expertise of implementing organisations in the Global North,[33] provide technical assistance at scale, and respond to ever increasing capacity building needs.[34]

This can be achieved by:

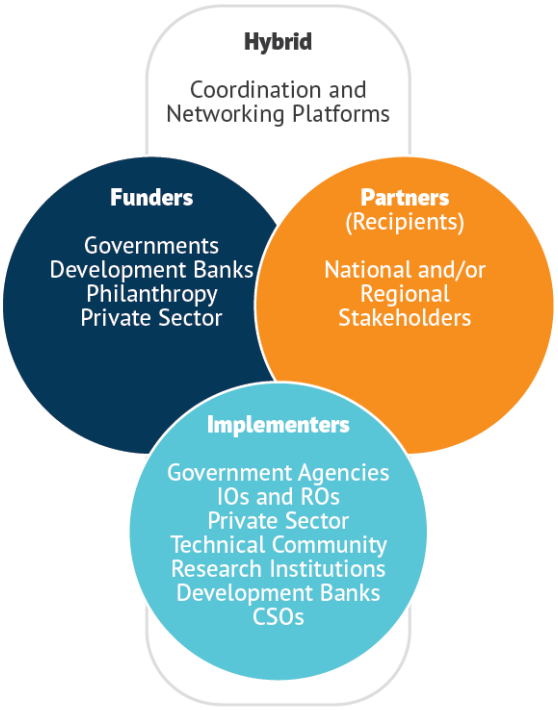
1. utilising local implementing partners (for example, Smart Africa and CyberSafe Foundation);
2. addressing structural barriers to local access to funding;
3. adapting sustainable partnership models with local actors; and
4. (d) considering diverse implementation modalities beyond traditional technical assistance and capacity building.

Hybrid actors

A ***hybrid*** category of actors exists whose activities' centre of gravity does not squarely fall under any of these three, as they serve as coordinating, networking, and aggregating platforms. The Global Forum on Cyber Expertise (GFCE) is the most prominent such actor internationally.

The GFCE is an apolitical multistakeholder community of over 200 members and partners including governments, international and regional organisations, the private sector, civil society, and academia. It is dedicated to the global coordination and promotion of CCB. Since its creation in 2015, the GFCE has occupied a unique position within the global CCB ecosystem by building a large multistakeholder community that facilitates and coordinates CCB efforts through neutral and bottom-up approaches. It enhances coordination through its thematic Working Groups and Regional Hubs, facilitates knowledge sharing and improves transparency of CCB efforts with its Cybil Portal, connects assistance requests with support or resources through its Clearing House mechanism, and supports thought leadership through its Research Agenda (*see details in Box 2*). The GFCE hosts an Annual Meeting open to its community and all interested stakeholders. It is also the main organiser of the Global Conference on Cyber Capacity Building (GC3B) series, which was launched in Accra, Ghana in November 2023 and

Figure 1. Interplay of the CCB ecosystem



Source: Authors' compilation

shall continue in Geneva, Switzerland in May 2025.

Moreover, the **Cybersecurity Alliance for Mutual Progress (CAMP)** was launched by the Korean government in 2016 as a mechanism for the Republic of Korea to share its expertise with a wide group of partner countries, facilitate knowledge exchange, and support their capacity development efforts. CAMP is implemented by KISA and its main activities include an Annual Meeting and Regional Forums. As of November 2024, it includes organisations from 52 countries.

Finally, the **Internet Governance Forum (IGF)** is an annual multistakeholder policy dialogue forum mandated by the UN to facilitate the discussion of Internet-related public policy issues and to promote the exchange of information and best practices. The IGF hosts a dedicated Best Practice Forum (BPF) on Cybersecurity which conducts analysis and offers thought leadership on various cyber policy challenges through the cooperation of its members. While it does not address CCB per se, the IGF is a platform where ad hoc exchanges on CCB take place depending on the submission of relevant sessions by the IGF community.

Box 2: The Global Forum on Cyber Expertise (GFCE)

Key contributions of the GFCE to the cyber capacity-building ecosystem include:

- The Cybil Portal is a global, open, neutral, multistakeholder, free knowledge-sharing portal that includes an extensive mapping of existing CCB actions, and a repository of resources (tools and publications) that funders, CCB project designers, recipients, and implementers can use. Currently, it includes information close to 950 projects and 400 tools and publications, allowing CCB actors to gain a baseline understanding of projects in a specific country or region. Updates to the Portal are primarily provided by the multistakeholder GFCE Community. By improving access to such information, Cybil enhances evidence-based approaches to CCB and fosters greater transparency.
- At the geographical level, the GFCE better connects national and global level initiatives and processes through its regional coordination function. It has **five Regional Hubs and liaisons** in Africa, the Americas and Caribbean, Europe, the Pacific, and Southeast Asia that support needs analysis, regional coordination, and delivery of capacity building support. The GFCE's regional coordination approach, in partnership with relevant regional organisations, offers efficiencies, as countries within a region tend to share similar priorities and can reach a mutual understanding, agreement, or way forward. Recognising that trust between implementers and beneficiaries is necessary for sustainable and long-term outcomes, the GFCE actively engages with regional organisations,

centres, and key leaders to bolster regional efforts.

- The GFCE also promotes knowledge exchange and coordination at the thematic layer, through working groups focused on different CCB themes, namely: Cybersecurity Policy and Strategy, Cyber Incident Management and Critical Infrastructure Protection, Cybercrime, Cybersecurity Culture and Skills, Emerging Technologies, and gender mainstreaming and inclusivity as a cross-cutting theme. These working groups share information on projects and good practices that are integrated in Cybil, foster peer-to-peer learning, and identify knowledge gaps. These gaps inform the GFCE's Research Agenda, which entails policy research projects that aim to support thought leadership and further professionalise the CCB community.
- The Clearing House is a GFCE tool that facilitates matchmaking between GFCE Members with cyber capacity needs and GFCE Partners and Implementers that can, in turn, offer cyber capacity support. Through practical coordination, it seeks to enable meaningful cooperation at the national level and improve efficiency in the delivery of CCB programmes.

Key Take-Away: Hybrid Actors

In general, the value added of multi-stakeholder platforms of a hybrid nature that serve as a convenors and aggregators of structured dialogue, relationship- and trust-building, knowledge exchange, and collaboration, lies in their ability to bring together a wealth of experience, lessons, and ideas. When curated effectively, these platforms can co-create smart solutions, spur innovative thinking, and inspire effective actions. Due to the cross-cutting nature of cyber issues across policy areas and the multi-stakeholder governance of cyberspace, it is only logical to invest in inclusive, diverse, and result-oriented partnerships and platforms for CCB. Hybrid actors have the potential to create the enabling space for 'whole-of-cyber-ecosystem,' and 'whole-of-society' engagement in order to share lessons, foster collaboration, improve ways of working, as well as challenge the orthodoxies in CCB practices. These efforts, aimed at achieving impactful and sustainable results, have the potential to positively shape the evolution of the international CCB ecosystem and drive its further professionalisation.

To date, the GFCE is the only multi-stakeholder vehicle on CCB with a global reach that brings together diverse interests and connects with practitioners on the ground at regional and national levels. This unique positioning enables the GFCE to mature into an impactful aggregator, provided it strengthens its links with different communities and thematic networks particularly those in the development field. By doing so, it can further promote informed policy dialogue and action, facilitate bottom-up coordination to reduce transaction costs, and incubate improved CCB approaches.

Dual role actors

At a closer look, we observe some actors fulfil two functions, usually with one function being at the centre of gravity. For example, a development bank serves primarily as a funder but at times also directly implements CCB projects; or a donor authority may serve as a funder and an implementer. In this complex environment, the most important **'dual role' actors** shaping the CCB ecosystem are **'dual character countries'** that are both receivers and providers of CCB. These

countries – such as Brazil, Colombia, India, Mexico, Morocco, Thailand[35] – are engaging in cyber South-South and Triangular Cooperation.[36] They are uniquely positioned to co-create CCB solutions with their partners and share good practices based on their experience in overcoming challenges during in their cyber maturity trajectory.

Key Take-Away: Dual Role Actors

South-South and Triangular Cooperation can enable flexible, cost-effective, and innovative solutions through effective knowledge and technology transfers among partners, informed by experiences developed under similar socioeconomic realities. In various fora addressing CCB, such as the UN OEWG, the GFCE, and the GC3B, South-South and Triangular Cooperation have been highlighted as important processes that can offer meaningful and diverse opportunities for cyber capacity development. While several examples of such initiatives exist, the CCB community has yet to fully embrace this approach and share the drawn lessons, while donor governments have also been slow in exploring the consistent incorporation of Triangular Cooperation in their CCB efforts.

Other cyber communities contributing to CCB

The cyber capacity-building ecosystem cannot be considered in isolation from the broader cyber ecosystem and the thematic (or 'parent')[37] communities that form its complex architecture. While earlier sections attempted to provide a systematised overview using the functions of different actors in CCB as a way to categorise them, it is essential to acknowledge the immense contributions of multiple communities that address various dimensions of cyber policy, operational, and technical issues and challenges. Actors within these thematic communities are guided by their overarching mission (e.g., cyber threat intelligence, digital forensics, professional cybersecurity certification, cybersecurity standard-setting, or human rights assessments on cybersecurity policies and practices) and work to enhance cybersecurity by creating solutions on their own or by working with others.

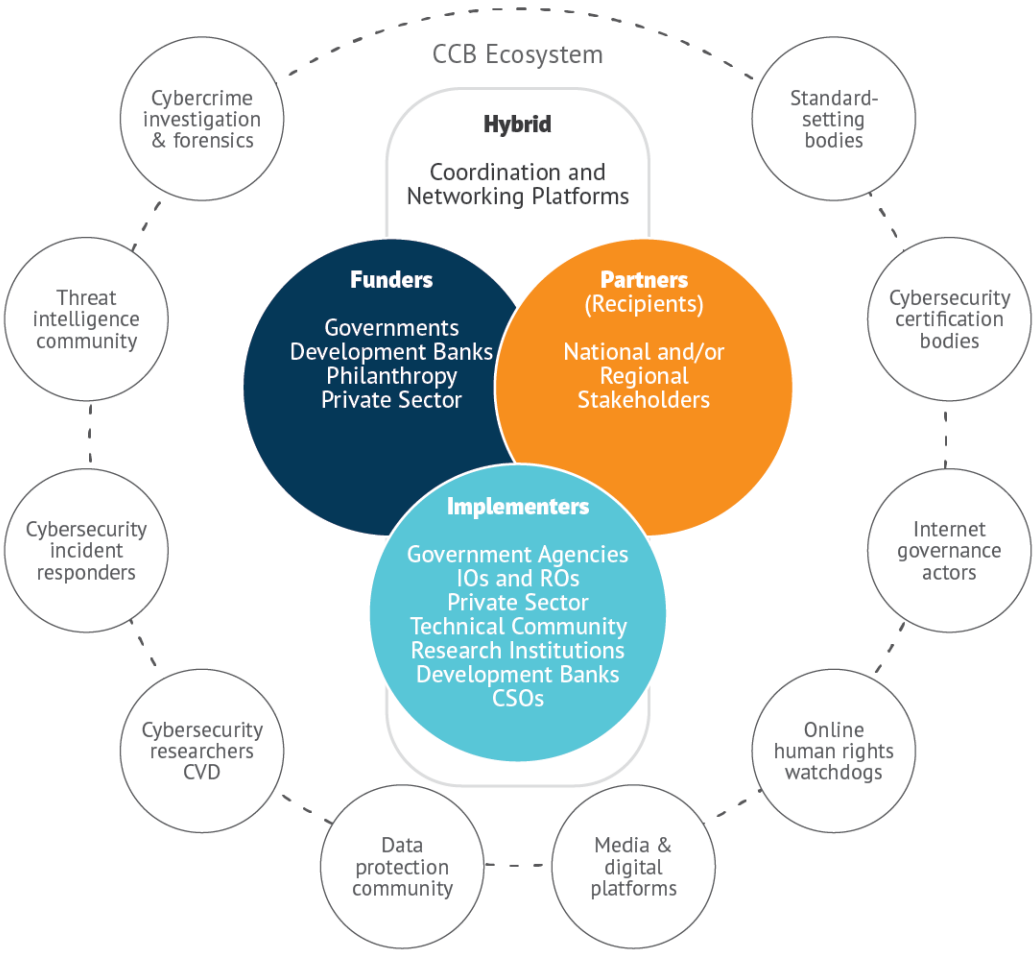
As a result, the broader cyber ecosystem generates a vast array of knowledge tools, products, services, and expertise that serve as **'global public cyber goods'** and are available for use by international cyber capacity-building programmes. A few illustrative examples include:

- The training courses created by ICANN on Domain Name System (DNS) threats and internet security hygiene, along with policy and operational advice on safety and security issues on the internet provided by its Governmental Advisory Committee (GAC).
- The freely available tools and solutions created by the Global Cyber Alliance (GCA) to reduce cyber risk for organisations and individuals, such as the GCA Toolkit for Mission-Based Organisations.
- The cyber threat intelligence of the Shadowserver Foundation that is offered for free to national CERTs/CSIRTs.
- The guides and tools designed by CREST for organisations to assess their vulnerability and resilience to cybersecurity incidents, as well as its guidance for national regulators to help the private sector incorporate cybersecurity standards.
- The guides and tools by Access Now and the Electronic Frontier Foundation on digital security and online digital surveillance self-defence. absolute

Within this broad category of contributors, efforts are underway to aggregate existing resources, raise awareness of 'global public cyber goods,' and support sustainable models for cybersecurity. Prominent examples include:

> The Nonprofit Cyber coalition unites non-profit organisations that develop, share, deploy, and promote cybersecurity best practices, tools, standards, and services. Coalition members have compiled an index of their cybersecurity resources.

Figure 2. Contribution of the broader cybersecurity ecosystem to cyber capacity-building



Source: Authors' compilation

> The Global Cyber Alliance has launched the Actionable Cybersecurity Tools (ACT) wiki as a user-friendly directory of cybersecurity tools and resources tailored for diverse stakeholder groups (e.g., journalists, small businesses, parents).

> The Common Good Cyber initiative, launched by a coalition of cybersecurity non-profit organisations to elevate the recognition of their role within the global cyber ecosystem, has created a database of free cybersecurity tools, services, and platforms.

Key Take-Away: Broader cyber communities

In general, while some of the actors from the broader cybersecurity ecosystem may directly engage in CCB as partners, more often they contribute indirectly by delivering on their core missions. Enhancing connections between these efforts will be crucial to improve CCB efficiency. A key challenge is that different initiatives within the cybersecurity ecosystem and its thematic sub-

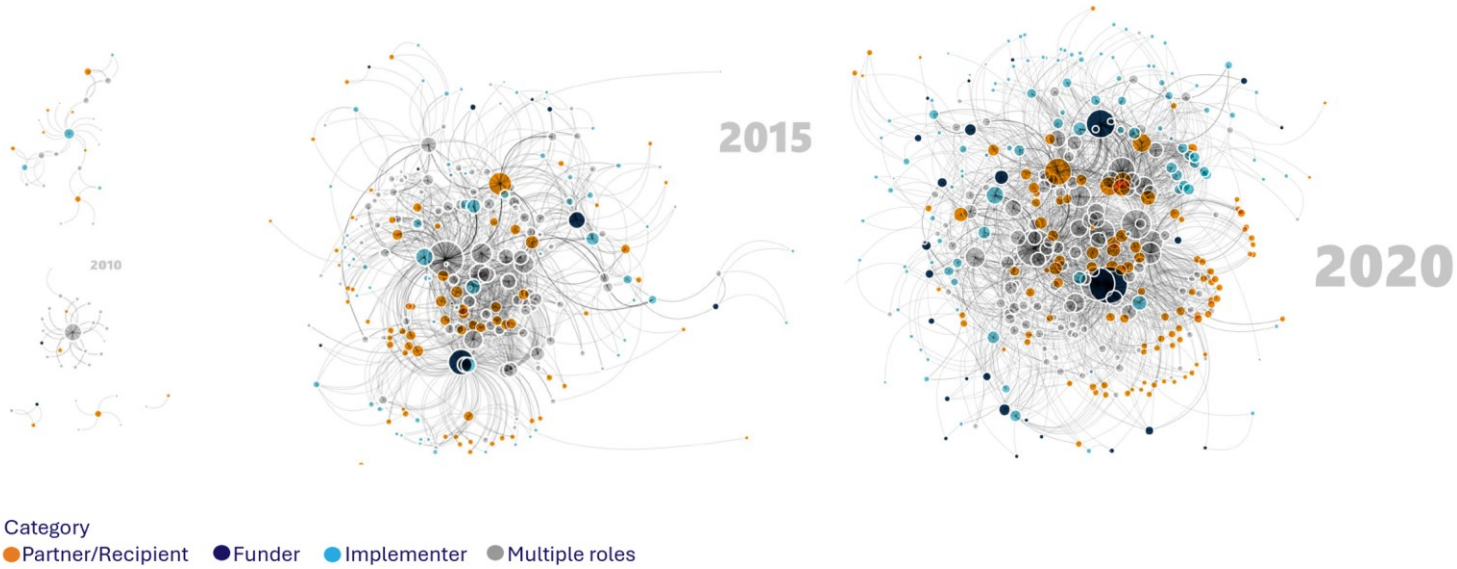
communities rarely align their individual strengths into collaborative action for the good of the broader cyber ecosystem. Efforts to combine the resources and strengths of **non-profit organisations** are a notable exception to this challenge. On the one hand, driven by a commitment to the common good, several non-profits develop and expand free, practical cybersecurity solutions that can be particularly useful for the CCB community and for supporting under-resourced governmental bodies, small enterprises, and civil society groups. On the other hand, collaborative initiatives that connect non-profits and their resources, such as Nonprofit Cyber and Common Good Cyber, show how other groups of cyber stakeholders and sub-communities can cooperate to enhance cyber capacities. However, further efforts and funding are needed to improve the inclusivity and diversity platforms such as the Cybil Portal, the ACT wiki, and the mapping of Common Good Cyber that are invaluable for centralising knowledge resources but originate predominantly from the Global North and offer resources almost exclusively in English.

KEY DIMENSIONS IN THE GLOBAL CCB ECOSYSTEM EVOLUTION

The multiplicity of actors in international cyber capacity-building reflects the diversity of stakeholders engaged in cyberspace issues, combined with the layer of international and development cooperation. Considering the growing relevance of cyber issues in the public policy realm and in the practical aspects of digitalisation, key reflections on the CCB ecosystem's evolution over the last decade can provide a baseline for shaping the next generation of CCB. This evolution is characterised by an **'expansion'** across three dimensions:

- **Expanded CCB ecosystem in numbers:** The number of projects, stakeholders across the world (Figure 3), and invested funds in CCB has drastically grown in the past decade. Early-mover donors have steadily increased their financial contributions, while new funders – including the development cooperation sector – have started contributing more[38] and bringing in new implementers. This increases the diversity in CCB approaches as each actor applies the practices and culture of its respective community, creating additional complexities to coordination.
- **Expanded CCB ecosystem in scope:** The most common areas of CCB interventions ten years ago – notably cybercrime, national cybersecurity strategies, and the development of CERTs/CSIRTs – have evolved overtime to include more advanced activities (e.g., trans-border cyber exercises drills). Additionally, new priority themes have emerged, including critical infrastructure protection, cyber diplomacy, cyber workforce development, and women in cybersecurity. As the cybersecurity aspects in digital infrastructure and new and emerging technologies gain prominence, the scope of CCB actions has further expanded, blurring its conceptual boundaries.[39] This complicates efforts to establish a common narrative, coordinate actions, and prioritise resources.
- **Expanded CCB approaches:** While traditional technical assistance focused on supporting the development of national cybersecurity strategies, cybercrime legislation, and CERTs/CSIRTs, the current CCB ecosystem encompasses different approaches in its implementation. There is an increase in the establishment of regional CCB centres,[40] fellowships and mentor programmes, partnerships with the private sector, loans from development banks, and in integrating human rights-based and gender-responsive approaches in the design and delivery of CCB actions. However, the limited available expertise to meet increasing capacity demands requires further adaptation and expansion of approaches, implementation modalities, and partnerships to enhance the scalability of CCB actions and improve their effectiveness and sustainability.

Figure 3. CCB Actors' Evolution



Source: International Cyber Capacity Building: Global Trends and Scenarios, EUISS, 2021

These shifts, when viewed outside the global geostrategic context, could be interpreted as positive, provided that mitigating measures are in place to address emerging complexities. Yet, we are operating within a multipolar world order characterised by divergent worldviews on the future of cyberspace and its governance, conflicting digital development models, and heightened geopolitical tensions amidst global economic uncertainty and multiple cascading crises. These factors need to feed into our collective thinking about the future of cyber capacity-building.

CAPACITY BUILDING IN A FRACTURED CYBER WORLD

Changes in the political, economic, and social context over the past decade have significantly influenced the evolution of the cyber capacity-building (CCB) ecosystem and the field of cyber capacity-building more broadly. The increasing divergence of views on the future of cyberspace has led to the emergence of new donors beyond the traditional ones. The politicisation of issues previously considered purely technical has intensified competition in the field of development assistance, including cyber-related projects. Additionally, the use of cyber operations as tools for conflict, espionage, or interference in the democratic processes of other countries has prompted certain donors to recalibrate their funding priorities, shifting towards enhancing cyber resilience and defence capabilities.

The economic context has also undergone significant changes. Political polarisation has raised questions about existing models of international trade. The focus on economic recovery in the aftermath of the COVID-19 pandemic, combined with growing domestic needs driven by high inflation, has affected the funding available for cyber capacity-building. Meanwhile, emerging donors have leveraged their economic track records, supported by financial aid and loans, to promote their own models of development, including in the digital domain. This has led to the emergence of new policy concepts such as "digital sovereignty," "de-risking," "decoupling," and "onshoring," linking CCB to broader geopolitical debates about technology transfers, industrial policies, raw materials, and environmental protection.

Furthermore, the emphasis on digital transformation as a pathway to post-COVID recovery has drawn significant attention to digitalisation projects. The resurgence of digitalisation efforts in development cooperation has resulted in new funding for initiatives focused on building information infrastructure and improving access to technology for delivering

public services, including digital public infrastructure. Ensuring the sustainability of such projects, in line with the foundational development cooperation principle of "do no harm," has prompted new approaches to cybersecurity. Cybersecurity is increasingly viewed not as a cost but as an investment and a prerequisite for the success of digitalisation projects. Reducing digital risks to these investments across supply chains has become a new trend in international cooperation.

Ultimately, these developments and the growing use of cyber capacity-building as a foreign policy instrument have reflected geopolitical dynamics and led to a more fragmented CCB ecosystem. Two dimensions of this fragmentation – ideological and operational – are particularly relevant to the future of cyber capacity-building efforts. Their negative impact on coordination efforts poses a significant challenge, resulting in inefficient use of already scarce resources. Striking a balance between these dimensions and agreeing on practical, actionable approaches to developing and implementing capacity-building programmes is essential for closing the cybersecurity capability gap, enhancing global cyber resilience, and advancing international security and stability.

Ideological fragmentation

Although states agree in principle on the importance of an open, free, global, safe, and secure cyberspace, their visions of what these ideals mean in practice often diverge. These differing interpretations are particularly evident in discussions surrounding the UN Framework of Responsible State Behaviour (FRSB) and its implementation. Policies introduced at the national level or agreed upon regionally become tangible expressions of these varying – and sometimes conflicting – visions. As governments enact laws to regulate data flows, access to information, or cybersecurity standards, they inevitably translate abstract principles into specific rights and obligations for citizens, companies, and other entities under their jurisdiction.

Cyberspace has increasingly become an arena for interstate conflicts. It is used either as an enabler for conducting kinetic operations (e.g., disabling radar systems), as a vector for incapacitating critical infrastructure (e.g., energy or transportation sectors), or as a tool for conducting hybrid and interference operations. Additionally, debates over internet governance and the future of cyberspace have become battlegrounds for states with diverging views on the future of digital society. In other words, cyberspace is not a borderless domain. Its borders are drawn and redrawn through ideological and political battles, making it an increasingly geopolitical construct.

Consequently, decisions regarding cyber capacity-building investments, programme designs, and implementation modalities are also influenced by geopolitical considerations. The emergence of new donors and funding institutions with differing methodologies and approaches has created new opportunities for countries seeking alternatives to traditional development assistance, which often involves strong conditionalities or stringent implementation, monitoring, and reporting obligations. As a result, cyber capacity-building and digital development projects have become more competitive.

Operational fragmentation

Ideological differences are not the sole drivers of fragmentation in cyber capacity-building (CCB). Another significant factor is operational fragmentation, driven by three key trends: the growth of the CCB community, the use of CCB by more communities of practice to pursue their objectives, and the widening gap between the aspirations for and realities of CCB coordination. The evolving boundaries and content of cyber capacity-building have heightened institutional and financial differences among donors, ultimately undermining deeper coordination and cooperation within the ecosystem.

Operational fragmentation stems from a fundamental paradox: while funding for cyber capacity-building remains limited and dispersed among numerous stakeholders in the CCB ecosystem (beyond traditionally defined donors), the expanding scope of CCB introduces new institutional logics, missions, and interests that hinder closer coordination and efficient resource utilisation. This challenge is further compounded by the proliferation of digital transformation projects, which are frequently designed and

implemented without adequate cybersecurity risk mitigation strategies.

Moreover, reconciling the differing objectives of digital transformation and cyber capacity-building, through de-risking and mainstreaming cybersecurity, is complicated by the absence of clear procedures and guidelines, as well as intra-institutional politics. At the same time, the emergence of new issues across cyber agendas – such as hybrid threats, disinformation, or AI-related risks – introduces new communities with distinct institutional identities and missions. This diversification contributes to further diffusion of responsibilities and potential conflicts among policy communities (e.g., human rights, law enforcement, foreign policy, development).

These factors highlight the increasing need for innovative partnerships among diverse stakeholders in the capacity-building ecosystem, including more prominent involvement of multilateral financial institutions, investors, and the private sector.

Implications of fragmentation for cyber capacity-building

There are no indications that the ideological and operational tensions underlying these forms of fragmentation will be resolved in the near future. However, with the international community placing cyber capacity-building (CCB) at the centre of discussions in the Open-Ended Working Group (OEWG) and the forthcoming Regular Institutional Dialogue, states must address these tensions and propose practical, actionable measures to foster robust CCB efforts. These efforts should be grounded in international principles and enhanced coordination, including engagement with the multi-stakeholder community.

The implications of ideological and operational fragmentation for principle-based[41] cyber capacity-building efforts are significant and warrant careful consideration:

- **Ownership:** While openness, trust, and mutual respect are widely recognised as core elements of effective partnerships for development goals, these principles are not currently reflected in the environment of cyber capacity-building. Ideological fragmentation means that funding decisions often aim to align donors and partners around shared worldviews and visions of cyberspace, rather than addressing the actual needs identified by partners. This approach can undermine the sense of ownership over CCB initiatives. The 2021 OEWG report emphasises that capacity-building activities should support "the shared objective of an open, secure, stable, accessible, and peaceful ICT environment."[42] Yet, in the absence of a universal definition of these concepts, stakeholders must interpret them in practical terms. Ideological fragmentation complicates the pursuit of CCB activities that are "politically neutral, transparent, accountable, and without conditions."
- **Results-Orientation:** Ideological fragmentation can lead to a disconnect between donor-identified priorities and the actual needs of partners. Diverging donor values and interventions may result in certain needs being overlooked, leaving societies more vulnerable. For instance, networks built using equipment deemed risky by certain donors may reduce their willingness to invest in related CCB projects. Initiatives like the EU's Global Gateway or the Blue Dot Network, which promote quality infrastructure investments, may deter donors from engaging in countries that participate in alternative frameworks, such as China's Digital Silk Road. Additionally, operational fragmentation leads to inefficiencies through duplication of efforts and poor coordination, placing undue burdens on partners who must navigate conflicting donor interests and expectations.
- **Inclusive Partnerships**: Effective implementation of a whole-of-society approach requires the participation of all stakeholders across the CCB ecosystem. However, ideological, and operational fragmentation impede this inclusivity. For example, ideological fragmentation has restricted non-governmental actors' participation in UN debates and limited market access for certain service providers and companies deemed high-risk. This fragmentation has also exacerbated disparities between "donor darlings" and "orphans." While political considerations

have long influenced development cooperation – such as decisions on programming priorities and project design – geopolitical competition and security concerns have made these challenges more pronounced. For instance, in response to Russia's invasion of Ukraine, many European donors have redirected significant resources to Ukraine, Moldova, Georgia, and the Western Balkans.

- **Transparency and Accountability**: The stronger influence of values and worldviews on CCB decisions impacts the transparency and accountability of project priorities and implementation. Political considerations can skew risk assessments, potentially ignoring or misrepresenting certain risks. The diffusion of responsibility between political and operational levels further reduces transparency around specific decisions, undermining accountability in the medium to long term.[43] Similarly, while political motivations drive donor support, partners' decisions are influenced by broader political considerations and alliances. The issue linkages and bargaining that emerge during this process significantly affect partners' cost-benefit analyses and contribute to less transparent and accountable CCB processes.

Different authors have proposed alternative approaches to conceptualise the future of cyber capacity-building (CCB).[44] This paper examines the interplay between ideological and operational fragmentation, resulting in four scenarios for the future of CCB (see Figure 4):

- **Zone of Confrontation:** A high level of ideological fragmentation, driven by competition between blocs of states, amplifies operational fragmentation, leading to suboptimal outcomes due to poor coordination among donors. Partner countries are theoretically in the driver's seat, as competition among donors creates an abundance of offers. However, this often results in a "race to the bottom," where partner countries prioritise short-term gains over long-term benefits. This dynamic is further fuelled by ad hoc coalitions and ideologically motivated alliances. For donors, this environment does not necessarily foster partnerships based on thorough needs assessments. Disagreements over the role of non-governmental actors persist, while international institutions and organisations become arenas for contesting ideals and worldviews. This scenario reflects the current trajectory of CCB.

- **Zone of Stability and Prosperity**: A low level of ideological fragmentation presents a significant opportunity for operational alignment among donor groups, consistent with the principles of effective development. International organisations become forums for dialogue, enabling the international community to chart a collective path forward. Greater donor alignment promotes principles-driven CCB efforts focused on delivering results. Coordination among donors supports needs-driven funding decisions, allowing partner countries to prioritise effectively rather than engaging in "donor shopping." Duplication is minimised through enhanced transparency about funding and better information sharing, facilitated by coordination platforms. The whole-of-society approach, embraced by all donors, strengthens the role of non-governmental stakeholders, fostering inclusive partnerships. This inclusivity injects additional human and knowledge resources into CCB projects. Greater transparency enhances accountability, including that of donors.

- **Zone of Stability:** While low levels of ideological fragmentation create favourable conditions for stakeholder cooperation, operational fragmentation persists due to challenges such as poor coordination, intra-institutional politics, and traditional hurdles in international development. The absence of ideological conflict among donors simplifies engagement with partner countries, aligning efforts with universally agreed principles. However, duplications persist due to inadequate information flows and poor coordination during project design and programming stages. Donors' independent needs assessments contribute to partner fatigue and resource inefficiency. Although the low level of ideological confrontation facilitates the involvement of non-governmental actors, their participation remains uneven, with preferences for low-

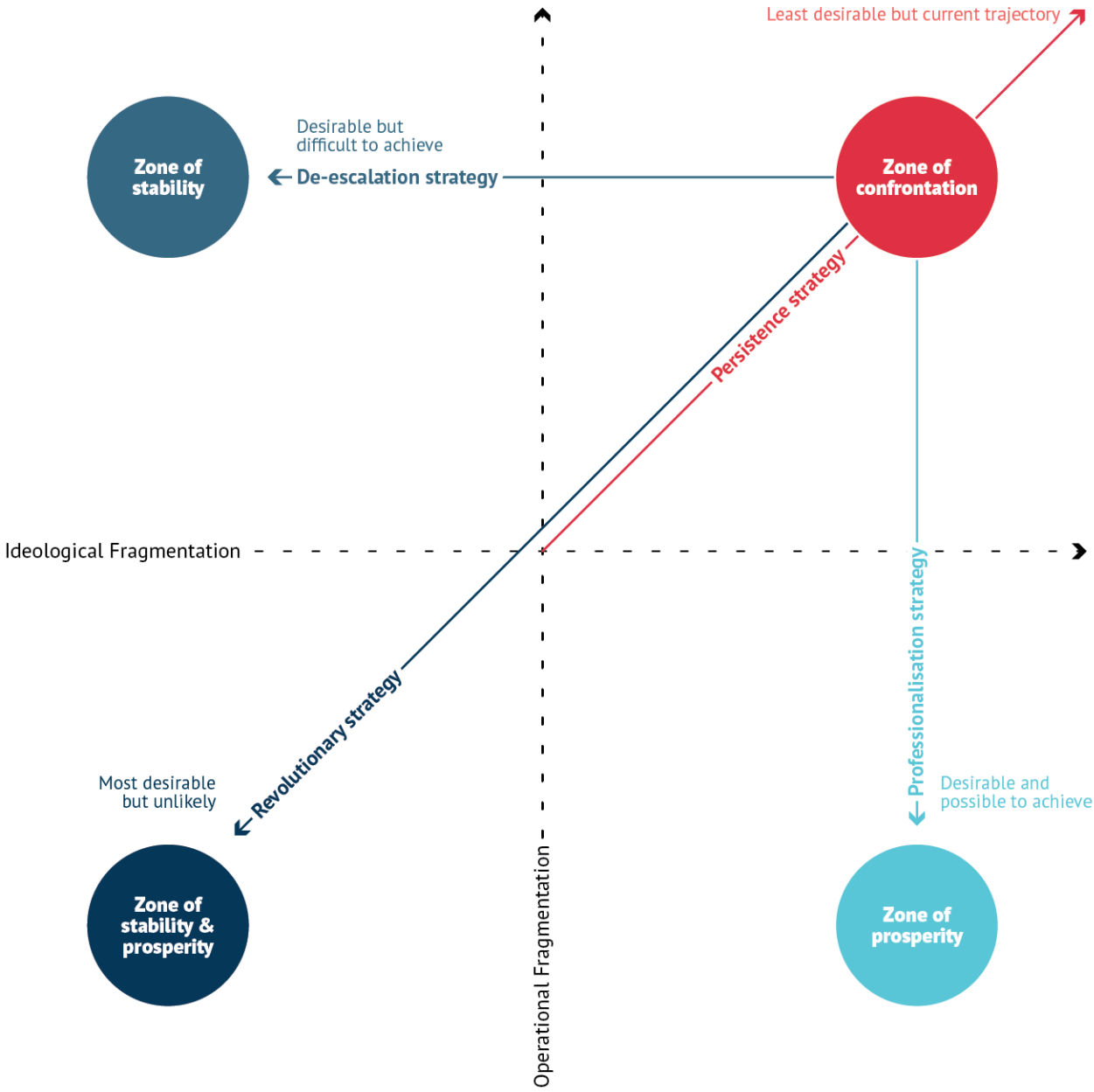
Figure 4. Implications of ideological and operational fragmentation for cyber capacity-building

Source: Authors' compilation

risk partners, particularly in the private sector and tech companies. Nonetheless, the reduced ideological fragmentation provides opportunities for establishing accountability standards and reviewing CCB working methods.

> **Zone of Prosperity**: Despite persistent ideological fragmentation, the status quo in CCB becomes untenable due to the accelerating digital transformation and the development of digital public infrastructures. Emerging disruptive technologies such as AI and quantum computing exacerbate cybersecurity challenges, particularly for developing countries seeking expertise. To address these challenges, the CCB ecosystem adopts measures to reduce inefficiencies through greater professionalisation. While ideological divisions continue to pressure partner countries into choosing among competing offers, operational-level

Figure 5. Strategies for navigating ideological and operational fragmentation in cyber capacity-building



Source: Authors' compilation

cooperation among capacity-building communities helps mitigate some negative effects of donor competition. Transparency in funding decisions and consideration of partner needs remain limited. Partner countries can still engage in "donor shopping," though improved knowledge-sharing mechanisms, such as repositories and portals, help reduce negative consequences. While CCB partnerships are not always inclusive, some donors maintain strong commitments to multistakeholder cooperation and whole-of-society approaches. Ideological fragmentation continues to foster coalitions of like-minded countries.

MOVING FORWARD: STRATEGIES FOR MANAGING FRAGMENTATION

The field of cyber capacity-building (CCB) has matured significantly over the past decade, with notable advancements in its goals and working methods.[45] The future trajectory of CCB will largely depend on the ability of the community to learn from past experiences and adapt to an evolving geopolitical landscape.

A key distinction between the options proposed in this paper and those identified in earlier studies on CCB trends is the explicit acknowledgment of geopolitical forces and inter-state competition as central factors influencing cyber capacity-building. Accordingly, the central argument of this paper is that many challenges in CCB will require solutions rooted in political dialogue at the international, domestic, and institutional levels.

The strategies outlined below (see Figure 5) provide a framework for addressing ideological and operational fragmentation and steering CCB towards a more desirable future. Given that the de-escalation and professionalisation strategies are the most practical and probable scenarios, this section offers detailed recommendations for action at the UN, regional or bilateral, and national levels.

Persistence strategy

The high level of ideological fragmentation in contemporary cyber capacity-building stems from the current geopolitical landscape, characterised by intense competition among major digital powers, low levels of trust due to inter-state conflicts involving key global players (including P5 members), the proliferation of divergent visions for the future of cyberspace that often conflict with existing approaches to internet governance, and the ineffectiveness of international organisations traditionally tasked with mediation and conflict resolution.

This geopolitical context and the associated ideological differences also influence operational decisions in cyber capacity-building, resulting in low levels of coordination, duplication of efforts, and inefficient resource utilisation. The increasing prevalence of conflicts with a cyber dimension further drives investment in cyber resilience and defence initiatives. This reflects the current trajectory, with the "zone of confrontation" emerging as the most likely outcome – a trend already evident today.

The strategy of persistence for individual actors involves maintaining or intensifying confrontational policies and approaches. While such an approach may align with value-driven perspectives – such as the need for proponents of a human-centric approach to digital transformation to advocate for and defend their principles in international and bilateral arenas – it also perpetuates the politicisation of cyber capacity-building. This politicisation leads to inefficient resource allocation and minimal coordination, imposing additional burdens on partner countries.

As a result, international organisations and bodies that provide guidance or funding for cyber capacity-building risk becoming battlegrounds for clashing visions of cyberspace, leading to paralysis in their operations. This scenario may eventually drive capacity-building efforts into ideologically aligned venues dominated by coalitions of like-minded states.

Revolutionary strategy

Avoiding permanent fragmentation and the "zone of confrontation" requires a significant departure from the current trajectory of international relations and a paradigm shift in the implementation of cyber capacity-building initiatives. Addressing the challenge of ideological fragmentation, which stems from broader conflicts among major international players over the future of digital societies and cyberspace, would necessitate ideological and value-based alignment between current competitors – if not entirely, then at least regarding their shared vision for cyberspace.[46]

A revolutionary strategy would also demand a complete overhaul of operational approaches to cyber capacity-building, including much closer coordination of activities and concrete methods for deconflicting interventions by different

donors. In this scenario, international organisations would serve as platforms for identifying the most effective ways to foster cooperation, including through the active involvement of non-governmental actors. Partner countries would assume a more prominent role, actively shaping the global capacity-building agenda and investment priorities through meaningful participation in international venues.

While a comprehensive political and operational transformation in cyber capacity-building is highly improbable, two alternative strategies – de-escalation and professionalisation – could partially address existing challenges and incrementally improve the functioning of the CCB ecosystem.

De-escalation strategy

Effectively mitigating political polarisation and ideological fragmentation is one of the central challenges on the path toward achieving a "zone of stability." The de-escalation strategy envisions the implementation of measures to foster a degree of ideological convergence despite ongoing geopolitical tensions. The widespread recognition of cyber capacity-building as a priority for the international community offers a valuable starting point for this approach.

Ongoing efforts by UN agencies such as the ITU and UNDP, with their broader focus on enhancing cyber resilience within the development agenda, play a crucial role in this context. However, detaching these efforts from the broader political landscape and the ongoing debate about responsible state behaviour remains challenging. Consequently, discussions within the OEWG on establishing a future permanent mechanism will form an essential piece of this puzzle.

To advance the conversation, it is critical to focus on cyber confidence-building measures, which can provide a framework for mitigating escalation risks and clarifying differing views, positions, and policies. Identifying who should lead and how such measures should be implemented is another matter. While the participation of key players is vital, the experience of the OEWG demonstrates that leadership and active engagement from Global South countries can be instrumental in bringing conflicting parties to the negotiating table. The proliferation of various platforms for discussing cyber-related issues within the UN and other forums suggests that ample opportunities for dialogue exist.

Box 3. Options for the implementation of the de-escalation strategy

UN level

Establish a Mechanism for Regular Dialogue

Create a mechanism to facilitate ongoing dialogue on the framework for responsible state behaviour in cyberspace. This could leverage existing UN structures to clarify key stakeholders' positions on terminology and potential threats. The outcomes of discussions in the current OEWG on a permanent mechanism and the proposed Cyber Programme of Action will be pivotal. A unified, single-track approach will better support the de-escalation strategy. This initiative should also align with de-escalation efforts led by other UN agencies (e.g., ITU, UNDP) or broader digital processes like the Global Digital Compact and SDG Digital, which encompass wider mandates beyond international security.

Promote Global Confidence-Building Measures (CBMs)

Encourage the implementation of global CBMs, such as those outlined in the Initial List of Voluntary Global Confidence-Building Measures (Annex II to the 2024 Annual Progress Report of the OEWG).

Consider developing new CBMs to address emerging challenges and strengthen international trust and collaboration in cyberspace.

Systematise the OEWG's Work

Organise the OEWG's current body of work into a structured framework to identify issues spanning from full consensus to full divergence. Divergent topics should be addressed separately in smaller thematic groups, such as "Friends of the Chair," tasked with mapping conflicting issues. Topics with broader consensus should be finalised during OEWG sessions to streamline progress and enhance focus.

Enhance Engagement of G77 Countries

Actively support and promote cyber capacity-building (CCB) initiatives to encourage greater participation from G77 countries in international debates on CCB. This can be achieved through targeted fellowships, funding schemes, and engagement in hybrid networking and coordination platforms. Facilitating broader representation will enrich the global conversation and address diverse needs.

Catalogue Policy Mechanisms to Incentivise Cyber Resilience

Identify and compile policy tools and mechanisms that incentivise governments to adopt and implement measures that enhance cyber resilience, ideally aligned with the Framework for Responsible State Behaviour (FRSB). A better understanding of the unique needs of developing countries is critical to strengthening their capacity to observe and implement the cumulative and evolving framework for responsible state behaviour in ICT use.

Leverage Existing Organisations and Initiatives

To address operational fragmentation, the UN should partner with existing organisations and initiatives, such as hybrid entities like the GFCE. These partnerships can facilitate the exchange of information on ongoing projects, needs assessments, lessons learned, and good practices, avoiding redundancy and promoting efficient resource use.

Regional and bilateral level

Strengthen Regional Organizations and Inter-Regional Dialogue

Enhance the role of regional organizations and platforms in addressing cyber-related issues by clarifying key concepts, approaches, and methodologies. These organisations should actively engage in discussions to develop and refine their positions on the Framework for Responsible State Behaviour (FRSB) and advocate for its implementation within their respective regions.

Facilitate Dialogue Across the CCB Ecosystem

Create platforms for dialogue that bring together parliamentarians, standard-setting bodies, consumer organisations, civil society, and other key actors from the broader cyber capacity-building (CCB) ecosystem. This will help raise awareness and foster more inclusive exchanges about global CCB efforts, ensuring diverse perspectives are considered in shaping the future of cyber capacity-building.

Promote South-South, Triangular, and Regional Cooperation

Support South-South, triangular, and sub-regional cooperation alongside traditional North-South partnerships. This approach will help identify and leverage diverse implementation modalities that

are better suited to local contexts, fostering flexible, cost-effective, and innovative solutions that meet the unique needs of different regions.

National level

Mainstream Capacity Building Principles

The principles of capacity building, as defined by the development community and adopted in successive OEWG reports, should be further integrated into initiatives focused on enhancing security in the use of ICTs.[47] This will help ensure a more consistent and comprehensive approach to capacity building in this critical area.

Align National Legislation and Frameworks with the FRSB

National legislation and institutional frameworks should be aligned with and contribute to strengthening the Framework for Responsible State Behaviour (FRSB). The implementation of the FRSB should prioritise provisions that reduce international escalation risks, such as establishing rules and procedures to prevent malicious cyber activities originating from a country's territory and promoting greater transparency and accountability for cyber operations conducted by entities within that state.

Professionalisation strategy

An alternative strategy, centred on enhancing the effectiveness of CCB, is professionalisation. This approach aims to make the ecosystem and CCB activities more efficient and effective, even in the face of ongoing ideological fragmentation. It represents the most pragmatic and realistic pathway to move away from the current trajectory toward the zone of confrontation.

The professionalisation strategy relies on increasing the use of technocratic processes and procedures to foster closer coordination, even among actors with differing ideologies. In this approach, partner countries play a crucial role. The strategy emphasises the importance of the entire CCB ecosystem, particularly multistakeholder engagement and whole-of-society approaches, to ensure better access to resources throughout all stages of project management – design, implementation, monitoring, and evaluation.

In this scenario, the UN may lose significance unless it adapts by promoting new, action-oriented forms of cooperation beyond platforms like the OEWG. It must proactively position UN entities with deep development expertise, such as UNDP and the United Nations Sustainable Development Group (UNSDG), within the broader CCB ecosystem. The professionalisation strategy also calls for strengthening accountability mechanisms in line with established development assistance standards, in order to minimise the impact of ideological polarisation on cyber capacity-building.

Box 4. Options for the implementation of the professionalisation strategy

UN level

Ensure Closer Coordination Across the UN System

Strengthen collaboration among relevant UN bodies and agencies, such as UNDP, UNCTAD, ITU, UNOCT, and UNIDIR. This collaboration should aim to maximise the collective knowledge and tools developed across the UN system. Ensure that the implementation of key initiatives, including the Pact for the Future, the Global Digital Compact, the UN Global Principles for Information Integrity, and the OEWG recommendations, are coordinated and mutually reinforcing to enhance the overall impact of cyber capacity-building (CCB) efforts.

Identify Concrete Pillars for CCB Monitoring

Establish clear and measurable pillars to monitor completed, ongoing, and planned CCB initiatives. These pillars should assess the alignment of these efforts with the Framework for Responsible State Behaviour (FRSB). Utilise tools like the Voluntary Checklist of Practical Actions from the OEWG Annual Progress Report to help guide and track progress on the implementation of UN-agreed norms.

Promote Transparency in Funding for Cyber Projects

Create standardised reporting mechanisms for funding of cyber-related projects that impact international security and the FRSB. These mechanisms should ensure transparency regarding existing and planned funding, enabling stakeholders to understand how resources are allocated and facilitating better decision-making in the allocation of funds for CCB activities.

Convene a Global Panel for CCB Modalities

Establish a global panel involving private sector stakeholders, major donors, and development banks, or integrate with existing forums such as the Global Conference on Cyber Capacity Building (GC3B). This panel should focus on discussing and adapting CCB modalities to address the evolving cyber ecosystem and growing cyber-related needs. Such a panel would also be essential for the successful establishment of initiatives like a potential trust fund under the UN's auspices.

Develop a Platform for Information Sharing and Resources

Identify and develop an effective platform for sharing information about ongoing CCB activities. This platform should serve as a repository for guidance, training materials, best practices, and lessons learned in ICT security capacity-building. It should build on existing initiatives like the GFCE, UNIDIR portals, and Cybil Portal, creating a centralised and accessible resource for stakeholders.

Strengthen Accountability in CCB Initiatives

Improve accountability mechanisms within CCB initiatives, both within and outside of the UN system. This should include mechanisms for positive accountability (i.e., recognising successful efforts) and negative accountability (i.e., addressing inefficiencies and failures).[48] Strengthening these mechanisms will promote greater transparency and ensure that CCB initiatives are effective and aligned with their stated goals.

Regional and bilateral level

Promote Closer Coordination at the Regional Level

Strengthen regional collaboration through existing platforms such as the GFCE Regional Hubs or the EU's LAC4. This will enhance coordination among regional stakeholders, creating a more unified approach to cyber capacity-building (CCB) efforts and ensuring regional challenges and opportunities are addressed effectively.

Invest in Knowledge Tools for CCB Programming

Develop and invest in knowledge tools that support better programming, identification, formulation, and implementation of CCB actions. Establish regional repositories that house existing tools, guidelines, and other instruments to facilitate the CCB ecosystem in meeting its commitments and enhancing regional cyber resilience.

Stimulate Intra- and Cross-Regional Discussions

Facilitate intra-regional and cross-regional discussions involving major donors and financial institutions to explore diverse implementation modalities for cyber capacity-building. These discussions should focus on how to reflect regional characteristics, including the absorption capacities of partner countries, the contributions of other CCB communities, and the involvement of the private sector in funding and implementing CCB initiatives.

National level

Identify and Promote Good Practices in Programme Management

Establish and promote best practices in programme management and development. This includes adopting a needs-based approach to project duration, strengthening programme management teams, addressing human rights risks, using systematic monitoring and evaluation, leveraging research, mainstreaming gender, and adapting implementation methods to ensure greater effectiveness.

Ensure Demand-Driven Actions in CCB Initiatives

Donor countries should prioritise demand-driven actions based on thorough needs assessments, developed in close collaboration with partner countries. This ensures that projects are aligned with local priorities, promoting national ownership, and maximising the impact of CCB efforts.

Adopt a Whole-of-Government Approach to CCB

Implement a whole-of-government approach in the design, implementation, and monitoring of cyber capacity-building initiatives. This approach encourages coordination and coherence across all government departments and agencies involved in CCB efforts, ensuring a unified strategy and better results.

Promote Diversity in the CCB Ecosystem

Foster a diverse ecosystem of CCB implementers by creating opportunities for locally-based implementors to participate in tendering processes. Provide incentives for bidding consortia leaders to include local implementing partners, thereby increasing the effectiveness and inclusivity of the CCB field.

Shift to Regularised Inter-Agency Coordination on CCB

Countries and large organisations should move away from ad hoc inter-agency or inter-departmental meetings and instead adopt regularised processes that bring together all relevant teams. These regular meetings should focus on discussing strategy, sharing progress, and ensuring alignment on cyber capacity-building efforts.

Strategically Integrate Non-State Actors in CCB

Develop a framework to strategically integrate non-state actors into the CCB ecosystem. Create engagement options that enhance awareness, transparency, and public-private cooperation, ensuring that non-governmental entities contribute to the success and sustainability of CCB initiatives.

CONCLUSION

The growth of the cyber capacity-building (CCB) ecosystem over the past two decades has transitioned from a small group of early movers to a wide array of diverse actors. These actors often operate within their own silos, dictated by their institutional mandates or thematic expertise. This expansion has not encouraged the cross-pollination of ideas across different communities, which could have improved their efforts and accelerated results. Simultaneously, the development of the CCB field has been shaped by broader geopolitical dynamics, including global trade, economic, and technological competition, coupled with the force of digitalisation and its impact on development and international cooperation.

As this paper argues, these elements have led to ideological and operational fragmentation within the CCB ecosystem, presenting a significant challenge to the effectiveness and sustainability of global CCB efforts. Tackling this fragmentation requires the involvement of all relevant stakeholders and the adoption of specific management strategies. The two most feasible strategies in the current international context are advancing the professionalisation of the CCB field toward the zone of prosperity and implementing de-escalation measures toward the zone of stability. These strategies require a more refined, practical, and action-oriented approach that acknowledges and leverages the strengths and expertise of the different communities, thereby strengthening a more holistic yet distributed CCB ecosystem.

This will involve connecting key nodes with different mandates and approaches to CCB – such as international security, cyber resilience, cybercrime, and digital development – that can work toward similar goals while learning from each other.

In the realm of international security, an open-ended, action-oriented permanent mechanism, like the one proposed in the third Annual Progress Report of the OEWG[49] or the Cyber Programme of Action proposal[50], could serve as one such pivotal node within the CCB ecosystem. However, it must be designed and implemented in a way that involves a broader multistakeholder community and demonstrates its clear value in order to attract the engagement of other critical communities. Their participation is essential for the implementation of norms and other components of the Framework for Responsible State Behaviour.

In the broader cyber resilience domain, the Global Conference on Cyber Capacity Building (GC3B) could serve as another action-oriented node that strengthens dialogue and cooperation between the cybersecurity and development communities, with the Accra Call for Cyber Resilient Development serving as a blueprint to stimulate practical actions that integrate cyber resilience

into international and national development agendas.

Given the ideological and operational fragmentation dynamics within the current CCB ecosystem, it is essential to recognise that its future is also intrinsically tied to the broader digital acceleration efforts. These efforts involve an even larger and more diverse group of stakeholders, with development actors playing a leading role. Therefore, it is crucial for the different cyber communities involved in capacity-building to actively seek opportunities for structured dialogue and collaboration, both among themselves and with peers in adjacent fields. In such a complex system of relevant communities and stakeholders, a top-down, centralised approach to CCB, such as through the United Nations, may not be the most effective. Instead, strategies to address CCB fragmentation could involve closer cooperation at the UN across its competent bodies, complemented by other multilateral and multistakeholder initiatives.

[1] World Economic Forum (2024), *Global Cybersecurity Outlook 2024*.

[2] Established pursuant to the United Nations, General Assembly (2020), *Resolution 75/240 Developments in the field of information and telecommunications in the context of international security*, A/RES/75/240, 31 December 2020.

[3] The scope of the paper relates to the international cooperation dimension of cyber capacity-building efforts and does not cover such activities undertaken within a given country or organisation by its own internal resources.

[4] Information in this section on CCB actors and initiatives draws from several mapping efforts that the readers are invited to look into more detail. These resources include: (a) the Global Forum on Cyber Expertise Cybil Portal, with a vast repository of past and present international cyber capacity-building projects; (b) the written submissions by Member States, United Nations system entities and non-governmental stakeholder entities to the Secretariat of the OEWG; (c) the United Nations Open-ended working group on security of and in the use of information and communications technologies 2021–2025 (2024), *Mapping exercise to survey the landscape of capacity-building programmes and initiatives within and outside the United Nations and at the global and regional levels: Paper by the Secretariat*, A/AC.292/2024/2, 22 January 2024; (d) Robert Collett and Nayia Barmpaliou (2021), *International Cyber Capacity Building: Global Trends and Scenarios* and *Annex on CCB Funders*, European Union Institute for Security Studies; (e) the EU CyberNet website, Mapping of EU-funded and EU Member States-funded external cyber capacity-building projects; and (f) Estonian Ministry of Foreign Affairs (2020), *Mapping Study for the High-Level Panel on Digital Cooperation and its Recommendation 4 on Digital Trust and Security.*

[5] The following terminology is used frequently in the paper and should be understood to mean: (a) funders refer to any entity (e.g., government authority, international financial institution/development bank, private sector firm, philanthropic organisation, etc.) that finances CCB programmes, projects, and activities with an international dimension i.e., in countries or regions other than their own; (b) partner countries and partner regional organisations refer to those that receive international and development cooperation assistance on cyber-related issues; (c) implementers refer to any organisation (e.g., government agencies, international and regional organisations, civil society and non-governmental organisations, private sector firms, associations, etc.) engaged in the execution of CCB programmes or projects.

[6] Multilateral organisations such as UN agencies and regional organisations, such as OAS, OSCE, etc, were purposefully not included in the funders section as they are primarily engaging in CCB as implementors with contributions by donors rather than using their core funding to undertake CCB actions.

[7] United Nations (2021), *Final Substantive Report of the open-ended working group on developments in the field of information and telecommunications in the context of international security 2019-2021*, A/AC.290/2021/CRP.2, 10 March 2021, para. 56.

[8] As is the case for the Department of Foreign Affairs and Trade of Australia (DFAT), Global Affairs Canada, the Dutch Ministry of Foreign Affairs, the Ministry of Foreign Affairs and Trade of New Zealand, the Swiss Federal Department of Foreign Affairs (FDFA) and the United Kingdom's Foreign, Commonwealth and Development Office (FCDO).

[9] The EU is included in this section of government donors as it is a unique case of supra-national organisation with governmental characteristics in its function as an external cooperation donor.

[10] Notably the Neighbourhood, Development and International Cooperation Instrument – Global Europe (NDICI – Global Europe), and the Instrument for Pre-accession Assistance (IPA III).

[11] See Organisation of American States, Inter-American Committee against Terrorism (2019), *Summary of Cybersecurity Activities Implemented by the OAS/CICTE Secretariat*, OEA/Ser.L/X.2.19, CICTE/INF. 1/19, 15 May 2019.

[12] Collett and Barmpaliou 2021, p. 43.

[13] There are numerous examples of such efforts. Indicative cases include: the Absa Cybersecurity Academy in South Africa established by the Absa Group in 2019 in partnership with the Maharishi Invincibility Institute and the Hein Wagner Academy for the Visually Impaired to address the cybersecurity skills shortage while creating job opportunities for previously disadvantaged and visually impaired learners; and Palo Alto's Global Cybersecurity Academy that partners with qualifying universities, colleges and high schools to integrate into degree programmes entry-level to intermediate courses and hands-on labs at no cost.

[14] For example, the Data Security Council of India (DSCI) in partnership with Microsoft launched CyberShikshaa in 2018 to equip young female engineers across India with essential cybersecurity skills.

[15] For example, the Cybersecurity Innovation Council is an alliance created between the OAS and Cisco to promote innovation in cybersecurity in the Americas.

[16] Such as the Cisco Networking Academy, IBM's SkillsBuild platform, the Google Cybersecurity Certificate programme, and Trailhead's Cybersecurity Career Path by Salesforce.

[17] For example, the International Chamber of Commerce (ICC) is creating policy guidance for its members on key cybersecurity issues, and also plans to partner with other organisations to improve the cybersecurity preparedness of SMEs. The GSMA, a non-profit mobile network operators industry association, has created a Capacity Building programme offering free training courses for policymakers and regulators, including on mobile cybersecurity. The Cybersecurity Tech Accord, an alliance of global technology industry players, develops guides, webinars, and other resources to raise the cybersecurity awareness of consumers and other stakeholders, such as IoT manufacturers.

[18] Most notably, Microsoft has supported a series of compendia in partnership with others, such as Compendium of Multistakeholder Perspectives on Protecting the Healthcare Sector from Cyber Harm (2022); Multistakeholder Compendium on Advancing Opportunities and Responsibilities for a Peaceful, Safer and Rights Respecting Cyberspace (2023); and Bridging the cybersecurity gap: a collaborative compendium for global development (2024).

[19] Indicative examples are research collaborations the Organization of American States has established with Amazon Web Services, Cisco, Microsoft, and Trend Micro, among others.

[20] See for more information the OECD webpage on leveraging private finance for development.

[21] Such flagship initiatives include the Partnership for Global Infrastructure and Investment (PGII) which aims to better respond to the global demand for high-quality infrastructure financing in low- and middle-income countries, and combines the Group of Seven (G7) relevant initiatives (e.g., the EU's Global Gateway that spells out digital as a priority cooperation area that includes robust cybersecurity governance measures, and the US Digital Connectivity and Cybersecurity Partnership (DCCP) that supports the development of communications infrastructure and digital markets as well as increasing partners' cybersecurity capacity. Another relevant flagship is the Digital Silk Road strand of China's Belt and Road Initiative that finances "telecommunications networks, artificial intelligence capabilities, cloud computing, e-commerce and mobile payment systems, surveillance technology, smart cities, and other high-tech areas". The private sector is considered a key financing partner in all these efforts.

[22] While they are commonly referred to as recipient or beneficiary countries and regions, in line with current development practice we prefer 'partner countries' as a more equitable term that indicates their active role in CCB rather than 'recipients' that has passive connotations and, conceptually, largely precludes the ownership of the partner government.

[23] Patryk Pawlak and Nayia Barmpaliou (2017), "Politics of cybersecurity capacity building: conundrum and opportunity", *Journal of Cyber Policy*, Vol. 2, Issue 1, pp. 137-138.

[24] Nayia Barmpaliou and Patryk Pawlak (2023), *Operational Guidance. The EU's International Cooperation on Cyber Capacity Building. Second Edition*, European Commission, pp. 49-50.

[25] See the Donor Statement on Supporting Locally Led Development (2022) as a recent example on how donors should reinforce local leadership and ownership, echoing existing principles and commitments mentioned in the Statement. Also see OECD (2019), *Managing for Sustainable Development Results: Guiding Principles*, OECD Publishing, Paris. Within the CCB context, Action 10 of the 2023 Accra Call for Cyber Resilient Development puts forward the need for local leadership in the coordination of CCB efforts, while one of the OEWG principles for capacity-building in relation to State use of ICTs in the context of international security underlines that it "should be based on mutual trust, demand-driven, correspond to nationally identified needs and priorities, and be undertaken in full recognition of national ownership" (United Nations 2021, para. 56).

[26] Commonwealth of Australia, Department of Foreign Affairs and Trade (2021), *Australia's International Cyber and Critical Technology Engagement Strategy*, p. 55.

[27] It is relevant to note that for the implementation the CCB actions it finances, the EU often uses its Member States' external cooperation agencies (e.g., Belgium's Enabel, France's Expertise France, Germany's GIZ, Spain's FIIAPP, among others).

[28] U.S. Government Accountability Office (2024), *Cyber Diplomacy: State's Efforts Aim to Support U.S. Interests and Elevate Priorities*, Report to Congressional Addressees GAO-24-105563, pp. 19-22.

[29] In joint EU-CoE projects, the CoE co-finances 10% of the total amount, and this is not calculated in the externally mobilised funds mentioned here. For details on CoE's past and current projects on cybercrime see the C-PROC webpage and its analytical annual reports.

[30] Such as the Internet Engineering Task Force (IETF), the Institute of Electrical and Electronic Engineers (IEEE), and the European Telecommunications Standards Institute (ETSI).

[31] Leonie Maria Tanczer, Irina Brass, and Madeline Carr (2018), "*CSIRTs and Global Cybersecurity: How Technical Experts Support Science Diplomacy*", *Global Policy* 9 (S3): 60-66.

[32] The calls for a stronger localisation agenda and the concept of locally led development are well established in development cooperation policy and scholarship going beyond the ownership principle. In the context of CCB, they are reflected most notably in the 2023 Accra Call for Cyber Resilient Development (actions 11, 15).

[33] Collett and Barmpaliou 2021, pp. 63-65.

[34] Barmpaliou and Pawlak 2023, pp. 66-67.

[35] The examples used are based on the written submissions of these countries to the OEWG mapping exercise and/or their oral interventions during the inaugural Global Roundtable on ICT Security Capacity Building convened by the OEWG Chair on 10 May 2024.

[36] For more details on these concepts see the website of the United Nations Office for South-South Cooperation (UNOSSC).

[37] Collett and Barmpaliou 2021, pp. 34-44.

[38] Collett and Barmpaliou 2021, pp. 14-16.

[39] Idem, pp. 19-22.

[40] Silvia Baur-Yazbeck and Jean-Louis Perrier (2020), "Regional Centers Can Help Low-Income Countries Build Cyber Resilience", CGAP, 8 July 2020.

[41] OECD (2011), *Busan Partnership for Effective Development Co-operation: Fourth High Level Forum on Aid Effectiveness*, Busan, Republic of Korea, 29 November - 1 December 2011, OECD Publishing, Paris.

[42] United Nations 2021.

[43] Patryk Pawlak (2024), "The pursuit of positive accountability in the cyber domain", *Global Policy Journal*, 15:1.

[44] See for instance: Collett and Barmpaliou 2021; Patryk Pawlak (2014), "Models for cyber capacity building" in Patryk Pawlak (editor) *Riding the digital wave. The impact of cyber capacity building on human development*, European Union Institute for Security Studies.

[45] See, for instance, activities under the EU-funded Cyber Capacity Building Task Force at the European Union Institute for Security Studies, which addressed many of the questions debated today: *Capacity building in cyberspace: taking stock* (2013), *Cyber capacity-building as a development issue: What role for regional organisations?* (2014), *Cyber NEEDS and development: identifying the needs of Networks Enhancing the Economy, Development and Security (NEEDS)* (2015).

[46] Xymena Kurowska and Patryk Pawlak (2022), *Bad options only? Transforming EU-Russia relations in cyberspace*, Policy Brief, February 2022, Foundation for European Progressive Studies.

[47] United Nations 2023.

[48] See for instance: Patryk Pawlak (2024), "The pursuit of positive accountability in the cyber domain", *Global Policy*, Vol. 15, Issue 1; Patryk Pawlak (2024), *Accountability in Cyberspace: The Holy Grail of Cyber Stability?*, EU Cyber Direct.

[49] United Nations 2024. The third annual progress report (APR) of Open-ended Working Group on security of and in the use of information and ICTs 2021–2025 was adopted on 12 July 2024, at the conclusion of its 8th substantive session.

[50] United Nations 2022.