Integrating Cyber Capacity into the Digital Development Agenda

November 2021

Wilhelmina van Pruisenweg 104
2915 AN, the Hague
Netherlands

This report was written by Melissa Hathaway and Francesca Spidalieri. The report was commissioned by the Global Forum on Cyber Expertise (GFCE) and funded by the World Bank's Digital Development Partnership (DDP). DDP offers a platform for digital innovation and development financing, bringing public and private sector partners together to advance digital solutions and drive digital transformation in developing countries. For more information, please visit: www.digitaldevelopmentpartnership.org.

ACKNOWLEDGEMENTS

This report is the result of significant contributions from across the broader digital development and cybersecurity communities, including Multilateral Development Banks (MDBs), national and international development agencies, international and non-governmental organizations, and government officials responsible for or involved in designing, implementing, and evaluating digital development projects and/or cybersecurity capacity building activities. The report was written by Melissa Hathaway and Francesca Spidalieri. The report was edited and designed by Sherry Loveless.

The authors extend their appreciation to the World Bank staff and the Global Forum on Cyber Expertise (GFCE) Foundation who participated in internal discussions and review of this report. The authors would also like to thank all the organizations and agencies interviewed (see Annex I) for taking the time to provide input and/or peer review for this report. The authors accept responsibility for any errors or inaccuracies in this report.

This report identifies pathways to bridge the development community to the cybersecurity capacity building community.

ABOUT THE AUTHORS

Melissa Hathaway is globally recognized as a thought leader in the fields of cybersecurity and digital risk management and has relationships with the highest levels of governments and international institutions, including NATO, the ITU, the OAS, and the World Bank. She has a distinguished affiliation at the Harvard Kennedy School's Belfer Center for Science and International Affairs. Internationally, she advises programs and research initiatives at the Center for Asymmetric Threats Studies — National Defense College in Sweden; the Digital Science Institute — European School of Management and Technology in Germany; the Centre for International Governance Innovation in Canada; the Kosciuszko Institute in Poland; and the CyberLaw Research Program at Hebrew University in Israel.

Ms. Hathaway served in two Presidential administrations where she spearheaded the Cyberspace Policy Review for President Barack Obama and led the Comprehensive National Cybersecurity Initiative for President George W. Bush. She built a broad coalition from within the Executive Branch for two Presidents, developing a cybersecurity strategy covering unprecedented scope and scale that facilitated revolutionary improvements for the United States to secure and defend its critical national infrastructures. She received the National Intelligence Reform Medal in September 2009 and the National Intelligence Meritorious Unit Citation in December 2011 for her leadership.

As President of Hathaway Global Strategies, she consults Fortune 500 companies on cybersecurity, enterprise risk management, and technology assessment. She helps organizations understand their most critical assets, services, and data; maps digital risks to the organization's business, financial, and risk objectives; and advises clients regarding industry leading practices, emerging cyber threats, policy initiatives, regulation, legislation, court decisions, and other industry matters that may affect their current and future business. Having served on the board of directors for four public companies and three non-profit organizations, and as a strategic advisor to a number of public and private companies, Ms. Hathaway brings her clients a unique combination of policy and technical expertise, as well as board room experience that allows her to help clients better understand the intersection of government policy, developing technological and industry trends, and economic drivers that impact acquisition and business development strategy in this field.

Ms. Hathaway holds a B.A. degree from the American University in Washington, D.C. She has completed graduate studies

in international economics and technology transfer policy, and is a graduate of the US Armed Forces Staff College, with a special certificate in Information Operations. She publishes regularly on cybersecurity matters affecting companies and countries; these articles can be found here: https://www.belfercenter.org/person/melissa-hathaway. Follow Ms. Hathaway on Twitter at: @CyberReadyIndex.

Francesca Spidalieri is a highly credentialed cybersecurity professional with a decade of experience in cyber policy development, cyber risk management, and strategic planning. As a cybersecurity consultant for Hathaway Global Strategies, she provides strategic consulting services to business executives and senior government officials on global security trends, emerging cyber threats, enterprise risk management, and cybersecurity-related policies, laws, and regulatory matters affecting business decisions. Ms. Spidalieri is also an Adjunct Professor for Cyber Policy at the University of Maryland's School of Public Policy and at Salve Regina University, where she teaches graduate courses on cyber policy, cyber defense strategy, and the prospects and challenges of digital transformation and technological innovation. In addition, she is the Co-Principal Investigator for the Cyber Readiness Index 2.0 project at the Potomac Institute for Policy Studies, and a non-resident Senior Fellow for Cyber Leadership at the Pell Center for International Relations and Public Policy at Salve Regina University.

Ms. Spidalieri serves also as a cybersecurity subject-matter expert for the World Bank, the International Telecommunications Union, the Global Forum on Cyber Expertise, and the EU CyberNet, and advises programs and research initiatives at other research institutes in Europe, including the Center for Cyber Security and International Relations Studies at the University of Florence in Italy and the Kosciuszko Institute in Poland. Her academic research and publications have focused on cyber leadership development, cyber risk management, digital transformation, and national cyber preparedness and resilience. She lectures regularly at cyber-related events in the United States and Europe and contributes to journal articles and other publications on cybersecurity matters affecting countries and organizations worldwide. Ms. Spidalieri holds an M.A. in International Affairs and Security Studies from The Fletcher School at Tufts University, a B.A. in Political Science and International Relations from the University of Milan, and has completed additional cybersecurity coursework at the U.S. Naval War College's Center for Cyber Conflict Studies. Follow Ms. Spidalieri on Twitter at: Twitter: @Francesca_cyber.

ACRONYMS

5G	Fifth Generation of Mobile Communications
AI	Artificial Intelligence
CBM	Confidence Building Measure
CCB	Cyber Capacity Building
CERT	Computer Emergency Response Team
CISO/CIO	Chief Information Security Officer/Chief Information Officer
CSIRT	Computer Security Incident Response Team
DAC	Development Assistance Committee (OECD)
DCO	Development Coordination Office (United Nations)
DDP	Digital Development Partnership (World Bank)
DPGs	Digital Public Goods
GDP	Gross Domestic Product
GFCE	Global Forum on Cyber Expertise
GP	Global Practice (World Bank)
ICS	Industrial Control Systems
ICT	Information and Communications Technology
IoT	Internet of Things
ISAC	Information Sharing and Analysis Center
ISAO	Information Sharing and Analysis Organization
LAC	Latin America and the Caribbean
LDC	Least Developed Countries
MDB	Multilateral Development Bank
MNOs	Mobile Network Operators
ODA	Official Development Assistance (OECD)
OECD	Organisation for Economic Co-operation and Development
PoC	Point of Contact
RC	Resident Coordinator (United Nations)
SDGs	Sustainable Development Goals (United Nations)
SOC	Security Operation Center
WB	World Bank
WDR	World Development Report
WSIS	World Summit on the Information Society

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Digitization and connectivity yield unquestionable benefits, including improving competitiveness, productivity, efficiency, innovation, and modernization; generating more revenue; and advancing human and social development. This is why promoting digital transformation has become a priority for sustainable development and why organizations like the United Nations, large donor organizations, and countries involved in development assistance are prioritizing digitization as one of the key enablers of inclusive and sustainable economic growth and development. Yet, rapid digital transformation – underpinned by affordable communications and cheap devices – has introduced new risks and vulnerabilities that cannot be ignored. Organizations and countries alike are becoming increasingly concerned about the misuse of digital technologies that might lead to critical infrastructure failures, financial destabilization, increased surveillance, human rights abuses, disinformation, data exploitation, and other negative impacts on public health and safety.

It is important to recognize that digitization and resilience are two sides of the same coin. The digital development community and the cybersecurity community share related goals of strengthening digital capacity building, including the ability to effectively use advanced technologies while simultaneously ensuring that citizens remain safe, protected, and productive online. Despite these similar aims, the two communities operate primarily within their own disciplines, rarely partner, and embed cybersecurity activities within digital development projects. This report identifies pathways to bridge the development community to the cybersecurity capacity building community.

Multiple benefits can arise from integrating cybersecurity, digital resilience, and cyber capacity into digital development. At a foundational level, decision-makers need to gain a deeper understanding of the threats emanating from the potential misuse of information and communications technologies (ICTs) and emerging technologies, such as becoming tools for unauthorized surveillance, disinformation, digital authoritarianism, data exploitation, espionage, etc. This understanding can guide the development community in supporting countries' digital adoption and increasing their maturity in maximizing the use of new digital technologies as enablers of sustainable and secure development. On a more practical level, it is clear that integrating these aspects into development programs would lead to achieving better outcomes; streamlining processes/eliminating duplication of efforts/maximizing resources; and building stronger resilience, safety, security, and trust into recipient countries' digital transformation projects.

This report is the result of significant contributions across the broader digital development and cybersecurity communities, including Multilateral Development Banks (MDBs), national and international development agencies, international and non-governmental organizations, and government officials responsible for or involved in designing, implementing, and evaluating digital development projects and/or cybersecurity capacity building

activities. The recommendations provided in this report are intended to help multilateral organizations and other donors investing in digital development and cyber capacity building (CCB) activities to integrate cybersecurity and digital resilience throughout the lifecycle of a project, identify areas where they can partner, build mechanisms to de-risk their investments, build stronger and enduring digital infrastructures and projects, and accelerate the safe adoption of technologies to meet the intended outcomes of the SDGs.

A few recommendations stand out.

1. The development and cybersecurity communities need to update their "playbook" for the digital era by connecting cybersecurity and digital resilience to the economic aspirations, digitization strategies, and development priorities of recipient countries. Digital capacity building must be more needs-driven and tailored to individual and national circumstances, and better coordinated globally. Tailored programming and approaches based on a demand-driven signal and the political, economic, and social context of a recipient country is central to ensuring the long-term sustainability and scalability of any capacity building efforts. Providing sufficient funding should also remain an important objective.

2. The cybersecurity narrative in the context of international development should be reframed in terms of digital resilience, safety, trust, sustainability, and risk management rather than security.

3. The OECD Development Assistance Committee (DAC) should add "digital resilience" to the eligibility criteria for Official Development Assistance (ODA) as part of the peace and security activities to enable cybersecurity-related assistance.

4. To ensure the continuity and sustainability of a project (e.g., continuity of the program, staff, equipment, etc.), funds should be programmed into the country's national budget. Both the development community and recipient countries see ICTs as long-term capital assets and expenditures, rather than commodities that will need updating and replacing within a five to ten-year period. ICTs that are still in use and no longer supported by hardware and software updates make the recipient country more vulnerable to digital risks. This vulnerability leaves a critical shortfall in a program's sustainability and its ability to achieve the desired resilient outcomes. A digital development project's total-cost-of-ownership and ICT refresh must, therefore, be included in project formulation and programmed into assistance packages.

5. The development and cybersecurity communities should invest in the development of "Digital Public Goods" (universal tools and instruments) that can be shared and applied broadly.

6. Growing a cybersecurity skilled local labor force/talent pools and indigenous capacity should be a key objective of any digital development project. This requires addressing many related challenges, including the affordability of cyber certifications, the need to reform school and university curricula, and the need to identify and cultivate local talent and commercial implementors.

7. Funding should be allocated to students and local institutions in order to build knowledge of local ecosystems, culture, and digital risks to society. Local data, trends, statistics, and field research that characterize the threat within a country or region can provide compelling evidence to drive economic and political arguments as to why cybersecurity is an important and necessary component of digital development.

8. Development organizations should be used as a conduit to raise cybersecurity awareness and build capacity in low- and middle-income countries. While digital risks stemming from increased reliance on ICTs and the expansion of e-services, digital systems, and platforms may not be prioritized, the development community has established connections and better understanding of local challenges within these countries and can offer particular insights and valuable relationships with local "implementors."

9. Duplication of efforts should be avoided by developing greater coherence and coordination between stakeholders. Scalable approaches and solutions are needed as well as innovative platforms and pilot projects that identify on-the-ground/local partners to implement the necessary actions and improve coordination efforts with local authorities. The practice of favoring "darling countries" that receive multiple offers of foreign aid from different donors, while neglecting "orphan countries" should be evaluated to maximized development resources more broadly.

10. There are a number of venues that should be leveraged to bridge the international development community with the cybersecurity capacity building community. Networking the networks may lead to cybersecurity becoming an integral activity within digital development and help both communities achieve more resilient outcomes.

VISION AND MISSION

AIM AND OBJECTIVES

This report aims to bridge two communities – the broader development community and the cybersecurity capacity building community – to achieve more resilient outcomes by ensuring incorporation of cybersecurity and digital resilience into digital development activities. This report is a product of the partnership between the World Bank and the Global Forum on Cyber Expertise (GFCE) Foundation, who recognize the importance of including cybersecurity, digital resilience, and cyber capacity building (CCB) as components of development projects. They also understand that advocates are needed to promote the eligibility of these activities for assistance in the broader development agenda.

SPONSORS

The World Bank (WB) has been working to help over 100 developing countries and countries in transition to embrace the importance of scientific and technological innovation for meeting sustainable development challenges and for accelerating human progress. In 2016, the World Bank's World Development Report (WDR) on *Digital Dividends*, a cardinal document in the development community that is often used to drive overall community strategy, explicitly acknowledged the importance of cybersecurity as an international development concern. For the first time in a WDR, the importance of managing digital risk was enumerated, as the report noted, "some of the perceived benefits of digital technologies are offset by emerging risks."[1]

In 2019, the World Bank's General Counsel Sandie Okoro, during her remarks at the Council of Europe's Octopus Conference, clearly stated the Bank's commitment to be "at the forefront of helping [its] members participate in the global digital economy [and] take advantage of globally connected markets in this digital age." She also acknowledged "the challenges faced by both developed and developing countries in ensuring the safety and security of their citizens," specifically noting the need to support "global cybersecurity, including building capacity to combat cybercrime" as key enablers of these efforts and the Bank's development mandate.[2]

The 2021 WDR on *Data for Better Lives* emphasized the need for low- and middle-income countries to adopt "overarching safeguards for cybersecurity and cybercrime" as part of their legal and regulatory frameworks in order to establish "trust in the data ecosystem for both personal and non-personal data" and ensure "the security of the network infrastructure and elements over which data flow." The report states that those safeguards should be "established, effectively

implemented, and continually updated in response to new risks or deficiencies."[3]

Today, the majority of World Bank's projects have an ICT or digital component, and this number has continued to increase in the post-pandemic world. The World Bank began working on cybersecurity as part of its technical assistance in the early 2010s (e.g., Morocco, 2011). In 2016, cybersecurity became a major focus area with the launch of the Global Cybersecurity Capacity Program. This Program aligns with the World Bank's commitment to promote widespread sustainable development and aims to enhance the cybersecurity capacities of developing countries through technical assistance and capacity building activities such as convening policy dialogues, preparing national cybersecurity assessments, and creating knowledge products like the Combatting Cybercrime Toolkit (developed in partnership with a number of organizations).[4] In addition, the World Bank has initiated projects to increase countries' capacities to respond to cyber threats posed to their public systems and infrastructure, and to develop best practices to minimize the effects of malicious cyber activities on the financial sector.

In August 2021, the World Bank launched a Cybersecurity Multi-Donor Trust Fund, developed as an associated trust fund under the broader Digital Development Partnership (DDP) umbrella program.[5] The fund aims to better define, understand, articulate, structure, and systematically roll out the cybersecurity development agenda. The emerging work program intends to offer comprehensive cybersecurity capacity development, including developing global knowledge, country assessments, technical assistance, capacity building, and training supported by necessary infrastructure and technology investments.

Inspired by the vision that every citizen of the world must reap the benefits of ICTs in an open, peaceful, and secure digital world, the Ministry of Foreign Affairs of the Netherlands led the launch of the Global Forum on Cyber Expertise (GFCE) at the 2015 Global Forum on Cyberspace. In 2020, the GFCE spun off into an independent foundation. The GFCE is an international, multi-stakeholder, and consultative forum committed to strengthening cyber capacity and growing expertise globally through international collaboration and cooperation. The GFCE developed the *Cybil Portal*, an online platform that catalogues expertise, tools, publications, and CCB projects.[6] Today, the GFCE serves as a global platform for countries, international organizations, and private companies to identify and exchange successful policies, practices, and ideas for cyber capacity building and to communicate these activities globally. It also functions as a clearinghouse to match requests for cyber capacities with potential funders and expert implementors. The GFCE structures its work around five themes of cyber capacity, which were first outlined in the 2017 "*Delhi Communiqué on a GFCE Global Agenda for Cyber Capacity Building*," namely: 1) Cyber Security Policy and Strategy; 2) Cyber Incident Management and Critical Infrastructure Protection; 3) Cybercrime; 4) Cyber Security Culture and Skills; and 5) Cyber Security

Standards.[7] While not an exhaustive list of capabilities that a country or organization must implement to achieve a desired level of cyber resilience, the GFCE identified these capacity building themes as a baseline reference for good cyber practices internationally.

The World Bank joined the GFCE in support of the overarching development angle of cybersecurity capacity building and supports the "GFCE Cybersecurity Capacity and Platform" project, which aims to promote greater collaboration and deeper knowledge in cybersecurity. To this end, the World Bank is working closely with the GFCE to bring together important stakeholders from governments, academia, the private sector, and the development community to: 1) produce cutting-edge research on newly evolving cybersecurity topics; 2) facilitate knowledge sharing mechanisms and networking opportunities through the Cybil portal and other venues; 3) provide an avenue to better understand the cybersecurity challenges faced by developing countries; and 4) engage in capacity building activities.

In June 2021, the GFCE and the World Bank came together to identify pathways to bridge the development community to the cybersecurity capacity building community and create mechanisms by which digital development could see the benefits of incorporating cybersecurity into their projects and initiatives to achieve more resilient outcomes.

This report highlights some of the key challenges and benefits of incorporating cybersecurity, digital resilience, and cyber capacity building into the broader development agenda. The report also features several best practices and bridging venues and activities that could facilitate tighter alignment and collaboration between the digital development and cybersecurity capacity building communities and among initiative donors and implementors.

METHODOLOGICAL APPROACH AND RECOMMENDATIONS FORMULATION

Based on primary and secondary data and information sources, this report builds upon existing literature on digital development and cyber capacity building frameworks, methodologies, and capacities within the multi-stakeholder and international GFCE Community and beyond, including MDBs and international organizations like the International Telecommunications Union (ITU) and the European Union (EU). Primary data was collected over 40 semi-structured interviews with selected experts and organizations involved in the design and implementation of digital/ICT development projects and/or cybersecurity initiatives (see list in Annex I). Additional primary data was obtained through a World Bank workshop ("roundtable discussion") including representatives involved in digital development lending operations and technical assistance projects from the

World Bank's Digital Development (DD) Global Practice. Secondary data was collected through the GFCE's *Cybil* Portal of cyber capacity building projects, additional open-source research, and the interviews with community stakeholders and experts who provided publicly available and confidential sources and supporting documentation, including strategies, methodologies, toolkits, primers, guidance notes, and other reports.

Interview findings and observations were supplemented by additional desk research. This report identifies successful programs and highlights digital public goods to showcase where cybersecurity and cyber capacity building efforts were incorporated into digital development projects, including those funded/implemented by regional and international organizations, as well as by national governments and other major donors. Other success stories include digital development projects that increased cybersecurity maturity of an entity or country, and digital infrastructure investment projects that embedded cybersecurity and digital resilience de-risking mechanisms (safeguards). The data collected through the interviews and desk research was analyzed to identify and recommend best practices (effective methods) to incorporate cybersecurity, digital resilience, trust, sustainability, safety, and risk management into digital development programs and lending operations.

TARGET AUDIENCE

The target audience of this report is MDBs, international and non-governmental organizations, field workers, experts, government policymakers, and officials responsible for or involved in designing, implementing, and evaluating digital development projects and/or cybersecurity capacity building activities. Additionally, the findings formalized in this document can be of value to cybersecurity policy experts and researchers at the national and international levels.

STAKEHOLDERS/EXPERTS INTERVIEWED

The following GFCE Members[8] and additional international non-governmental institutions, regional organizations, MDBs, and government representatives participated in the semi-structured interview process to inform the project:

- African Union Commission (AUC);
- Asian Infrastructure Investment Bank (AIIB);
- Australia National University (ANU);
- Australian Department of Foreign Affairs and Trade (DFAT);
- Bill & Melinda Gates Foundation;
- Council of Europe (CoE);
- CREST;
- Digital Public Goods Alliance (DPGA);
- DiploFoundation (Diplo);
- Dutch Ministry of Foreign Affairs;
- Estonian Ministry of Foreign Affairs;
- European Bank for Reconstruction and Development (EBRD);
- European Commission (EC);
- European Investment Bank (EIB);
- German Federal Office for Information Security (BSI);
- GFCE Foundation;
- Inter-American Development Bank (IDB);
- International Criminal Police Organization (INTERPOL);
- International Telecommunications Union (ITU);
- Islamic Development Bank (IsDB);
- Israel National Cyber Directorate (INCD);
- Italian Ministry of Foreign Affairs and International Cooperation;
- Japan International Cooperation Agency (JICA);
- Korea Development Bank (KDB);
- Korea International Cooperation Agency (KOICA);
- MITRE Engenuity;
- Norwegian Institute of International Affairs (NUPI);
- Organisation for Economic Co-operation and Development (OECD);
- Organization for Security and Co-operation in Europe (OSCE);
- Organization of American States (OAS);
- UK Foreign, Commonwealth & Development Office (FCDO);
- UN Development Coordination Office (DCO);
- UN Development Program (UNDP);
- UN Executive Office of the Secretary-General (EOSG);
- UN Institute for Disarmament Research (UNIDIR);
- UN Office for Disarmament Affairs (UNODA);
- UN Office of the Secretary-General's Envoy on Technology (OSET);
- UN Office on Drugs and Crime (UNODC);
- U.S. Agency for International Development (USAID);
- U.S. Department of State; and the
- World Bank.

1 INTRODUCTION

Innovative technologies of the twentieth century have profoundly transformed society and the global economy. Nations and corporations alike have embraced, adopted, and embedded information and communications technologies (ICTs) into their networked environments and infrastructures and realized phenomenal business and economic growth through improved services, increased productivity, and decreased costs. Global economic growth today is increasingly dependent upon the rapid adoption of ICTs and internet uptake. As of 2021, 4.66 billion people were connected to the internet (59.5% of the global population) and the global digital economy represented about 20% of the world's GDP, with ICTs as a principal driver of social and economic growth.

Digitization and connectivity yield unquestionable dividends, including improving competitiveness, productivity, efficiency, innovation, and modernization; generating more revenues; and advancing human and social development. This is why promoting digital transformation has become a priority for sustainable development and why organizations like the United Nations, large donor organizations, and countries involved in development assistance are prioritizing digitization as one of the key enablers of inclusive and sustainable economic growth and development. In the last decade, in particular, these entities have allocated significant funds toward the use of digital technologies as part of their development assistance for lower- and middle-income countries to help them increase their participation in the global economy; bridge divides between developed and developing countries; tackle global challenges such as poverty, hunger, and inequality; and accelerate human well-being.

Despite the clear benefits of embedding digital technologies into society and the economy, organizations and countries alike are also becoming increasingly concerned about the misuse of digital technologies that might lead to critical infrastructure failures, financial destabilization, increased surveillance, human rights abuses, disinformation, data exploitation, and other negative impacts on people's health and safety. Cyber incidents are increasing in volume, scope, and sophistication. As UN Secretary-General Guterres noted, "the pandemic has ushered in some of the most intrusive surveillance technologies we have ever seen, together with a significant increase in cynical ransomware attacks on hospitals and healthcare facilities,"[9] all the while malicious actors continue to steal sensitive data, knock businesses offline and, in some cases, destroy the ICTs that power businesses and essential services.

Moreover, digital risks are also reinforcing and magnifying existing fault lines, including social and economic inequalities, and amplifying the "digital divide" between the connected and unconnected. As both the development and cybersecurity communities try to address some of these challenges, focus is still insufficient on building resilience and growing human and institutional capacity, particularly in developing countries.

2 BACKGROUND

The international development community — which spans national and international development agencies to Multilateral Development Banks (MDBs), to other large philanthropic donors and private foundations — began using the concept of "capacity building" in the 1990s.

The cybersecurity "communities of practice" emerged from different disciplines (e.g., law enforcement, technical, foreign policy, human rights). Cyber capacity building emerged as an international policy concept in the first decade of the 21st century, when a handful of countries and international organizations began to include it within policy documents and national strategies.

iStock.com/marchmeena29

2.1 Origins and Evolution of the International Development Community

Just after World War II, a network of national and international aid agencies, programs, and related institutions and donors emerged that today constitutes the international development community. Its foundations were rooted in four distinct initiatives, including "the development activities of the colonial powers in their overseas territories, the institutions and programs for economic co-operation created under United Nations auspices after the Second World War, the United States Point Four Program, and the large scale support for economic stability in the countries on the periphery of the Communist bloc of that era."[10] The success of the Marshall Plan and the establishment of the International Bank for Reconstruction and Development (World Bank) and the International Monetary Fund (IMF) in the mid-'40s provided the additional impetus for the development of this

broader community dedicated to helping less-developed countries through external assistance.

As more countries gained independence, several multilateral organizations (e.g., Inter-American Development Bank [IDB], Organization of American States [OAS], Organisation for Economic Co-operation and Development [OECD]) and specialized UN agencies (e.g., International Labour Organization [ILO], UN Children's Fund [UNICEF], World Health Organization [WHO], UN Development Programme [UNDP]) were established "to promote social progress and better standards of life" and "to employ international machinery for the promotion of the economic and social advancement of all peoples."[11] In 1960, a dedicated Development Assistance Group (DAG) was created under the aegis of the OECD (then, still called Organisation for European Economic Co-operation) to serve as a forum for consultations among aid donors on assistance to less-developed countries. The establishment of DAG was part of an extraordinary upsurge of related institutional developments in the early 1960s that laid the foundation of the current aid system. This entire decade was designated by the UN as the "United Nations Development Decade." Several developed countries also began to establish their own foreign assistance agencies, like the U.S. Agency for International Development (USAID), Canadian International Development Agency (CIDA), Japan International Cooperation Agency (JICA), and the Swedish International Development Authority (SIDA); or ministries/departments for development cooperation (as in France and Italy); or other development assistance programs responsible for administering economic assistance to developing countries (as in Germany). In the meantime, DAG turned into a permanent Development Assistance Committee (DAC) responsible for setting the financial terms, conditions, and criteria for donor countries' development aid worldwide.

In 1969, DAC adopted the concept of "Official Development Assistance" (ODA) to identify official transactions made with the main objective of "promoting and specifically targeting the economic development and welfare of developing countries." This set of rules and criteria for ODA-eligible activities (so-called "DAC-ability") is considered the "gold standard" of foreign governments' assistance, and remains the main source of financing for development aid today.[12] These criteria specifically exclude "military aid and promotion of donors' security interests," which is noteworthy because this often excludes some donor countries' cybersecurity-related assistance.

The OECD Development Assistance Committee's (DAC) eligibility criteria for Official Development Assistance (ODA) are considered the "gold standard" of foreign governments' assistance, and remain the main source of financing for development aid today.

Most of the development aid provided by donor countries and international organizations in the earlier years was dedicated to the financing of basic infrastructure – roads and railroads, dams, power

plants, telecommunications systems, etc. – for the reconstruction of war-ravaged countries. In the early-1970s, the World Bank and other development financing institutions introduced technical assistance (e.g., agricultural development, food production, disaster relief, etc.) into their development tool offerings to countries in the process of development, and expanded their lending operations to educational activities and other fields that could further contribute to socio-economic development.[13] In 1971, the UN established the category of least developed countries (LDCs) and incorporated special measures in favor of these most vulnerable countries as part of its "International Development Strategy for the Second UN Development Decade."[14] The focus of foreign assistance continued to expand to support building modern infrastructure development, industrialization, refugee protection, and knowledge projects in the late 1970s, reflecting increased attention to problems of poverty, unemployment, and inequality. They fundamentally recognized that meeting "basic human needs [was] not a substitute for, but an essential component of, more economic growth which involves modernization, provision of infrastructure, and industrialization."[15] The notion of sustainable development appeared in 1987 in the UN Brundtland Commission Report "Our Common Future," where it was defined as "development that meets the needs of the present without compromising the ability of future generations to meet their own needs."[16] All of this paved the way for increased investments in building local human and institutional capacity, promoting national policy reforms, and creating the conditions for long-term sustainable economic growth and social development. Other important notions introduced in aid policy formulation included participatory development, environmental sustainability, and the promotion of human rights.

In the 1990s, the international development community – which, by that time spanned from national and international development agencies, to Multilateral Development Banks (MDBs), to other large philanthropic donors and private foundations – began using the concept of "*capacity building.*" Since then, this community has also played an important role in providing access to affordable telecommunications to enable internet use driving digitization and enabling inclusive and sustainable economic growth and development. The 2003 and 2005 World Summit on the Information Society (WSIS) called specifically for cyber capacity building (CCB) to support development. However, the field of CCB, with a few exceptions, continued to evolve outside of the development umbrella.[17]

The concepts and notions introduced in aid policy formulation evolved into the Sustainable Development Goals (SDGs) agreed to in 2015 by the UN General Assembly, and adopted by all UN member countries as part of the "*UN 2030 Agenda for Sustainable Development.*" These 17 interlinked global goals include: SDG1 on Ending Poverty; SDG2 on Ending Hunger; SDG3 on Ensuring Good Health and Well-Being; SDG4 on Quality Education; SDG5 on Achieving Gender Equality; SDG6 on Clean Water and Sanitation; SDG7 on Affordable and Clean Energy; SDG8 on Decent Work and Economic Growth; SDG9 on Industry, Innovation, and Infrastructure; SDG10 on Reduced

UN Image

Inequalities; SDG11 on Sustainable Cities and Communities; SDG12 on Responsible Consumption and Production; SDG13 on Climate Action; SDG14 on Life Below Water; SDG15 on Life on Land; SDG16 on Peace, Justice, and Strong Institutions; and SDG17 on Partnership for the Goals.[18]

Each SDG includes a digital component, although some SDGs are more digitally-oriented than others (e.g., SDG 4, 7, 8, 9, 11, 16). The connections between digital technology and growth have been demonstrated through statistics on the use of ICTs, and the extent that countries are connected correlates with increases in their GDP (according to the World Bank, every 10% point increase in internet connectivity in a developing country increases its GDP growth by 1-2%).[19] Additional studies have highlighted the impact of the internet, data, artificial intelligence (AI), Internet of Things (IoT), cloud computing, and other transformative technologies directly on the SDGs. These activities range from e-banking and e-money solutions to increased access to financial services, in particular in rural areas, and improve financial inclusion (SDG10), to AI and machine learning to improve energy efficiency and reduce electricity costs (SDG7), to increased internet access that allows more people to enjoy decent working conditions and increased income (SDG8), to digital solutions in healthcare to provide people with access to increased and improved health services (SDG 3), to better educational opportunities around the globe (SDG 4). Reports and the work of special high-level panels and commissions all support the notion that digitization can accelerate realization of all SDGs,[20] and can become the most important development tool for billions of people living in developing countries.[21] The 2030 UN Agenda also created a "Multi-stakeholder Forum on Science, Technology, and Innovation" to promote capacity building activities to develop, transfer, and disseminate relevant technologies for the SDGs.

Today, most international institutions (e.g., European Union, Economic Commission for Latin America and the Caribbean), UN specialized agencies, as well as countries from LDCs and small-island developing states (SIDs) to larger developed nations have integrated the SDGs into their respective development agendas and strategies. For example, the International Telecommunications Union (ITU) – the UN specialized agency responsible for all matters related to ICTs – has aligned its strategic and operational plans to specific SDGs (i.e., SDGs

4, 9, 11, 16, and 17).[22] The work of the European Bank for Reconstruction and Development (EBRD) explicitly contributes to 14 of the 17 SDGs (their *Annual Review 2020* provides specific case studies that indicate which SDGs their projects support).[23] Even the OECD's Official Development Assistance criteria recognize the importance of aligning allocation of development aid to implementation of the SDGs. Moreover, digitization increasingly affects how national or international funding agencies, development financing institutions, and other donor organizations "contribute assistance to sustainable development and to help achieve the SDGs. There is broad consensus about the importance of connecting developing countries to digital networks, so as not to widen the gaps between rich and poor states."[24] However, the funding needs have never been greater to ensure progress toward delivering on the global demand for physical and digital infrastructure to achieve the SDGs. "The UN estimated that the funding gap for building the [digital] infrastructure in developing countries is over one trillion dollars annually**.** Official Development Assistance (ODA), even during the record year of 2020, amounted to only 161 billion dollars."[25] Multiple organizations have called for better cooperation and coordination among donors to fund the SDGs, ensure "trusted digital connectivity," and bridge the digital infrastructure financing gaps in developing countries.

"The UN estimated that the funding gap for building the [digital] infrastructure in developing countries is over one trillion dollars annually."

In 2020, the UN reiterated the SDG goals in its "*Roadmap for Digital Cooperation*" and emphasized the need to strengthen human and institutional digital capacity building, including development of digital skills, "effective use of advanced and emerging technologies," ability to advance broadband access, adoption, and meaningful use and "ensuring that individuals stay safe, protected and productive online."[26] It recognized that "digital capacity building must be more needs-driven and tailored to individual and national circumstances, and better coordinated globally." The roadmap set out specific objectives as a way forward, including: 1) developing Digital Public Goods Platforms to share digital public goods, engage talent, and pool data sets; 2) creating a broad multi-stakeholder network to promote holistic, inclusive approaches to digital capacity building with a "clearing house function" embedded within the UN system to better direct support requests; and 3) growing the on-the-ground UN presence to enhance support of national capacity building efforts and to amplify country-level support (See Annex I).[27]

"Digital capacity building must be more needs-driven and tailored to individual and national circumstances, and better coordinated globally."

Digital capacity building, however, has remained separate from the concept of "cyber capacity building" and when conducted without proper consideration for cybersecurity and digital resilience could actually be antithetical to CCB's aims.

Building digital capacity encompasses everything from expanding broadband access and internet connectivity, to automating and digitizing industry sectors and critical infrastructures, to providing e-government services, to developing the skills and attitudes needed to meet the demands of a digital society. But "digitalization in countries that suffer from lack of development, poor governance, and poverty might provide new breeding grounds for organized crime, terrorism, and cybersecurity challenges, [and] these digital vulnerabilities and risks need to be addressed."[28] Nonetheless, the more technical and security-related cyber issues, including cybercrime, critical infrastructure protection, and data protection and privacy, have yet to be mainstreamed into the development thinking – especially into sectoral projects not strictly digital (e.g. health, energy, transport). This is due, in part, to the perception that cyber issues are linked to national security, military, law enforcement, or intelligence efforts, and, therefore, should fall outside the scope of Official Development Assistance (ODA eligibility criteria). Even the World Bank and other international organizations that may not be constrained by ODA criteria have only recently begun to recognize that cybersecurity and digital resilience should be a part and parcel of "development" in the digital age.

International organizations have only recently begun to recognize that cybersecurity and digital resilience are an essential element of development in the digital age.

"Baseline studies have demonstrated [a persistent] gap between development goals and intentions in donor policies on the one hand, and digital vulnerability and cybersecurity in developing countries on the other."[29]

2.2 Origins and Evolution of the Cybersecurity Community

Separate from the broader development community, there is an ever-expanding cybersecurity community – "a loose community of practice consisting of government agencies (from ministries of foreign affairs to ministries for development and telecommunication regulators), intergovernmental organizations, nonprofit/nongovernmental organizations, [technical incident responders, law enforcement officials tackling cybercrime, civil society trainers,] and private companies."[30] This community grew out of the technical discipline of computer science in the late 1970s and was mostly focused on tackling cybercrime and providing law enforcement training (criminal justice community) or offering technical assistance for incident response (incident management community). The latter has evolved into a broader community of technical experts (IT and network managers) who provide essential security services and respond to security problems and malicious activities against networked infrastructures. They are a community of passionate people that include former government and law enforcement officials, academics, ethical hackers, civil society, and other experts who champion efforts that help ensure the ICT environment remains "open, secure, stable, accessible and peaceful."[31]

In the last two decades, the foreign policy and internal affairs community and the defense community, typified by Ministries of Foreign Affairs, Ministries of Interior (or similar), and Ministries of Defense, respectively, have also become increasingly active actors in cyber capacity building activities around the world. In this context, cybersecurity assistance has become a foreign policy tool that can influence domestic policy, deepen market access, and promote the adoption of specific standards or technology, such as those for 5G or AI systems. As expected, these countries align their foreign assistance funding to their national security and/or economic priorities and target specific countries and regions of the world that align with their strategic interests.

The human rights community also plays an important role in defending rights and freedoms online, including protecting privacy, enabling freedom of expression and freedom of association, preventing discrimination and incitement of violence against vulnerable communities, ensuring the right to a fair trial, advocating for child online protection, and assuring access to online services and information. In the last decade, the human rights community – comprising governments, international and local civil society organizations, and human rights experts around the world – has been sounding alarms and bringing attention to existing and potential human rights violations through the misuse of digital technologies such as social media, autonomous intelligent systems, and other tracking and monitoring technology. The UN via its Special Rapporteurs, as well as the Council of Europe (CoE), have reiterated several times through their respective official documents and resolutions that the rights that exist in the analogue world also extend to the digital world and that "universal human rights apply equally online as offline." Their advocacy also focuses on "the need to keep human rights and human agency at the centre of technological development and the imperative to improve cooperation on digital security and trust."[32]

All these various cybersecurity "communities of practice" work at times together and other times separately to grow human, technical, and organizational capacity to address "essentially the same interconnected set of cyber challenges, [but] approach them from different angles with distinct mandates, aims, and cultures."[33] This has created a fragmented approach toward addressing the misuse of ICTs and digital technologies internationally. Each sub-discipline of the cybersecurity field has a strong network of individuals, but few of these people are connected to all of the sub-disciplines. This lack of coherence contributes "to the absence of an overarching global public policy narrative that connects the different communities' interests and elevates cyber policy to a strategic, cross-cutting issue for global policy leaders."[34] Unfortunately, the disconnect between these loosely connected communities of practice (arising from their distinct aims, mandates, and cultures) has cascaded down to create fragmentation within the cyber capacity building ecosystem, where various organizations involved in cybersecurity projects continue to use CCB activities to pursue their own aims and mandates.

Given the strong push to achieve the SDGs – and the availability of foreign assistance from multi-national donors, many governments in the developing world have begun to embrace digitization and digital technologies to foster their own economic growth and social development. However, "the trajectory of digitalization in the Global South diverges in various ways from that of more industrialized countries. As relative late adopters of digital technologies, developing countries engage in 'technological leapfrogging,' which in turn is interlinked with the risk of new and unprecedented vulnerabilities."[35] These governments' focus is on becoming more digitally connected, and cybersecurity is not necessarily a priority. As a result, many of these countries often lack the legal and regulatory frameworks to adequately combat cybercrime, and the indigenous expertise or the trained personnel who understand the digital threats within their country and who can effectively manage cyber risks and vulnerabilities in their society.

Many governments in the developing world are focused on becoming more digitally connected, and cybersecurity is not necessarily a priority.

They also often lack adequate institutional capacity (e.g., designated overarching units or competent authority that can set up the cybersecurity agenda and coordinate national efforts). This capacity gap can undermine the demand for digital resilience or requests/understanding of why cybersecurity activities are an important component of their digital development agenda.[36] Because countries' rapid digitization was not accompanied by adequate investments in cybersecurity and resilience, they are now experiencing greater vulnerabilities and malicious activities that are causing harm to their national critical infrastructure and services and to their citizens. As lower- and middle-income countries become even more digitized and reliant on ICTs, understanding digital threats and developing local institutional and workforce capacity to harness and manage their digital transformation and mitigate related risks become indispensable components of a growing digitized economy and society. It is also important to recognize that increased internet connectivity and digitization can lead to economic prosperity and sustainable development, but only if the internet and the ICT infrastructure that underpin them are safe, secure, and resilient.[37]

As lower- and middle-income countries become even more digitized and reliant on ICTs, understanding digital threats and developing local institutional and workforce capacity to harness and manage their digital transformation and mitigate related risks become indispensable components of a growing digitized economy and society.

Despite their related goals, however, the digital development community and the cybersecurity community continue to operate primarily in their own disciplines. There are a number of reasons for this disconnect – some intentional and some accidental.

2.3 Defining "Cyber Capacity Building"

Cybersecurity preparedness/readiness, digital resilience, and cyber capacity building have become a growing priority for those seeking assistance – both in developed and developing countries.[38] The need to align and expand cybersecurity and digital resilience efforts has been growing exponentially as the scope, volume, and sophistication of cyber incidents, state-sponsored attacks, ransomware, supply chain compromises, and digital disruptions increases.

Cyber capacity building emerged as an international policy concept in the first decade of the 21st century, when a handful of countries and international organizations began to include it within policy documents and national strategies. As awareness of the concept grew, a *core cyber capacity building community* started to develop around it, bringing together those original parent communities (e.g., law enforcement, technical, foreign policy, human rights) that had been pioneers in undertaking CCB activities. Nonetheless, "the 'niche' nature of cybersecurity in the global policy agenda" has kept these issues relegated to a smaller community of experts or practitioners, and "negatively impacted the integration of cyber capacity building into the development agenda." [39] This is not helped by the fact that the concept of *cyber capacity building* remains an amorphous term. No consistent definitions nor internationally agreed-upon standards or frameworks exist to define what should be included within this term or who should be responsible for these efforts.

During the desk research and several interviews conducted to inform this report, it emerged that major stakeholders in both the cybersecurity and the development communities have outlined different – sometimes overlapping – CCB themes, topics, principles, pillars, dimensions, or sets of activities that they include in their specific "buckets of capacity" (see Figure 1 on page 26). These concepts span from creating or adapting organizations to promoting institutional reforms, to establishing cyber incident management plans, to developing human resources, and more. Figure 1 depicts a variety of activities included as part of cyber capacity building by major international organizations and donor countries.

At least one definition from the literature describes international cybersecurity capacity building as "an umbrella concept for all types of activity in which individuals, organizations or governments collaborate across borders to develop capabilities that mitigate risks to the safe, secure and open use of, and relationship with, the digital environment."[40]

Interestingly, the country of Israel has adopted the broadest definition of cyber capacity, including: building the capacity of government organizations to defend themselves from cyber risks; the capacity of regulators and government agencies to guide, control, regulate, and support their own organizations and those they oversee; the capacity of the state to monitor, mitigate, and respond to national-level cyber threats through national and sectoral CERTs, CSIRTs, SOCs, ISACs, ISAOs, and other expert centers; the development of institutional, legal, and regulatory capacity;

ITU	**Cybersecurity Strategy/ Frameworks**	**Develop National CSIRT & Conduct CyberDrills**	**Facilitate Access** to existing resources to develop national legislation to combat cybercrime (i.e., Combatting Cybercrime Toolkit)	**Combat SPAM** (Solutions and Awareness)	**Technology Standards**		**Inclusivity** of women and youth (workforce development, Child Online Protection)
GFCE (themes)	**Cybersecurity Strategy and Policy**	**Cyber Incident Management and Critical Infrastructure Protection**	**Cybercrime**	**Cybersecurity Culture and Skilled Workforce**	**Cyber Security Standards**		
European Commission (pillars)	**Strategic Framework**	**Incident and Crisis Management**	**Criminal Justice in Cyberspace**	**Cyber Hygiene and Awareness**			
African Union	**Cybersecurity Policy and Strategy** (national strategies, assessments, cyber diplomacy)	**Cyber Incident Management & Critical Information Protection** (national computer security incident response)		**Cybersecurity Culture & Skills** (cybersecurity awareness, education and training, workforce development)			
OAS (pillars)	**Policy Development** (development of national or regional cybersecurity strategies)	**Technical Capacity Development** (critical infrastructure protection, development of CSIRTs, training and cyber exercises)		**Research and Outreach** (development of technical documents, toolkits, & research-based reports to guide stakeholders on current developments, cybersecurity problems, and key challenges in the region)			
IDB	Provide funding to LAC governments to develop cybersecurity **strategies, policy, and initiatives**	**Technical Assistance** (critical infrastructure protection, development of CSIRTs/SOCs, training, information sharing, incident response)	**Cybercrime**	**Cybersecurity Research, Knowledge Dissemination, and Outreach** (societal issues, cybersecurity education and awareness, workforce development)			
U.S. State Department	**Cybersecurity Strategy and Policy**	**Incident Management** (coordinate cybersecurity watch, warning, response, and recovery efforts)	**Fight Cybercrime** (updating criminal laws, procedures, and policies)	**Cybersecurity Culture and Skills** (increasing awareness of citizenry and industry of their critical role in protecting cyber systems [following UN GA Resolutions 57/239 and 58/199])		**Increase government-industry collaboration** (public-private partnerships) to manage cyber risk and share knowledge	
UK (dimensions)	**Policy and Strategy**	**Incident Management**	**Cybercrime**	**Culture and Society Education, Training and Skills**	**Standards and Technology**		

Figure 1: CCB themes, topics, principles, pillars, or dimensions as defined by organizations/agencies within the cybersecurity community.

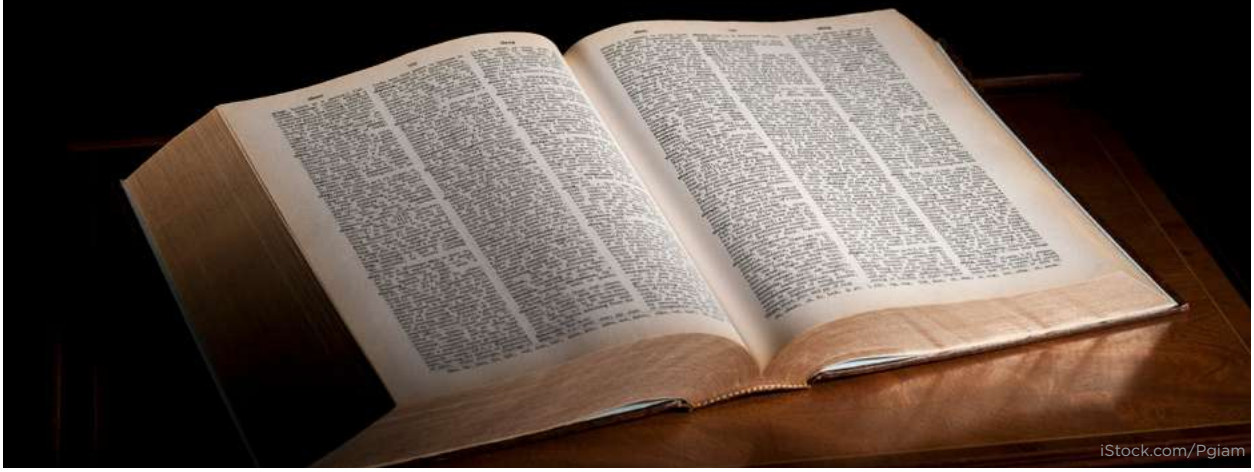
the capacity to collaborate with other countries to share information and promote collective defense; and supply side market capacity – the ability to develop products, services, and capabilities to prevent, manage, and respond to cyber risks (including industrial capacity, academic capacity, and the development of a professional workforce) and to transfer/export Israeli know-how, innovation, technologies, and expertise abroad.[41]

Perhaps even more important is that there is no common definition of even the word "capacity" between the development community and the cybersecurity community. According to the Merriam-Webster dictionary, the word "capacity" is defined as: "one's mental or physical ability" or "the facility or power to produce, perform, or deploy." Some organizations also define it as enhancing individual and institutional knowledge and skills to address (policy) challenges. Neither the development nor the cybersecurity communities, however, see "capacity building" in the same way. Some view it as technical assistance or strictly training programs and digital skills formation, whereas others view it as connectivity. Very few organizations view capacity building as the whole gamut – institutional, governance, legal, technical, and operational capacity development. Because they do not have a common definition of what "capacity" is or how it should be developed, they often talk past each other.

The rest of this report highlights some of the key challenges and benefits of incorporating cybersecurity, digital resilience, and cyber capacity building into the broader development agenda. It also features some good practices and identifies select bridging venues and activities that could facilitate tighter alignment and collaboration between the two communities and among donors and implementors of both digital development and cyber capacity building initiatives.

No Common Definition of Capacity

Very few organizations view capacity building as the whole gamut – institutional, governance, legal, technical, and operational capacity development. Because they do not have a common definition of what "capacity" is or how it should be developed, they often talk past each other.



3 BRIDGING THE DEVELOPMENT COMMUNITY AND THE CYBERSECURITY COMMUNITY

3.1 Understanding the Gaps Between Digital Development Assistance and Cybersecurity Activities

Despite having related goals of strengthening digital capacity building, including the ability to effectively use advanced technologies while at the same time ensuring that citizens remain safe, protected, and productive online, the digital development community and the cybersecurity community operate primarily within their own disciplines. They rarely partner and embed cybersecurity activities within digital development projects. This is partly because they do not see that digitization and resilience are two sides of the same coin. Building digital capacity encompasses a wide range of activities that span from expanding broadband access and internet connectivity, to facilitating participation in the digital sphere, to modernizing industries and critical infrastructures with advanced technologies that are dependent on internet connectivity. Digital capacity has a positive narrative – it benefits society. Yet, rapid digital transformation – underpinned by affordable communications and cheap devices – has introduced new risks and vulnerabilities that cannot be ignored. The cybersecurity community, which can be more technical and more security-oriented, views these threats to networked infrastructures and society as risks that must be managed. Cybersecurity, therefore, is often seen as an activity best delivered by those with expertise from the military, law enforcement, or intelligence disciplines. This is antithetical to how the development community operates and delivers assistance. Because cybersecurity capacity has associations with the security sector, cybersecurity capacity building would be better framed in the context of "digital" resilience, safety, trust, sustainability, and risk management, linking security with sustainable economic development and human rights.

Cybersecurity capacity building should be framed in terms of "digital" resilience, safety, trust, sustainability, and risk management, linking security with sustainable economic development and human rights.

Moreover, these two communities do not typically frame their activities in the context of the broader economic objectives or specific needs and circumstances of the countries where they fund projects, digitize infrastructures, or hope to build capacity – nor do they usually coordinate their respective capacity building efforts on the ground. There are a number of reasons for this lack of partnership – some of which are intentional, and some accidental.

3.2 Cybersecurity and Digital Resilience are Not Viewed as a Necessary Component of Development

The broader international development community is beginning to recognize that cybersecurity and digital resilience are important components of development.

While the development community continues to invest hundreds of millions of dollars in developing countries to achieve the SDGs by building "smart" infrastructures and digitizing greater portions of society, the assistance projects have not placed the necessary attention (or de-risking mechanisms) to the heightened and novel digital risks that come with digitization and increased use of ICTs. First, there is a knowledge gap. MDBs do not see old-school infrastructure projects as digital and, therefore, do not build in de-risking measures. "Development donors are hesitant to fully embrace cybersecurity as a development issue."[42] Instead, this community sees digital technologies as a necessary means to accelerate the achievement of the SDGs and does not necessarily appreciate the "dark side of the innovations."[43] The risks of the misuse of digital technologies, including becoming tools for cybercrime, unauthorized surveillance, promoting disinformation, enabling digital authoritarianism, exploiting data, facilitating espionage, etc., and how they could harm their development projects and goals are not top of mind. Coupled with the knowledge gap is a communication challenge. Digital risks to projects come in many forms and usually have a technical underpinning. If risks are not evaluated and communicated at the formulation of a project, the translation may not be carried through the lifecycle of the project. As a result, most organizations are not building the necessary de-risking processes or safeguards (similar to environmental or social safeguards) into their procurement, assistance, or investment operations to manage cybersecurity/technology-related risks.

Most development organizations are not building the necessary de-risking processes or safeguards into their procurement, assistance, or investment operations to manage cybersecurity/ technology-related risks.

Yet, even when cybersecurity or digital resilience are considered or embedded in the formulation of a project, there is often an internal disconnect between the policy people and the programmatic people dedicated to a given project – within both the development and cybersecurity communities. In addition, national or international funding agencies and other large donors do not always have the right "implementors" for their projects/lending operations. This sub-community of organizations that implement projects and provide technical assistance range from global consultancy firms to small and specialized consultancies, to international organizations (e.g., OSCE, ITU, UNODC), to academic and non-governmental institutions. However, it is difficult to find implementors who will instinctively include cybersecurity or de-risking mechanisms in the project, especially if it was not part of their contract requirements or budget allocation. Moreover, the implementors who have become translators

between stakeholders within the development and the cybersecurity communities are not necessarily equipped to communicate the technical nuances. Understanding the specific needs of a country or region and knowing how to navigate highly politicized cyber-related issues are key skills. For example, implementors should remain impartial. If a recipient country needs to reform or update its cybercrime legislation, the implementor should know, and be able to communicate the differences and similarities of existing regional conventions or agreements (i.e., Council of Europe's Convention on Cybercrime vs. Shanghai Cooperation Organization's Agreement on Cooperation in the Field of Information Security vs. African Union Convention on Cybersecurity and Personal Data Protection).

Highly publicized cyber incidents have also further politicized the already complex topic of cybersecurity from a geopolitical perspective. When the national rail transportation is knocked offline in Iran, or the Ministry of Justice is ransomed in South Africa, or the oil and gas pipeline and food supply is ransomed in the United States, these events are seen within the ambit of national security, national defense (military), criminal justice (law enforcement), or as an intelligence problem. Additionally, cybersecurity is often entangled with data protection/privacy, trade and competition, and/or other geostrategic issues (e.g., Chinese vs. American vs. Russian technologies). Therefore, cybersecurity is often perceived as too political, and avoided as a focus area or investment line by donors across the board. Moreover, "because development spending can be perceived as zero-sum, money spent on cybersecurity could be seen as taking away from money potentially invested in alleviating other development stresses."[44] These circumstances, thus, both elevate the political sensitivity of digitization and have an indirect negative effect for international organizations or countries who want to provide foreign aid but are unable to include it as part of their development assistance because it falls outside the scope of the DAC criteria for Official Development Assistance. To circumvent this situation, in the Asia Pacific, the 2018 "Boe Declaration on Regional Security" was helpful in up-leveling cybersecurity as a cross-cutting issue and a development priority for investment and collaboration in the Pacific (Strategic Focus Area 5 is dedicated to "Cyber-enabled Crime and Cybersecurity").[45] This showed that, ideally, cybersecurity can become an integral component of the development agenda – beginning with the design of any new development project – and, can be considered an eligible development assistance criterion for foreign aid and development support if it has the right political backing and buy-in. (DAC would still need to update its ODA eligibility criteria to include "cybersecurity" and/or "digital resilience.") Other countries, including the U.S., UK, Germany, Israel, and Estonia have found other pathways to fund cybersecurity initiatives (e.g., development of institutional capacity, cybersecurity training for government entities or police forces, rapid incident response assistance, cybersecurity awareness campaigns, cyber hygiene education, and more) as part of their development assistance programs or as special items outside ODA-eligible programs (e.g., U.S.-funded cybersecurity activities in Georgia via NATO's Partnership for Peace program). In the case of the UK, for example, assistance funding for CCB activities was allocated by designing projects

whose primary objective is to support delivery of the SDGs and that do not work with military or intelligence agencies (but can work with police). However, these approaches are not necessarily scalable by a small group of Ministries of Foreign Affairs who are pioneering the use of ODA funding for CCB activities, and incorporating cybersecurity and digital resilience is still not considered foundational to digital development by the broader development community.

Recipient countries are also faced with a similar challenge, and may not appreciate the increased exposure to cyber risk that comes with digitization. Therefore, recipient governments may not request cybersecurity or digital resilience enhancing capacity when accepting donor funds/grants/loans to support their digital transformation and developing their digital agenda. "In part due to the perceived complexity of cybersecurity, some recipients of development assistance – the stakeholders who largely drive the direction of spending – struggle to include cybersecurity in their development investment strategies."[46] This is also partly because the recipient country may lack awareness of why cybersecurity matters to its digital transformation or lack innovative approaches to its own strategy/policy development and simply wants to copy what other larger countries have developed and that is perceived as successful. However, many developing countries cannot absorb the best practices developed by other more advanced countries.

Moreover, both the development community and recipient countries see ICTs as long-term capital assets and expenditures, rather than commodities that will need to be updated and replaced within a five to ten-year period. This leaves a critical shortfall in the sustainability of a program and its future fragility, because it can no longer be used safely. For example, many developing countries cannot afford the longer-term costs to sustain institutions (e.g., national cybersecurity agency, national CERT/SOC) or the workforce salary requirements incubated and funded using development loans or donors' money. A digital development project's total-cost-of-ownership and ICT refresh must, therefore, be included in project formulation and programmed into assistance packages. The future sustainability of these projects also requires the recipient country to embed ICT commodity refresh, new systems upgrades, workforce training and retention, etc., into their national budgeting process.

Both the development community and recipient countries see ICTs as long-term capital assets and expenditures, rather than commodities that will need to be updated and replaced within a five to ten-year period.

Both the development community and the cybersecurity community need to think ten years out when developing a project involving digital technologies and ensure its sustainability as a basis of programming/lending. If continued costs have not been considered and incorporated into the recipient country's national budget to support the local workforce, to update or replace equipment or software, or to buy licenses after the first five to ten years, then the programs/

institutions developed become unsustainable or obsolete after depletion of the initial funds occurs. In most cases, development aid or other types of low-interest loans for CCB activities simply end up becoming an extra financial burden on the recipient country. In order to sustain capacity, the development community and the cybersecurity capacity building community need to ensure that programs in recipient countries incorporate the sustainment funds (e.g., continuity of the program, staff, equipment, etc.) into the country's national budget. Digital capacities broadly should be elevated into the government budget and become a recognized contribution to the country's GDP as the digital economy grows.[47]

Both the development community and the cybersecurity community need to ensure that a digital development project's total-cost-of-ownership and ICT refresh are included into the project formulation and programmed into assistance packages, and that the sustainment funds for the continuity of the development program, staff, equipment, etc. are incorporated into the country's national budget.

3.3 Supply vs. Demand and Exporting Capabilities vs. Building Indigenous Capacity

Sustainability – the ability to maintain a certain rate or level of capacity – requires focus upon developing an indigenous ability to maintain, support, and defend digital or cybersecurity investments. However, the cybersecurity capacity building community mostly continues to address the perceived shortfalls of a recipient country with a supply-driven approach, and uses a standard set of activities (e.g., development of national cybersecurity strategies, establishment of CERTs/CSIRTs, development of cybercrime legislation, etc.) that more advanced countries have and believe should be prioritized by developing countries. The CCB community does not regularly take a more strategic approach – including listening to the real needs of the recipient country – to meet the specific country demands or shortfalls. A cultural, historical, and socially nuanced evaluation should be considered when solutions are offered. Even the UN Roadmap for Digital Cooperation recognized that "one of the primary challenges to date is that a large part of digital capacity-building has been supply-driven as opposed to needs-based."[48]

"A large part of digital capacity-building has been supply-driven as opposed to needs-based."

This set of predetermined activities that the CCB community continues to "supply" is part of an "outdated" playbook that needs to be updated to the digital era and tailored to individual and national circumstances. Many of the people and organizations interviewed for this report stressed the need to connect cybersecurity and digital resilience with the economic aspirations, digitization strategies, and development priorities of recipient countries. This is a key area for digital cooperation among the donor and CCB communities.

A related problem is that many developed countries have adopted an export model for capacity building. They are exporting

Cybersecurity and digital resilience activities should be connected with the economic aspirations, digitization strategies, and development priorities of recipient countries.

knowledge, tools, people, and capabilities, rather than building robust indigenous capacity as part of their aid programs. Some donor activities are intended to project national influence to meet foreign policy objectives, fulfill economic mandates, and extend corporate operations (and influence) into the recipient countries, but they rarely involve local experts or build on existing local communities, structures, or grassroots networks. "In many cases, cybersecurity [or digital] capacity builders – donor government representatives, their contractors, corporations, and sometimes nonprofits – fly in, conduct a workshop or training session, and leave. While this is not universally the case and some projects or programs involve more extended in-country engagement, these projects appear to be the exception rather than the rule."[49] Many recipient countries have raised these issues, pointing out that donors only occasionally ask the local community (e.g., political, commercial, or academic leaders) what they need or conduct a baseline assessment of what they have. In some cases, various foreign entities may have conducted multiple assessment studies. However, some assessments remain unpublished, while others are open only to the commissioning government, are not publicly available, or are not built upon further because they were only meant to justify the continuation or expansion of development or CCB projects.

Establishing an understanding of the political, technical, and social maturity and capacity to absorb help is an important first step to building capacity. Indeed, sustainable socio-economic-technical change requires an understanding of the political, cultural, and economic context in which a digital intervention or CCB initiative takes place. Therefore, "having a local sense" and developing "digital solutions [and cybersecurity activities] designed with knowledge of local ecosystems and culture" is crucial.[50] Tailored approaches can determine the extent to which capacity building efforts can be adaptable and scalable. However, because so many current projects do not involve local experts or build on existing local communities/structures, indigenous capacity is not being created.[51] This lack of local capacity – cybersecurity professionals equipped with robust tools – has led many recipient countries to outsource services to meet their cybersecurity needs and thus, perpetuate the export model.[52] Unfortunately, the donor community is also perpetuating this export model.

Establishing an understanding of the political, technical, and social maturity and capacity to absorb help is an important first step to building local capacity.

3.4 Bringing Transparency to Digital Development and CCB Activities

To maximize resources, avoid duplication of initiatives (which is expensive and inefficient), and/or find potential synergies, the donor organizations or countries should first understand who else is supporting the recipient country. They should conduct an assessment of other ongoing or forthcoming development and/or CCB projects in the country or region before designing, funding, or implementing their new digital development and/or CCB projects to better serve that country. This assessment could precede or occur concurrently with a digital risk/maturity assessment of the country or sector under consideration for foreign assistance.

Donors involved in digital development and/or CCB activities fall primarily into two main categories: multilateral organizations or foundations and nation-states (bilateral donors). International organizations, MDBs, and foundations base their digital development lending operations or technical assistance projects on their mandate. Some have a specific focus region, like the OAS and IDB for Latin America and the Caribbean. Others, such as EBRD, prioritize emerging economies, while the EU prioritizes Africa and Europe's eastern and southern neighborhood. Donor countries tend to prioritize their foreign assistance funding to their national foreign policy and economic interests and, therefore, target specific countries/regions of the world that support those interests. These different approaches have also contributed to what has become termed a group of "darling countries" (e.g., Kenya, Ukraine, Vietnam), which receive multiple offers of foreign aid from different donors, versus a group of "orphan countries" (e.g., Somalia, Syria, Yemen, Sudan) that is rarely the focus of foreign assistance by developed countries or donor organizations, partially because of their territorial conflicts.

If donor organizations' digital development initiatives and CCB activities were

Different approaches to digital development lending operations and foreign assistance funding have contributed to the practice of favoring "darling countries" that receive multiple offers of foreign aid from different donors, while neglecting "orphan countries" that are rarely the focus of foreign assistance.

more visible to each other project and responsible entity, some of these challenges could be mitigated. "To overcome these challenges, two aspects are central: greater coherence and coordination in capacity-building efforts; and a concerted effort at scaling up solutions."[53] Local communities should be deeply involved and consulted in the very planning of these actions and in the shaping of activities based on what makes sense and what can/will be sustainable, while donor organizations should do more to coordinate their efforts and develop cooperation policies, co-investments, hand-off mechanisms, and business models tailored to the specific needs of a country/region – which, in turn, would help increase the sustainability, adaptability, and scalability of projects. "Holistic, inclusive approaches that bring together existing initiatives, United Nations entities, regional and subregional bodies, and other relevant organizations that promote digital capacity-building are necessary to improve support for governments and other stakeholders."[54]

The UN Development Coordination Office (DCO)[55] maintains Resident Coordinators (RCs) in each of the UN program countries, resulting in a vast on-the-ground presence. These RCs are the key conduit for supporting UN's activities for sustainable development, which could also be a natural point of visibility for other donors. It can "connect the dots" and help donor organizations understand the activities underway in the recipient country and potentially highlight underserved needs. In particular, RCs have a convening authority and influence in their country of operations and could serve as the natural conveyor/aggregator among other donors, as well. The RCs are responsible for coordinating programs on the ground across all UN agencies, which provides them with the most-centrally coordinated view of all the UN programs in a given country. They can also receive additional requests or signals from recipient governments and guide those requests to the right agency that can provide the right kind of support.

3.5 Lack of Local Data, Trends, and Field Research to Make a Compelling Argument

Developed countries use data to drive decisions. Local data, trends, statistics, and field research that characterize the threat within a country or region can provide compelling evidence to drive economic and political arguments as to why cybersecurity is an important and necessary component of digital development. Nonetheless, having reliable, accessible, and up-to-date data on digital risks and cyber threats remains a challenge, particularly for developing countries. Data are needed to better understand and characterize the threats and risks associated with ICT adoption, internet uptake, and digitization without incorporating risk-reduction activities.

Local data, trends, statistics, and field research that characterize the threat within a country or region can provide compelling evidence to drive economic and political arguments as to why cybersecurity and digital resilience are important and necessary components of digital development.

The few available reports and statistics on cyber-related issues in developing countries still cite western sources and are not based on local data sets from the region/country. Moreover, finding, aggregating, and disseminating the right data (e.g., cost of cybercrime/ransomware and its impacts on society) remains challenging even for more developed countries. The OECD, a well-known knowledge hub for data and analysis, has a formalized reporting system to collect specific data from bilateral and multilateral providers of development cooperation to developing countries, but also struggles to find the necessary data to estimate the cost of cybercrime (methodological and empirical issues).[56]

Engaging different local stakeholders – including governments, civil society, and academia – to cooperate on data production and use, and dedicating funding to local universities or researchers to gather local evidence and necessary data or to conduct trend analysis may help generate local buy-in.

4 CREATING DIGITAL PUBLIC GOODS

Some organizations involved in digital development and/or cyber capacity building have started to develop **"Digital Public Goods"** (DPGs). These universal tools and instruments can promote sharing of best practices and assessment tools; identify talent, and pool data sets; serve as a "clearinghouse" to better direct requests for support (e.g., GFCE); enhance support to national capacity building efforts; and amplify country-level support (e.g., CREST). These types of efforts can serve multiple communities, allowing the focusing of funding toward developing countries' greatest needs. Even the 2020 UN Roadmap for Digital Cooperation acknowledged the need for the global community to "undertake a concerted global effort to encourage and invest in the creation of digital public goods [such as] open source software, open data, open AI models, open standards and open content," as a way to help support and accelerate the SDGs.[57] There are a number of efforts already underway to develop DPGs that emerged during the interview process, including:

- The **Gates Foundation** is funding projects to create "digital public goods" (e.g., institutional and operational capacity; frameworks/tools to measure the maturity of the cybersecurity ecosystem of a country and/or specific sectors; good practice guides on how to create a CERT/SOC, how to lead the procurement of security services and products, how to hire the right personnel, and how to train the local workforce, among others). Examples include:

a. The **African Union-GFCE** Collaboration on "Enabling African countries to identify and address their cyber capacity needs."[58] As part of this two-year collaborative project (2020 - 2022), the GFCE serves as Secretariat to an **African Coordinating Committee** that includes relevant organizations from all 55 African countries that have a stake in CCB. The goal is to enable these countries to better understand cyber capacities and support them in strengthening their cyber resilience. In particular, the project intends to: 1) bridge "foundational" expertise (supply-driven approach) and grow a trusted community of cyber leaders from the different African countries; 2) identify relevant cyber capacity gaps on a national and sub-regional level in African countries, and enable these countries to prioritize, address, and communicate their national cyber capacity in a tailored way; and 3) foster coordination and increase international collaboration between (existing) cyber capacity building efforts in Africa. The project focuses on three key CCB themes: 1) Cyber Security Policy and Strategy (i.e., Strategies, National Assessments, Confidence Building Measures and Norms, Cyber Diplomacy); 2) Cyber Incident Management & Critical Information Protection (i.e., National Computer Security Incident Response); and 3) Cyber Security Culture & Skills (i.e., Cyber Security Awareness, Education and Training, Workforce Development). The project and final report will come to fruition in 2022.

b. The **CREST Cybersecurity Maturity Model Assessment** is a freely accessible, affordable, sustainable, and scalable framework to measure the maturity and financial inclusion of the cybersecurity ecosystem of a country across five dimensions: 1) National Cybersecurity Strategy & Capabilities; 2) Cybersecurity Information Sharing; 3) Cybersecurity Service Provision; 4) Cybersecurity Professional Development; and 5) Banking Sector Risk Posture. The resulting country assessments can be used to compare country sector organizations, identify good practices and areas of common concern, monitor the impact of investments, and define clear, measurable objectives for improvement. CREST, an international not-for-profit accreditation and certification body, has made building capacity in the global cybersecurity market its main mission. It is working to identify other good practice guidance/Digital Public Goods as part of its capacity building efforts to support maturity level improvement in all areas of the cybersecurity ecosystem, especially financial inclusion.[59] Their available good practices guidance includes: 1) How to establish an effective cybercrime unit; 2) How to create a CERT/SOC; 3) How to re-skill/up-skill the workforce; and 4) How to procure cyber products and services (i.e., "Service Selection Platform" to help governments, regulators, and buyers in identifying trusted suppliers that can deliver high-quality technical security services).

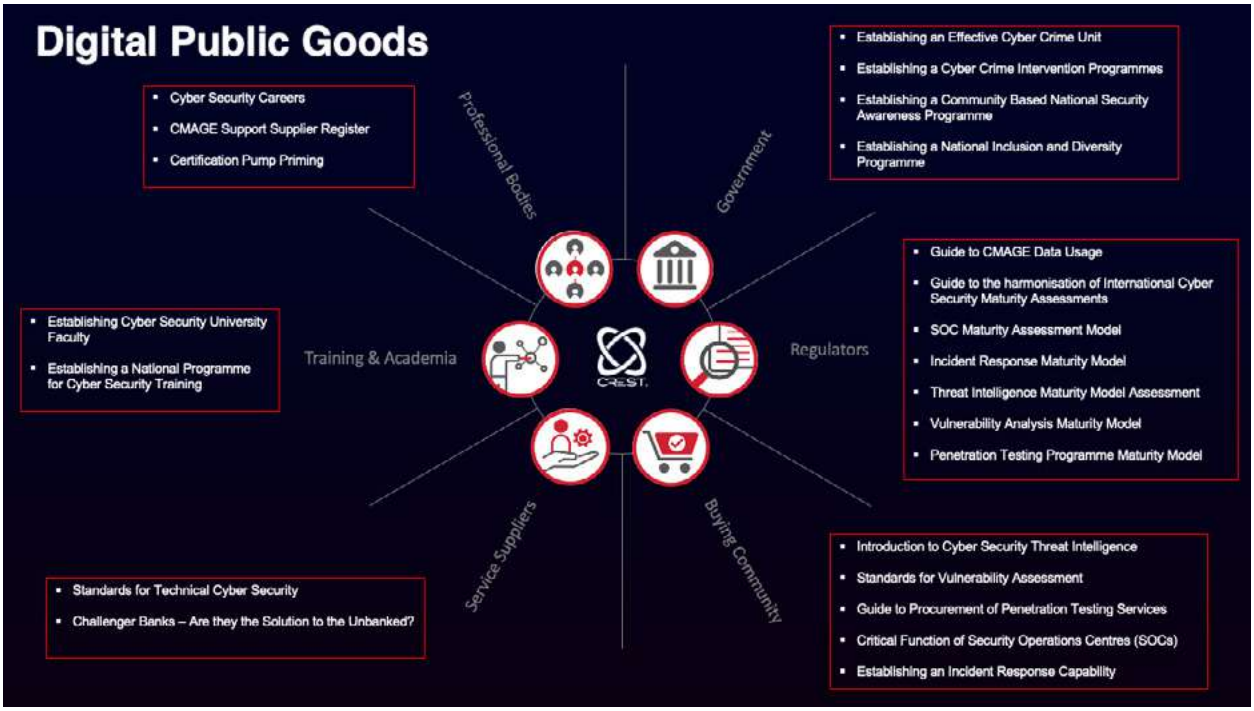


Image provided by CREST

c. The **CyberLab-Africa initiative** – a collaboration between Carnegie Mellon University's (CMU) CyLab and CMU-Africa that aims to improve access to financial technologies and to build public trust in those technologies. This investment consists of five primary initiatives implemented via a network of university partnerships in Africa. In one research area, the CMU team conducts assessments of the current cybersecurity landscape among African FinTech operators to better understand the cyber readiness of the sector and to evaluate the maturity of financial inclusion. This leads to an evaluation of the digital identity infrastructure (based on a Modular Open-Source Identity Platform or MOSIP) for identity management – a predicate to fielding a test deployment of the MOSIP identity management platform at CMU-Africa. They also use the results of these assessments to develop open-source tools for threat intelligence sharing and diagnosis to enable network operators (e.g., of digital identity systems like MOSIP) to outsource the detection of malicious activity to trained professionals. Finally, they are designing training programs for cybersecurity workforce development, with a particular focus on identifying female participants who may not already be in cybersecurity-related roles.[60]

- The **Digital Impact Alliance** (DIAL) – a "think, do, replicate" tank housed at the United Nations Foundation with a mission to help countries accelerate their digital transformation and responsible data use journey and to "overcome the systemic barriers preventing digital solutions from going to scale." DIAL serves as a neutral broker, bringing together government, industry, and other development stakeholders to promote new solutions to old problems. One of the primary ways DIAL promotes new solutions for historically underserved regions and populations worldwide is by leveraging big data analytics to support sustainable development. They aggregate and analyze relevant data gathered by mobile network operators (MNOs) to shed light on how data and digital technology can transform the development and humanitarian sectors and help to solve some of the most intractable development problems.[61] The Gates Foundation, the UK Foreign and Commonwealth Development Office (FCDO), U.S. Agency for International Development (USAID), the Swedish International Development Agency (Sida), and the United Nations Foundation founded this initiative in 2015.[62]

- The **Digital Public Goods Alliance** (DPGA) – "a multi-stakeholder initiative with a mission to accelerate the attainment of the sustainable development goals in low- and middle-income countries by facilitating the discovery, development, use of, and investment in digital public goods."[63] The Alliance defines DPGs as "open source software, open data, open AI models, open standards, and open content that adhere to privacy and other applicable laws and best practices, do no harm by design, and help attain the SDGs," and promotes DPGs to create a more equitable world. They maintain the DPG Standard and Registry, in which they curate available DPGs based on their usefulness and robustness. They also financially support DPG capacity building activities and oversee DPGs pathfinding

pilots (e.g., the Global Digital Library; platforms to aggregate and layer sector-specific health data; etc.) in low- and middle-income countries that can inform the creation of new DPGs aimed at building local capacity or support existing DPGs that are locally managed through adaptation and implementation. In addition, the DPGA convenes expert communities of practice (CoPs), which are groups of experts who work to discover, assess, and support the advancement of DPGs with high potential for addressing critical development needs.[64] Incubated by the government of Norway and the UN Children's Fund (UNICEF), the DPGA relies on engagement and leadership from pathfinder countries, private sector technology experts, think tanks, governments, philanthropic donors, international implementing organizations, and the UN. The Rockefeller Foundation is integrally involved in this initiative.

- The **World Bank**, in partnership with seven other organizations including CoE, ITU, and UNODC, has developed a **Cybercrime Toolkit** dedicated to building capacity among policy-makers, legislators, public prosecutors, investigators, and civil society in developing countries in the policy, legal, and criminal justice aspects to better combat cybercrime. This resource includes a Toolkit that synthesizes good international practice in combating cybercrime; an Assessment Tool for countries to evaluate their current capacity (or lack of capacity) to combat cybercrime and to highlight priority areas to direct capacity building resources; and a Virtual Library with materials provided by partner organizations and other participants to share information, experience, and expertise on combating cybercrime.[65]

- The **GFCE** hosts the ***Cybil Portal*** – the largest database of existing CCB methodologies, frameworks, expert organizations, and projects, and a knowledge hub that brings together stakeholders from the cyber capacity building community to collaborate on and share CCB research and initiatives.[66] It also serves as a clearinghouse to match needs for cyber capacities with offers of support and help to connect donors, beneficiaries, and implementors.

- **USAID** has recently released a **"Cybersecurity Primer"** for missions and for implementing partners that shows how to incorporate cybersecurity and digital resilience safeguards throughout USAID's Programming Cycle. This tool provides an overview of why cybersecurity and digital resilience should become a first-order strategic and operational priority across all phases of a project design and implementation in order to ensure digital sustainability and resiliency. The Primer is intended to increase awareness and provide a basic understanding of cybersecurity, cyber threats trends by sector, and digital resilience as they relate to development programming for USAID staff, which can serve as a resource to help streamline cybersecurity into the broader development community.[67]

- The **UK FCDO** developed a **Digital Access Diagnostic** tool, as part of its Digital Access Programme (DAP), to conduct detailed country assessments to determine the most relevant investments of their DAP development aid. These country diagnostics look at the current state of the country under three main areas: 1) digital inclusion;

2) capacity of government, society, and the economy to manage cyber risks; and 3) status of the local digital economy. The resulting assessment and business case serve to guide the FCDO in tailoring their DAP program to the specific needs of the recipient countries (i.e., Brazil, Kenya, Indonesia, Nigeria, South Africa) and to diversify the delivery models across three pillars (in-house delivery, outsourced delivery, or a mix of the two). This diversification also helps keep the program flexible, sustainable, and adaptable to current circumstances (e.g., increased use of telemedicine and remote learning during COVID-19 crisis). What is most unique about this tool, and the overall DAP program, is its focus on the local digital economy, the enablers for digital inclusion, and the development of sustainable digital solutions that can be applied locally – as an example of "tech for good."

- The **UNDP** developed a **Digital Readiness Assessment** (DRA) tool (they conducted a first pilot in Kosovo[68]) to provide rapid, high-level insights into a country's digital strengths and weaknesses; to map out the shape, pace, and types of transitions happening; and to identify what can be done to accelerate digital transformation efforts and agendas of a country, while ensuring an inclusive, whole-of-society approach to digital development – to "leverage digital to achieve the SDGs." The tool starts with a survey, followed by a longer-term, thorough consultative process. The resulting assessment provides a detailed Digital Readiness Index of the country for each of the key pillars (i.e., Infrastructure, Government Services, Regulations[69], Business, People) of the UNDP Whole-of-Society Digital Transformation framework. The UNDP uses this tool as a basis to discuss possible UNDP support. It serves as a top-level framing that could encompass other frameworks, and as an "entry point" to increase engagement with the country's government and improve coordination and clarity to drive a whole-of-government and whole-of-society approach to digital transformation.[70]

Inclusive Whole-of-Society Digital Transformation Framework

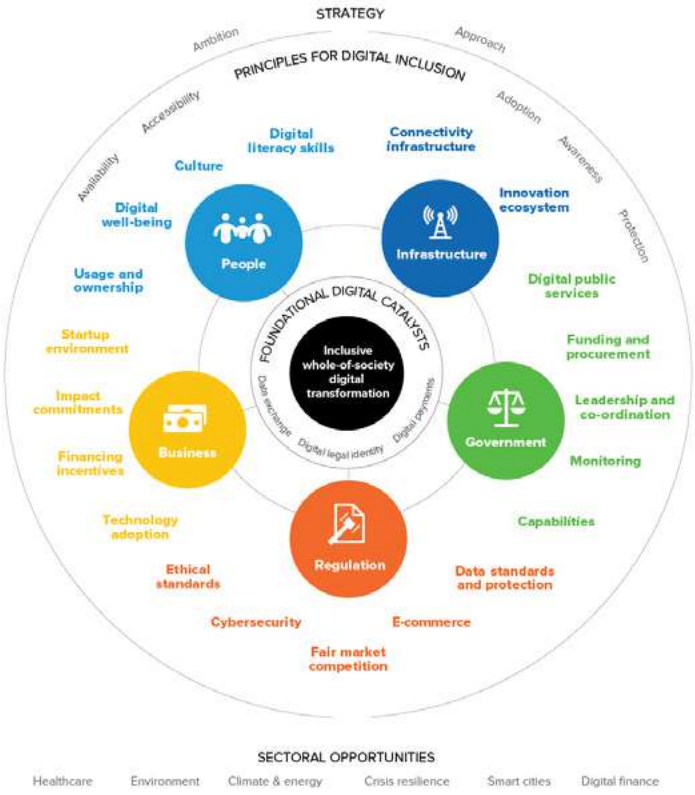


Image provided by UNDP - draft version, November 2021

- The **DiploFoundation** has developed a tool to map how digital technologies can facilitate the successful implementation of each of the sustainable development goals (SDGs), and provides specific examples of broad digital transformation initiatives and local measures that can support the realization of specific SDGs. For instance, "#eSkills4Girls," an initiative based on cooperation between several actors, namely, the G20, UNWomen, OECD, ITU, UNESCO, and the German Federal Ministry for Economic Cooperation and Development (BMZ), seeks to contribute to SDG 5 on Gender Equality, in particular in developing countries, by sharing information, recommendations, and good practices on digital inclusion of women. Platforms such as "Ecubi" in Mexico or the "Too Good to Go" application in Europe are currently used to fight food waste, but also to distribute excess food to those in need at the local level and, therefore, contribute to SDG 2 on Ending Hunger. Other local projects such as the "e-Rezeki" and the "eUsahawan" launched by the Malaysia Digital Economy Corporation promote SDG 1 on Ending Poverty by helping individuals acquire digital skills and find work online.[71]

5 BENEFITS OF INTEGRATING CYBERSECURITY, DIGITAL RESILIENCE, AND CYBER CAPACITY INTO DIGITAL DEVELOPMENT AGENDAS

According to the ITU, at least 127 countries have published a national cybersecurity policy or strategy[72] and many of these countries have also articulated their focus on building a strong digital economy. While a positive development, it is also important that countries align their digital (economic) development agenda with their cybersecurity priorities, thus bringing heightened attention to the need to secure critical digital dependencies and to identify specific companies, services, infrastructures, and assets that, if harmed, would have grave economic and national security consequences on the country.[73] The recommendations within this report are intended to help multilateral organizations and other donors investing in digital development and cyber capacity building activities to integrate cybersecurity and digital resilience throughout the project lifecycle; to identify areas where they can partner and build mechanisms to de-risk their investments; to build stronger and enduring digital infrastructures and projects; and to accelerate the safe adoption of technologies to meet the intended outcomes of the SDGs. Risk mitigation, in particular, is essential to effective and sustainable digital development programs.

There are multiple benefits of integrating cybersecurity, digital resilience, and cyber capacity into digital development. At a foundational level, decision-makers need to gain a deeper understanding of the threats emanating from the potential misuse of ICTs and emerging

- √ Decision-makers need to gain a deeper understanding of the threats emanating from the potential misuse of ICTs and emerging technologies (e.g., tools for cybercrime, surveillance, disinformation, digital authoritarianism, data exploitation, espionage, etc.). This understanding can guide the development community in supporting countries' digital adoption and increasing their maturity in maximizing the use of new technologies as enablers of sustainable and secure development.
- √ Integrating cybersecurity insights and activities into development programs would lead to achieving better outcomes; streamlining processes/eliminating duplication of efforts/maximizing resources; and building stronger resilience, safety, security, and trust into recipient countries' digital transformation projects.

technologies (e.g., tools for cybercrime, unauthorized surveillance, disinformation, digital authoritarianism, data exploitation, espionage, etc.). This understanding can guide the development community in supporting countries' digital adoption and increasing their maturity in maximizing the use of new technologies as enablers of sustainable and secure development. On a more practical level, based on the interviews conducted with stakeholders responsible for digital development and cyber capacity building efforts in different organizations, regions, and countries, it is clear that integrating these aspects into development programs would lead to achieving better outcomes; streamlining processes, eliminating duplication of efforts, and maximizing resources; and building stronger resilience, safety, security, and trust into recipient countries' digital transformation projects. Also worth noting is that "developing countries are increasingly becoming hosts to the infrastructure and actors behind malicious cyber activities. Bridging the digital divide [and incorporating cybersecurity and digital resilience are] therefore important also with regard to responding to national security and various types of cyber threats in donor countries" and that we must "strengthen the global security landscape by limiting the number of safe havens for cybercriminals."[74]

Integrating cybersecurity, digital resilience, and cyber capacity into digital development programs would lead to achieving better outcomes.

5.1 Examples of Where Cyber Capacity Efforts Bridged to Digital Development or Where Digital Development Efforts Brought Increased Cybersecurity Maturity

During the interview process, some unique examples surfaced that could be replicated by other institutions. For example, some donor organizations have begun to embed digital safeguards (or de-risking mechanisms) into their digital development and infrastructure projects. There are also instances where cybersecurity activities have been incorporated into digital development initiatives (and vice versa) and helped to build real indigenous capacity. Additionally, there are communities of practice that have devised effective partnerships or cooperation mechanisms to build synergies and avoid duplication of efforts. Although anecdotal evidence is not a sufficiently strong foundation to bridge the gaps highlighted in this report and to link best practices to effective project impacts or outcomes, it is still worth highlighting some of those successful examples:

5.1.1 Value of Having Point-of-Contact Networks

- **Council of Europe**: The CoE has established a 24/7 Network of contact points to combat cybercrime under the Budapest Convention on Cybercrime (Art. 35). Parties to the Convention can send and receive requests for assistance not only for computer-related crime, but for all matters in which electronic evidence is involved – including receiving initial technical or legal advice to the requesting service, preserving essential data, or obtaining information on foreign forums about possible threats

(e.g., France-Charlie Hebdo terrorist attacks, business email compromises, fraud, etc.). The channel can also transmit requests for immediate assistance in cases when a person's physical safety is in question (from kidnapping, threats, etc.) and can provide useful information and alerts on cyber threats to critical infrastructures in other countries and indicators of compromise, if available.[75]

- **INTERPOL**: The International Criminal Police Organization (INTERPOL) established a secure global police communications network called I-24/7 that serves to connect member countries' national law enforcement with other countries and with INTERPOL General Secretariat. Each member country hosts an INTERPOL National Central Bureau (NCB) that can search for the information needed from other NCBs to help investigate crime or criminals in their own country and to share criminal data and intelligence to assist other countries through the I-24/7 network.[76]

- **OSCE Point-of-Contact Network**: The Organization for Security and Co-operation in Europe (OSCE) has established a "Point-of-Contact Network" to build partnerships and confidence among peer communities. This project is specifically dedicated to promoting the operationalization of the Confidence Building Measure (CBM) 8 on Points of Contact (PoCs) by enhancing its functioning both as a crisis communication network and as a platform for cooperation. This closed online platform/database, only accessible with a password, contains contact details of national PoCs – both technical (CERTs) and policy – and allows them to connect directly. The aim of this directory is not to duplicate already existing technical communities (e.g., FIRST, EU CSIRT network, etc.) but to serve as a regional risk-reduction mechanism aimed at preventing conflicts stemming from the misuse of ICTs by states. The OSCE Secretariat keeps the database up-to-date and validates the contact information (through so-called "Communication Checks"). Previously these people attended annual meetings of PoCs aimed at further building trust and confidence between experts, strengthening regional partnerships, exchanging best practices, promoting a common understanding of cyber/ICT threats, and discussing co-operative actions that can meaningfully address them – however, these in-person engagements have been disrupted by COVID.

  OSCE is now sharing its experience on establishing and maintaining this directory of policy and technical PoCs with other regional organizations and the UN as an example of good practice on how to operationalize CBMs.[77]

- **EU CyberNet**: The EU CyberNet platform was launched in 2019 to bring together a group of vetted experts from the cybersecurity community across the EU to increase cyber resilience and capacities worldwide, provide technical assistance to partner countries in tackling the growing challenge of malicious cyber activities, and strengthen the delivery, coordination, and coherence of the EU's external cyber capacity building projects.[78] In addition to creating a pool of EU cybersecurity experts, this voluntary-based network serves as a forum for connecting the stakeholder community in Europe, providing support to the European Commission's

services (i.e., expertise on external cyber actions), and building cybersecurity "train-the-trainers" curricula and training modules, as needed.

- **USAID Digital APEX:** USAID developed the Digital APEX resource of vetted cybersecurity services/experts/companies to strengthen the digital resilience of organizations across the range of sectors in which USAID invests, and to ensure successful international development outcomes. Implementing partners and beneficiary teams can tap into this list of pre-approved, U.S.- and regionally-located small businesses to receive rapid technical assistance if they experience significant cyber incidents, or to preemptively reduce vulnerabilities in digital systems to prevent or mitigate damages from malicious cyber activities. The program equips non-government beneficiaries with tools and skills to improve digital hygiene, secure digital financial transactions, implement safe storage of private or protected data, improve the capacity to use advanced encryption, and field other diagnostic and defensive tools to protect digital infrastructures. Digital APEX can also be used to support other cyber-related projects, including risk assessments, network penetration testing, software and hardware procurement, cyber training, network monitoring, and incident response.

- **CREST** Service Selection Platform: CREST developed a Service Selection Platform of vetted vendors to offer free guidance for governments, regulators, and buyers on procurement of ICT and security services, with a list with contacts of recommended qualified companies and suppliers that can deliver high-quality technical security services.[79]

5.1.2 Partnership Effect

- **IDB - Uruguay**: The IDB is funding the government of Uruguay through a specific multi-million dollar loan operation to strengthen its cybersecurity posture. The Uruguayan AGESIC (Agencia de Gobierno Electrónico y Sociedad de la Información) – the National Agency for e-Government and Information Society – is considered by the OAS and the IDB as a role model for the region for the way it has integrated cybersecurity and promoted the use of ICTs to improve government management with a focus on citizens, democratizing public services, and mitigating regional inequalities. The IDB provided technical and financial assistance to AGESIC through seven different loan operations to implement the different digital agendas that support their cybersecurity policy. For example, Uruguay's Digital Development Policy integrated cybersecurity and risk mitigation measures into the country's action plan. Uruguay currently leads the region in terms of e-government services, information security, interoperability, citizen services, personal data protection, access to information and electronic signatures, competitiveness, etc. This leadership has enabled the country to quickly scale positions globally, making a difference for an innovative approach to open government policies and the application of ICTs focused on citizens.

- **ITU - Kenya**: With financial and expert assistance from the ITU, Kenya established and then improved the capabilities of its National Computer Incident Response Team-Coordination Centre (National KE-CIRT/CC). This Centre continued to mature and expand its reactive

and proactive capabilities, became a trusted, central coordination point of contact for cybersecurity in the country, and eventually led the national strategy development and policy updates for the country.[80] It also became a regional example and extended its knowledge of technical capabilities into the East African Communications Organization (EACO) and continues to provide leadership to extend capacity throughout the region (Tanzania, Uganda, etc.).[81]

- **USAID – Ukraine:** The four-year USAID-funded Cybersecurity for Critical Infrastructure in Ukraine activity aims to improve the country's cyber preparedness and build critical infrastructure resiliency through three complementary objectives: 1) strengthening the cybersecurity enabling environment; 2) developing Ukraine's cybersecurity workforce; and 3) building a resilient cybersecurity industry. The project, led by Development Alternatives, Inc (DAI), has leveraged partnerships with the government and ministries to develop capacity on the ground; raise awareness of cyber threats; strengthen the legal, regulatory, and institutional frameworks for national cybersecurity oversight and align them with international standards and best practices; improve national cybersecurity sector governance and coordination; expand collaboration and communication among key governmental stakeholders; support and empower cybersecurity institutions; build technical capacity of critical infrastructure sectors through demand-driven assistance; and incorporate specific security protections in the industrial control systems (ICS) of the energy sector and other vulnerable critical infrastructures.[82]

- **EU – CoE – INTERPOL**: The European Union (Instrument Contributing to Peace and Stability) and the Council of Europe – now also with INTERPOL – launched a joint project called the Global Action on Cybercrime Extended (GLACY+) to strengthen the capacities of countries to apply legislation on cybercrime and electronic evidence; enhance the abilities of police authorities to investigate cybercrime and of criminal justice authorities to prosecute and adjudicate cases of cybercrime; and engage in effective international cooperation in this area. The project supports fifteen priority and hub countries in the African, Asia-Pacific, Latin America, and the Caribbean regions (Benin, Burkina Faso, Cabo Verde, Chile, Costa Rica, Dominican Republic, Ghana, Mauritius, Morocco, Nigeria, Paraguay, Philippines, Senegal, Sri Lanka, and Tonga). These countries may serve as hubs to share their experience within their respective regions.[83]

- **DG NEAR – Estonia MFA – Ukraine:** The EU Commission's Directorate-General for Neighborhood and Enlargement Negotiations (DG NEAR)[84] is part of the European eastern and southern neighborhood assistance actions dedicated to supporting reform and democratic consolidation, taking forward EU's neighboring and enlargement policies, and strengthening the prosperity, stability, and security around Europe. This program created a special unit to support Ukraine's digital transformation and reforms after the revolution in 2014. This broad-reaching Digital Transformation initiative, in partnership with the European External Action Service (EEAS) and the Estonian Ministry of Foreign Affairs,

goes beyond digital development assistance. This special team provides advice and guidance on legal, regulatory, and policy reforms in energy, environment, justice, and home affairs in Ukraine (in support of EU values, policies, and interests); supports the government's efforts to expand availability and adoption of digital services (Ukraine was the first country in the world to adopt a digital passport and to offer a COVID vaccine digital certificate fully integrated with the EU system "Green Pass"), ensure interoperability of systems, and upgrade and strengthen critical infrastructure (update software for the Soviet era); and provides capacity building for all government agencies responsible for digitalization. Cybersecurity is an intrinsic component of all these digital projects, and all the financial support (overall budget of €25 million) and technical assistance provided is considered "DAC-able." They framed it as "reforms support" and "digital transformation," but incorporated cybersecurity in the design of all their efforts.[85]

- **OAS – EU Cyber4Dev:** The OAS has partnered with the EU Cyber Resilience for Development (Cyber4Dev) project to offer online training for incident responders (CSIRTs) in Ecuador, Paraguay, Dominican Republic, and Costa Rica, and tabletop exercises (e.g., national-level cybersecurity exercise "Cyber llamas" in the Dominican Republic).[86] The online training courses intend to build local capacity, test maturity, identify areas of vulnerability for improvement, reduce the impact of cyber attacks, increase cyber resilience, and tackle other cyber threats from managing disinformation to more technical issues.[87] The OAS also works with the EU CyberNet to offer a cadre of subject-matter experts and provide specific training on other requests for assistance from member states in the region.

- **JICA – Indonesia:** As part of their CCB initiatives, JICA focuses on university partnerships as the natural place to develop indigenous capacity. In Indonesia, they are implementing a master-level program on cybersecurity and developing the curriculum together with their local counterparts. (Sometimes their projects are developed from scratch with local university partners and other times they import their curricula and experts.)

- **World Bank:** The World Bank has begun to include cybersecurity in its financing operations. An early example was the project that financed the establishment of the National CERT in Morocco. More recently, discreet country financing operations embedded cybersecurity components in a project to connect Tonga. The project includes building a high-speed broadband capacity submarine cable to provide better internet coverage and assisting the country in drafting a cybercrime law, which paved the way for Tonga to join the CoE Convention on Cybercrime. Likewise, programmatic interventions, such as the Identity for Development (ID4D) initiative, include cybersecurity in each of their 40 or so projects ensuring security of national identification (ID) systems and data.[88]

- **IFC – Private Sector Firms**: The International Finance Corporation (IFC), part of the World Bank, helps advance economic development by investing in private sector companies in low- and medium-income countries across a range of

sectors (e.g., energy, transport, and telecommunications). They leverage the private sector to open up markets and mobilize other investments for companies in the lowest-income countries that are eligible for ODA funding/grants and in fragile and conflict nations (for every dollar the IFC invests, they bring $5 of private sector financing).[89] The IFC has also incorporated de-risking mechanisms through its financing. Their investment officers appraise risk according to each sector's exposure. Their risk management framework helps assess risks (high-medium-low) for specific industry sectors. The sectors considered to have higher risk exposure (e.g., energy, logistics) receive additional scrutiny, versus sectors considered low risk (e.g., finance, telecommunications) because of existing industry frameworks, best practices, regulations, or experience.

5.1.3 Using Organizations' Convening Power: The Bridging Effect

- **UN DCO Resident Coordinators**: The UN Development Coordination Office (DCO) provides Resident Coordinators (RCs) and UN country teams in each of the countries where there is a UN program with regional-specific support, and acts as a key conduit for supporting UN's activities for sustainable development, informing policy, programs, and operations on the ground.[90] The RCs, in turn, are responsible for coordinating local programs across all UN agencies involved, which provides them with the most-centrally coordinated view of all the UN programs in a given country. They can also receive additional requests or signals from recipient governments and guide those requests to the right agency that can provide the right kind of support. The RCs have a convening authority and influence in their country of operations, and could serve as the natural conveyor/aggregator among other donors, as well.

- **UNODC – El Salvador:** The UN Office on Drugs and Crime's Global Program on Cybercrime has developed a natural bridging function between donors' recipient countries, international organizations, and local entities. For example, in 2004, they started a collaboration in El Salvador with the country's Attorney General Office, Supreme Court of Justice, and El Salvador National Civil Police in order to develop and strengthen institutional capacity. They created a Cybercrime Unit within the National Civil Police and delivered joint workshops and tailored training for law enforcement officials, judges, forensics experts, and local prosecutors from different units, as part of the project "Strengthening of the Capacities of El Salvador National Civil Police in the Effective Identification and Investigation of Cybercrime Cases in El Salvador." UNODC also coordinated their efforts and invited other partner organizations, including the International Centre for Missing and Exploited Children (ICMEC) and INTERPOL, to work together on their specific areas of expertise (i.e., online child sexual abuse and exploitation, cyber operations, and connecting to the International Child Sexual Exploitation [ICSE] database). The initiative received financial support from the Bureau of International Narcotics and Law Enforcement (INL) of the Embassy of the United States in El Salvador, and is still receiving financial support from other donors such as Canada, the UK, and Norway.[91]

6 KEY RECOMMENDATIONS: INTEGRATING CYBERSECURITY AND DIGITAL RESILIENCE INTO THE BROADER DIGITAL DEVELOPMENT AGENDA

6.1 Call for Stakeholders Action to Bridge Digital Development and Cybersecurity

- Advocate for the development community and the cybersecurity community to update their "playbook" to the digital era by connecting cybersecurity and digital resilience with the economic aspirations, digitization strategies, and development priorities of recipient countries. Digital capacity building must be more needs-driven and tailored to individual and national circumstances, and better coordinated globally. Tailored approaches and programming based on a demand-driven signal and the political, economic, and social context of a recipient country are central to ensuring the long-term sustainability and scalability of any capacity building efforts. Providing sufficient funding should also remain an important objective.

- Change the cybersecurity narrative, in the context of international development, and reframe it in terms of digital resilience, trust, sustainability, safety, and risk management.

- Encourage "more data-driven guidance for cybersecurity good practices, cybersecurity community awareness of and participation in key dialogues in the development community around the use of metrics and identification of good practices in capacity development.

  The donor community's reliance on metrics to steer investment means that the cybersecurity capacity building community will need to create an empirically convincing argument that an absence of better cybersecurity leads to demonstrably worse outcomes. … In the event that the need to integrate cybersecurity into development is empirically convincing, the cybersecurity community more broadly has yet to develop truly useful measurements to evaluate cybersecurity and cybersecurity capacity building interventions. Lacking these metrics, it becomes difficult to craft meaningful, empirically driven arguments for what capacity development interventions produce the most positive outcomes. Better outcome-oriented metrics are needed to identify and communicate these good practices, whether government policy interventions, corporate policies, or technological interventions."[92]

- Encourage the OECD's Development Assistance Committee (DAC) to add "digital resilience" to the eligibility criteria for Official Development Assistance (ODA) as part of the peace and security activities to enable cybersecurity-related assistance.

- Ensure the continuity and sustainability of a project (e.g., continuity of the program, staff, equipment, etc.) by programming funds into the country's national budget. Both the development community and recipient countries still see ICTs as long-term capital assets and expenditures, rather than commodities that will need updating and replacing within a five to ten-year period. ICTs that are still in use and

no longer supported by hardware and software updates make the recipient country more vulnerable to digital risks. This vulnerability leaves a critical shortfall in a program's sustainability and its ability to achieve the desired resilient outcomes. A digital development project's total-cost-of-ownership and ICT refresh must, therefore, be included in project formulation and programmed into assistance packages.

- Educate national leaders and policymakers in recipient countries to embrace the benefits of digital capacities and encourage them to program funds into the country's national budget. This will help address the sustainability issue and prevent development aid/low-interest loans from becoming an extra financial burden on the country that cannot be sustained after the end of a project (e.g., lack of funding for the local workforce, to develop indigenous capacity, pay to update/replace equipment or software, etc.).

- Facilitate growing a cybersecurity skilled local labor force/talent pools and indigenous capacity (e.g., local training on good cyber hygiene, awareness of cyber threats, development of local cybersecurity expertise, implementation of tailored digital solutions, etc.). This requires addressing many related challenges, including the affordability of cyber certifications, the need to reform school and university curricula, the need to identify and cultivate local talent, the problem of retaining people who have been trained ("brain drain"), and the problem of low government salary scales that makes it more difficult to attract capable CISOs, CIOs, and other technical figures.

- Promote inclusivity in cybersecurity (women, youth, and minorities). Digital inclusion is the basis for a more thriving digital ecosystem that can stimulate innovations for local development challenges, create local skilled jobs, and generate opportunities for business partnerships. Inclusivity should be one of the overarching principles when designing school/university curricula, training programs for cybersecurity workforce development, or awareness campaigns about cybersecurity-related professions, with a particular focus on identifying participants who may not already be in cybersecurity-related roles.

- Engage in raising awareness of the donor community on the risks and benefits of ICTs, especially when protected data is involved. Show the development community how digital transformation and digital technologies can become existential threats to some of their digital development projects and goals (e.g., tools for cybercrime, surveillance, disinformation, digital authoritarianism, human rights abuses, data exploitation, espionage, etc.) – ultimately making the recipient country more fragile (see USAID's *Cybersecurity Primer*). Understanding these threats will better guide the development community in supporting countries' digital pathways and in making the most of new technologies as enablers of sustainable and secure development. A few "champions" on board would make a quick win.

- Sensitize the donor community about the need to embed cybersecurity, digital resilience, and CCB into their digital development projects and other

lending operations at project design/ inception and throughout the entire program lifecycle (a sort of CCB for the donor community).

a. Convene an ongoing global partnership on cybersecurity and digital resilience for the development community.

b. Consider some of the "bridging venues" listed below, which could provide different fora to educate donors across governments and international organizations about both the "dark side of digital innovations" as well as the benefits of integrating cybersecurity, digital resilience, and cybersecurity capacity building into digital development.

c. "Bring more expertise into cybersecurity donor institutions by exploring short-term solutions like fellowships and secondments and leveraging funding mechanisms to create long-term cybersecurity portfolios in development donor institutions."[93]

- Align digital development projects to the recipient country's digital economy and national vision, ensuring that cybersecurity and digital resilience are included to produce successful outcomes.

- Consider capacity initiatives in the context of the country's technical maturity and political will and tailor them to the circumstances therein (demand-driven approach).

- Build knowledge of local ecosystems, culture, and digital risks to society using local data, students, and institutions. Stimulate local/regional academic/policy research and data gathering in developing countries, which would further help shape local development projects based on local research/needs. Local data, trends, statistics, and field research that characterize the threat within a country or region can provide compelling evidence to drive economic and political arguments as to why cybersecurity is important and a necessary component of digital development:

a. Allocate funding to local universities, students, and researchers to gather local evidence or conduct trend analysis in the country/region. Stimulate multidisciplinary academic projects, connecting technical sciences with economic, social, legal, and political aspects – such multidisciplinary research and curriculum development would help effectively connect cybersecurity and digital resilience with digital development in the context of a given country;

b. Include the local private sector – "a crucial partner in building digital [and cybersecurity] ecosystems," accessing local data, and providing a driver of economic and societal growth.[94]

c. Build partners/client countries' cybersecurity capacity to address shared threats through engagement with the private sector, local government, and civil society.

- "Build [regional or country-specific] libraries of credible and politically useful information to present to key decision makers, like deep statistical studies on the impact of cybersecurity on development and a library of case studies and examples of the positive and

negative impacts of cybersecurity on key development outcomes."[95]

- Develop baseline requirements for cyber capacity building for digital development projects run by major donor communities. Start with MDBs and cybersecurity of digital infrastructure (e.g., telecommunications, finance, energy) first; but then expand to other donors (countries, development agencies, foundations) and a broader scope of digital policies (e.g., data protection, privacy, digital inclusion, etc.). The goal should be for each digital development support/project to have a digital policy and cybersecurity component (and capacity building for it) attached to the main project aim:

  One particular example can be embedding baseline requirements for security of digital products (e.g., software, cloud services, IoT, etc.) into development programs that support innovations in this field (e.g., "smart products") or projects which end up producing some e-government or other online services and applications (e.g., e-banking and e-money solutions, telehealth, etc.). Some useful resources that discuss such security baselines include the OECD recommendations on digital security of products, which offer practical recommendations for policymakers to leverage specific tools – from public procurement, certification, and multi-stakeholder partnerships, to labels and ex ante legal requirements – to increase transparency and information sharing, promote co-operation (including at the international level), and ensure the duty of care of supply-side actors (e.g. through the principles of security-by-design, security-by-default, and responsible end-of-life).[96] Another resource of good industry practices is the Geneva Dialogue on Responsible Behavior in Cyberspace, which provides common policy baseline requirements for companies to boost the security of their digital products and overall supply chain and works to enhance their understanding of and contribution to global policy processes in order to achieve a trusted, secure, and stable cyberspace.[97]

- Use development organizations as a conduit to raise cybersecurity awareness and build capacity in low- and middle-income countries. While the development community may have not traditionally addressed the digital risks stemming from increased reliance on ICTs and the expansion of e-services, digital systems, and platforms, their established connections in the local community and better understanding of the local challenges faced by these countries offer particular insights and valuable relationships with the local "implementors." This can be a great opportunity for practical collaboration between the development community, which brings on-the-ground expertise and networks, and the cybersecurity capacity building community that provides extensive expertise but has little or no presence on the ground. "Drawing on the development communities local presence and association with grassroots actors could be critical in enabling the delivery of better cybersecurity capacity building programs."[98]

- Leverage the UN Development Coordination Office's (DCO) Resident Coordinators (RCs) in a given country to gain a perspective on other local projects

and opportunities to partner, and to better assess where to focus and how to best deploy program/money/assets in service of the recipient country/government. RCs can serve as a natural conveyor/aggregator for other donors/implementors on the ground, and help donor organizations understand the activities already underway in recipient countries and potentially highlight underserved needs. They can also receive additional requests or signals from recipient governments and guide those requests to the right agency that can provide the right kind of support. Moreover, they can work with UN Headquarters entities to ensure overall coherence with the broader UN approach on digital and cyber issues, including through mechanisms such as the Roadmap Response Team, developed in response to the 2020 UN Secretary-General's Roadmap for Digital Cooperation.

Other organizations such as the EU or MDBs' local offices could also be leveraged in this regard.

- Conduct digital risk/maturity assessments of the country or sector under consideration for foreign assistance, along with an assessment of other development or CCB projects by other donors in the same country or region before designing, funding, or implementing new digital development and/or CCB projects. Include a mapping of local experts and communities of existence that could/should be involved in the conceptualization and realization of/support to the projects. When these types of assessments are conducted by donors, consultants, or other international organizations, they should be made publicly available (perhaps with some jointly agreed redactions with the recipient government when covering sensitive topics) in order to increase transparency into lending operations or technical assistance programs and help avoid duplication of efforts and/or help find potential synergies.

For example, organzations can use the UNDP Digital Readiness Assessment (DRA) tool as a baseline assessment to know what other digital development projects (mapped to the SDGs) are already undergoing in a recipient country.

6.2 Call for Greater Cooperation and Coordination Among Donors and Implementors

- Encourage both the cybersecurity community as well as the development community to invest in the development of "Digital Public Goods" or DPGs (universal tools and instruments) that can be shared and applied broadly. One such DPG is the development of primers (e.g., USAID Cybersecurity Primer) for missions and implementing partners on how to incorporate cybersecurity and digital resilience safeguards into all phases of project design and implementation to ensure digital sustainability and resiliency. Another tool is the development (or further support) of platforms to share good practice guidance, assessment tools, and technical assistance (e.g., *Cybil* Portal, USAID Digital APEX, CREST platform); and pool data sets; engage talent; promote more holistic approaches to capacity building; or serve as a "clearinghouse" to better direct support requests (e.g., GFCE), enhance support to national capacity building efforts, and amplify country-level support. All these efforts to facilitate the discovery, development,

use of, and investment in DPGs can serve multiple communities and allow for funding to be focused toward the greatest deficiencies, in addition to helping to accelerate the SDGs. Some examples of DPGs highlighted in this report included:

a. The GFCE's *Cybil* Portal is a global resource of existing CCB methodologies, frameworks, expert organizations, and projects, and a knowledge hub that brings together stakeholders from the cyber capacity building community to coordinate and share CCB research and initiatives. The GFCE also serves as a clearinghouse to match needs for cyber capacities with offers of support and to help connect donors, beneficiaries, and implementors.

b. USAID's Digital APEX is a resource of vetted cybersecurity services/experts/firms that USAID's implementers, program partners, and partner governments can tap into to receive rapid technical assistance if they experience significant cyber incidents or to preemptively reduce vulnerabilities in digital systems. It can also undertake other cyber-related projects (e.g., security assessments, pen-testing, software and hardware procurement, cybersecurity training, network monitoring, incident response) to build accessible and affordable digital infrastructure and promote adoption of accepted international standards.

c. CREST's Service Selection Platform is a resource of vetted ICT and security companies and trusted suppliers that can provide high-quality technical security services to governments, regulators, and other buyers.

- Develop greater coherence and coordination between stakeholders to avoid duplication of efforts and focus on approaches/solutions that scale. Develop dedicated platforms, pilot projects, and coordination mechanisms; and identify on-the-ground/local partners to implement necessary actions and improve coordination efforts with local authorities (see role of UN RCs and other EU or MDBs' local offices to promote greater coherence and coordination on the ground).

- Alleviate the practice of favoring "darling countries," which receive multiple offers of foreign aid from different donors, while neglecting "orphan countries," which are rarely the focus of foreign assistance by developed countries or donor organizations. Active donor coordination on this topic is necessary to ensure sustainable development for a broader set of countries.

- Develop a third community ("community of translators") that can bridge the gaps to work across the digital development community and the cybersecurity community. This speaks to the ability of not just building technical capacity, but also finding existing program cycles/functions where donors and implementors can incorporate cybersecurity as part of their digital development portfolios – if an infrastructure project is digital, there should be a cybersecurity component, which can be defined as "digital sustainability" to build in the necessary safeguards into the fabric of the institutional functions from a project's inception, just like other environmental and human rights safeguards.

6.3 Explore Potential Venues for Bridging the International Development Community with the Cybersecurity Capacity Building Community

Networking the networks may lead to cybersecurity becoming an integral activity within digital development projects and may help both communities achieve more resilient outcomes. Consider the following venues and forthcoming events to bring together the international development community with the cybersecurity capacity building community (other bridging venues could be promoted through regional engagements and then replicated in other regions):

- Forum of MDBs Presidents and Director Generals' Meeting (facilitated by AIIB) – a key topic was digital infrastructure: October 2021;
- GFCE-OAS LAC Donors and Implementers Forum: 9 November 2021;
- GFCE Annual Meeting: 30 November - 2 December 2021;
- Internet Governance Forum (IGF) Annual Meeting, hosted by Poland in Katowice, under the overarching theme "Internet United" – they will have a session on capacity building: 6-10 December 2021;
- Democracy Summit (to be held in the USA): 9-10 December 2021;
- Dutch table on ICT development for trust and security as part of the UN Roadmap for Digital Cooperation: December 2021;
- Programme for Infrastructure Development in Africa (PIDA week) in Swakopmund, Namibia: 10-14 December 2021;
- 5th UN Conference on the Least Developed Countries (LDC5) in Doha, focused on building a new program for action for LDCs and realizing the SDGs as part of the UN decade of action for the 2030 agenda: January 2022;
- World Summit of the Information Society (WSIS) 2022, co-organized by ITU, UNESCO, UNDP, and UNCTAD, is the largest annual gathering of the "ICT for development" community and will be focused on cooperation for accelerating progress on the SGDs: March-June 2022;
- Indonesia Presidency of G20: 2022;
- OEWG (currently under Singaporean chairmanship);
- African Internet Governance Forum: Summer 2022;
- Smart Africa Summit (an annual forum bringing together regional and global leaders from government, business, and international organizations to collaborate on ways to shape, accelerate, and sustain Africa's digital transformation): Summer 2022;
- High-Level CCB Conference being organized by the GFCE Foundation, World Bank, and other key stakeholders: September 2022;
- Europol-INTERPOL Cybercrime Conference: 2022.

CONCLUSIONS

This research paper identified effective methods and practical initiatives to engage the broader development community and encourage them to embrace cybersecurity as a development issue. The intent of this paper is to catalyze further discussions among GFCE and World Bank partners as well as other regional and international institutions working on digital development and CCB projects and to provide inputs into the formulation of comprehensive digital development strategies and projects that incorporate safety, digital resilience, cyber risk management, and other safeguards.

Many reports have highlighted the connections between digital technology and economic growth and emphasized the notion that digitization can accelerate the realization of every SDG. "But in order to fully reap the immense benefits of connectivity and digitalization, the technology [and ICT infrastructure] that underpin them must be secure,"[99] safe, and resilient. Cybersecurity and digital resilience should become a recognized issue of concern and an integral component of the development agenda – beginning with the design of any new development project. As well, cybersecurity and digital resilience should be considered an eligible development assistance criterion for foreign aid and development support. "Cyber capacity building is not an end in itself. Rather, it is a cross-cutting concern across all SDGs."[100]

At the same time, stakeholders in both the cybersecurity and the development community must realize that "digital development is inextricably linked to geopolitics" and increasing geopolitical competition is leading to a decoupling and breakdown of technological platforms, norms, and standards.[101] "As governments and technology companies align along geopolitical fault lines and competing national and regional data and digital ecosystem models emerge," stakeholders in the development community are facing increased limitations in their access, reach, and cooperation capacity. Accordingly, development community stakeholders may decide to limit their digital development project scope to areas not perceived as controversial or highly politicized. However, this limitation may also restrict the stakeholders' ability to build necessary safeguards (e.g., cybersecurity, digital resilience, data protection, data privacy, risk management) into their development projects.

Any new investments in digital development projects and/or cyber capacity building should, first and foremost, be aligned to the recipient country's digital economic development agenda and cybersecurity priorities, and based upon an informed expectation of what the projects will achieve. The interviews highlighted some unique examples of successful development projects that have started to embed cybersecurity and digital resilience and help build real capacity on the ground. However, anecdotal evidence is not a sufficiently strong foundation to bridge the gaps highlighted in this report and link best practices (or "menus of options") to specific country needs and to real project impacts.

For better evidence-based programming, and a compelling narrative for investment, the development and cybersecurity communities need to update their "playbook"

for the digital era; connect cybersecurity and digital resilience with the economic aspirations, digitization strategies, and development priorities of recipient countries; develop local institutional and indigenous capacity; and reframe their narrative in the context of digital resilience, safety, trust, sustainability, and risk management rather than security. Moreover, digital development and CCB programs/projects should be tailored to individual and national circumstances. Indeed, tailored approaches based on a demand-driven signal are central to ensuring the long-term sustainability and scalability of any capacity building efforts.

In addition, improved integration among stakeholders is needed to facilitate learning across policy communities – spanning technical, law enforcement, foreign affairs, development, human rights, etc. – and to ensure project success. As described in Section 3 of this report describing key findings and observations, there is a strong interest in promoting greater coherence and coordination in capacity building efforts among donor countries and organizations and scaling up solutions. We suggest this as the next priority for the GFCE and other benefactors ("champions"). These organizations should develop cooperation policies, co-investments, hand-off mechanisms, and business models tailored to specific country/regional needs. Also, a need exists for further research and data collection into the experience and perspectives of low- and middle-income countries as the recipients and direct beneficiaries of digital development and CCB projects, and programs to better understand how these countries become (trans)formed through their entanglement with global digital connections, broader digital economy, international policies, standards, and regulations.

APPENDICES

ANNEX I
ORGANIZATIONS INTERVIEWED AND RELATED DIGITAL DEVELOPMENT AND/OR CCB ACTIVITIES

African Union Commission (AUC): The Commission of the African Union (AU), which is headquartered in Addis Ababa, Ethiopia, acts as the executive/administrative branch or Secretariat of the AU. It consists of a number of Commissioners dealing with different areas of policy, including: peace and security; political affairs; trade and industry; infrastructure and energy; social affairs; rural economy and agriculture; human resources, science and technology; and economic affairs.[102] The AU has organized cybersecurity training in partnership with the U.S. State Department for more than 450 local experts in over 50 AU member states. The training focused on how to develop a national cybersecurity strategy; a national CERT/CSIRT; and a modern legal framework to adequately combat cybercrime. The AU is also partnering with the GFCE for a two-year collaborative project, funded by the Gates Foundation, aimed at developing cyber capacity building knowledge to enable AU member states to better understand cyber capacities and support them in strengthening their cyber resilience. This collaborative project intends to help African countries prioritize and address their national cyber capacity needs and "foster coordination and increasing international collaboration between (existing) cyber capacity building efforts in Africa".[103] The project is building on and utilizing existing cyber structures, plans, expertise, and capacities within the AUC, as well as within the multi-stakeholder and international GFCE community (see additional information below under the GFCE section). The AU-GFCE project has already established an African Cyber Experts (ACE) Community consisting of small cohorts of selected national experts from participating AU member states, other AU affiliates, and GFCE Africa Multi-stakeholder group who sit together (virtually or in-person) and work on resource sharing and better coordination of efforts across the African continent. It is also tapping into the knowledge and expertise of GFCE community members to develop Knowledge Modules (KMs) associated with identified cyber capacity building priorities of AU member states and to better address their specific challenges.[104]

Asian Infrastructure Investment Bank (AIIB): The AIIB is a multilateral development bank, located in Beijing China, focused on providing financial support to developing countries (mostly in East Asia) to build the "Infrastructure of Tomorrow" (i4t) and to foster sustainable economic development, wealth creation, and improved infrastructure connectivity.[105] In 2020, the bank launched a Digital Infrastructure Sector Strategy, which covers both hard (transport and connectivity, processing and storage) and soft (software and applications, terminal and devices) infrastructure. The Strategy interfaces with and supports other Bank strategies, and aims to guide AIIB's

activities as a catalyst for financing digital infrastructure growth in Asia, supporting AIIB Members efforts in bridging the digital divide, increasing economic competitiveness, and improving infrastructure efficiency. While there is no systemic approach to cybersecurity or cyber resilience as part of AIIB lending operations, they have identified cybersecurity as one of the main regulatory risks to investing in digital infrastructure, which is now being incorporated as a component of some of their projects.[106] (**Note: AIIB does not have a role in policy changes in the countries of operation, but has built an in-house capacity to ensure that its digital infrastructure projects 1) comply with specific country regulations and laws, and 2) are based on regulatory risks analysis that balance out data privacy risk with reputational risk.)

Australia Department of Foreign Affairs and Trade (DFAT): The DFAT, headquartered in Barton ACT, is the department of the Australian federal government responsible for foreign policy and relations, international aid, consular services, and trade and investment.[107] They work with international partners and other countries to tackle a variety of development challenges, including digital connectivity (e.g., laying of undersea cables connecting Papua New Guinea and the Solomon Islands to Australia) and cyber and critical technology issues. DFAT has recognized "cyber affairs" and "critical technology" as foreign policy priorities, and established the Ambassador for Cyber Affairs role (since expanded to include Critical Technology) that is responsible for coordinating Australia's international cyber engagement.[108] In 2016, DFAT established a AUD$4 million Cyber Cooperation Program to improve cyber resilience across the Indo-Pacific and to support Australia's commitment to deliver on the UN SDGs and drive global economic growth and sustainable development.[109] (**Note: the Program does not generally provide funding for equipment (software/hardware), but supports recipient countries to develop institutional capacity, establish policy and regulatory frameworks, raise awareness of cybersecurity, and build a community of cybersecurity operators in the Indo-Pacific region). In 2017, the Program was expanded with the launch of Australia's International Cyber Engagement Strategy, which also committed to developing Guidance Notes to incorporate cybersecurity de-risking measures – similar to environmental and social safeguards – into DFAT aid funding and to ensure the achievement of DFAT development programs.[110] In April 2021, Australia launched a broader International Cyber and Critical Technology Engagement Strategy. Australia's eight-year, AUD$74 million investment supports the country's goal of strengthening national security; promoting economic growth; and ensuring a safe, secure, and prosperous Australia, Indo-Pacific region, and world enabled by cyberspace and critical technology. The Strategy guides all of Australia's practical international engagements across cyber and critical technology issues, including cyber capacity building and cyber resilience, with a strong focus on the Indo-Pacific region. The Strategy renamed the flagship Cyber Cooperation Program into the Cyber and Critical Tech Cooperation Program.[111] Moreover, the Strategy committed an additional AUD$20.5 million to strengthen cyber resilience in Southeast Asia and AUD$17 million to support Pacific neighbors in strengthening their cyber capabilities and resilience efforts, including fighting cybercrime, improving

online safety, and countering disinformation and misinformation.[112] Other Australian-funded initiatives, like the AFP-led Cyber Safety Pasifika and Cyber Safety Asia programs, help assist regional law enforcement practitioners to develop further cybercrime-relevant skill sets and provide broader community awareness and education regarding the risks of cybercrime. Other priority areas for Australia's capacity building program include online safety and harms, regional connectivity, and internet governance. (**Note: major projects, like subsea cables, are funded from Australia's development budget, not the capacity building program.)

CREST: CREST is a UK-based "international not-for-profit accreditation and certification body that represents and supports the technical information security market."[113] CREST awards internationally-recognized accreditations to service providers of vulnerability assessments, penetration testing, cyber incident response, threat intelligence, Security Operations Centre (SOC) services, etc., as well as professional-level certifications and career pathways for individuals. There are more than 200 accredited member companies across the world, and over 3,500 individuals hold CREST qualifications in more than 50 countries. In collaboration with industry and governments, CREST has built a framework for measuring the capability of cybersecurity companies and their workforce. It also developed a Service Selection Platform that can help governments, regulators, and buyers identify suppliers capable of delivering high-quality technical security services. In addition, it helps regulators build schemes that support assurance frameworks allowing them greater levels of confidence in the operation of regulated entities (e.g., financial services, telecommunications, government, energy, aviation). CREST practices an open and transparent approach to the development of all frameworks for supporting the growth and development of the entire cybersecurity ecosystem, facilitating the sharing of common good practice guides/Digital Public Goods to speed assurance frameworks implementation and support maturity level improvement across the cybersecurity ecosystem of various countries.[114] For example, as part of a project funded by the Gates Foundation, CREST developed a Cybersecurity Maturity Model Assessment – a freely accessible, affordable, sustainable, and scalable framework to measure the maturity and financial inclusion of the cybersecurity ecosystem of a country across five dimensions: 1) National Cybersecurity Strategy & Capabilities; 2) Cybersecurity Information Sharing; 3) Cybersecurity Service Provision; 4) Cybersecurity Professional Development; and 5) Banking Sector Risk Posture. The resulting country assessments can be used to compare country sector organizations, identify good practice and areas of common concern, monitor the impact of investments, and define clear measurable objectives for improvement.

DiploFoundation: Diplo is a Swiss-Maltese non-profit organization, headquartered in Malta with offices in Geneva, Washington D.C., and Belgrade. It specializes in "capacity development in the field of internet governance and digital policy," and works to 1) increase the role of small and developing states in global diplomacy by developing digital tools for inclusive and impactful governance and policy-making and 2) providing online courses, workshops, and simulation exercises for government officials on internet

governance, data, artificial intelligence, and other emerging tech issues.[115] In particular, Diplo designs and implements capacity building programs and cybersecurity policy education, online trainings, workshops, webinars, events, and educational material for policymakers and diplomatic personnel.[116] Diplo sees CCB education and traning as a process rather than a set of themes/modules. First, Diplo considers the technical environment. From there, they discuss digital risks; instruments of crime, peace, and security; existing regional and national partnerships (CERTs, PPPs); international organizations (ITU, GFCE); soft skills; digital policy; cyber diplomacy; reporting; researching; data mining; and more. They have also contributed to the work of the UN Open Ended Working Group (OEWG) on developments in the field of information and telecommunications in the context of international security with specific recommendations on "Comprehensive Capacity Building." Their contributions included advocating for a multi-stakeholder, multidisciplinary, and holistic approach to CCB and CBMs and recognizing capacity building as a comprehensive, long-term, and sustainable process rather than simply training.[117] This process should include developing organizational capacities of governments, civil society, business associations, and academia; nurturing established communities; embedding CCB in budgetary planning, commitment, and investments by states and regional organizations; and incorporating aspects of cybersecurity and digital literacy into the curriculum of academic and professional training centers.[118]

European Investment Bank (EIB): The EIB, headquartered in Luxembourg, is the lending arm of the European Union (EU). Owned by the EU member states, EIB is the largest multilateral financial institution/lender in the world. They fund projects that support the priorities and objectives of the EU, including integration of the region, digitalization, and most recently, increasingly sustainable recovery from the COVID-19 pandemic. They provide loans, guarantees, and technical assistance in the areas of sustainable development, infrastructure, innovation and skills (including cybersecurity), climate and environmental sustainability, SMEs, etc. All EIB-financed projects must comply with high technical, environmental, and social standards.[119] The European Investment Advisory Hub (a joint advisory initiative of the EIB Group and the European Commission) and the European Cyber Security Organisation (ECSO) have recently announced a feasibility study for the creation of a European Cybersecurity Investment Platform (ECIP) aimed at attracting more investment in the European cybersecurity market.[120]

European Bank for Reconstruction and Development (EBRD): The EBRD, which operates from headquarters in London and a network of Resident Offices, is owned by 71 shareholder governments, the EU, and the EIB. It seeks to promote the transition to a sustainable market economy and the emergence of a strong private sector. The Bank operates in nearly 40 economies in Europe, Asia, and Africa that are committed to applying the principles of multiparty democracy, pluralism, and market economics. Through investment, policy reform, and advisory projects, the EBRD works to make economies more competitive, well-governed, green, inclusive, resilient, and integrated – six "transition qualities" that are also aligned with the UN Sustainable Development Goals. The

EBRD focuses on projects that bring economic, social, or environmental benefits. The Bank works mainly with private clients, although it also finances public entities that deliver essential infrastructure and services.[121] It has begun incorporating cybersecurity and digital resilience safeguards into its lending operations, conducting digital risk assessments for sector-specific projects that involve digital technologies with closer scrutiny for projects that involve personally identifiable information. The Bank recently adopted its first Digital Approach to accelerating digital transition (2021-2025), which "sets out a comprehensive framework on how the Bank will use its three instruments – investment, policy engagement, and advisory services – to support the digital transition in the economies where it invests… and aims to mainstream technology throughout the Bank's activities."[122] The document expressly recognizes cybersecurity and the protection of data privacy as "essential parts of the digital transition" and states that the Bank will "develop a cross-cutting approach to cyber resilience to protect itself, its clients, and the economies in which it operates."[123]

Bill and Melinda Gates Foundation: The Gates Foundation is an American private non-profit foundation dedicated to fighting poverty, disease, and inequity around the world. They have a program on digital financial inclusion that focuses on building trustworthy digital infrastructure for a fairer world and funding organizations around the globe that identify and develop tailored solutions to the needs of developing countries. The Gates Foundation recognizes that cybersecurity is fundamental to ensuring digital financial inclusion and developing a more secure world, and they support efforts to create Digital Public Goods, including tools to measure the cyber maturity of the financial sector in developing countries (CREST); threat models for the financial sector in low-income countries (MITRE Engenuity); training courses and educational material to build local capacity of policymakers; networks of universities focused on improving cybersecurity of financial systems in Africa and other emerging economies, and scaling identity and payment digital public goods (CMU CyberLab-Africa)[124]; etc. Their focus is on Africa because they see it as a region where digitization can be introduced in disruptive, innovative, and new ways. The digital transformation can drive innovation (e.g., digital mobile wallets to facilitate the movement of money) and create opportunities for economic growth. Together with the World Bank, the Gates Foundation is trying to better align the cybersecurity capacity building community with the larger development agenda (and development donors).

Global Forum on Cyber Expertise: The GFCE, headquartered in The Hague, Netherlands, is a non-profit, multi-stakeholder foundation whose mission is "to strengthen cyber capacity and expertise globally through international collaboration and cooperation."[125] Today, the GFCE serves as a consultative forum and global platform for governments, international organizations, and private companies to identify and exchange best practices and expertise on CCB; coordinate cyber capacity projects; maintain a cyber capacity database (the *Cybil* Portal) with tool, publications, and CCB projects;[126] and act as a clearinghouse to match needs for cyber capacities with offers of support while connecting implementors with potential beneficiaries. The GFCE structures its work around five CCB

themes, namely: 1) Cyber Security Policy and Strategy; 2) Cyber Incident Management and Critical Infrastructure Protection; 3) Cybercrime; 4) Cyber Security Culture and Skills; and 5) Cyber Security Standards.[127] In 2020, the GFCE launched a two-year collaborative project with the African Union on "Enabling African countries to identify and address their cyber capacity needs."[128] This project aims to enable African countries to better understand cyber capacities and to support them in strengthening their cyber resilience. In particular, the project intends to grow a trusted community of cyber leaders from the different African countries; identify relevant cyber capacity gaps on a national and sub-regional level within African countries; enable African countries to prioritize, address, and communicate their national cyber capacity needs; and foster coordination and increase international collaboration between (existing) cyber capacity building efforts in Africa. The project focuses on three key CCB themes: 1) Cyber Security Policy and Strategy (i.e., Strategies, National Assessments, CBMs and Norms, Cyber Diplomacy); 2) Cyber Incident Management & Critical Information Protection (i.e., National Computer Security Incident Response); and 3) Cyber Security Culture & Skills (i.e., Cyber Security Awareness, Education and Training, Workforce Development). Publication of their final report is expected at the end of 2022.[129]

Inter-American Development Bank (IDB): The IDB, headquartered in Washington D.C., is the largest source of development financing for the Latin America and the Caribbean (LAC) region. Among its large portfolio, the IDB provides funding to governments in the region to support their digital transformation strategies and cybersecurity initiatives.[130] For example, the IDB is funding a multi-million and multi-year project to support Chile's national cybersecurity readiness and operational capacity building. The project includes CCB activities to improve the country's technological tools, infrastructure, training programs, and cybersecurity policies; build resilience to digital threats; develop or implement additional strategies, processes, technologies, and personnel needed to keep Chile's critical infrastructure, digital ecosystem, and government institutions secure; and establish Chile as a cybersecurity leader in South America. Additionally, the IDB provides technical and financial support through specific activities included in loan operations in Brazil, Honduras, Panamá, Paraguay, Uruguay, and The Bahamas. The IDB also supports the cybersecurity agenda in key sectors, such as health, energy, finances, water, and transportation.

International Telecommunications Union (ITU): The ITU, headquartered in Geneva, Switzerland, is the UN's specialized agency responsible for all matters related to ICTs. The ITU Cybersecurity program offers member countries – particularly developing countries – "the opportunity and tools to increase cybersecurity capabilities at the national level, in order to enhance security, build confidence and trust in the use of ICTs, and make the digital realm more safe and secure for everyone." The work and mandate of the ITU Cybersecurity program builds on Objective 2 of the Buenos Aires Action Plan adopted at the 2017 World Telecommunication Development Conference and related resolutions (Dubai, 2014; Hammamet, 2016; etc.). Under this program, there are several CCB initiatives that the ITU supports, which can be grouped

under five CCB areas: 1) develop effective national cybersecurity strategies or frameworks; 2) develop national CSIRTs and conduct CyberDrills; 3) adopt appropriate cybersecurity legislation and harmonize the legal and policy framework (i.e., Child Online Protection; Combatting Cybercrime Toolkit); 4) promote inclusivity (women and youth) in cybersecurity and workforce development; and 5) combat SPAM.

Islamic Development Bank (IsDB): Headquartered in Jeddah, Saudi Arabia, the IsDB is a multilateral development finance institution focused on Islamic finance. They provide funding for sustainable infrastructure projects in their 57 member countries and Muslim communities worldwide. They foster innovative and sustainable solutions in line with the UN Sustainable Development Goals.[131] In 2019, they developed an ICT Policy that included cybersecurity as an enabler in the contexts of corporate governance and access to e-government services.

Korea Development Bank (KDB): The state-owned KDB, headquartered in Seoul, South Korea, acts as the primary supporter of Korean public and corporate sector finances and manages major industrial projects to expedite industrial development of Korea.[132] KDB has identified cybersecurity as a key risk factor in its infrastructure investment area but does not have clear guidelines for its projects. They are discussing what guidelines to incorporate into projects as well as a risk-rating to appraise project risk.

MITRE Engenuity: MITRE Engenuity – a subsidiary of The MITRE Corporation, a non-profit operator of Federally Funded R&D Centers for the U.S. government – is a Tech Foundation for Public Good. MITRE Engenuity brings MITRE's deep tech expertise and intellectual property (across a variety of capabilities including cybersecurity standards, zero trust architectures, cyber threat and risk modeling, cyber defense tools, AI, quantum, 5G, etc.) to expand MITRE's impact beyond federal borders to protect citizens and critical infrastructure, safeguard assets, promote democratic principles, and enable economic stability and growth. MITRE Engenuity, through the support of the Bill and Melinda Gates Foundation, has developed a cyber threat-based risk model for digital financial mobile services (dFMS) in developing countries in Africa and India. This dynamic cyber risk model incorporates MITRE's threat informed defense approach, attacker methods, and technology-specific vulnerabilities from MITRE and its cyber defense community sources including Adversary Tactics Techniques and Common Knowledge (ATT&CK), Common Attack Pattern Enumeration and Classification (CAPEC), and the Cloud Security Alliance's Cloud Controls Matrix. Using this threat model, significant threat vectors that relate to mobile money applications within a particular technology/governance environment can be extracted and analyzed to produce a set of relative risks and associated impacts. These analyses can be used to identify existing and potential activities, including technical and non-technical initiatives, to improve access while remediating risks. Findings can also inform potential investors about decision-making options, including technical approaches as well as policy, governance, training, human resources, and other non-technical approaches to investment that can have ecosystem-wide impacts.

Norwegian Institute of International Affairs (NUPI): NUPI, headquartered in Oslo, Norway, is the country's leading center for "research and information on international political and economic issues and on areas of central relevance to Norwegian foreign policy." Their Centre for Digitalization and Cybersecurity Studies is dedicated to bridging the gap between the technical community and the policy world with research focusing primarily on the political dimension of cybersecurity and its role in international relations, global governance of cyberspace, capacity building, development, and the security vs. freedom dilemma. They partner with an extensive number of international and national institutions and organizations in the cybersecurity community to produce academic studies, expert analysis, and strategic policy recommendations on a variety of cybersecurity-related topics – from digital threats to critical sectors to cyber capacity building efforts in developing countries, to the use of digital means to subvert democratic processes, to digital value chains, and more. NUPI also organizes several seminars and events aimed at enhancing public awareness and knowledge of the various challenges associated with cybersecurity in Norway and internationally.[133]

Organization of American States (OAS): The OAS, headquartered in Washington D.C., is a multilateral regional organization that comprises 35 countries from the Americas. The OAS, through the Inter-American Committee against Terrorism (CICTE) and the Cyber Security Program, sponsors and organizes multiple cybersecurity projects in the LAC region with a wide range of national and regional entities from the public and private sectors. In particular, the OAS' Cyber Security Program is focused on building and strengthening cybersecurity capacity in its member states across three CCB areas: 1) Policy development (development and implementation of national or regional cybersecurity strategies and/or legal frameworks); 2) Capacity development (development of CSIRTs, protection of critical infrastructures, improving ability to monitor and respond to cyber incidents, training and crisis management exercises, increasing capabilities of central bodies tasked with coordinating cybersecurity activities, among others.); and 3) Research and outreach (development of technical documents, toolkits, and research-based reports to guide policy makers, CSIRTs, infrastructure operators, private organizations, and civil society on current developments and cybersecurity problems and key challenges in the region, building user trust in online platforms and e-commerce services).[134] The OAS also addresses capacity building in the area of cybercrime through CICTE, with an emphasis on the development of digital investigative capacities of law enforcement, implementation of appropriate legal tools, and promotion of information exchanges between law enforcement and CSIRTs. In addition, the OAS has set up an Inter-American Cooperation Portal on Cybercrime and a Working Group on Cybercrime under the auspices of its Department of Legal Cooperation. The Portal and Working Group were two of the major outcomes of the process of Meetings of Ministers of Justice or Other Ministers or Attorneys General of the Americas (REMJA) aimed at strengthening hemispheric cooperation in the investigation and prosecution of these crimes.[135] Among other things, this project

has resulted in the creation of a directory of national points of contact, cybercrime questionnaires, and training to build capacity to fight cybercrime.

Organisation for Economic Co-operation and Development (OECD): The OECD, headquartered in Paris, France, is an international organization focused on "building better policies for better lives" and shaping policies that foster prosperity, equality, opportunity, and well-being for all.[136] They bring together representatives from governments, businesses, and industry, as well as civil society to establish evidence-based international standards and find public policy solutions to a range of social, economic, and environmental challenges, including digital security. OECD work focuses on many policy areas, including Digital Economy, Science and Technologies, and Consumer Policy & Product Safety. The Organisation undertakes a wide range of activities to better understand how ICTs contribute to sustainable economic growth and social well-being, and their Digital Economy Papers series covers a broad range of ICT-related issues.[137] The OECD has long been supporting cooperation on the management of digital security risk to economic and social prosperity, alongside other organizations that focus on defense and international security, criminal law enforcement, and technical standards. They provide a unique forum for stakeholders to develop digital security policies that build trust in the global digital environment while preserving internet openness, innovation, and digitally-driven growth. They also serve as a knowledge hub for data collection and analysis, exchange of experiences, best-practice sharing, and advice on public policies and international standard setting. OECD work is led by formal bodies gathering policy-makers from the Organisation's membership as well as non-members and non-governmental stakeholders' communities. The first working party addressing digital security was created in the mid-1990s and OECD work in this area is currently led by the Working Party on Security in the Digital Economy (SDE), supported by the OECD Secretariat's Directorate for Science, Technology and Innovation (DSTI). The SDE develops analytical reports and drafts recommendations on topics such as national cybersecurity strategies, digital security of critical activities, products, and services, as well as the treatment of vulnerabilities. Adopted by consensus, these recommendations are non-binding international legal instruments ("soft law"). In addition, the OECD launched a Global Forum on Digital Security for Prosperity in 2018 to champion multilateral and multi-stakeholder dialogue and facilitate the convergence of views for a trusted and resilient digital environment.

Organization for Security and Co-operation in Europe (OSCE): The OSCE, headquartered in Vienna, Austria, is the world's largest regional security organization. It comprises 57 participating states from Europe, Central Asia, and North America, and serves as a forum for political dialogue on a wide range of security issues and as a platform for joint action. The organization uses a comprehensive approach to security that encompasses the politico-military, economic, environmental, and human dimensions. OSCE helps bridge differences and build trust between states by cooperating on conflict prevention, crisis management, and post-conflict rehabilitation. Through their institutions, expert units, and extensive network of field operations, they

addresses issues that impact common security problems, including cyber/ICT security, cybercrime, arms control, terrorism, good governance, energy security, democratization, among others.[138] Specifically, OSCE has a mandate to support its participating states in enhancing their criminal justice response to cybercrime, while upholding human rights, fundamental freedoms, and the rule of law. OSCE defines capacity building broadly as building the capacity of the entire system, strengthening national institutions, and engaging all possible stakeholders with a holistic and comprehensive approach to security. This approach encompasses initiatives related to fighting cybercrime, including capacity building for law enforcement, fostering dialogue with the private sector and civil society, and serving as a venue for promoting coordination and collaboration at the international level.[139] Other cybersecurity-related efforts focus on developing and implementing confidence-building measures (CBMs) and on cyber diplomacy. The OSCE Permanent Council adopted two sets of cyber/ICT security CBMs for a total of 16 non-binding, voluntary measures. These measures are designed to "enhance interstate co-operation, transparency, predictability, and stability, as well as to reduce the risks of misperception, escalation, and conflict that may stem from the use of ICTs."[140] OSCE's work in this field continues to focus on the implementation of CBMs and on providing support for the countries that implement them, including through the "Adopt a CMB" initiative and a dedicated cyber/ICT security and CBM course on their e-learning platform – available both in English and Russian.[141]

UN Executive Office of the Secretary-General (EOSG): The EOSG assists the Secretary-General with relations with members and organs of the United Nations and with specialized agencies and non-governmental organizations, in addition to assisting with policy and coordination of the Secretariat. Current UN Secretary-General, António Guterres, has prioritized ensuring that digital technology is used to "strengthen human rights, advance peace, and improve all lives, including the most vulnerable" as part of the UN Sustainable Development Goals (SDGs), and addressing the risks that digital technologies pose to "global peace, stability, and development."[142] Achieving the SDGs has remained foundational to every strategy and high-level report the UN has published in the last six years, including the "High-Level report on Digital Cooperation – The Age of Digital Interdependence" and the "Data Strategy of the Secretary-General for Action by Everyone, Everywhere (2020-22)." The Data Strategy expressly stated that technology tools and processes can be an enabler of sustainable development, but also highlighted some of the key risks of digital technology when we fail users with solutions that do not meet their needs; lose trust by mismanaging cybersecurity and privacy; or lock ourselves in inflexible "one-size-fits-all" systems.[143] Many of these concepts were also reiterated in the 2020 *UN Roadmap for Digital Cooperation*, which emphasized the need to strengthen digital capacity building (both human and institutional), including the development of digital skills, "effective use of advanced and emerging technologies," ability to advance broadband access, adoption, and meaningful use, and "ensuring that individuals stay safe,

protected and productive online" (see below for more on this important UN document).[144]

UN Office of the Secretary-General's Envoy on Technology (OSET): This Office was created in 2021 with a policy coordination mandate to promote digital cooperation, including sustainable digital development and capacity building efforts writ large, work closely with all UN entities to ensure synergy and non-duplication, participate in interagency and UN system-wide processes, and collaborate with ongoing multilateral and international processes and forums, in particular the Internet Governance Forum (IGF). OSET, working with key UN entities and other stakeholders, coordinates the implementation of the 2020 *UN Roadmap for Digital Cooperation* and the range of actions envisaged therein to ensure overall coherence, with full respect for the mandates of different UN entities. This Office also facilitates dialogue on the recommendations of the Roadmap to accelerate global digital cooperation, seizing on the opportunities – while mitigating the risks – presented by technology to ensure collective progress towards achieving the SDGs by 2030. Finally, it serves as an advocate and focal point for digital cooperation so that member states, the private sector, civil society, academic and technical communities, and other stakeholders have a first port of call for the broader UN system.[145] The Roadmap clearly recognizes that "the need for digital capacity-building is substantial" and that

> *...achieving real and sustained progress in the various dimensions of digitalization requires skills development and effective training, in particular in developing countries. This is necessary to unlock the benefits of technology, including the more effective use of emerging technologies and ensuring that individuals stay safe, protected, and productive online. For example, it is estimated that there will be 230 million 'digital jobs' in sub-Saharan Africa by 2030 that could generate nearly $120 billion in revenue, but this would require some 650 million training opportunities by 2030.* [146]

The document also acknowledges that

> *...one of the primary challenges to date is that a large part of digital capacity-building has been supply-driven as opposed to needs-based. Insufficient investment also remains a significant limiting factor. Given variances within and among countries and regions, there is no one-size-fits-all approach, and better evidence is therefore needed of which capacity-building approaches are most effective, considering political, economic, and social contexts. To overcome these challenges, two aspects are central: greater coherence and coordination in capacity-building efforts; and a concerted effort at scaling up solutions. Holistic, inclusive approaches that bring together existing initiatives, United Nations entities, regional and subregional bodies, and other relevant organizations that promote digital capacity-building are necessary to improve support for Governments and other stakeholders.* [147]

The Roadmap emphasizes the need to foster digital capacity building (both human and institutional) across four CCB areas: 1) digital literacy and skills training, 2) "effective use of advanced and emerging technologies," 3) ability to advance broadband access, adoption, and meaningful use, and 4) "ensuring that individuals stay safe, protected and productive online." It also launched a new Joint Facility for Global Digital Capacity, led by the International Telecommunication Union (ITU) and the UN Development

Programme (UNDP), to serve as a single structure facilitating joint resourcing, roles, and responsibilities tasked with mapping existing digital capacity building initiatives to assess gaps and provide strategic, operational, and programmatic support in executing digital strategies, capacity development initiatives, or other high-priority operational areas for partners.[148] Efforts to implement the Roadmap are underway, along with the establishment of a Roadmap Response Team – an interagency effort among the above-mentioned entities and DCO to better support the Resident Coordinators and the UN's in-country presence on these issues.

The UN Shared Cyber Hub brings together a large group of UN cyber focal points across the system (over 20 UN bodies), including those that deal with capacity building and policy, to make sure they speak with one voice on cybersecurity and share lessons learned.[149]

The UN Development Coordination Office (DCO) serves as the secretariat for the UN Sustainable Development Group (UN SDG), which comprises 34 agencies, funds, and programs working on development at the regional and global levels. The Office acts as a key conduit for supporting UN's activities for sustainable development, which inform policy, program, and operations on the ground.[150]

UN Development Programme (UNDP): the UNDP is the UN's global sustainable development organization, headquartered in Geneva, Switzerland, working across 170 countries. The agency has launched a broad Digital Transformation initiative – an organization-wide effort – to harness the power of new technology to improve the lives of those furthest behind. The UNDP is proactively investing in the key area of digital capacity building and its wide field presence and topic expertise aim to help match key local contexts to relevant digital solutions. They have developed a Whole-of-Society Digital Transformation framework as an overarching reference model to identify, structure, and prioritize national digital transformation efforts and agendas, and to serve as a basis for discussion for possible UNDP engagement (or to complement ongoing digital work) in countries that request UNDP support. They also developed a Digital Readiness Assessment (DRA) tool to identify digital strengths and weaknesses, and to map out the shape, pace, and types of transitions and what can be done to accelerate them, while ensuring an inclusive, whole-of-society approach to digital development.[151] Other projects in the Digital Transformation program include a Digital ID project, a Misinformation project, and an AI Readiness project.

UN Institute for Disarmament Research (UNIDIR): UNIDIR is a voluntary funded, autonomous institute within the UN, headquartered in Geneva, Switzerland, primarily focused on disarmament and security issues with the aim of assisting the international community in their disarmament thinking, decisions, and efforts. UNIDIR offers training and materials for diplomats focusing on cybersecurity norms, and hosts conference series and a Cyber Policy Portal.[152]

UN Office for Disarmament Affairs (UNODA): Headquartered in New York, U.S., UNODA is a UN office dedicated to supporting multilateral deliberations on the security and use of information and

communications technologies in the context of international security. UNODA has provided substantive support on this topic to the work of the Group of Governmental Experts (GGE) and to the Open-Ended Working Group (OEWG). UNODA will continue to provide substantive support to a new OEWG that was established for the period of 2021-2025. Through the leadership of the High Representative for Disarmament Affairs, UNODA supports member states in fostering a culture of accountability and adherence to emerging norms, rules, and principles on responsible behavior in cyberspace with a view to ensuring safety and security of the digital domain.

UN Office on Drugs and Crime (UNODC): UNODC, a UN office headquartered in Geneva, Switzerland, is dedicated to strengthening member states' capacities to confront threats from transnational crime, terrorism, corruption, and drug trafficking; to build effective criminal justice systems and transnational approaches to the world drug problem; and to promote peace and sustainable well-being as deterrents to these crimes. They were given the mandate to address cybercrime issues in 2009. The UNODC Global Program on Cybercrime assists developing countries in their efforts to prevent and combat cyber-related crimes through law enforcement capacity building and technical assistance.[153] Their activities can be grouped around three CCB areas: 1) Increase efficiency and effectiveness of investigation, prosecution, and adjudication of cybercrime (e.g., online child sexual exploitation and abuse); 2) Promote long-term whole-of-government response to cybercrime (national coordination and effective legal frameworks); and 3) Strengthen national and international communication between government, law enforcement, and the private sector).

World Bank: The World Bank, headquartered in Washington D.C., is an international financial institution that provides financing and technical assistance to low- and middle-income countries for the purpose of pursuing projects to fight poverty through sustainable solutions. The World Bank's expertise is organized across Global Practices (GPs) serving clients in 7 regions. There are 14 key technical areas of development expertise and Cross-Cutting Solution Areas addressing global challenges including gender, jobs, and fragility. The World Bank has been working to help over 100 developing countries and countries in transition to embrace the importance of scientific and technological innovation for meeting many sustainable development challenges and for accelerating human progress. Today, the majority of World Bank's projects have ICTs as a fundamental component, and every GP is introducing digital technologies in its portfolio and beginning to incorporate a cybersecurity sub-component as part of their loan operations for digital economy projects. The World Bank has also been involved in the Global Cybersecurity Capacity Program since 2016, which aims to enhance the cybersecurity capacities of developing countries through technical assistance and capacity building activities. The Bank's Digital Development (DD) GP offers technical assistance across five CCB areas ("menu of options"), namely: 1) Technical and legal support (including policy dialogues, strategy development, review of regulatory/legislative frameworks, stakeholder engagement,

benchmarking); 2) Diagnostics and policy/strategy assessments (such as national cybersecurity assessments, recommendations on CERTs, cybersecurity advice to government, best practices to mitigate cyber risk to the financial sector); 3) Institutional and governance framework (developing national cybersecurity authority, governance plans, operational and administrative standards, cyber essentials and cybersecurity regulation for SMEs); 4) Technical support and technical capacity (e.g., establishing or strengthening national CERT/SOC, procurement of hardware/software/applications, threat intelligence gathering, assurance, monitoring, audit, CERT capabilities [prevention, mitigation, response], drills, simulation, sandboxing, training for national [civilian] CERTs, support for critical infrastructure agencies and for agencies handling biometric data); and 5) Digital skills development and cybersecurity capacity training and education (providing access to skilled security professionals; training for judges, police, prosecutors, parliamentarians, legislators, senior national leaders, teachers; technical training for IT people throughout government; public awareness campaign for parents, students, children, SMEs, government staff [non-IT], entrepreneurs, and the public at large). Under a grant from the Korea-World Bank Partnership Facility, the World Bank, along with other development partners, has also developed a specific toolkit dedicated to building capacity to combat cybercrime. In August 2021, it launched a Cybersecurity Multi-Donor Trust Fund to help better define, understand, articulate, structure, and systematically roll-out the cybersecurity development agenda. The emerging work program intends to offer comprehensive cybersecurity capacity development, including the definition of result expectations, country assessments, technical assistance, capacity building and training, underpinned with necessary investments in infrastructure and technology.[154]

International Finance Corporation (IFC): The IFC, part of the World Bank Group, advances economic development by encouraging the growth of the private sector in developing countries. The IFC works on creating new markets, mobilizing other investors, and sharing expertise to create jobs, improve the lives of people, and raise living standards, especially for the most vulnerable. Their work supports the WBG's twin goals of ending extreme poverty and boosting shared prosperity.[155] The IFC has incorporated de-risking processes in its digital investment strategy and developed a risk management framework for specific industry sectors to help assess risk (high-medium-low). The sectors considered to have higher exposure to cyber risks (e.g., energy, logistics) receive additional scrutiny, versus sectors considered low risk (e.g., finance, telecom) because of existing industry frameworks, best practices, regulations, and experience.

Estonia Ministry of Foreign Affairs: Estonia, despite its small size, has developed significant cyber expertise and regularly invests in CCB projects, especially with Eastern partners (Ukraine, Georgia). Their largest digital development and cybersecurity project in Ukraine – in support of the €25 million EU Digital Transformation program in Ukraine, funded by the EU Directorate-General for Neighbourhood and Enlargement Negotiations (DG NEAR) – focuses on supporting enhancement of

its government's digital infrastructure and digital services; investing in updating legacy, Soviet-era infrastructure; improving system interoperability; building capacity of government agencies responsible for digitalization; providing advice on reforms and policy for energy, environment, justice, and home affairs (political influence); aligning with international standards; and strengthening citizens' trust in ICTs. The program includes a strong, foundational cybersecurity component and multiple CCB activities (e.g., cyber hygiene awareness and training, advice on national strategy and policy, and protection of critical infrastructure, among others).

Israel's Agency for International Development Cooperation in the Ministry of Foreign Affairs (MASHAV) & Israel National Cyber Directorate (INCD): MASHAV, located in Jerusalem, Israel, is responsible for the design, coordination, and implementation of Israel's worldwide development and cooperation programs in developing countries, with the goal of contributing to the fight against poverty and global efforts to achieve sustainable development. MASHAV activities are based on capacity building, technical assistance, and the transferring of Israeli know-how, innovation, technologies, and expertise. In particular, they focus on sectors in which Israel has accumulated expertise and a comparative advantage, like cybersecurity, and provide cyber capacity building in regions of the world that are of strategic interest to Israel (i.e., the wider Middle East, Latin America, and Central/South Asia).[156] The Israel National Cyber Directorate (INCD) – the country's locus of cyber expertise – delivers the cybersecurity capacity building programs for those countries where Israel provides development and CCB assistance. These efforts are aligned with the broader International Cyber Strategy and priorities of Israel, including developing long-term partnerships and cyber defense cooperation with key countries; improving capacity and confidence building measures and fostering better reach between markets to support the economy on both sides; and improving security at home – "when the tide rises, all boats rise."[157] Their CCB activities abroad are focused on securing, rather than developing, digital and critical infrastructure; helping countries create national CERTs/SOCs (to monitor threats, share threat information, respond to cyber incidents); and developing core expertise and capacity, regardless of the maturity of the country's digital infrastructure or legal infrastructure. Both organizations are working in close cooperation to achieve Israel's development goals.

JICA: The Japan International Cooperation Agency (JICA), headquartered in Tokyo, Japan, is a governmental agency that delivers the bulk of Official Development Assistance for the government of Japan. It is tasked with assisting economic and social growth in developing countries and promoting sustainable growth and international cooperation, with a strong focus on ensuring peace, sustainable well-being, equality, environmental protection, and social development. JICA dispatches experts and overseas volunteers to developing countries, and in return welcomes government officials and specialists as training participants and overseas students. People-to-people connections established through human resource development are considered foundational to building trust between developing countries and Japan.[158] While

the majority of JICA's development assistance projects are dedicated to infrastructure development, sustainable agriculture, and activities to increase and women and youth training and empowerment, JICA has also launched CCB initiatives to develop joint cybersecurity curricula at the university level. JICA focuses on university partnerships as the natural place to develop indigenous capacity. In Indonesia, for example, they are implementing a master-level program on cybersecurity and developing the curriculum together with their local counterparts.

UK FCDO: The UK Foreign, Commonwealth & Development Office (FCDO), headquartered in London, UK, is a ministerial department dedicated to furthering UK interests in the world, safeguarding UK security, defending UK values, reducing poverty, and tackling global challenges alongside their international partners.[159] The Cyber Policy Department, part of the National Security Directorate, is dedicated to addressing cybersecurity threats, building resilience to cybersecurity attacks, and promoting trusted and secure technology across the world. This department works closely with other lead UK government agencies such as the National Cyber Security Centre (NCSC), Government Communications Headquarters (GCHQ), Home Office, Ministry of Defence (MoD), and the Department for Digital, Culture, Media & Sport (DCMS) to improve cyber capabilities; educate different communities; increase digital literacy; provide technical assistance; and promote a free, open, peaceful, and secure cyberspace around the world. The FCDO recognizes that every development project and every single digital investment requires cyber, data, and technical security and is embedding digital/cyber de-risking mechanisms in both its cybersecurity and its digital development assistance programs. Their Digital Access Programme (DAP), a partnership between FDCO and DCMS with a total budget of £82.5 million, "aims to catalyze more inclusive, affordable, safe, and secure digital access for excluded and underserved communities" in five middle-income countries (i.e., Kenya, Nigeria, South Africa, Brazil, and Indonesia) and use digital inclusion as a basis for a more thriving digital ecosystem that can "stimulate innovations for local development challenges, create local skilled jobs, and generate opportunities for business partnerships."[160] The DAP was initiated in 2016-2017 after the publication of the World Bank's World Development Report (WDR) on Digital Dividends, which explicitly acknowledged the importance of cybersecurity as a concern for international development. The five program countries were chosen in 2018 after conducting detailed, in-country diagnostics to assess the current state of the country under three main areas (i.e., digital access and inclusion; capacity of government, society, and the economy to manage digital risks; and status of the local digital economy). The countries chosen already had a baseline digitization and capacities (e.g., connectivity, infrastructure, government agencies, some regulatory frameworks in place). The digital access diagnostic assessments, and the accompanying business cases, served to guide the FCDO in tailoring their DAP program to the specific needs of the recipient countries and to diversify the delivery models across three pillars (in-house delivery, outsourced delivery, or a mix of the two) – which, in turn, helped the

program maintain flexibility, sustainability, and adaptability to current circumstances (e.g., increased use of telemedicine and remote learning during COVID-19 crisis). The DAP program, expected to conclude by 2023, emphasizes the importance of managing digital risk; growing the local digital economy (including by embedding local tech experts in UK embassies to work on these projects); and supporting local-start-ups, technology accelerators, and digital solutions that can be applied locally – an example of "tech for good." The program also focuses on learning about sustainable models and enablers for digital inclusion, which will be shared with key stakeholders and other partner countries, thereby amplifying the impact of the program. (**Note: the FCDO does not provide funding for equipment [software/hardware] but supports key stakeholders in recipient countries to develop institutional capacity, understand how to do things by following available models or frameworks, and strengthen the capacity of local community networks).[161]

USAID: The U.S. Agency for International Development (USAID), headquartered in Washington D.C., leads the U.S. government's international development and humanitarian efforts. USAID works in over 100 countries and carries out U.S foreign policy by promoting human progress and economic and social development in the developing world.[162] In April 2021, USAID released its first-ever Digital Strategy, which identified cybersecurity as a new focus area for the Agency's technical programming and outlined its vision and commitment to improving their development and humanitarian assistance outcomes through the use of digital technology in support of open, inclusive, and secure digital ecosystems. The Digital Strategy is part of USAID's holistic approach to help achieve the UN SDGs. It offers a roadmap for staff, partners, and future programming, and "charts how USAID will change the way it does business – including embracing digital technologies by default in certain instances – in a manner that reflects best practice and is evidence-based."[163] USAID has also released a Digital Ecosystem Framework designed to provide an overview and shared understanding of the elements that influence a country's digital ecosystem across three overlapping pillars (i.e., Digital Infrastructure and Adoption; Digital Society, Rights, and Governance; and Digital Economy) and four cross-cutting topics (i.e., Inclusion, Cybersecurity, Emerging Technologies, and Geopolitical Positioning).[164] The Digital Strategy informs the work of the newly established Cybersecurity Team under the USAID Bureau for Development, Democracy and Innovation, which is helping the Agency define strategies and systems to build awareness and capacity to respond to current and future cybersecurity risks related to international development. This team has developed a "Cybersecurity Primer" for missions and for implementing partners to better understand why cybersecurity and digital resilience safeguards should become a first-order strategic and operational priority across all phases of a project (i.e., design, objectives, and implementation) and be incorporated throughout USAID's Programming Cycle. This tool introduces the concept of cybersecurity as a development challenge and as a core thread that should run through all aspects of digital development programs in order to ensure digital sustainability and resiliency. The Primer is intended to increase

awareness and provide a basic understanding of cybersecurity, cyber threats trends by sector, and cyber resilience as they relate to development programming for USAID staff, which can serve as a resource to help streamline cybersecurity into the broader development community.[165] In 2019, USAID also launched a $19.5 million Digital APEX program as part of their efforts to bridge the development and cybersecurity communities. It offers a pool of pre-approved, U.S.-based cybersecurity experts and companies that can provide implementing partners and partner governments with rapid technical assistance in the event of a significant cyber incident or help in reducing vulnerabilities in their digital systems. Beneficiaries can tap into this resource for other cyber-related projects, as well (e.g., security assessments, pen-testing, software and hardware procurement, cybersecurity training, network monitoring, incident response). This program helps expand USAID's capacities to support its partners and beneficiaries, build accessible and affordable digital infrastructure, and promote the adoption of accepted international standards. In 2020, USAID funded another cyber-related initiative – the "Greater Internet Freedom" project – that considers these issues from a democracy perspective and aims to enhance digital security for civil society and media organizations, engage citizens in internet governance debates, and advance human rights online. The global Internet Freedom Consortium that runs this initiative, organized by Internews, supports regionally-based organizations (including grantees, implementors, and other civil society organizations on the ground) that are leaders in digital rights and digital security. They promote efforts to strengthen digital hygiene, data protection and data privacy, and cyber awareness of civil society groups, and combat digital authoritarianism, disinformation, election interference, techno-solutionism, polarization, and human rights violations.[166]

U.S. State Department: The United States considers "cyber threats as the most significant security challenge facing the country, greater even than terrorism. To mitigate the risks, the U.S. promotes cybersecurity – the broad collection of tools, policies, best practices, and actions that can be used to protect organizations' and users' assets in cyberspace and better ensure that the intended availability, integrity, and confidentiality of online data and services are unaffected by malicious threats." The U.S. State Department also recognizes that working with partners to improve network defenses and cooperation with other countries to respond to cyber incidents is crucial. The Department engages with many countries on cybersecurity directly through embassy contacts and senior leadership cyber consultations, and bilaterally through such efforts as Memoranda of Understanding for CSIRT information exchanges, research and development, coordinated awareness efforts, and collective action on combating botnets. The State Department also sponsors cybersecurity and cybercrime capacity building workshops across multiple regions. Responsibility for the State Department's cyber capacity building work is spread across the regional and functional bureaus of the department using a range of foreign assistance authorities. The work to implement its cyber capacity building activities is coordinated across U.S. government agencies and with like-minded foreign government

partners, regional and global multi-stakeholder and multilateral organizations, and federally funded research and development centers. The State Department's efforts are generally focused on 1) reinforcing the international framework for responsible state behavior in cyberspace, and 2) encouraging the adoption of a set of internationally-recognized "best practices" – although both strands are considered mutually reinforcing. The "best practices" articulated in the 2007 *Framework for National Cybersecurity Efforts* have been the model for U.S. State Department national and international cybersecurity engagements and cyber capacity building efforts. U.S. assistance to nations in need of development, as outlined in the Framework, encompass five CCB areas, namely: 1) Develop national strategies to enhance cybersecurity and reduce the risks and effects of cyber disruptions; 2) Increase government-industry collaboration (public-private partnerships) to manage cyber risk and share knowledge; 3) Fight cybercrime by updating criminal laws, procedures, and policies; 4) Develop incident management capability that can coordinate cybersecurity watch, warning, response, and recovery efforts (frequently housed in a national CSIRT); and 5) Build a culture of cybersecurity, increasing awareness of citizenry and industry of their critical role in protecting cyber systems (following UN General Assembly Resolutions 57/239 and 58/199).[167] In addition, in 2018, the State Department and USAID launched the Digital Connectivity and Cybersecurity Partnership (DCCP) – a multi-year, whole-of-government initiative to provide a credible alternative to top-down, authoritarian approaches to internet connectivity and ICT development, and to enable countries to realize the economic benefits of the digital economy. Through the DCCP, the U.S. government is currently working with 17 countries in Asia, Africa, and Latin America to address shared threats through engagement with the private sector, government, and civil society.[168] DCCP aims to: expand and increase secure internet access in targeted emerging markets by supporting the development of secure communications infrastructure and enabling market entry (or expanded market access) for U.S. or like-minded tech companies; increase the adoption of transparent regulatory policies and positions that encourage open, interoperable, reliable, and secure digital infrastructure; promote exports of U.S. ICT goods and services and increase U.S. company market share in targeted markets; and increase adoption of cybersecurity best practices in targeted countries.

ANNEX II
DEVELOPMENT AND CCB-RELATED FRAMEWORKS AND REPORTS CONSULTED

In addition to the interviews conducted and the supporting documentation provided by interviewees, the following strategies, methodologies, frameworks, and reports found on the GFCE Cybil Portal[169] and on other open-source websites informed this report:

- United Nations' strategies and reports:
  - "UN Charter" (1945);
  - "High-Level report on Digital Cooperation – The Age of Digital Interdependence" (2019);
  - "Data Strategy of the Secretary-General for Action by Everyone, Everywhere (2020-22)";
  - "Roadmap for Digital Cooperation" (2020);
  - "Final Substantive Report of the Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security" (2021);
  - "UNDP pilots the Digital Readiness Assessment in Kosovo" (2021).
- "A History of the Development Assistance Committee and the Development Co-operation Directorate in Dates, Names and Figures" (OECD, 1996)
- "Capacity Building on Cybercrime" (Council of Europe, 2013);
- "Cyber Security Capacity Building in Developing Countries: Challenges and Opportunities" (Norwegian Institute of International Affairs (NUPI), 2015);
- "Cyber Readiness Index 2.0" (Potomac Institute for Policy Studies, 2015);
- "Delhi Communiqué on a GFCE Global Agenda for Cyber Capacity Building" (GFCE, 2017);
- "Operational Guidance for the EU's International Cooperation on Cyber Capacity Building" (European Union Institute for Security Studies (EUISS), 2018);
- "Securing Digital Dividends" (New America, April 2018);
- "The Cyber Frontier and Digital Pitfalls in the Global South" (NUPI, 2018);
- "Boe Declaration on Regional Security" (Pacific Island Forum, 2018);

DEVELOPMENT AND CCB-RELATED FRAMEWORKS AND REPORTS CONSULTED

- "Global Cybersecurity Capacity Program. Lessons Learned and Recommendations Towards Strengthening the Program" (World Bank, 2019);
- "International Strategy to Better Protect the Financial System Against Cyber Threats" (Carnegie Endowment for International Peace, November 2020);
- "Lessons Learned: Cyber Incident Management Capacity Building" (GFCE, 2020);
- "Transnational Governance of Cybersecurity: Policy Challenges and Global Inequalities in Cyber Capacity Building" (Cardiff University, 2020);
- "Unpacking the GGE's Framework on Responsible State Behaviour: Capacity Building" (Global Partners Digital (GPD) & Asia-Pacific Network Information Centre (APNIC), 2020);
- "Cybersecurity Capacity Building: Cross-National Benefits and International Divides" (Oxford GCSCC, 2020);
- "Reviewing Cybersecurity Capacity in a COVID-19 Environment" (Cybersecurity Capacity Centre for Southern Africa [C3SA] & Oceania Cyber Security Centre [OCSC], 2020);
- "Australia International Cyber and Critical Technology Engagement Strategy" (Department of Foreign Affairs and Trade, April 2021);
- "Israel International Cyber Strategy" (Israel National Cyber Directorate, July 2021);
- "Digital Vulnerabilities and the Sustainable Development Goals in Developing Countries" (NUPI, 2021);
- "Managing a Digital Revolution: Cybersecurity Capacity Building in Myanmar" (NUPI, 2021);
- "Cyber Capacity Building (CCB) Needs – Mapping Exercise and Gap Analysis for African Union (AU) Member States" (AU-GFCE Collaboration Project, July 2021);
- "International Cyber Capacity Building: Global Trends and Scenarios" (EUISS, September 2021);
- "Cybersecurity Primer" (USAID, October 2021);
- "EBRD's Digital Approach to Accelerating Digital Transition" (EBRD, November 2021).

ENDNOTES

1 World Bank, "World Development Report 2016: Digital Dividends," p. 3, https://www.worldbank.org/en/publication/wdr2016.
2 Remarks by Sandie Okoro, World Bank's General Counsel, at the Council of Europe Octopus Conference 2019.
3 World Bank, "World Development Report 2021: Data for Better Lives," pp. 190-194, https://www.worldbank.org/en/publication/wdr2021.
4 World Bank, "Combatting Cybercrime: Tools and Capacity Building for Emerging Economies," www.combattingcybercrime.org.
5 World Bank, "Cybersecurity Multi-Donor Trust Fund," https://www.worldbank.org/en/programs/cybersecurity-trust-fund.
6 Global Forum on Cyber Expertise, "Cybil Portal," https://cybilportal.org/.
7 GFCE, "Delhi Communiqué on a GFCE Global Agenda for Cyber Capacity Building," 24 November 2017, https://thegfce.org/wp-content/uploads/2020/04/DelhiCommunique.pdf.
8 GFCE Members, https://thegfce.org/member-overview/.
9 UN Secretary-General António Guterres' remarks to the virtual high-level meeting on the "Impact of Rapid Technological Change on the Achievement of the Sustainable Development Goals," New York, 11 June 2020.
10 Helmut Führer, A History of the Development Assistance Committee and the Development Co-operation Directorate in Dates, Names and Figures (OECD, 1996), https://www.oecd.org/dac/1896816.pdf.
11 UN Charter, 1945.
12 ODA-eligible funding (i.e. grants and soft loans) provided by official government agencies flows to countries and territories on the DAC List of ODA Recipients and to multilateral development institutions. Concessions to ODA- eligible countries and/or activity areas are administered with the main objective of promoting the economic development and welfare of recipient countries. See: OECD, "Official Development Assistance (ODA)," https://www.oecd.org/dac/financing-sustainable-development/development-finance-standards/official-development-assistance.htm and "What is ODA?" https://www.oecd.org/development/stats/What-is-ODA.pdf.
13 World Bank, "The McNamara Years at the World Bank," (1981), https://documents1.worldbank.org/curated/en/850631468336712540/pdf/332440PUB0McNa101Official0Use0Only1.pdf.
14 UN, "Conferences | Least Developed Countries," https://www.un.org/en/conferences/least-developed-countries.
15 OECD, "DAC Statement on Basic Human Needs" (1977), https://www.oecd.org/dac/1896808.pdf.
16 World Commission on Environment and Development, "Brundtland Report," https://www.britannica.com/topic/Brundtland-Report.
17 Robert Collett and Nayia Barmpaliou, "International Cyber Capacity Building: Global Trends and Scenarios," EUISS, September 2021, https://www.iss.europa.eu/sites/default/files/EUISSFiles/CCB%20Report%20Final.pdf.
18 United Nations, "Sustainable Development Goals," https://sdgs.un.org.
19 World Bank, "World Development Report: Digital Dividends," (2016): p. 3, https://www.worldbank.org/en/publication/wdr2016.
20 DiploFoundation, "Sustainable Development," https://dig.watch/issues/sustainable-development.
21 Carl Bildt, "Development's Digital Divide," Project Syndicate, 2015, http://www.project-syndicate.org?commentary/sustainable-development-goals-digital-divide-by-carl-bildt-2015-08.
22 ITU, "ICTs for a Sustainable World," https://www.itu.int/en/sustainable-world/Pages/default.aspx
23 EBRD, "Annual Review 2020," (2021), https://www.ebrd.com/news/publications/annual-report/annual-review-2020.html.
24 Niels Schia and Johann Willers, "Digital Vulnerabilities and the Sustainable Development Goals in Developing Countries," Norwegian Institute of International Affairs (NUPI), Oslo, Norway (2021), p. 2.
25 Atlantic Council, "The Role of Development Finance and Trusted Connectivity in Achieving the Sustainable Development Goals," 18 October 2021, https://www.atlanticcouncil.org/event/the-role-of-development-finance-and-trusted-connectivity-in-achieving-the-sustainable-development-goals/.
26 United Nations, "Roadmap for Digital Cooperation," June 2020, pp. 12-13, https://www.un.org/en/content/digital-cooperation-roadmap/assets/pdf/Roadmap_for_Digital_Cooperation_EN.pdf.
27 UN Office of the Secretary-General's Envoy on Technology, "Digital Capacity Building," https://www.un.org/techenvoy/content/digital-capacity-building.

28 Schia and Willers, "Digital Vulnerabilities and the Sustainable Development Goals in Developing Countries."
29 Ibid.
30 Robert Morgus, "Securing Digital Dividends," New America, April 2018, p.8, https://www.newamerica.org/cybersecurity-initiative/reports/securing-digital-dividends/.
31 UN General Assembly, "Final Substantive Report of the Open-Ended Working Group (OEWG) on Developments in the Field of Information and Telecommunications in the Context of International Security," 10 March 2021, https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf; and Internet Society, "What Do You Mean When You Say 'Open Internet'?" 3 September 2014, https://www.internetsociety.org/blog/2014/09/what-do-you-mean-when-you-say-open-internet/.
32 UN Secretary General's High-Level Panel on Digital Cooperation, "The Age of Digital Interdependence," (2019), https://www.un.org/en/pdfs/DigitalCooperation-report-for%20web.pdf.
33 Collett & Barmpaliou, "International Cyber Capacity Building: Global Trends and Scenarios," EUISS.
34 Ibid.
35 Schia and Willers, "Digital Vulnerabilities and the Sustainable Development Goals in Developing Countries."
36 Authors' interview with African Union Commission representative.
37 Melissa Hathaway and Francesca Spidalieri, "The Cyber Readiness Index 2.0," Potomac Institute for Policy Studies, https://www.potomacinstitute.org/academic-centers/cyber-readiness-index.
38 Tim Mauer and Arthur Nelson, "International Strategy to Better Protect the Financial System Against Cyber Threats," Carnegie Endowment for International Peace, November 2020, https://carnegieendowment.org/2020/11/18/priority-5-capacity-building-pub-83113.
39 Collet & Barmpaliou, "International Cyber Capacity Building: Global Trends and Scenarios."
40 Robert Collett, "Understanding cybersecurity capacity building and its relationship to norms and confidence building measures," *Journal of Cyber Policy,* 2021.
41 Israel National Cyber Directorate, "Israel International Cyber Strategy," July 2021; and authors' interview with the Israel National Cyber Directorate.
42 "Securing Digital Dividends," New America (2018).
43 "UN Secretary-General's press remarks on New Plan for Digital Cooperation," https://media.un.org/en/asset/k1x/k1x3tnmwei.
44 "Securing Digital Dividends," New America (2018).
45 Pacific Island Forum, "Boe Declaration Action Plan," https://www.forumsec.org/wp-content/uploads/2019/10/BOE-document-Action-Plan.pdf.
46 "Securing Digital Dividends," New America (2018).
47 Authors' interview with OAS representative.
48 United Nations, "Roadmap for Digital Cooperation," June 2020.
49 "Securing Digital Dividends," New America (2018).
50 ICT Works, "The Future of International Development Programmes in the Digital Age," 1 September 2021, https://www.ictworks.org/international-development-cooperation-digital-age/.
51 Authors' interview with DiploFoundation.
52 "A report conducted by analysts from Dataprotect, a Morocco-based data security firm, indicates that 55% of African financial institutions outsource their cybersecurity needs," https://cybersecforum.eu/wp-content/uploads/2020/08/ECJ-VOLUME-6-2020-ISSUE-1.pdf.
53 UN Roadmap for Digital Cooperation.
54 Ibid.
55 UN DCO, "About," https://unsdg.un.org/about/development-coordination-office.
56 Authors' interview with OECD representative.
57 United Nations, "UN Secretary-General's Roadmap for Digital Cooperation," https://www.un.org/en/content/digital-cooperation-roadmap/; and UN Office of the Secretary-General's Envoy on Technology, "Digital Capacity Building," https://www.un.org/techenvoy/content/digital-capacity-building.
58 "AU-GFCE Collaboration: Enabling African Countries to Identify and Address Their Cyber Capacity Needs," GFCE Cybil Portal, https://cybilportal.org/projects/auc-gfce-collaboration-enabling-african-countries-to-identify-and-address-their-cyber-capacity-needs/.
59 Authors' interview with CREST, 25 August 2021.
60 CMU CyberLab-Africa, https://www.cylab.cmu.edu/research/africa/index.html
61 DIAL, "Unlocking MNO data to enhance public services and humanitarian efforts," February 2018, https://digitalimpactalliance.org/wp-content/uploads/2018/02/DIAL_D4D-Report_2018.pdf.
62 Digital Impact Alliance, "Who We Are," https://digitalimpactalliance.org/home/who-we-are/.

63 DPGA, "Who We Are," https://digitalpublicgoods.net/who-we-are/.
64 DPGA, "What We Do," https://digitalpublicgoods.net/what-we-do/.
65 World Bank, "Combatting Cybercrime: Tools and Capacity Building for Emerging Economies," www.combattingcybercrime.org.
66 "Cybil Portal," https://cybilportal.org.
67 USAID, "Cybersecurity Primer," October 2021, https://www.usaid.gov/sites/default/files/documents/10-26-21_EXTERNAL_CyberPrimer-CLEARED-accessible.pdf.
68 UNDP, "UNDP pilots the Digital Readiness Assessment in Kosovo," 24 March 2021, https://www.ks.undp.org/content/kosovo/en/home/presscenter/articles/2021/03/24/undp-pilots-the-digital-readiness-assessment-in-kosovo.html.
69 Note: cybersecurity and data protection are mostly discussed as part of the Regulations pillar.
70 Authors' interview with the UNDP.
71 DiploFoundation, "Sustainable Development," https://dig.watch/issues/sustainable-development.
72 ITU, "Global Cybersecurity Index 2020," https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx.
73 Melissa Hathaway, "Managing National Cyber Risk," Organization of American States, (2018), https://www.oas.org/es/sms/cicte/ENGcyberrisk.pdf.
74 Schia & Willers, "Digital Vulnerabilities and the Sustainable Development Goals in Developing Countries," p. 2.
75 Council of Europe, "The Budapest Convention on Cybercrime: Benefits and Impact in Practice," July 2020, https://rm.coe.int/t-cy-2020-16-bc-benefits-rep-provisional/16809ef6ac.
76 INTERPOL, "National Central Bureau (NCBs)," https://www.interpol.int/en/Who-we-are/Member-countries/National-Central-Bureaus-NCBs.
77 GFCE Cybil, "Strengthening the Work of the CBM 8 PoC Crisis Communication Network," https://cybilportal.org/projects/strengthening-the-work-of-the-cbm-8-poc-crisis-communication-network/
78 EU CyberNet, https://www.eucybernet.eu/vision/.
79 Authors' interview with CREST.
80 ITU, "Kenya National CIRT Establishment," GFCE Cybil, https://cybilportal.org/projects/kenya-national-cirt-establishment/, and "Kenya National CIRT Enhancement," https://cybilportal.org/projects/kenya-national-cirt-enhancement/.
81 Authors' interview with the ITU, 31 August 2021.
82 USAID, "Cybersecurity for Critical Infrastructure in Ukraine."
83 Council of Europe, "Global Action on Cybercrime Extended (GLACY+)," https://www.coe.int/en/web/cybercrime/glacyplus.
84 DG Neighbourhood and Enlargement Negotiations (DG NEAR), https://ec.europa.eu/neighbourhood-enlargement/directorate-general_en .
85 Authors' interview with representative of DG NEAR – Ukraine special unit.
86 EU CyberNet, "EU CyberNet work in Dominican Republic, first national cybersecurity exercise "Cyber llamas," https://www.eucybernet.eu/eu-cybernet-work-in-dominican-republic-first-national-cyber-llamas-exercise/.
87 Cyber4Dev, "Cyber4Dev experts deliver wide-ranging virtual training alongside partners in Ecuador and Paraguay," https://cyber4dev.eu/2021/03/26/continuing-our-support-to-south-american-partners/, and "Cooperation in times of adversity creates opportunities for development," https://cyber4dev.eu/2020/08/11/cooperation-in-times-of-adversity-creates-opportunities-for-development/.
88 Authors' interview with World Bank representatives.
89 Remarks by Susan Lund, Vice President of Economics and Private Sector Development at the International Finance Corporation (IFC), 18 October 2021, https://www.atlanticcouncil.org/event/the-role-of-development-finance-and-trusted-connectivity-in-achieving-the-sustainable-development-goals/.
90 UN DCO, https://unsdg.un.org/about/development-coordination-office.
91 UNODC, "UNODC Strengthens El Salvador's Capabilities in the Fight against Cybercrime Committed against Children, Adolescents and People with Disabilities," 28 March 2017, https://www.unodc.org/ropan/en/unodc-strengthens-el-salvadors-capabilities-in-the-fight-against-cybercrime-committed-against-children--adolescents-and-people-with-disabilities.html.
92 "Securing Digital Dividends," New America (2018), pp. 35-6, 51.
93 Ibid.
94 ICT Works, "The Future of International Development Programmes in the Digital Age," 1 September 2021, https://www.ictworks.org/international-development-cooperation-digital-age/.
95 "Securing Digital Dividends," New America (2018).

96 OECD, "Enhancing the digital security of products," https://www.oecd-ilibrary.org/science-and-technology/enhancing-the-digital-security-of-products_cd9f9ebc-en.
97 Geneva Dialogue on Responsible Behavior in Cyberspace, https://genevadialogue.ch.
98 "Securing Digital Dividends," New America (2018).
99 Ibid.
100 Schia & Willers, "Digital Vulnerabilities and the Sustainable Development Goals in Developing Countries."
101 ICT Works, "The Future of International Development Programmes in the Digital Age," 1 September 2021, https://www.ictworks.org/international-development-cooperation-digital-age/
102 African Union, "The Commission," https://au.int/en/auc.
103 GFCE, "AUC-GFCE Collaboration: Enabling African Countries to Identify and Address their Cyber Capacity Needs," 8 March 2021, https://thegfce.org/auc-gfce-collaboration-enabling-african-countries-to-identify-and-address-their-cyber-capacity-needs/.
104 GFCE, "AU-GFCE Collaboration Project: Cyber Capacity Building (CCB) Needs – Mapping Exercise and Gap Analysis for African Union (AU) Member States," July 2021.
105 AIIB, "Who We Are," https://www.aiib.org/en/about-aiib/index.html.
106 AIIB, "Digital Infrastructure Sector Strategy," June 2020, https://www.aiib.org/en/policies-strategies/operational-policies/digital-infrastructure-strategy/index.html.
107 DFAT, https://www.dfat.gov.au.
108 Authors' interview with former DFAT representative.
109 Australia's International Cyber and Critical Tech Engagement, "Cyber and Critical Tech Cooperation Program," https://www.internationalcybertech.gov.au/cyber-tech-cooperation-program.
110 DFAT, "Development risk management," https://www.dfat.gov.au/development/topics/development-risk-management.
111 Australia Government, "International Cyber and Critical Technology Engagement Strategy," April 2021, https://www.internationalcybertech.gov.au/our-work.
112 Ibid.
113 CREST, "Homepage," https://www.crest-approved.org/.
114 CREST, "About CREST," https://www.crest-approved.org/about-crest/index.html.
115 DiploFoundation, "About Diplo," https://www.diplomacy.edu/aboutus/about-diplo/.
116 Ibid; and "Cybersecurity," https://www.diplomacy.edu/cybersecurity.
117 DiploFoundation, "Comments on the Initial 'Pre-draft' of the Report of the Open-Ended Working Group (OEWG)," April 2020, https://front.un-arm.org/wp-content/uploads/2020/04/diplo-foundation-contribution-oewg-first-pre-draft-report.pdf.
118 Ibid.
119 EIB, "Who We Are," https://www.eib.org/en/about/index.htm; and "Priorities," https://www.eib.org/en/about/priorities/index.htm.
120 EIB, "European Investment Advisory Hub and European Cyber Security Organisation Announce First Step Towards a New pan-European Cybersecurity Investment Instrument," https://www.eib.org/en/press/all/2021-331-european-investment-advisory-hub-and-european-cyber-security-organisation-announce-first-step-towards-a-new-pan-european-cybersecurity-investment-instrument.
121 EBRD, "Who We Are," www.ebrd.com/who-we-are/.
122 EBRD, "EBRD Adopts First Digital Approach, 10 November 2021," https://www.ebrd.com/news/2021/ebrd-adopts-first-digital-approach.html.
123 EBRD, "The EBRD's approach to accelerating the digital transition, 2021-25," p. 17.
124 CyLab-Africa, https://www.cylab.cmu.edu/research/africa/index.html.
125 Global Forum on Cyber Expertise, "About the GFCE," https://thegfce.org/about-the-gfce/.
126 Global Forum on Cyber Expertise, "Cybil Portal," https://cybilportal.org/.
127 GFCE, "Delhi Communiqué on a GFCE Global Agenda for Cyber Capacity Building," 24 November 2017, https://thegfce.org/wp-content/uploads/2020/04/DelhiCommunique.pdf.
128 "AU-GFCE Collaboration: Enabling African countries to identify and address their cyber capacity needs," GFCE Cybil Portal, https://cybilportal.org/projects/auc-gfce-collaboration-enabling-african-countries-to-identify-and-address-their-cyber-capacity-needs/.
129 The project is funded by the Bill and Melinda Gates Foundation.
130 IDB, "Gobernarte Blog," https://blogs.iadb.org/administracion-publica/en/.
131 IDB, "Who we are," https://www.isdb.org/who-we-are.
132 KDB, "About KDB Bank," https://www.kdbbank.eu//kdb-bank-seoul.

133 NUPI, "Centre for Digitalization and Cyber Security Studies," https://www.nupi.no/en/Our-research/Research-centres/NUPI-s-Centre-for-Digitalization-and-Cyber-Security-Studies.
134 OAS, "Cyber Security," https://www.oas.org/en/topics/cyber_security.asp.
135 OAS, "Inter-American Cooperation Portal on Cybercrime," http://www.oas.org/en/sla/dlc/cyber-en/homePortal.asp.
136 OECD, "About," https://www.oecd.org/about/.
137 OECD, "OECD Digital Economy Papers," https://www.oecd-ilibrary.org/science-and-technology/oecd-digital-economy-papers_20716826?_ga=2.67327122.2099822214.1630675930-1561748895.1630675112; OECD, "Digital Security," https://www.oecd.org/digital/ieconomy/digital-security/.
138 OSCE, "Who We Are," https://www.osce.org/who-we-are.
139 OSCE, "Capacity-building Initiatives Related to Cybercrime in Focus at OSCE Technical Briefing," 8 September 2021, https://www.osce.org/secretariat/497434.
140 OSCE, "OSCE Activities Regarding Implementation of Cyber/ICT Security Confidence-building Measures," https://front.un-arm.org/wp-content/uploads/2020/04/1-osce-nonpaper-for-oewg-and-gge.pdf
141 OSCE, "CBM e-learning," https://elearning.osce.org/courses/course-v1:OSCE+TNTD-CYBERCBM_v1+2020_11/about.
142 Statement by António Guterres, UN Secretary-General, https://www.un.org/techenvoy/content/roadmap-digital-cooperation.
143 United Nations, "Data Strategy of the Secretary-General for Action by Everyone, Everywhere," p.33, https://www.un.org/en/content/datastrategy/images/pdf/UN_SG_Data-Strategy.pdf .
144 United Nations, "Roadmap for Digital Cooperation."
145 UN Office of the Secretary-General's Envoy on Technology, https://www.un.org/techenvoy/content/about
146 United Nations, "Roadmap for Digital Cooperation," pp. 12-13.
147 Ibid.
148 United Nations, "Joint Facility for Global Digital Capacity," May 2021, https://digital-capacity.org/joint-facility/; and "Strengthening digital capacity building," https://www.un.org/techenvoy/sites/www.un.org.techenvoy/files/general/Capacity_Building_Summary_PDF.pdf.
149 Authors' interview with representatives of the Executive Office of the UN Secretary-General (EOSG).
150 UN Development Coordination Office, https://unsdg.un.org/about/development-coordination-office.
151 UNDP, "UNDP Pilots the Digital Readiness Assessment in Kosovo," 24 March 2021, https://www.ks.undp.org/content/kosovo/en/home/presscenter/articles/2021/03/24/undp-pilots-the-digital-readiness-assessment-in-kosovo.html.
152 UN Institute for Disarmament Research, "UNIDIR Cyber Policy Portal," https://cyberpolicyportal.org/en/.
153 United Nations Office on Drugs and Crime, "Global Programme on Cybercrime," www.unodc.org/unodc/en/cybercrime/global-programme-cybercrime.html.
154 World Bank, "Cybersecurity Multi-Donor Trust Fund," https://www.worldbank.org/en/programs/cybersecurity-trust-fund.
155 IFC, "About IFC," https://www.ifc.org/wps/wcm/connect/corp_ext_content/ifc_external_corporate_site/about+ifc_new.
156 MASHAV, "About MASHAV," https://mfa.gov.il/MFA/mashav/AboutMASHAV/Pages/Guiding_Principles.aspx.
157 Israel National Cyber Directorate, "Israel International Cyber Strategy," July 2021, p. 9.
158 "JICA at a Glance," https://www.jica.go.jp/english/about/at_a_glance/index.html.
159 FDCO, "What the Foreign, Commonwealth & Development Office Does," https://www.gov.uk/government/organisations/foreign-commonwealth-development-office.
160 FCDO, "Digital Access Programme," https://devtracker.fcdo.gov.uk/projects/GB-1-204963/summary.
161 Authors' interview with FCDO representatives.
162 USAID, "Who We Are," https://www.usaid.gov/who-we-are.
163 USAID, "USAID Digital Strategy," https://www.usaid.gov/usaid-digital-strategy.
164 USAID, "USAID Digital Ecosystem Framework," https://www.usaid.gov/sites/default/files/documents/Digital_Strategy_Digital_Ecosystem_Final.pdf.
165 USAID, "Cybersecurity Primer," October 2021, https://www.usaid.gov/sites/default/files/documents/10-26-21_EXTERNAL_CyberPrimer-CLEARED-accessible.pdf.
166 Internews, "Global Consortium Launches Three-Year Effort to Strengthen Internet Freedom in 50 Countries," 10 September 2020, https://internews.org/global-consortium-launches-three-year-effort-strengthen-internet-freedom-50-countries/.

167 U.S. State Department Office for the Coordinator for Cyber Issues, "Cybersecurity," August 2015.
168 U.S. State Department, "Digital Connectivity and Cybersecurity Partnership," https://www.state.gov/digital-connectivity-and-cybersecurity-partnership/.
169 Cybil Portal, "Publications," https://cybilportal.org/publications/?_sf_ppp=148.

THE WORLD BANK
IBRD • IDA | WORLD BANK GROUP

DIGITAL
DEVELOPMENT
PARTNERSHIP