European Commission

INTERNATIONAL CYBER CAPACITY BUILDING: GLOBAL TRENDS AND SCENARIOS

Printed by Imprimerie Centrale in Luxembourg

Manuscript completed in 2021

Prepared by

ISS
EUROPEAN
UNION
Institute for
Security Studies

This report was written by Robert Collett and Nayia Barmpaliou. The project was coordinated by Dr Patryk Pawlak, Brussels Executive Officer (EUISS) and Ondrej Vosatka, Policy Officer (FPI).

This document has been prepared for the European Commission however it reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

The European Commission is not liable for any consequence stemming from the reuse of this publication.

Luxembourg: Publications Office of the European Union, 2021

Print	ISBN 978-92-9462-043-9	doi:10.2815/06590	QN-01-21-158-EN-C
PDF	ISBN 978-92-9462-044-6	doi:10.2815/346676	QN-01-21-158-EN-N

INTERNATIONAL CYBER CAPACITY BUILDING: GLOBAL TRENDS AND SCENARIOS

Robert Collett
Nayia Barmpaliou

September 2021

TABLE OF CONTENTS

TABLES AND FIGURES

ABBREVIATIONS

ACRC	Africa Cybersecurity Resource Centre
APCERT	Asia Pacific Computer Emergency Response Team
APNIC	Asia Pacific Network Information Centre
ARPANET	Advanced Research Projects Agency Network
ASCCE	ASEAN-Singapore Cybersecurity Centre of Excellence
ASEAN	Association of Southeast Asian Nations
ASPI	Australian Strategic Policy Institute
AU	African Union
C3SA	Cybersecurity Capacity Centre for Southern Africa
CAMP	Cybersecurity Alliance for Mutual Progress
CARICOM	Caribbean Community
CCB	(International) cyber capacity building
CEPOL	EU Agency for Law Enforcement Training
CERT/CC	Computer Emergency Response Team Coordination Centre
CERT NZ	New Zealand Computer Emergency Response Team
CGAP	Consultative Group to Assist the Poor
CSIRT	Computer Security Incident Response Team
CTO	Commonwealth Telecommunications Organisation
DAC	Development Assistance Committee
DFAT	Department of Foreign Affairs and Trade
DG	Directorate-General
DG INTPA	Directorate-General for International Partnerships
DG NEAR	Directorate-General for Neighbourhood and Enlargement Negotiations
EC3	European Cybercrime Centre
ECOWAS	Economic Community of West African States
EEAS	European External Action Service
ENISA	European Union Agency for Cybersecurity
EU	European Union
EU CyberNet	EU Cyber Capacity Building Network
EUISS	European Union Institute for Security Studies
FCDO	Foreign Commonwealth and Development Office
GFCE	Global Forum on Cyber Expertise
GIZ	Deutsche Gesellschaft für Internationale Zusammenarbeit
GLACY	Global Action on Cybercrime
GLACY+	Global Action on Cybercrime Extended
IADB	Inter-American Defense Board
IcSP	Instrument Contributing to Stability and Peace

IfS	Instrument for Stability
INTERPOL	International Criminal Police Organisation
ITU	International Telecommunication Union
JICA	Japan International Cooperation Agency
KISA	Korea Internet & Security Agency
M&E	Monitoring & Evaluation
MFF	Multi-Annual Financial Framework
NATO	North Atlantic Treaty Organization
NGO	Non-Governmental Organisation
NUPI	Norwegian Institute of International Affairs
NZ	New Zealand
OAS	Organization of American States
ODA	Overseas Development Assistance
OECD	Organisation for Economic Co-operation Development
OSCE	Organization for Security and Co-operation in Europe
PaCSON	Pacific Cyber Security Operational Network
PILON	Pacific Islands Law Officers' Network
PoA	Programme of Action
S/CCI	Office of the Coordinator for Cyber Issues
SEI	Software Engineering Institute
TF-CSIRT	Task Force on Computer Security Incident Response Teams

ACKNOWLEDGEMENTS

This report was made possible with EU funding and support. The authors would like to thank Ondrej Vosatka and Carlos Bandin-Bujan at the European Commission; Patryk Pawlak, Nils Berglund and Christian Dietrich at EUISS; and Rebecca Emerson-Keeler for her extensive contributions to the gender section. We are also grateful to the Cybil Portal, the designers at ONE and Pigeon Studios and the organisers of the GFCE Regional Meeting and the European Cyber Agora for the opportunity to discuss our initial findings. Most importantly, this report was only possible with the support of experts who agreed to talk with us about their experience and insights during focus group consultations, interviews and feedback discussions. We have kept their contributions anonymous, so they are not named here, but we are very grateful to them all for their assistance.

EXECUTIVE SUMMARY

International cyber capacity building (CCB) projects involve countries, companies and organisations helping each other across borders to develop functioning and accountable institutions that respond effectively to cybercrime and to strengthen a country's cyber resilience. These projects take many forms, such as advising government teams that respond to national cybersecurity incidents, helping countries design and run public awareness campaigns about staying safe online and training police to investigate cybercrime.

This report identifies four trends in cyber capacity building and extrapolates their development to explore four potential scenarios that can inform capacity builders' strategic decision making.

Trend 1: The field of cyber capacity building is growing.

The field of cyber capacity building started relatively recently, in the 1990s to 2000s, and is now estimated to include at least 250 projects a year. This growth has been driven by some of the field's early funders increasing their investment and by new donors starting to contribute. The number of countries and organisations involved in capacity building is also growing, and almost all countries have been involved with at least one project. Separately, the field is also deepening in terms of the range of issues it tackles. It began with a focus on cybercrime, but has added incident response, protecting critical national infrastructure, strategic planning, public awareness, skills for the workforce, diplomacy and more. Programme teams are beginning to include digital issues within their remits that blur the boundaries of cyber capacity building.

Trend 2: The gap between aspirations for coordination and its implementation is growing.

The principle that coordination is necessary and important has been established in at least two key international agreements. Coordination in practice is improving, but slowly and intermittently. The gap between aspirations and implementation persists, leading to frustration in the CCB community. Competition for funding is a barrier to coordination, and programme teams do not have sufficient time to devote to it or to monitor projects on the ground, where the problems arise. The Global Forum on Cyber Expertise (GFCE) is currently the sole multistakeholder forum dedicated to supporting coordination, but its effectiveness is constrained by its reliance on voluntary contributions from its members. New proposals – such as the Programme of Action (PoA) at the United Nations – also highlight the need to strengthen coordination.

Trend 3: More communities of practice are using CCB to pursue distinct aims.

Cybersecurity developed in parallel within different *parent communities*, including criminal justice, technical incident response, foreign policy, defence, development cooperation, civil society and the private sector. Each has their own culture and aims. In the early years, they did not think of their projects as ‘cyber capacity building’. However, as it became clear that this was a new area of international cooperation, it became recognized as its own field. A *core community of cyber capacity building* emerged, with members coming from those parts of the *parent communities* working on relevant projects. Nonetheless, each *parent community* still has its own aims and culture when running projects, and a new narrative, culture and set of shared aims for cyber capacity building has yet to emerge. This fragmentation is a challenge to having a coordinated approach and pulling in the same direction.

Trend 4. Cyber capacity building is gradually professionalising.

The growing maturity of CCB as a field of development cooperation is leading to greater professionalisation across this policy area. The field is increasingly applying lessons from the development community by running longer projects. The average project is also tackling more issues. Programme teams overseeing projects are expanding and bringing in new staff specialised in project management (e.g. grant issuing and monitoring processes, impact evaluation) or specific issues (e.g. cybersecurity, economics). There is also a renewed interest in strengthening evidence-based decision making in CCB, including through a GFCE Research Agenda. Finally, the approach to delivering projects is shifting from flying international advisors in and out of a country for short visits to other methods, such as hiring local staff, embedding international staff for longer periods and remote delivery. Remotely delivered training has been essential during the pandemic, with mixed feedback on effectiveness.

Recognising the potential impact of these trends, this report proposes **four scenarios** for potential directions cyber capacity building could take in the next ten years. It takes account of global megatrends including the shift of power away from states, the rise of the global East and South and the impact of the fourth industrial revolution.

Scenario 1: Siloed Stagnation. There is little new investment in cyber capacity building and weak coordination. This results in negligible change in other trends and the field looks much as it does today, grappling with the same challenges and having the same conversations.

Scenario 2: Frustrated Coordination. The CCB field does not grow any faster, but more effort is put into improving coordination. This leads to better projects and is a sign of more efforts aimed at professionalisation. However, the shortage of funding leads to frustration, as the extra coordination is done through volunteer activity and increased effort is not matched by additional donor investment.

Scenario 3: Resourced Fragmentation. The CCB field sees considerable growth in investment, but little improvement in coordination. The investment comes from deeper engagement in CCB by a range of communities, but primarily by those concerned with defence and stability. The level of coordination in this scenario is low because these communities work in silos, pursuing their own goals. All parent communities increase investment to protect their own work and interests, but with little coordination between communities and countries, except close allies. Projects cluster in a few countries considered critical for security or political reasons.

Scenario 4: Collaborative Transformation. Concern about issues of digital equity and safety in lower income countries and groups fuels increased investment to achieve positive, resilient digital development outcomes. Several politicians, philanthropists and global activists champion this cause. The investment drives improved professionalisation and a wide range of parent communities engage more deeply in this positive agenda. The level of coordination is high, facilitated by transparency about projects and globally agreed upon principles and goals for the field.

We conclude with recommendations for the field based upon each trend. These address three main stakeholder groups: the EU, which commissioned this research; the broad international cyber capacity building community of actors engaging in CCB projects; and the Global Forum on Cyber Expertise (GFCE), as the leading global coordination and knowledge exchange platform on CCB. Our recommendations provide actionable steps that would continue and accelerate the trend of professionalisation our report describes, while narrowing the gap between the field's aspirations for coordination and its patchy implementation. If applied, they would help shift the field of cyber capacity building from its current state of forming and storming to the more mature phases of norming and performing.

We conclude with **recommendations** addressed to three main stakeholder groups: the EU, which commissioned this research; the broad international cyber capacity building community of actors engaging in CCB projects; and the GFCE, as the leading global coordination and knowledge exchange platform on CCB.

Recommendations for the EU: The EU should build on its CCB successes and lessons to date to develop a strategic, harmonised narrative for CCB that reflects on its different institutional priorities (such as development, security, digitalisation, trade), identifies where the EU best adds value within the growing range of actors, and defines criteria for its investment priorities both in terms of thematic and geographic areas. This process should go hand in hand with an analysis of the available financing streams and how these can be maximised to enable efficient and scalable CCB programming, in particular relating to mainstreaming cybersecurity across digital transformation initiatives and to establishing synergies with sectorial infrastructure projects. Given the EU's complex institutional architecture, the report calls for a concerted effort to improve internal coordination amongst EU services and institutions as well as with Member States. To maintain a leadership role in the global CCB ecosystem, the EU should support further professionalisation of projects such as the EU

CyberNet and strengthen global coordination efforts, including through the GFCE. Finally, further investment in knowledge tools and training of staff will be needed to improve the understanding and use of CCB in the EU's external cooperation programming.

Recommendations for the cyber capacity building community: All organisations in the cyber capacity building community should prepare for the continued growth of the field by using approaches that can scale and by setting suitably ambitious goals. For example, the community should consider agreeing a global goal that all countries have in place basic, foundational cyber capacities by a certain date, receiving CCB assistance if they need it. To maintain the current rate of growth the community should better connect with parent communities, especially the development cooperation community, that are better resourced and could help scale CCB. Funding research and sharing project evaluations to build an evidence base of impact and lessons would support this. As the field continues to grow, coordination will become ever more important. Better coordination could be achieved by organisations improving their own internal information sharing, supporting processes for international coordination such as the GFCE and making better use of in-country coordination efforts in partnership with host governments. This will be part of a broader process of professionalisation that requires expanding CCB teams, bringing in specialist staff and making time for training.

Recommendations for the GFCE: The GFCE should enable the EU and the wider cyber capacity building community in achieving their goals and implementing the recommendations above. It should prepare for the continued growth of CCB with an onboarding process that helps organisations that are new to this field, or to the GFCE, quickly connect with others and understand where they can best contribute to and benefit from the network. The GFCE was the first organisation to propose global principles of CCB and it should build upon this by supporting the development of global CCB goals. Such goals and raised ambitions should be informed by research into the need for CCB, its cost and its impact, which the GFCE's Research Agenda can support. The 2022 GFCE Annual Conference with the World Bank, the World Economic Forum and the Cyber Peace Institute is a key opportunity to better connect CCB with the development community and the private sector. Last, but not least, supporting coordination and sharing knowledge amongst CCB practitioners should remain the GFCE's priority, notably by strengthening the regional liaisons and hubs, piloting local coordination networks in a few priority countries and sustaining the expansion of the Cybil Portal.

These recommendations together with more detailed proposals made throughout this report provide actionable steps that would accelerate the trends of growth and professionalisation, while narrowing the gap between the field's aspirations for coordination and its patchy implementation. If applied, they would help shift the field of cyber capacity building from its current start-up phase to being an established field of international activity and digital transformation.

METHODOLOGY

INFORMATION SOURCES AND CODING

This report is based on primary and secondary sources of data and information. We collected primary data through two workshops ('focus group sessions') held on 16 November 2020 with 19 key individuals involved in international cyber capacity building and through 59 semi-structured interviews (see list in Annex 1). Within the constraints of information sensitivity, we also drew upon our own experience in relevant roles: Nayia Barmpaliou was the Cyber and Organised Crime Programme Manager/Policy Coordinator at the European Commission's Directorate-General for International Cooperation and Development from 2013 to 2018; Robert Collett was the Head of the UK's National Cyber Security Programme – International from 2016 to 2019 and Senior Advisor and UK Liaison to the GFCE from 2019 to 2020. Secondary data was collected in three ways: a search of the Cybil Portal of cyber capacity building projects and resources; a structured document search using article databases; and a search of grey literature – press releases, blogs, project and organisation websites, news articles, event reports and documentation – using an unstructured snowballing approach using web search engines.

We coded the qualitative data from the focus groups, interviews and structured document search of article databases using coding tags based upon a trends framework. We developed the first, a priori iteration of our trends framework deductively using our own experience. We then refined the framework inductively using the themes emerging from the data.

We coded the quantitative data on projects using the four pillars of national cyber capacity in the EU's Operational Guidance: strategic frameworks; criminal justice; incident and crisis management; and cyber hygiene and awareness (European Commission et al. 2018). We created a fifth pillar – 'other' – for projects not captured by the first four. Our interpretation of the correspondence between the EU's four-pillar framework and other common frameworks – those of the GFCE, US and UK– is shown in Figure 1.

For the trends analysis, we triangulated the findings from the interviews and focus groups, the data from the document search and the project information from the Cybil Portal and open source search.

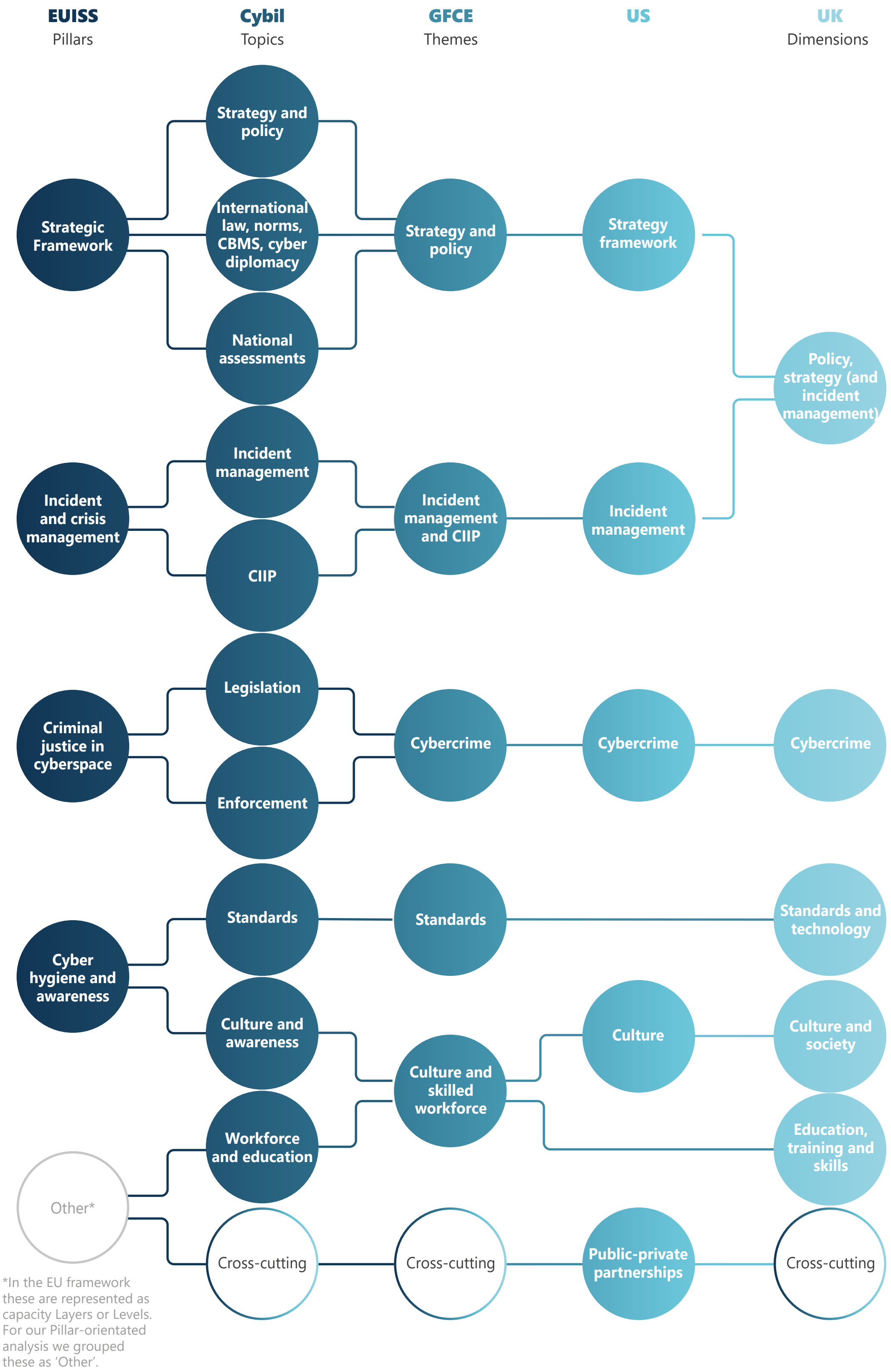
When identifying whether a country had a cybersecurity strategy, national incident response team or cyber legislation we referenced the Cyber Policy Portal of the United Nations Institute for Disarmament Research (UNIDIR). If we found conflicting information from other sources, we cross referenced against other relevant databases [1] and government websites.

To generate scenarios from the trends, we used an approach recommended to the OECD by Jonas Iversen in which a 2x2 matrix is generated from different paths that two of the trends or drivers

[1] The eGovernance Academy's National Cyber Security Index Portal, the NATO CCDCOE Strategy Library, ITU's National Cybersecurity Strategies Repository and ENISA's National Cyber Security Strategies Interactive Map.

could take in the future (Iversen 2005, 9). We solicited feedback on the scenarios from a conference workshop on 2 June 2021 as well as from earlier interviewees.

FIGURE 1. **COMPARISON OF CYBER CAPACITY FRAMEWORKS**



*In the EU framework these are represented as capacity Layers or Levels. For our Pillar-orientated analysis we grouped these as 'Other'.

THE STATE OF PROJECT INFORMATION AND PROJECT MAPPING

Our interviews identified a strong demand for information on previous cyber capacity building projects, what they did and what their impact was. We found that efforts to map basic information on projects are making progress, but that, with some notable exceptions, there is very little information available on the details of project activities, outputs and outcomes. This both posed a methodological challenge to our trends analysis and would constrain research into other issues our interviewees expressed interest in, such as the evidence for capacity building impact.

The Cybil Portal is the only source of project information to encompass the full range of international cyber capacity building projects. It is making progress in becoming a comprehensive source of basic project information. When Hameed et al. used the Portal for their analysis in 2018 it contained 165 projects (Hameed et al. 2018a). The dataset we used from the Cybil Portal contained 711 (as of 6 June 2021). The most significant weaknesses in its data are that some key actors have yet to upload any project information and that most project summaries contain little information on activities, outputs and outcomes. The Cybil Portal team, with the help of a World Bank project, are working to address both issues.

We found a small number of regional cyber capacity building mapping reports. Calandro and Berglund conducted a one-off mapping of projects in Southern Africa for a conference paper and research article (Calandro and Berglund 2019). Barbero and Berglund provided a mapping of projects in the Western Balkans to inform a regional coordination meeting in March 2021 (Barbero and Berglund 2021). In the Pacific, a community-driven effort to map projects was developed and refined alongside three regional capacity building events in Papua New Guinea, Fiji and Melbourne, Australia (Lagakali and Aiken 2020; Aiken and Lagakali 2019). All three of these efforts made use of Cybil Portal data.

As the Western Balkans and Pacific examples illustrate, and as we also found in Africa and Europe, regional cyber capacity building meetings are forums in which project mapping is being used to facilitate coordination. Event organisers have used the Cybil Portal as a starting point for their mapping then supplemented it with research prior to the meeting and with contributions at the meeting. New information has been fed back to the Cybil Portal, where it is available for others and can be held until the next regional meeting. We also found, through our interviews, examples of project design teams using the Cybil Portal as a starting point for their own stakeholder mapping and gap analysis.

Although we categorise the overall state of online information sharing about projects as poor, there are some exceptions that can be looked to as sources of good practice. The Council of Europe's approach to information sharing was exemplary. Each Council of Europe project has its own web page, following a standardised structure that contains documents including project summaries, records of workshops and events, output documents and resources that may be useful for other projects, such as templates [2]. The Council of Europe also included the creation of an online portal of useful cybercrime capacity building documents within its Octopus project. Another example of good practice came from the Organization of American States (OAS), who each year update an online report summarising every cyber capacity building activity they have ever conducted, grouped by country (Organization of American States (OAS) 2019). Turning to examples from government actors, we noted Korea's Global Cybersecurity Center for Development as an example of a national programme that publishes annual reports on its activities and Australia's Cyber and Critical Tech Co-operation Program website for helpfully providing information on both current and former partners (Korea Internet & Security Agency 2019; Australia, Department of Foreign Affairs and Trade 2021). Several implementers issue press releases or case studies on their projects, which they retain and make searchable on their websites (UK Foreign Commonwealth and Development Office 2020). We found these useful, but it was not possible to determine how comprehensive these were without an accompanying web page listing all cyber capacity building projects the organisation had run.

We found very few project or programme evaluation reports, but those that had been published were extremely useful for our research. An example of such a report is the World Bank's 'Global cybersecurity capacity program: Lessons learned and recommendations towards strengthening the program' (World Bank 2019). We know from our personal experience and interviews that other programmes have conducted similar evaluations and we encourage their owners to publish these, even if redactions are required.

Finally, the Global Forum on Cyber Expertise Magazine was a useful source of articles and interviews that provide information on what occurs within and around projects. The GFCE's working groups have also produced several reports on issues and trends within their own pillar of capacity building.

Notably lacking from the pool of information were peer reviewed, academic studies of cyber capacity building. The cyber capacity building literature in peer reviewed journals is limited and mainly composed of policy papers, not structured qualitative or quantitative studies. We return to the issue of research in the trends section of the report.

Applying a good practice established by other researchers, when we found open-source project information that was not already in the Cybil Portal, we passed it to the site's manager. They will discuss with each project's owners whether it can be added to the portal. We will also request that this report be made available through the resources section of the site.

[2] For example, the iPROCEEDS project page is available at: https://www.coe.int/en/web/cybercrime/iproceeds.

INTRODUCTION

> *Improving cybersecurity is essential for people to trust, use and benefit from innovation, connectivity and automation, and for safeguarding fundamental rights and freedoms, including the rights to privacy and to the protection of personal data, and the freedom of expression and information. Cybersecurity is indispensable to the network connectivity and the global and open Internet that must underpin the transformation of the economy and society in the 2020s.*
>
> *EU's Cybersecurity Strategy for the Digital Decade*
> *(European Union 2020, 4)*

In 1999, Bill Gates predicted that by 2020 "people will pay their bills, take care of their finances, and communicate with their doctors over the internet" (Gates and Hemingway 1999). He was writing at a time when 14% of Belgians used the Internet and 30% had a mobile phone, but he could see where the emerging trends were heading.

The world Bill Gates imagined is here and with it many of the hoped-for digital dividends. However, what few anticipated twenty years ago were the scale and complexity of the threats facing our digitally dependent world, threats to both its systems and its values. The annual cost of cybercrime alone is estimated to have reached one trillion US dollars and is rising (Malekos Smith, Lostri, and Lewis 2020).

The EU has a well-established track record in cyber capacity building, but the adoption of a new cybersecurity strategy in 2020 is an opportunity to look at the field afresh. The EU, and many other organisations, want to better understand this new field, what is happening in it, where it is going and how they should be involved. They want to know how it can support their goals, including domestic security, international development, promoting values, keeping the Internet safe and open, building bilateral partnerships, expanding exports and many other outcomes cyber capacity building can support.

Every country must protect itself and its citizens against cybersecurity threats, while preserving their online rights and freedoms, but their abilities to do so vary greatly. There is a cyber capacity gap between nations. International cyber capacity building (hereon: cyber capacity building, CCB) emerged as a policy area with the aim of closing this gap through transfers of knowledge, skills and technology between countries designed to strengthen and support local partners and, through them, the interconnected global digital system.

The term 'cyber capacity building' may sound abstract and technical, but at heart it means people joining forces across borders to better protect the benefits offered by the Internet and connected digital technology. In practice, CCB describes a policy space where everybody has a role to play: former and current police officers visit their counterparts in other countries to run training classes on digital forensics and take part in tabletop exercises; donor-funded education consultants join video calls with government officials to offer advice on designing online safety awareness campaigns for children; civil society experts write guides on how local NGOs can engage in the development of national cybersecurity strategies; companies provide free software to computer security incident response teams in low-income countries so they can respond to attacks more quickly; and staff from those incident response teams attend regional training courses run by volunteers from other such units around the world.

STATE OF THE ART AND OF THE FIELD

The field of cyber capacity building is now a complex network of people, organisations and projects that design, implement, coordinate and study this exchange of cyber experience around the world. However, it is still relatively young in comparison to other fields of international cooperation. While the field's earliest projects date to the late 1990s, cyber capacity building only took off in the last 20 years.

The outputs of the CCB field have included new national cybersecurity strategies, legislation, national incident response teams, public awareness campaigns and a wide array of training and education opportunities for professionals and young people. While researchers have not quantified the sum of this progress globally, they have demonstrated that improved cyber capacity contributes to improved indicators in personal, business and government benefits from digital technology and in indicators of voice and accountability, such as freedom of expression and association (Dutton et al. 2019; Creese et al. forthcoming).

This report is concerned with international cyber capacity building projects. There are several types of projects that are explicitly out of scope:

- Domestic cyber capacity building, where there is no international component.
- Purely commercial capacity building services that have been purchased by the beneficiary country from an international company at full cost without any pro bono assistance.
- International projects that contain some cyber capacity building activity, but have an alternative primary purpose, such as development of e-government services.
- Classified projects, such as capacity building cooperation between intelligence agencies.

Nonetheless, the report takes note of these projects where they were referenced in the sources and mentions them where relevant throughout the report.

This report aims to assist the EU and the wider international community in taking strategic decisions about their cyber capacity building activity. Its unique contribution is to examine the history of the field and identify key trends that can inform decision making. Our document search and interviews confirmed our expectation that there is a gap in the existing literature regarding cyber capacity building trend analysis. We found no papers that sought to identify trends across the full breadth of cyber capacity building experience. There were, however, a small number of papers that were closely related to the topic:

- Hameed et al.'s 'Analysing Trends and Success Factors of International Cybersecurity Capacity-Building Initiative' contains a high-level regional and thematic analysis of the project data on the Cybil Portal, which at the time of publication contained 165 projects, and sought to identify project success factors (Hameed et al. 2018a). It did not seek to identify other types of trends.

- Gray and Kaspar's 'Human rights based cybersecurity capacity building in international cooperation: Trends, lessons learned, recommendations' examined trends in cyber capacity building as they relate to human rights considerations (Gray and Kaspar 2018).

- Radunović and Rüfenacht's 'Cybersecurity Competence Building Trends' and Sabillon et al.'s 'National Cyber Security Strategies: Global Trends in Cyberspace' are examples of papers looking at trends within domestic efforts to address one or more pillars of cyber capacity (Radunović and Rüfenacht 2016; Sabillon, Cavaller, and Cano 2016).

- Pawlak et al.'s 'Introduction: Trends, Patterns and Challenges for International Cooperation in Cyberspace' and Pawlak's 'Confidence-Building Measures in Cyberspace: Current Debates and Trends' considered cyber capacity building, but as part of a wider assessment of trends in international cooperation on cyber issues (Pawlak and Missiroli 2019; Pawlak 2016a).

One feature of all the trends analysis papers we reviewed was that they did not clearly define what they understood the term 'trend' to mean. We have responded to this by providing our own definition, informed by future studies methodologies. Throughout the report, we use the following definitions of key terms and concepts.

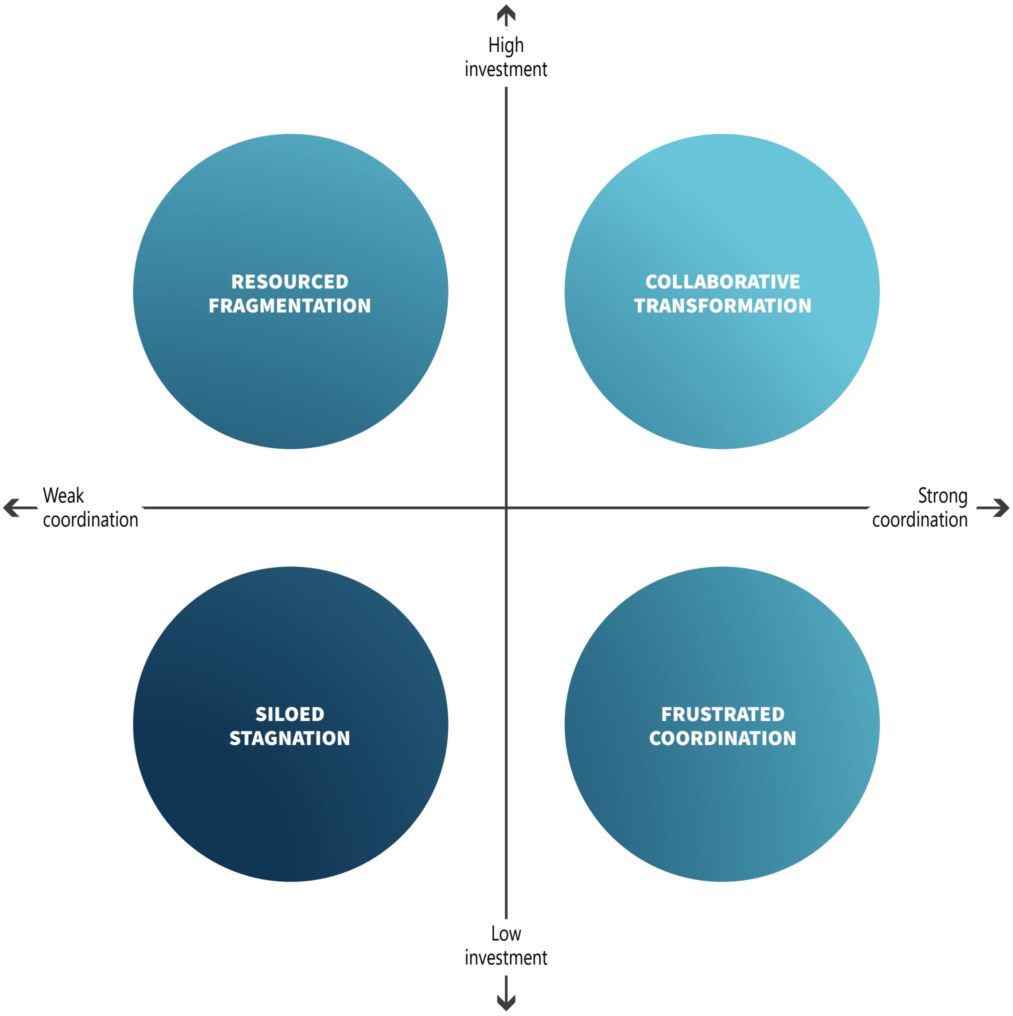
Cyber capacity building	Capacity building in the cyber domain aims to build functioning and accountable institutions to respond effectively to cybercrime and to strengthen a country's cyber resilience (European Commission et al. 2018, 10).
International cyber capacity building project	An international project whose main activities develop capabilities that mitigate risks to the safe, secure and open use of, and relationship with, the digital environment. Purely commercial projects are not included within our conceptual definition.
Trend	A sustained change that impacts the CCB landscape. To be sustained means the change should be ongoing for at least five years.
Megatrend	A long-term (20-plus year) trend that has global effects across multiple sectors. For example: world population growth.
Trendy / Fad	A change that is trendy or a fad will have a short lifespan (less than five years, and often just one or two years).
Emerging Issue	A change with a short history (e.g. one to two years) that could be the start of a trend or could be a fad.
Drivers	The causal forces behind trends and major events (e.g. political agendas; economic conditions; new technologies; etc). A trend can itself be a driver.

In this report, we discuss four trends in cyber capacity building. To generate scenarios, we applied a creative-narrative technique in which just two of the trends are selected as the 'axes of uncertainty' in a two-by-two grid of potential futures. For each trend one selects two different points within the range of possibilities. Combining the two trends in this way generates four different scenarios for which explanatory and exploratory narratives can be developed. Within this narrative, consideration can be given to the role of the other trends that were not selected as the axes.

The two trends we selected for our axes were the growth of the field and the level of coordination. We used investment in capacity building as a proxy for the field's growth as we believe it is its main driver. In selecting these two trends, we considered the factors that are within the control of the EU and how trends relate to each other – a subject we will explore in the scenarios section.

By combining the two trends, we generated the four scenario permutations in the grid at Figure 2. We call these scenarios Siloed Stagnation, Resourced Fragmentation, Frustrated Coordination and Collaborative Transformation. We will elaborate what each looks like after describing the trends in cyber capacity building that inform them.

FIGURE 2. **FUTURE SCENARIOS GRID**



The cyber capacity building scenarios occur against a backdrop of wider global trends, which we refer to as megatrends. The scenario narratives include the effects of some of these megatrends. To identify potential megatrends we looked at three sets proposed by different research teams: EU Foresight; the US National Intelligence Council; and the UK Development, Concepts and Doctrine Centre (DCDC).

We mapped these against each other (Annex 2) and noted that the following megatrends appear in two or more lists:

- Changing nature of work and workforce *
- Managing technological change (including AI) *
- Power shifting between states and away from states *
- Changing security paradigm (proliferation of advanced weapons) *
- Individual empowerment and education *
- Climate change
- Resource scarcity and competition
- Demographics
- Increasing inequality

From this list we chose the five (asterisked) most relevant to cyber capacity building to bring forward into our scenario elaboration. We also brought forward the following megatrends that appeared in just one list:

- Chaotic information space / fake news
- Challenge to the rules-based international system (which is related to the power shifting megatrend)

We considered inequality to be important to cyber capacity building, given the contributions CCB projects could make to its reduction, but we did not think that increasing inequality would affect our scenario narratives.

The scenarios are not intended to be predictions but internally consistent narratives built to help policymakers explore how their choices contribute to, and interact with, potential trend trajectories.

The report makes recommendations throughout, based upon insights from the trends, interviews and reading of the literature. A recap of key recommendations is provided in chapter seven.

PART I: TRENDS

TREND 1: THE FIELD OF CYBERSECURITY CAPACITY BUILDING IS GROWING

Cyber capacity building is a relatively young field of international cooperation: the earliest projects can be traced back 15 to 20 years. The first trend identified is the growth of this new community of practice from its zero baseline to a field of over 675 participant organisations and more than a thousand projects, reaching all but a handful of countries [3]. This trend also explores how the content and thematic structure of the field have evolved since its start.

Growth in projects, investment and actors

The growth of cyber capacity building can be described using several metrics, of which we will consider three: the number of projects active each year, the volume of investment from a sample of funders and the number of actors.

The number of projects

The Cybil Portal data set shows that the number of projects grew rapidly from the late 2000s on (Figure 3). This coincides with the end of the World Summit on the Information Society (WSIS) in 2005 and the follow-on International Telecommunication Union (ITU) Global Cybersecurity Agenda in 2007. These were among the first global initiatives to formally recognise the need for broad cyber capacity building as an enabler of digital development (Portnoy and Goodman 2008, 5–6). After this rapid increase in active projects, the Cybil Portal data shows a peak in 2019 at over 250 active projects per year.

After 2019, we observe a drop in the number of active projects per year. The analysis of the data, in combination with feedback from several interviewees, leads to the conclusion that this is not due to an actual decline in project numbers, but to a lag in programme managers and implementers supplying project information to the Cybil Portal, from which we took our data set. [4]

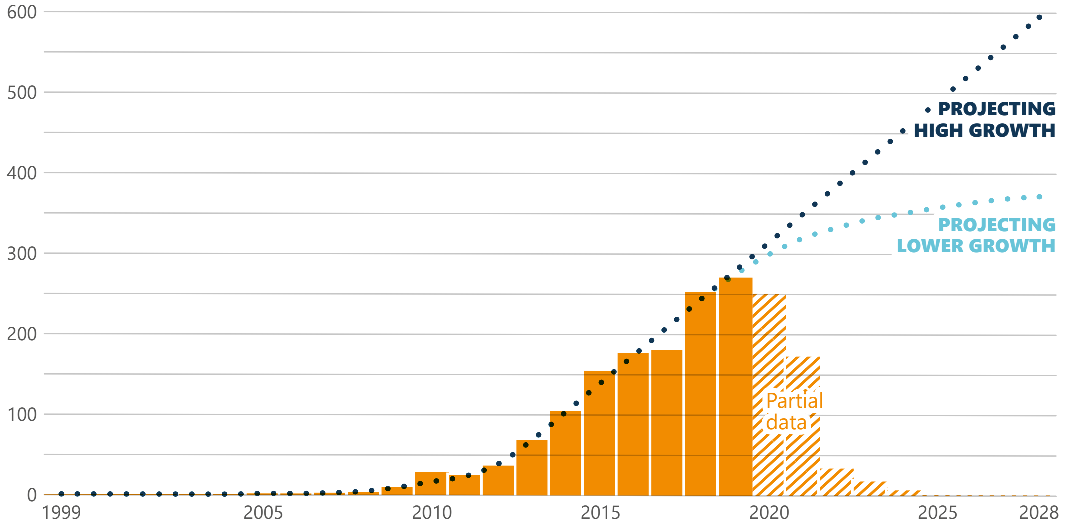
[3] Sources: Cybil Portal data set contained 675 unique actors on 6 June 2021. The number of projects is our lower bound estimate based on the number of projects in the Cybil data set and the proportion we believe are unrecorded. A map of countries participating in projects is at Figure 6.

[4] A significant number of the CCB community wait until projects are well established or complete before they publicise them. In practical terms, projects starting in 2020 might not be publicised until the end of their first or second year (2021 or 2022). The community is even less likely to provide information on projects that are planned and have yet to start.

To account for this, we have shown what the trend from 2019 onwards would look like if the growth in project numbers continued as before (projection 1) or slowed (projection 2).[5]

FIGURE 3. **NUMBER OF ACTIVE PROJECTS**

Per year, 1999-2028



Data: Cybil Portal, 2021

Investment in cyber capacity building

The second metric we use for the growth of cyber capacity building is the level of investment.

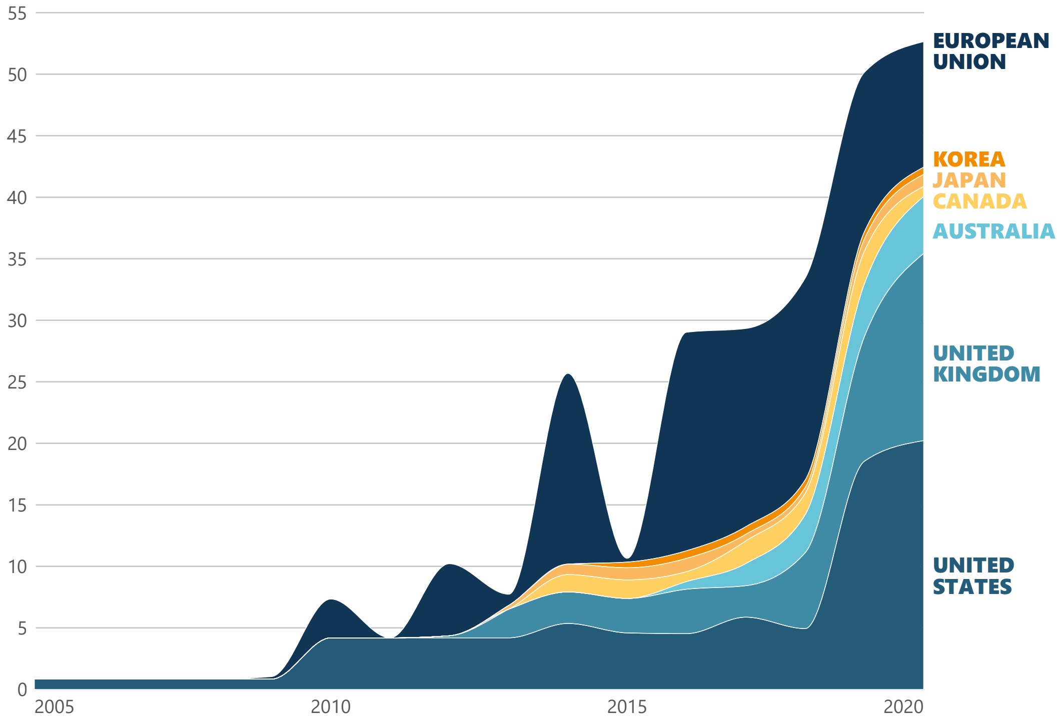
There is limited published data on programme investments and even estimating the total investment has proved difficult. Robert Morgus found that most experts he interviewed gave estimates of total investment between $100m (€85m) and $300m (€250m), but the lowest estimate was $50m (€43m) and highest $1billion (€850m) (Morgus 2018, 29).

Our own interviews and workshop identified growing investment as one of the most significant trends in international cyber capacity building. This growth comes from two sources: several established funders increasing their investment and new funders entering the field.

[5] To approximate a higher growth projection, we extended the 2014 to 2019 growth rate. During this five-year window, the number of active projects each year increased by approximately 35. The higher growth projection shows this continuing indefinitely. In the lower growth projection, the growth rate tapers off to the point where it reaches zero by 2030. This models what could happen if the CCB field soon maxed out the annual investment that its current funders could make, while not bringing in a new wave of donors to fuel further growth.

FIGURE 4. **SPEND PROFILES OF A SAMPLE OF CCB PROGRAMMES**

Data may not reflect a country's full spend on CCB.
See Annex 3 for details of which CCB programmes are included.
2005-2020, € million



Data: Data supplied by CCB programmes (see Annex 3)

As examples of increasing investment, the annual spends of the UK and two US programmes [6] have risen five-fold since 2017 (Figure 4) [7]. However, not all donors have followed this pattern. For example, the investments of Canada, Korea and Japan have remained at similar levels since they started.

These countries have all funded cyber capacity building projects since at least 2015. In more recent years, a growing number and variety of funders have started to support cyber capacity building. These include Singapore, Israel, New Zealand and Germany, as well as international organisations, companies and foundations (see Annex 3 for further information on funders).

Size of the cyber capacity building community

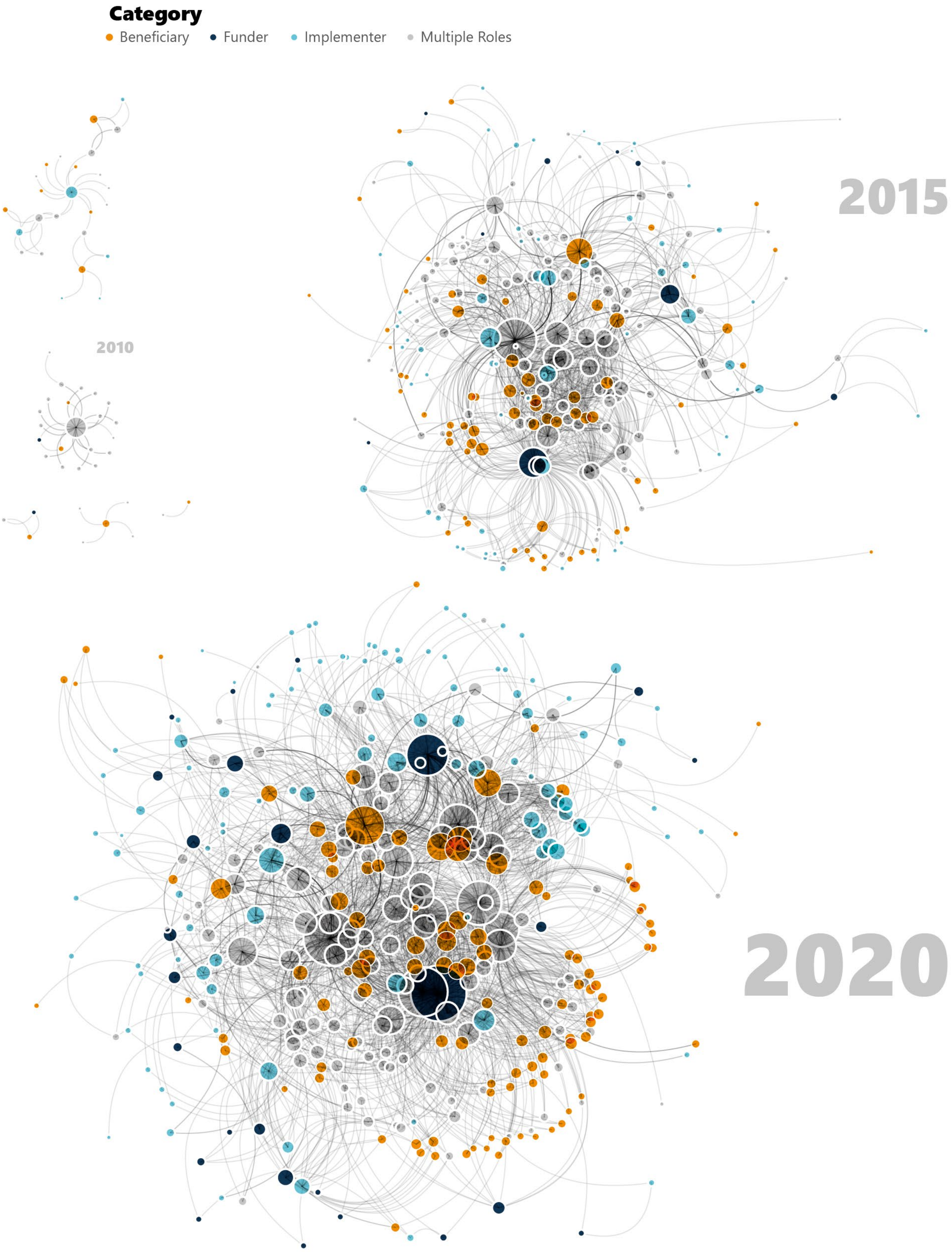
The increase in funders has been accompanied by an increase in the number of implementers, implementing partners and beneficiaries. The number of actors involved in cyber capacity building is growing rapidly. The network diagrams at Figure 5 illustrate this growth in the number of

[6] US Cyber Security Capacity Building Program and the cyber component of their Digital Connectivity and Cybersecurity Partnership.

[7] Spend data tables for the countries in Figure 4 are included in Annex 3. The programmes included within the totals are listed in this Annex. They may not represent all the programmes run by the country.

FIGURE 5. **CCB ACTORS NETWORK**

2010, 2015, and 2020

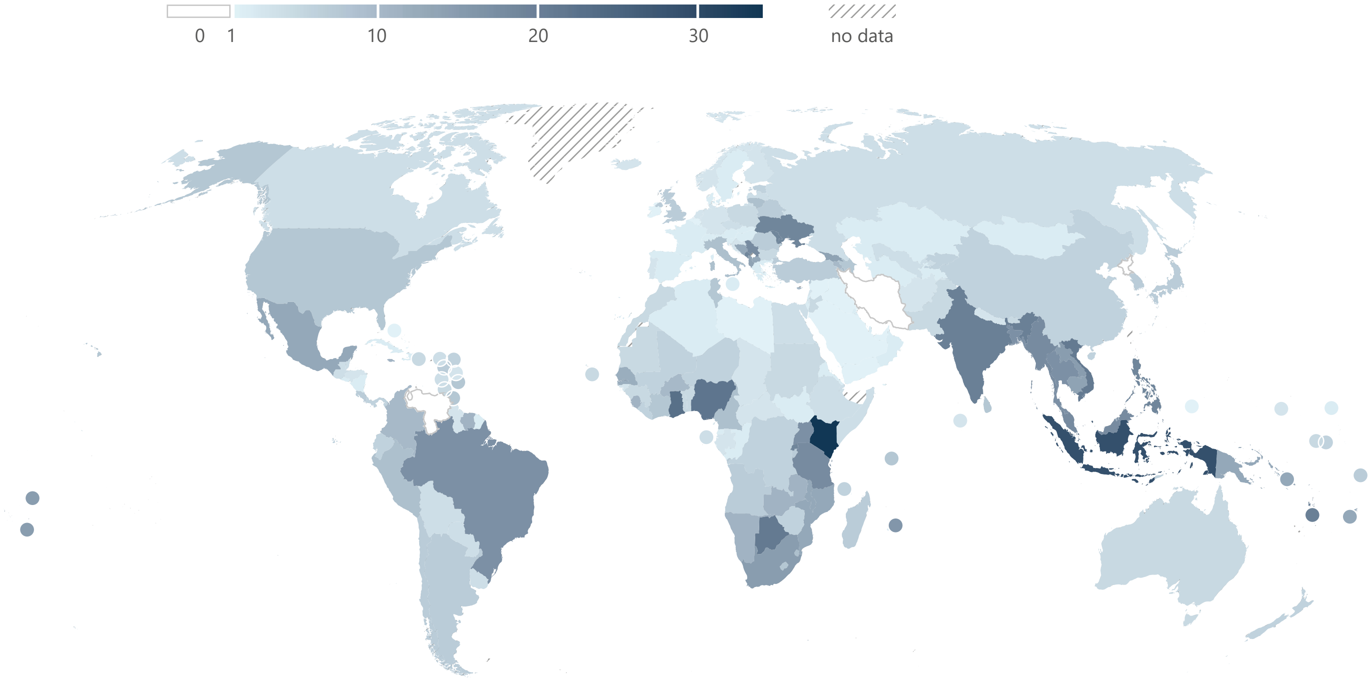


Data: Cybil Portal, 2021

actors and the project relationships between them with snapshots at three points in time: 2010, 2015 and 2020.

FIGURE 6. **NUMBER OF PROJECTS BY BENEFICIARY COUNTRY**

2000 to present



Data: Cybil Portal, 2021

The increase in the number of actors participating in CCB has two important caveats. First, while more countries are involved in cyber capacity building as project beneficiaries, there are still some low- and middle-income countries that have received little assistance. Hameed et al. found in their trends analysis that some countries had benefitted from a disproportionate number of projects, while others had been "marginalised": the darling and orphan problem (Hameed et al. 2018a, 2). Pawlak and Barmpaliou have previously identified this risk as one of the conundrums of cyber capacity building (Pawlak and Barmpaliou 2017, 18–19). Our trends analysis confirmed that this remains an issue. In Africa, according to the Cybil Portal data, five countries – Kenya, Ghana, Nigeria, Botswana and Rwanda – account for 25% of the projects involving African Union (AU) member countries, which is the same as the percentage accounted for by the 28 AU members (of 55 total) receiving the fewest projects. The concentration of projects by country is illustrated in Figure 6 [(8)].

Although the darling/orphan divide remains a challenge, the situation is improving. The community is aware of the issue and taking steps to address it. For example, the Global Forum on Cyber Expertise held its 2019 Annual Meeting in Africa with the aim of introducing countries disconnected

[(8)] Calculations for the African Union and Figure 6 count only where a project lists a country as a direct beneficiary on the Cybil Portal.

from cyber capacity building to its members and initiatives. Somalia attended the event and has since started a project with the World Bank supporting the country's first national cybersecurity strategy and strengthening its governance and technical and operational capacity, including its national incident response capabilities. This will be informed by a national capacity assessment supported by the Global Cyber Security Capacity Centre and the Cybersecurity Capacity Centre for Southern Africa (C3SA) (Cybil Portal 2021a). The desire of some funders to influence the positions of 'middle ground' countries in international negotiations on the future of cyberspace governance and 5G technology may also shift funding towards countries that had previously been marginal beneficiaries.

A second caveat to the positive trend in the number and variety of actors is that the increase in project implementing organisations has not affected all pillars equally. For example, most funders still heavily rely on a single implementer for training in the international law of cyberspace.(9) Some programme managers also note that quality is as important as quantity. Funder contracting processes are finding companies or consortiums to take on projects, but there were indications that some lacked the necessary experience and capabilities to deliver as desired, especially for more technical projects.(10) This is a consequence of the shortage of suppliers with the necessary mix of technical and international capacity building experience.

The breadth and complexity of cyber capacity building

The boundaries and content of cyber capacity building have never been static and continue to evolve. The first cyber capacities to benefit from projects were those needed to tackle cybercrime. As we discuss further in the communities of practice trend, these projects started when international criminal justice projects received requests from counterparts to add cybercrimes and digital evidence to their material and to provide advice on cybercrime legislation(11). Incident response and strategy development followed soon after. Cyber hygiene was the last of the four EU framework pillars to be established. This sequence is evidenced by interviews, the literature and Cybil Portal data.(12)

Between 2012 and 2018, the UK, US, GFCE and EU developed cyber capacity frameworks describing the core capacities a county needs for good cybersecurity. They aimed to be objective but were nonetheless influenced by the types of capacity building support on offer and what each organisation felt was within the scope of cyber capacity building at the time. For instance, online content issues play a minor role within the four frameworks. This is because the frameworks were developed at a time when the EU and like-minded partners were resistant to agreeing with Russia

(9) Interview with a government official on 9 December 2020.

(10) Interview with a private sector expert on 18 December 2020.

(11) See for example the Council of Europe's Global Project on Cybercrime Phase I, 2006-2009 (Council of Europe 2021d).

(12) Interviews with pillar experts on 10, 11 and 15 December 2020.

and China that content control should be treated as a national or international security issue. There was also a strong tradition within the countries developing CCB frameworks that cybersecurity was a technical issue, heavily dominated by protecting the integrity of critical systems and data.

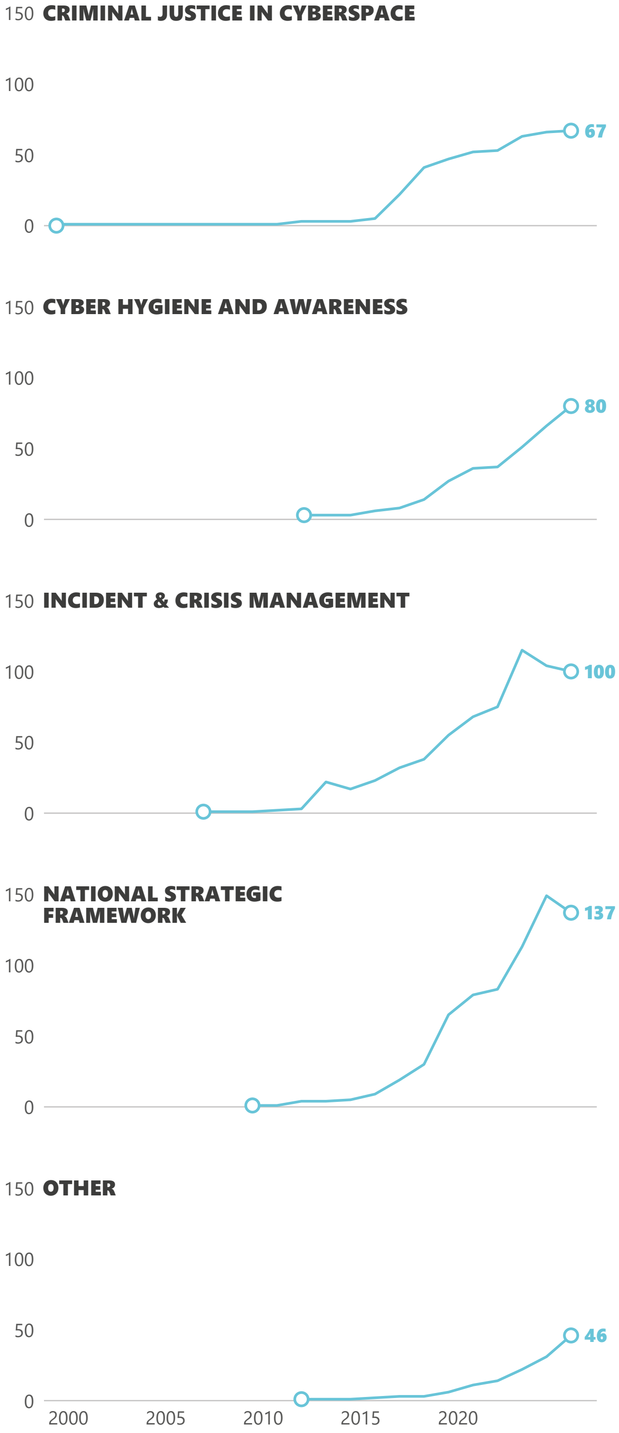
What the EU's and the other frameworks capture is those organisations' views of cyber capacity and cyber capacity building at a moment in time: broadly, the mid-2010s. The issues addressed by projects had evolved up to that point and they have continued to evolve since. Cyber capacity building's evolution since the mid-2010s means:

- some capacities have emerged or grown in prominence;
- granularity is increasing – beneficiaries are more detailed in their requests and projects are more targeted in addressing specific components of a capacity pillar;
- there is increasing investment in the capacities for specific sectors or issues;
- geopolitical tensions have greater influence on the scope and prioritisation of activities; and
- the boundaries between cyber capacity building and other fields of capacity building activity have shifted outwards and blurred.

The **emerging capacities** that were most frequently mentioned during our interviews were those related to international relations in cyberspace.[13] These included the capacity to develop and act upon an understanding of how international law applies in cyberspace, norms of responsible state behaviour and confidence building measures. They also included the

FIGURE 7. **DISTRIBUTION OF PROJECTS BY PILLAR**

1999–2020, number of projects



Data: Cybil Portal, 2021

[13] Interview with government officials, 27 January 2021; and focus group with cyber capacity building experts on 16 November 2020.

capacity to engage in the international cyber diplomacy around these issues, for example in the UN Open-Ended Working Group and UN Group of Government Experts. One interviewee thought these projects may expand further to include the capacity to attribute incidents and implement a deterrence policy. [14]

Within pillars, we found a trend towards **increasing detail and sophistication** in what was being requested by beneficiaries and delivered by projects. For example, projects addressing national strategic frameworks began with a strong focus on the strategy drafting process itself. Sometimes this led to the criticism that a "cookie cutter" approach was being used in some countries to rapidly roll out template strategies, with limited adaptation to local context [15]. Projects addressing this pillar then evolved by: making greater use of national capacity assessments; later adding national cyber risk assessments; and including activities to engage more stakeholders and promote rights-respecting strategies. Each of these has become an area of project specialism in its own right, with multiple implementers and good practice guides (Weisser Harris et al. 2021; Kaspar and Shears 2018; Collett, Kaspar, and Weisser Harris 2021). This increasing level of detail is a trend across the pillars. Some experts are using this detail to create lists (sometimes called menus or catalogues) of sub-capacities within a pillar, mapped to activities that help develop them, that can be selected from for inclusion within a project (Global Forum on Cyber Expertise 2020a).

The focus of capacity building when the EU, US, UK and GFCE frameworks were developed was national level capacities. Our focus groups and interviews highlighted that while most projects are still national, there has been a trend towards **sector-oriented** and **issue-oriented** projects. These are designed to develop the cyber capacities needed to protect a specific sector or address a specific issue. This trend does not necessarily invalidate or change the pillar framework.

Among **sector-oriented projects**, the finance sector was most frequently cited in our interviews and most clearly appeared in the mapping. Other sectors include telecommunications, health, energy and maritime [16]. We found some supporting evidence for this in our own experience and the project mapping.

An example of an emerging **issue-oriented** area of capacity building is financial inclusion. This is the driver behind the Africa Cybersecurity Resource Centre (ACRC): a pan-African information sharing and training project for the financial sector that is currently being established with Africa Development Bank funding from its Africa Digital Finance Initiative [17]. It is also a priority issue for several actors, including the Gates Foundation and the Carnegie Endowment for International Peace and its Cybersecurity and the Financial System initiative. The need for cybersecurity is also on the radar of the CGAP (Consultative Group to Assist the Poor), a global partnership of more than

[14] Interview with a government official on 27 November 2020.

[15] Interview with a project implementer on 11 December 2020.

[16] Interview with a programme manager on 18 December 2020.

[17] This pools funding from, inter alia, Gates Foundation, L'Agence Française de Développement and Luxembourg (Africa Cybersecurity Resource Centre 2021).

30 development organisations working to advance the lives of poor people through financial inclusion (Frickenstein and Baur-Yazbeck 2020).

A second issue towards which a number of projects are oriented is digital access and economy. The US launched its Digital Connectivity and Cybersecurity Partnership programme in 2018 and the UK's Digital Access Programme, with a cybersecurity pillar, began in full in 2020. The case for protecting the expansion of digital access with better cybersecurity was made in the World Bank's World Development Report 2016 on Digital Dividends (World Bank Group 2016) and led the Bank to establish its Digital Development Partnership fund, with a cyber window, while most recently the EU launched, in partnership with several EU Member States, the Digital for Development Hub initiative to support a human-centric digital transformation across regions while mainstreaming data and cybersecurity (European Commission 2021a).

The **scope and orientation** of cyber capacity building actions have also been **influenced by the rising geopolitical tensions** between nations. The sources of these tensions lie in the competing values and visions of cyberspace, in particular regarding the role of governments and the involvement of other stakeholders in governance of cyberspace.[18] This competition affected international cyber capacity building in numerous ways, including the increase in projects that help countries engage in international diplomacy negotiations on cyber issues and other projects with a geopolitical dimension, such as the development of 5G networks and supply chain security. While states acknowledge that cyber capacity building activities should be "evidence-based, politically neutral, transparent, accountable, and without conditions" (United Nations Open-Ended Working Group 2021, 8), there is not yet consensus on the details of what implementing that principle would mean in practice.

Finally, the **boundaries around cyber capacity building** have expanded and blurred. This is a subjective assessment, but one made by several interviewees and our focus groups. When the Global Forum on Cyber Expertise was founded, discussions around what was within the scope of cyber capacity building tended to agree that addressing online harms was outside it. Opinions on this have since shifted and projects are now more willing to discuss, and give advice on, tackling online harms. Similarly, five years ago there was a clear distinction between cybersecurity and emerging tech, but several government departments, international strategies and cyber programmers are now breaking down the barriers between the two.[19] For example, last year Australia renamed the now Cyber & Critical Tech Programme and the UK began a transition to a new Cyber & Tech Programme, while Singapore's capacity building team is considering how they can pivot towards digital tech requests. A third issue that is increasingly mentioned as being within the scope of cyber capacity building is data regulation and privacy. The World Bank, for example, took the decision to structure lending projects such that sub-components dealing with cybersecurity also include data

[18] Interviews with international organisation, private sector and government representatives on 15 December 2020, 20 January 2021, 1 February 2021 and 11 March 2021, respectively.

[19] Focus group of cyber capacity building experts, 16 November 2020.

protection activities, while the Council of Europe has been asked by partner countries to include data protection elements in its cybercrime projects in relation to the requirements for the transfer of personal data in criminal investigations or proceedings.

Why does this trend matter?

The growth of cyber capacity is clearly a positive trend: it speaks to the formation of a new field of international cooperation that is attracting investment and defining its area of expertise and boundaries. However, within the details of the trend we can find signs of challenges and important questions for the field ahead. CCB programme teams are being pulled towards the fields of emerging and digital tech, and towards serving sector- and issue-orientated needs. We should welcome the fact that these teams are being responsive to the interests of beneficiaries and their own leadership, whose focus is often upon higher level digital-enabled outcomes, rather than just the cybersecurity that enables them. Those digital development outcomes are also more likely to attract the funding that the field will need to continue to grow as fast as it has. However, there are risks to manage.

The field of cyber capacity building emerged when the international community agreed that national cybersecurity capacities were important in their own right and countries should assist each other in strengthening them. This did not overlook that security always serves some higher goal, but rather recognised that cybersecurity capacities should not be an afterthought and needed international support. A successful future for the cyber capacity building field is one in which it can grow in a way that works with, and for, adjacent digital fields without becoming subsumed by them and losing sight of its original purpose. Cyber capacity building should be more than a risk mitigating measure in international digital programmes or a tool to achieve an influence outcome. It will also be more effective when it can connect a core community of practitioners, with an improving body of knowledge, shared principles, coordinating mechanisms and uniting goals.

Recommendations

Growth in projects, investment and actors

For the EU:

- Develop an EU External Cyber Capacity Building Agenda – as proposed by the 2020 EU Cybersecurity Strategy – that will help determine the EU's priorities and funding strategy, especially in the light of new Multiannual Financial Framework and the new unified financing instrument of EU external action, the Neighbourhood, Development and International Cooperation Instrument (NDICI). This could entail reflection on what the level of EU investment should be, using Overseas Development Assistance (ODA) and non-ODA funding, to best address the needs of partner countries in line with EU priorities, and identify where the EU best adds value within the growing range of actors.

- Make use of the new EU Cyber Capacity Building Board to steer and help take the above decisions by bringing together different policy communities within the EU system, including setting up a proper reporting system for the EU funding that would allow better assessment of the EU's overall contribution to global cyber capacity building efforts.

For the whole CCB community[20]:

- Current and potential donors should consider whether their own CCB programmes and teams are keeping up with a growing field and its future potential and take steps to address any potential gaps.
- Implementers can prepare for the growth of capacity building by investing in their own capacity to deliver programmes and proactively advise funders on scalable solutions.

For the GFCE:

- Improve the process for bringing new actors into the GFCE and explaining how they can best benefit from it and participate. Potential actions include: returning to having a Day Zero before major conferences to bring new attendees up to speed; producing more introductory guides and videos for new members; providing more intensive support to help new members join the right working groups and make new contacts; and making it clearer to key stakeholder groups, such as academia and civil society, how they can observe or participate in GFCE events and processes.

The breadth and complexity of cyber capacity building

For the EU:

- Revisit the four-pillar model elaborated in the EU's Operational Guidance for the EU's international cooperation on cyber capacity building, and consider what changes or updates are needed, in particular with regards to better integrating cyber diplomacy issues and the protection of critical infrastructure.
- The EU Cyber Capacity Building Board could offer guidance on how adjacent themes that are EU political priorities (e.g. 5G toolkit, Network and Information Security Directive) should be taken into account in the identification and formulation of cyber capacity building programmes. This dimension could be also included in an updated version of the EU's Operational Guidance.
- Prioritise the roll-out of training courses for programme managers at EU headquarters and EU Delegations by EU CyberNet, building on the pilot course developed by the EU Institute for Security Studies in July 2021, to improve understanding and use of the EU's cyber capacities framework in external cooperation programming.

For the whole CCB Community:

- Set a SMART[21] goal that all countries should have a core set of basic, foundational cyber capacities in place by a certain date.
- As the complexity of capacity building increases, there is a greater need to include cyber specialists and expertise within the programme design. This might be achieved through various means, including recruiting specialist staff into programme teams, increasing the involvement of cyber experts from other departments/ministries and making more use of external cyber/design experts when programmes are being created.

[20] Advice for the whole CCB community is intended for all actors participating in the field. Advice provided specifically for the GFCE is targeted at the processes of this forum, because we consider its role in coordination and knowledge sharing important, although it does not contain all actors in the field.

[21] Specific, measurable, achievable and time bound.

For the GFCE:

- Consider the role of the GFCE and its Research Agenda in responding to the SMART goal recommendation above, including through funding a piece of research to estimate the cost of such a goal, based on prior experience building those capacities.
- Share experience and perspectives on how more capacities can be designed in a 'modular' way and how best to manage the sequencing challenge, when more advanced capacities need to be built before more foundational ones are in place.

TREND 2. THE GAP BETWEEN ASPIRATIONS FOR COORDINATION AND ITS IMPLEMENTATION IS GROWING

The CCB community has shown an increasing desire for coordination through its discourse and the creation of coordination mechanisms. However, implementation of the aspiration for greater coordination has been very patchy. There are examples of good coordination, but also concern among programme managers, implementers, beneficiaries and researchers that these are the exception rather than the rule. Overall, the practice of coordination is improving more slowly than the community aspires it to.

Aspirations for coordination

The aspirations and expectations of coordination within cyber capacity building have grown steadily since the field began. In its early years, the World Summit on the Information Society (WSIS) and the process to develop ITU's Global Cybersecurity Agenda included discussions of the importance of coordination. The ITU's Global Cybersecurity Agenda resulted from a High-Level Experts Group whose 2008 report, containing a compilation of proposals, and dissenting opinions, that touch on coordination. The report includes a proposal for "a network for coordinating [cyber capacity building] activities, initiatives and projects, through agreements or memoranda of understanding" (International Telecommunication Union 2008, 138). It also proposes that the ITU should coordinate its own activities with others and play a facilitating role to international coordination, where there are the political will, resources and consent of other organisations. In response, the ITU established a cybersecurity team to manage its own capacity building and contribute to international coordination.

In 2015, the idea of the proposed coordinating network was implemented by 42 countries, companies and international organisations when they established the Global Forum on Cyber Expertise. This has a mandate to facilitate project coordination within its own membership and to contribute to wider global coordination (see Box 1). The GFCE has since grown to 90 members and 46 partners. Coordination is both a central goal of the forum and a principle its members explicitly reaffirmed in the 2017 Delhi Communiqué on a GFCE Global Agenda for Cyber Capacity Building.

The Global Forum on Cyber Expertise

The Global Forum on Cyber Expertise is the only international, multistakeholder forum with the primary purpose of strengthening global cyber capacity by supporting international coordination and cooperation. Since it was formed in 2015 its membership has grown from 42 to 90 countries, companies and international organisations, plus an additional 46 partner organisations. Among its members are 55 governments as well as UN entities such as ITU, United Nations Office on Drugs and Crime (UNODC) and UNIDIR, and several regional organisations. It is a neutral, apolitical, multistakeholder and community-driven platform that is free for members to join.

The GFCE primarily supports coordination at the thematic layer through working groups focused on each pillar of capacity (Figure 1). These working groups share information about projects and good practice, and sometimes produce their own papers, drawing on their members' experience to help inform the design of future projects. Project information and useful resources are passed to the Cybil Portal.

The GFCE has also supported coordination at the regional, country, programme and project level. Examples include:

- GFCE events provide a networking and coordination platform for programme managers.
- The GFCE has held coordination sessions for projects in Africa at several Annual Meetings and has recruited a secretariat staff member with a focus on supporting coordination in Africa.
- The GFCE supports coordination in Latin America and the Caribbean through OAS acting as a regional hub partner and is working to establish a regional hub in the Pacific.
- When a country asks to be matched with project assistance through the GFCE clearing house, as, for example, Sierra Leone did in 2019, the process begins by mapping past, present and planned projects and ensuring they are aware of each other.
- Individual projects have conducted coordination by informing working groups of their plans. One UK project on incident response training in the Commonwealth used this as a way to deconflict from other projects and received offers of pro bono assistance from other organisations.

Sources: www.thegfce.org accessed 21 March 2021; (Painter 2020)

In 2021, two key UN-led processes on cyber issues reiterated the need for improved coordination on capacity building. The UN Open-Ended Working Group's report called for "further promotion of coordination and resourcing of capacity-building efforts, including between relevant organizations and the United Nations" (United Nations Open-Ended Working Group 2021, 9), followed by the report of the Group of Governmental Experts on Advancing responsible state behaviour in cyberspace in the context of international security, which suggested "approaching cooperation in ICT security and capacity-building in a manner that is multidisciplinary, multi-stakeholder, modular and measurable" (United Nations Group of Governmental Experts 2021, 22). The UN and the next round of the Open-Ended Working Group have yet to agree on what further action will be taken to support coordination, including the details of a proposed Programme of Action to support coordination, but the 2021 report has secured in principle agreement amongst all UN Member States on its necessity.

Accumulating examples of good coordination

Each year, the field of cyber capacity building accumulates more examples of good coordination. In line with this, the common, but not universal, opinion of our interviewees was that the direction of travel regarding coordination is a positive one, but progress has been slow.

Nascent cyber capacity building coordination is occurring through several channels, including:

- the Global Forum on Cyber Expertise and other international fora, such as the Paris Call working groups and Korea's Cybersecurity Alliance for Mutual Progress (CAMP);
- ITU as the facilitator of WSIS Action Line C5 ("Building Confidence and Security in the use of ICTs") and with its mandate to foster international cooperation and solidarity in the delivery of technical assistance to telecommunication/ICT equipment and networks in developing countries;
- regional organisations, including the OAS, EU, Economic Community of West African States (ECOWAS), ASEAN and AU;
- the individual efforts of organisations, projects and programmes to directly coordinate their own activities with others;
- the formation of consortiums and close partnerships between organisations, such as a region-specific coordination group between Australia-NZ-US-UK in the Pacific and a research 'constellation' connecting Oxford University, the Oceania Cyber Security Centre and the Cybersecurity Capacity Centre for Southern Africa; and
- pillar-specific organisations or initiatives that take on a coordination role, such as the Pacific Cyber Security Operational Network (PaCSON) (for incident response), CyberSafety Pasifika (for law enforcement) and the Pacific Islands Law Officers' Network (PILON) (for law officers).

The practical forms that this coordination takes are as diverse as the mechanisms through which it occurs. The following examples illustrate types of coordination good practice we found that could be replicated:

a) **Deconfliction (and collaboration) by content**: In 2019, the EU's Cyber4Dev programme alerted the OAS to their intention to offer remote technical training to Caribbean countries. The OAS identified the opportunity to deconflict their training and collaborate. They directed relevant requests for assistance to Cyber4Dev and focused their own assistance in other areas.

b) **Deconfliction by time**: In 2020, PACSON and PILON were planning to start a series of unrelated incident response and cybercrime trainings whose timings would have conflicted. A member of both groups identified that some participants would be invited to both and helped the two organisations agree a timetable that would work for both as well as the participants.

c) **Coordination by country**: In 2019, Sierra Leone requested assistance from the GFCE with finding capacity building partners and coordinating projects. The GFCE formed an informal 'cyber friends of Sierra Leone' group that mapped their existing and planned activity before meeting together with the Minister of Information and Communication to hear his priorities. Activities were started or redirected to support these in a coordinated way. One outcome was that Sierra Leone adopted its national cyber strategy in March 2021 following coordinated assistance from several of the informal group's members.

d) **Coordination by region**: Regional cyber capacity building coordination meetings have been held both under the umbrella of the GFCE and outside it (Lagakali and Aiken 2020; Barbero and Berglund 2021). Several good practices have emerged from these: open the events to all and advertise them widely; prepare a mapping of regional projects for review at the meeting; update the Cybil Portal project information afterwards; publish a report of the event; and aim for concrete outcomes so that the coordination is followed by action.

e) **Public-private partnerships**: When the UK government designed its programme supporting cybersecurity in the Commonwealth it published an invitation to companies wanting to contribute. As a result, Microsoft, Citi Group and Templar Executives worked with the UK government to deliver pro bono coordinated and collaborative activities, including mentoring, exercising and a report on the public awareness campaigns and capacity of Commonwealth members (UK Foreign Commonwealth and Development Office 2020).

f) **Coordination projects**: Another example of coordination good practice within the UK's Commonwealth cyber programme was designing a project solely focused upon coordination and knowledge sharing across the programme. This was accomplished through networking events, issue-themed workshops and reports. Similarly, in 2019 the EU launched the EU CyberNet project, inter alia, to enable better coordination of activities and know-how amongst EU-funded CCB projects.

g) **Pooled funding**: Pooled funds have the benefit of baking coordination in to the way funds are used. The World Bank experimented with pooled funding through a cybersecurity window in its Digital Development Partnership fund and in July 2021 launched an associated Cybersecurity Multi-Donor Trust Fund [22] (World Bank 2021).

[22] Initial contributions to the fund have come from Estonia, Germany, Japan and the Netherlands.

h) **Complementary funding to successful projects**: After considering how to increase their support for capacities in the criminal justice pillar, the US decided to support the existing work of the Council of Europe and boost its financing of the Octopus project to complement activities undertaken under the Global Action on Cybercrime Extended (GLACY+). While it has been relatively common since the start of the capacity building field to have several co-funders of a project from the start, it has been less common for funders to opt for burden-sharing in support of existing programmes. When financing arrangements make it possible, new donors could also join existing programmes, creating potential to scale successful projects more quickly and reducing the risk of duplication. Other global criminal justice programmes that have attracted funding to their existing work include UNODC, INTERPOL, International Association of Prosecutors and the World Bank [23].

The gap between coordination in principle and in practice

Although aspirations are increasing, and the field is accumulating examples of good practice, the overall state of coordination falls short of the community's formal commitment to it. Those interviewees who mentioned coordination as a trend almost universally described it as better than it once was, but well below the level they felt it should be at.

Among the strongest critics of the status quo were programme managers, who described examples of funders "piling in" and "dumping half-baked projects" with little thought to what other activities had occurred or were planned. They gave examples of different funders providing the same type of activity to the same group of participants, sometimes on the same day. The pandemic may have exacerbated the problem, because of the increased pressure to execute programmes in difficult circumstances. Furthermore, being able to hold events remotely made it easier to overlook the same participants being invited to two, sometimes three, trainings that would be held at the same time.

In their mapping of capacity building in southern Africa, Calandro and Berglund identified lack of coordination between projects as one of the main reasons for poor implementation of global and regional cyber policies, protocols and declarations (Calandro and Berglund 2019, 1). Papers considering the global state of cyber capacity building have also identified poor coordination as among the key weaknesses of cyber capacity building (Pawlak and Barmpaliou 2017, 11; Hohmann, Pirang, and Benner 2017).

The GFCE's first regional meeting in the Pacific, in February 2020 in Melbourne, identified coordination as one of the three most important issues to participants. Pacific Island representatives stressed the challenges of being over-served by assistance when it exceeded their capacity to absorb it and of being unable to attend competing events when calendars clashed. The meeting

[23] The World Bank attracted support for its Combatting Cybercrime project (https://www.combattingcybercrime.org/).

explored the political and cultural reasons countries find it hard to decline offers of assistance and the ways funders could improve their coordination. One concrete outcome of the event was an ongoing project, delivered by a GFCE-contracted expert, to explore options for establishing a GFCE hub in the region.

Implementers can feel stuck in the middle of these coordination challenges between funders and beneficiaries. Some feel that they must take corrective measures themselves to make up for insufficient coordination at the funder level. This might mean turning down funding for a programme that has not been well prepared or putting more effort into coordination than they would need to if there had been better coordination by the funder. In practice coordination works best when all three parties – funders, implementers and beneficiaries – make it a priority and devote time to it.

Among experts with mainstream development expertise, it was noted that the in-country funder meetings that occur in other fields very rarely occur in cyber capacity building. Nor is there often coordinating direction coming from the beneficiary government, in the form of a prioritised country cyber capacity development plan that includes the role of international partners.

Why the gap? Coordination challenges

Some of the challenges impeding cyber capacity building coordination result from inherent features of the field, while others result from choices actors make.

The nature of cyber capacity building means that it will always span a diverse range of capacities and parent community interests and cultures, and that some of those involved may be restricted in the information they can share about their capacity building. This reality creates unavoidable coordination challenges. However, they are offset by the fact that the core cyber capacity building community is young, which creates an opportunity to embed collaborative principles from the start and also means the number of actors involved is relatively small.

In contrast to these unavoidable challenges, there are several that are within the control of the community. Interviews suggested that coordination could be improved if started during a programme's design rather than being left until the implementation phase, i.e. when an implementer has been selected or after activities have been designed. Coordination at this point misses the opportunity to collect information that could be useful for programme design and makes effective coordination less likely.

One reason coordination is occurring late in the project cycle is that funder programme teams are overstretched. Project teams feel they lack the time to better coordinate and gather information during the programme design phase, which pushes these tasks towards the implementation phase and onto the implementer.[24] They also lack the time to conduct frequent visits to meet beneficiaries and see projects in action. The coronavirus pandemic has exacerbated this problem, but it originally stemmed from cyber capacity programme managers having more (smaller) projects to manage than their mainstream development counterparts. This creates an additional barrier to programme teams being able to conduct the effective coordination themselves or monitor the quality of their implementers' coordination.

The competition for funding between implementers may also constitute a significant obstacle to coordination.[25] The continual need for funding is a driver of competitive, as opposed to collaborative, relationships with other implementers. This in turn creates disincentives to sharing information and adjusting projects to deconflict from others.

Some see a discussion about funding transparency and how country beneficiaries are selected as a taboo.[26] They found it difficult to see how much funding went into cyber capacity building and from whom. This is in contrast to the development community, where overseas development assistance data is consistently published and can be traced down to the project and beneficiary level.

Contributing to the lack of transparency, the competition for funding encourages implementers to overstate what a project will or has achieved. A similar problem affects funders when their projects have an influence function. It is in their interests to portray their projects in the best possible light and hide problems. The most important negative consequence of this behaviour is that it hinders lesson learning within the field, but it also impedes coordination. For example, we heard several examples of actors saying they diverted their resources to another country or pillar when they were told that a project would address a capacity building gap they were planning to meet, only to later discover that the reality of what was delivered was much smaller than had been stated or implied.[27] Had the other actor been more transparent in their plans, and collaborative, then it may have been possible for both to provide support for a better outcome.

Coordination channels and forums established to manage coordination problems, including the GFCE, have not yet managed to overcome the above challenges. In the case of GFCE, interviewees suggested several reasons why it has yet to fulfil its potential:

- limited funding for its secretariat and events;
- it has become difficult for new members to work out which processes to take part in and how they can benefit;
- working groups rely on their members to achieve their collective goals, but their members have very little spare time to contribute;

[24] Interviews with a government official on 1 December 2020 and EU officials on 14 December 2020 and 6 January 2021.

[25] Interviews with international organisation officials/project implementers on 4 December 2020 and 23 March 2021.

[26] Interview with a government official on 1 February 2021.

[27] Interview with a project implementer on 8 December 2020.

- the coordination discussions in the GFCE have primarily been at the level of strategy and theory, and not reached down to the coordination that is needed at the country level – it does not have the bandwidth to assist such coordination in all countries, but could in a few; and
- it is perceived as a Western initiative.

There was strong support for the GFCE's networking, regional meetings, knowledge sharing and project mapping. The clearing house function was identified as the most difficult to deliver, with one interviewee explaining they find it difficult to match beneficiary needs with the right department within their own organisation.

Some interviewees stressed that the GFCE is one of several channels and forums through which coordination can occur. There was overwhelming support for coordination mechanisms to be multi-stakeholder and therefore doubt about whether the UN should or could take a greater direct coordination role than it currently has when it is so state-centric. What the UN's role will be in supporting the coordination of cyber capacity building is something that the international community will need to decide following the recommendation in the UN Open-Ended Working Group's 2021 report (United Nations Open-Ended Working Group 2021). Where other channels or forums were preferred to the GFCE it tended to be because they were able to provide more practical coordination closer to the in-country, operational level.

Why does this trend matter?

Coordination is not an end in itself. However, in a complex field where the need greatly exceeds the supply of resources, better coordination is essential for achieving the specific policy objectives (Pawlak 2014b, 17). Furthermore, when the lack of coordination results in the duplication of effort or conflicting projects, it impedes effectiveness and can lead to beneficiaries losing confidence in their capacity building partners.

The 2018 Council Conclusions on EU External Cyber Capacity Building Guidelines recognise that the increasing number of stakeholders globally involved in this field 'creates opportunities for synergies and burden-sharing but also poses challenges in terms of coordination and coherence' and encourages the EU and its Member States 'to continuously engage with key international and regional partners and organisations as well as with civil society, academia and the private sector in this field with the aim of avoiding duplication of effort given the limited resources' (Council of the European Union 2018). Similar focus on coordination can be found in the EU's 2020 Cybersecurity Strategy (European Union 2020).

Recommendations

For the EU:

- The EU should capitalise on the EU Cyber Capacity Building Board and define criteria that allow the EU to identify investing priorities in a targeted and iterative manner, both in terms of regions and pillars of capacity, instead of trying to build capacity in all pillars and in all regions at the same time. The creation of an informal EU Cyber Diplomacy Network with EU Delegations and Member States Embassies, as proposed in the 2020 EU Cybersecurity Strategy, could offer vital input and needs analysis in the Board's iterative priority assessment exercise.

- The EU should pursue new alliances and international partnerships or strengthen existing ones with key regional and international organisations around its thematic cyber capacity building priorities. This could be achieved by strengthening its dialogue on CCB with regional organisations that will translate in the development of joint CCB programmes.

- The EU could provide more support for the coordination of programmes with EU Member States through utilizing EU CyberNet for a systematic mapping of projects.

- The EU should assign a point of contact for international coordination of CCB projects and activities that could then link up with all relevant services to enable the EU's better coordination capability.

- To enhance the EU's situational awareness on the status of CCB globally and support global multistakeholder coordination, the EU could provide direct support to the GFCE Foundation and fund coordination meetings at the regional level in partnership with the GFCE.

For the whole CCB community:

- Start by improving coordination within one's own organisation, for example by reviewing the process by which all departments and agencies share information and collaborate on CCB.

- At the country level, hold regular coordination meetings between programmes operating in key countries, and with the host government – locally led coordination is the most effective. Staff in embassies and country offices can better support coordination and projects if they are provided with some cyber capacity building training.

- At the regional level, hold at least annual coordination meetings that are informed by a project mapping and contribute to updated information on the Cybil Portal.

- If the UN starts new cyber capacity building coordinating processes, following the Open-Ended Working Group's 2021 report, it should ensure that these complement and work with other coordination efforts.

- Funders should take steps to support coordination with each other, for example by designing joint programmes when priorities are shared, using pooled funding mechanisms and being open to topping up successful existing programmes that may have been established by other funders.

- To support wider and more effective coordination, funders should hold meetings for their own implementers to network with each other, run longer projects that allow time for coordination from the design phase, include a requirement for coordination in contracts, fund coordinating events and forums and ideally have a project within larger programmes focused on coordination and sharing lessons.

- Funders should also explore ways to have longer-term relationships with implementers so their funding is more secure and the pressure of competition for tenders feels less ever-present and is therefore less of a brake on coordination.

- Break down national capacity requirements into modules that can be tackled by different projects – the division of labour in supporting national capacity assessments and national strategies is an example of where this has worked well.

For the GFCE:

- Support the country-level and regional-level coordination activities proposed above for the whole CCB community, for example by helping to arrange the first country-level coordination groups and strengthening the GFCE regional hubs and focal points.

- Promote coordination and knowledge sharing by showcasing success stories and good practices.

- Spread awareness of the GFCE's clearing house function and produce catalogues of assistance for each pillar of capacity so that countries have better information on what types of support they can request.

TREND 3. MORE COMMUNITIES OF PRACTICE ARE USING CCB TO PURSUE THEIR AIMS

Cybersecurity grew out of the technical discipline of computer science (Singer and Friedman 2014, 4–8) and subsequently cyber policy approaches grew organically within different *parent communities of practice*, such as the criminal justice community and incident response community. Although these communities all work on essentially the same interconnected set of cyber challenges, they approach them from different angles, with distinct mandates, aims and cultures (Hohmann, Pirang, and Benner 2017, 11). This has created a fragmented international cyber policy architecture that lacks strong coherence, yet is flexible and adaptable in its loose and ad hoc connections (Nye 2014, 9). It has also contributed 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. The cyber policy architecture of loosely connected communities of practice has cascaded down to the cyber capacity building ecosystem, which is best understood as a set of parent communities of practice with their own aims and cultures.

Cyber capacity building emerged as an international policy concept in the late 2000s and early 2010s when a handful of countries and international organisations began to include it within policy documents and national strategies [28]. As awareness of the concept grew, a *core cyber capacity building community* started to develop organically around it, bringing together those parent communities that had been pioneers in undertaking CCB activities. As Figure 7 shows, work in some pillars of cyber capacity building started earlier than others, reflecting some parent communities being first movers and others being late adopters [29]. The Cybil Portal data and literature suggest that the cybercrime community was the pioneer, with projects launched as early as the 1990s,

[28] Indicative examples include: ITU Global Cybersecurity Agenda, 2007; US International Strategy for Cyberspace, 2011; UK Cyber Security Strategy, 2011; Cybersecurity Strategy of the European Union, 2013.

[29] See the evolution of the different CCB waves in the section "Growth in projects, investments and actors".

followed by the incident management community. At that time, CCB was considered an extension of existing peer-to-peer exchanges or training programmes rather than a new field of international cooperation.

The trend within this history is that an increasing number of communities of practice are using CCB activities to pursue their own distinct aims. A core CCB community has emerged, helped by the launch of the GFCE, but not all parent communities are equally well connected with it. Its connections with the cybercrime, incident management and foreign policy communities are stronger than those with the development, defence, private sector and online rights communities. This section considers how each of these communities' involvement in CCB has evolved – the trends within a trend – and reasons why they have become more or less integrated with the core CCB community and coordinated effort.

Criminal Justice Community

Members of the criminal justice community have been responding to the challenge of cybercrime since the introduction of computers in the late 1970s. In the 1990s, generalist police training projects started to add cybercrime and digital evidence to their modules, at the request of trainees who were facing cybercrime in their daily work. In addition to practical training, from the late 1980s cybercrime started being discussed within international fora such as the Council of Europe (Council of Europe, Committee of Ministers 1989; 1995; Council of Europe 2001), the OECD (OECD 1992), the G8 (G8, Birmingham Summit 1998) and the UN (United Nations 1991, 140–43). Having established this foundational policy framework, in the 2000s the international criminal justice community turned its attention to helping countries adopt legislation and strengthen their national cybercrime capacities through more ambitious projects than the earlier ad hoc police training courses.

Criminal justice community support for cybercrime capacity building has grown significantly with the launch of larger programmes, such as UNODC's Global Programme on Cybercrime, INTERPOL's Global Cybercrime Programme and the US' Global Law Enforcement Network of International Computer Hacking and Intellectual Property (ICHIP), as well as the establishment of expertise hubs, such as the Council of Europe's Cybercrime Programme Office (C-PROC) in Bucharest and INTERPOL's Global Complex for Innovation (IGCI) in Singapore.

There has been growth in regionally focused programmes. Since the Council of Europe started running regional projects with EU funding in the Western Balkans and Eastern Europe in the early 2010s (Council of Europe 2021b; 2021a), more regional organisations have started to play a significant CCB role. They're working both as implementers of training activities in their member countries – as is the case with the OAS and the Organization for Security and Co-operation in Europe (OSCE) – as well as key project partners serving as convening and amplifying fora for CCB activities – for example the cases of ECOWAS, the Caribbean Community (CARICOM) and ASEAN.

Following the overall trend in cyber capacity, cybercrime projects have grown in scope as well as number. Their scope has expanded from single-issue projects addressing mainly cybercrime legislation or law enforcement training to comprehensive programmes building multiple components of counter-cybercrime capacity. More recently, we have seen the emergence of capacity building that focuses on cryptocurrencies and ransomware, especially in light of the impact of the coronavirus pandemic on the global cybercrime threat landscape. This has necessitated pulling in more national experts (both retired and in active duty).

The long-term engagement of criminal justice actors in cyber capacity building has fostered the creation of a network of experts that includes law enforcement personnel, prosecutors, members of the judiciary and civil servants in ministries of justice and the interior. The culture and past experience of this community has lent itself to cyber capacity building projects that use a law enforcement mentorship model based on a long-term partnership. Similarly, thanks to their early involvement, the community has had more opportunities to learn about the importance of strong local ownership and projects designed to bring together all relevant national stakeholders to support a longer-term process of change linked to national structures (Seger 2013). The fact that tackling cybercrime has been a priority for many partner countries has aided integration into the core CCB community. Nevertheless, there are still areas where better connections with the core CCB community could be pursued, for example in better reflecting strategic planning of cybercrime aspects in the development of national cybersecurity strategies.

CSIRT and Technical Community

The broad technical community of IT specialists is at the heart of the Internet's creation and its evolution into a global decentralised infrastructure. While this community includes a very wide range of technical actors with multiple functions in the Internet governance ecosystem [30], with regards to CCB this analysis focuses on the key stakeholder community of IT experts and network managers that deal with the security of essential shared Internet infrastructures, provide essential security services and respond to security problems and cyberattacks.

Establishing and strengthening national Computer Security Incident Response Teams (CSIRTs) has been a longstanding priority for the CCB field, because of their importance underpinning national cybersecurity (International Telecommunication Union 2021; Lipson 2002, 5) and their role working with international partners to respond to and mitigate threats (Skierka et al. 2015). Following some success in increasing the number of national CSIRTs [31], several interviewees [32] said that CCB projects are now shifting towards helping these CSIRTs secure necessary, more advanced capabilities,

[30] For a comprehensive analysis see the disaggregated Internet governance taxonomy proposed by Raymond and DeNardis (Raymond and DeNardis 2015, 585–94).

[31] The ITU's record of national CSIRTs shows the number increased from 102 in 2014 to 131 in 2020 (International Telecommunication Union 2021).

[32] Focus group meeting with cyber capacity building experts, 16 November 2020.

especially those needed to support critical national infrastructure. However, this still leaves a significant number of countries without a national CSIRT, and organisations are collaborating to fill gaps in existing guidance with information suited to their needs (Duijnhoven et al. 2021).

Although one can identify a parent community of technical experts from a CSIRT background involved in cyber capacity building, they provide their CCB assistance through a variety of channels. A lot of national CSIRT teams provide direct support to one another and engage in mutual exchanges of information, skills and even staff [33]. Staff from 591 national and organisational CSIRTs come together to support one another, and new CSIRTs, through the Forum of Incident Response and Security Teams (FIRST) [34] and its training and fellowship programme. The other main channels are regional collaborative mechanisms [35], non-commercial organisations with international CSIRT training programmes [36] and cybersecurity companies that provide pro bono incident response services and training.

This parent community of technical experts contributes not only essential expertise, but also a collaborative culture and interpersonal networks that connect different types of organisations and countries, between which technical-level cooperation may continue despite fraught political relationships (Tanczer, Brass, and Carr 2018). Because of their fundamental importance, early start, collaborative culture and concrete aims, the parent community of technical experts is well integrated into the field of CCB and its core community. However, one constraint upon the CSIRT community's ability to engage on cyber capacity building across borders has come from international sanctions. In 2019, FIRST expressed its regret that it had to suspend Huawei's membership to ensure compliance with US Export Administration Regulations (EAR) (Forum of Incident Response and Security Teams 2019). This is an example of how the aims of one community, and its decisions on how those aims are best achieved, can affect the cyber capacity building work of others.

Foreign Policy Community

The foreign policy community, typified by ministries of foreign affairs, were not the first to start funding cyber capacity building, but they have been one of its leading driving forces since at least 2015, when they were deeply involved in the creation of the Global Forum on Cyber Expertise. The

[33] Examples mentioned during our interviews include Japan's JP-CERT, the Korean Internet and Security Agency (KISA), New Zealand's CERT-NZ, the French National Agency for the Security of Information Systems, Estonia's Information System Authority, the UK's National Cyber Security Centre and China's National Computer Network Emergency Response Technical Team/Coordination Center.

[34] Figures as of 20 July 2021 (Forum of Incident Response and Security Teams 2021).

[35] Including (i) the training and activity coordination work of regional bodies such as OAS, ASEAN and the Commonwealth Telecommunications Organisation (CTO), (ii) other regional coordination groups like PACSON in the Pacific and (iii) the programmes of regional CSIRTs or cybersecurity agencies such as the European Union Agency for Cybersecurity (ENISA), the Task Force on Computer Security Incident Response Teams (TF-CSIRT) and the Asia Pacific Computer Emergency Response Team (APCERT).

[36] For example, ITU, the CERT/CC at Carnegie Mellon University and Asia Pacific Network Information Centre.

trajectory of their involvement, as well as their aims and approach, are of significance to the current state and future of the field.

The first Global Conference on Cyberspace, in 2011, was a watershed moment for foreign ministry involvement in cyber capacity building. One of the viewpoints that received strong support among delegates was that it was not enough to talk about shared, global security risks in cyberspace, there also had to be action: “practical collaboration and capacity development on cross-border law enforcement, to take place at a rapid pace” (‘London Conference on Cyberspace: Chair’s Statement’ 2011). This was followed by several foreign ministries starting cyber capacity building and the Ministry of Foreign Affairs of The Netherlands using the 2015 Global Conference on Cyberspace to launch the CCB-focused Global Forum on Cyber Expertise.

The contribution of the foreign policy community to cyber capacity building in the last five to ten years has been significant, but there is a strong case for strengthening the involvement of other communities to maintain a balance of actors and approaches. A recurrent theme in the early literature on cyber capacity building has been its use as 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 (Hohmann, Pirang, and Benner 2017, 10; Pawlak 2016b, 85). The risk highlighted by authors such as Pawlak is that development objectives will be diluted when foreign policy and Western security interests play a dominant role in directing capacity building. In addition, we identify the following risks:

- Foreign policy programme budgets are small compared with those of the development sector. The field may soon max out foreign policy community funding and need to draw more on funding from other communities to continue growing.
- Foreign policy objectives evolve more rapidly than those of most other communities. This could impede the field’s ability to set itself a stable agenda.
- The foreign ministry approach to programme management has stressed speed and agility over the more rigorous, but slower, processes of the development community. The complexity and risks of cyber capacity building suggest that a more rigorous programme management approach is needed.
- It is easier to build a collaborative global effort around common interests, but foreign policy interests are intrinsically divergent: if all countries agreed on an issue there would be no need for a foreign policy on it.

Development Community

The international development community has been using the concept of ‘capacity building’ since the 1990s (Zamfir 2017, 2) and the 2003 and 2005 World Summit on the Information Society called for CCB to support development. However, the field of CCB has, with a few exceptions, evolved outside of the development realm.

The 'niche' nature of cybersecurity in the global policy agenda has negatively impacted the integration of cyber capacity building into the development agenda, in part due to the impression that cyber issues are linked to national security and therefore would largely fall outside the scope of official development assistance. However, even the recognition of ICT as a broad enabler of development, affecting every Sustainable Development Goal, has only been widely recognised within the development community in the past decade (United Nations, General Assembly 2015). Therefore, it is perhaps unsurprising that technical cyber sub-issues are yet to be mainstreamed into development thinking.

Some of the key actors who have tried to break through the glass wall between cyber capacity building and development include the EU, ITU, Japan, Norway, the World Bank, UK and US. The EU was one of the first donors to systematically use its development cooperation funds to finance CCB projects. This funding came from pre-accession and partnership financing instruments and then consolidated as a priority to "utilise different EU aid instruments for cybersecurity capacity building" in the 2013 Cybersecurity Strategy (European Union 2013). The evolution of the EU's policy narrative since 2013 has focused upon addressing cybersecurity as a governance issue and cybercrime as a criminal justice reform priority, both closely linked to the Sustainable Development Goals (Council of the European Union 2015; 2018). The ITU oversaw the drafting of a Global Cybersecurity Agenda to follow up the WSIS outcomes (International Telecommunication Union 2008, 104–11) and subsequently its Telecommunication Development Sector (ITU-D) was set as an objective to "build human and institutional capacity, provide data and statistics, promote digital inclusion and provide concentrated assistance to countries in special need" (International Telecommunication Union (ITU) 2014, 32). The World Bank, UK and US have all created funds or programmes that intentionally combine digital development and cyber capacity building using overseas development assistance.

These examples and the others we found demonstrate a slow but steady trajectory in connecting development funding with cyber capacity building. The pace could accelerate with the pivot towards digital development as a new priority that requires the integration of cybersecurity.

Human Rights Online Community

The human rights online community advocates for a free, open, peaceful and secure cyberspace – goals shared by the core CCB community. Furthermore, several of the internationally active members of this community had pre-existing relationships with CCB funders through cyber policy projects and fora such as the Freedom Online Coalition and RightsCon. All of this would suggest that international and larger local human rights online organisations should have been well integrated into the field of CCB by now. However, while members of this community have been invited to play a role in key CCB conferences and decision making processes, this has not yet amounted to strong integration. Three factors help explain why: distance, culture and aims.

Locally focused civil society organisations are playing an increasingly visible role in cyber capacity building projects as stakeholders in government processes or as implementers or both. However, the fact that the core CCB community is concentrated in a few capital cities means there is a physical divide that many on both sides still find hard to bridge. This makes it less likely that these organisations will be consulted during project design, know about tender or grant opportunities, or be invited to the events of the core capacity building community. Online tools and knowledge repositories are being explored as solutions, but here issues of language and access to technology are challenges to be overcome.

A multistakeholder approach is deeply rooted in the culture of the human rights online community and essential for the inclusion of civil society in government-led processes. There have been positive examples of a multistakeholder approach in the development of CCB, such as the use of Internet Governance Forum events to hold consultations on new programmes (Viatchaninova et al. 2013). However, there have also been examples of civil society not having the level of involvement they wanted, including at the Global Conferences on Cyberspace in 2015 and 2017 and the recent UN Open-Ended Working Groups discussions on principles of CCB (Duru Aydin 2015; Lea Kaspar 2017; Ferrari and Kumar 2020). In 2011, Ron Deibert made the case that civic networks must be a part of the rule-making forums where cyberspace rules of the road are agreed upon and implemented (Deibert 2011). The same could be said of the forums where cyber capacity building is discussed.

Although the aims of the human rights online community and core CCB community align, there are important differences in emphasis. The core cybersecurity capacity building community has the primary aim of strengthening national cybersecurity and cybercrime capacities, in a way that respects rights and freedoms. In contrast, the primary aim of the human rights online community is defending those rights and freedoms which need cybersecurity for their protection. There should not be a trade-off between security and rights, but when the human rights online community participate in a security-centric and state-centric field, as CCB has been, they are conscious of the need to ensure their rights-centric objectives are not sidelined.

Defence Community

The defence community has been involved with the Internet since its earliest origins in the Department of Defence's Advanced Research Projects Agency Network (ARPANET) in the late 1960s. It is therefore not surprising that this community were among the first to respond to the need for international cooperation to address transnational cyber threats and to engage in cyber capacity building. In 2002, NATO called for cyber capacity building to address the inequalities between states in capabilities and human capacity in their report on 'Vulnerability of the Interconnected Society' (North Atlantic Treaty Organization 2002, 12). The US Department of Defense has funded cyber capacity building since at least 2009 under its Security Cooperation activity.

Many of the projects, issues and trends within the defence cyber capacity building community have a lot in common with their civilian counterparts. Priorities for NATO and US include: promoting information and coordinated action in the face of threats; helping partners understand their needs; and supporting a strategic planning approach. They similarly think in terms of putting in place the 'building blocks of capacity'. Furthermore, these can be the same building blocks that the mainstream capacity building community are supporting, in particular incident response teams and digital forensics capability. In countries where the defence ministry has responsibility for national cybersecurity, these may fulfil the national incident response role. An example of this is Jordan, where NATO's Science for Peace and Security Programme helped Jordan establish a military CSIRT that had national responsibilities to protect government and civilian systems (NATO 2017).

Spending figures are rarely published for projects funded by the defence community, but there is reason to think their scale is significant. For example, in Ukraine the US Department of Defense has contributed over $1.6 billion (€1.3 billion) to security assistance since 2014, some of which has been for cyber capacity building (U.S. Department of Defense 2019). If at least 1% of this assistance went towards cyber capacity building, that would mean this was one of the field's largest programmes, at over $16 million (€13 million).

Identifying the common interests between defence and civilian capacity building, Global Affairs Canada began a new project with the Inter-American Defense Board (IADB) and its Foundation in 2020 to start the IADB Cyber Defense Programme (Inter-American Defense Foundation 2020). Canada recognised that the defence community had routes into national cybersecurity leadership that Canada's civilian projects found difficult to access. Furthermore, in several countries in Latin America the military plays a leading role in national cybersecurity and emergency response. The programme began by agreeing to a Framework for Cyber Defense Cooperation in the Americas to establish shared and clear values and approaches. It is now strengthening the cyber defence strategies and response capacities of six countries in the region.

Private Sector Community

Private sector companies help build capacity through direct contracts from foreign governments, by implementing projects with donor funding and by themselves acting as donors and implementers through pro bono activity. The last two of these we classify as international cyber capacity building, while the first is purely commercial activity without any voluntary contribution component.

The private sector's role in cyber capacity building has grown in size, investment and prominence. Companies are creating new not-for-profit organisations, forming alliances and consortia, launching cyber training academies, financing CCB projects directly or through their foundations, convening strategic events, presenting proposals and taking an active role in platforms such as the Global Forum on Cyber Expertise. We distinguish the following groups with notable activity in cyber capacity building to date:

- ICT and technology companies, such as Microsoft, Cisco, Accenture/Symantec, Hewlett Packard Enterprise and IBM.
- Professional services companies, such as Deloitte, EY and KPMG.
- Global cybersecurity companies, such as FireEye, Kaspersky, Palo Alto Networks and Trend Micro.
- Telecoms companies, including AT&T, Huawei, Vodafone and Telstra.
- Financial sector entities, such as Citigroup Inc., Mastercard, Absa Group Limited, Sberbank Group, FS-ISAC, SWIFT, etc.
- Other project implementing companies, many of them small and medium-sized enterprises, with cyber capacity building expertise.

The role of multinationals is significant because they fill multiple roles: implementing projects funded by others, financing projects themselves, providing pro bono services, engaging in international policy negotiations and contributing at the front line of incident detection and response. Several have established free cybersecurity training programmes and/or public-private tech hubs in partner countries.

Zooming in on multinational cybersecurity companies, we include a few indicative examples of the different modalities they use:

- FireEye is an implementer for government donors and provides €4-8 million per annum in pro bono assistance through its Research Partnership Programme. Kaspersky launched a pro bono capacity building programme for government entities and universities to enhance their knowledge on evaluating product security and also delivers, through the DiploFoundation, a capacity building exercise on technical attribution for cyber diplomats and policy and legal researchers without technical backgrounds.
- Palo Alto Networks Cybersecurity Academy is focused on skills development, delivering entry-level to intermediate courses and hands-on labs, integrated into degree programmes, at no cost to qualifying universities, colleges and high schools.
- Trend Micro demonstrates a wide range of corporate social responsibility programmes, including Internet Safety for Kids and Families, the Initiative for Education aimed at schools, Cybersecurity Education for Universities, Internet Safety for Small Businesses and the Cyberwomen Challenge with the OAS.

Several companies have developed expertise in implementing competitively tendered international cyber capacity building projects. These tend to be smaller cyber companies with a footprint in one country, but the ability to deliver internationally and combine the skillset needed for cybersecurity with that of international development projects. This trend has been concentrated in several countries where local ecosystems of smaller cyber capacity building companies, consultants and academics are taking root. These include the US, UK, Israel, France, Australia and the Baltics.

Recognising the opportunity to connect companies with common interest in global cybersecurity, and to connect larger multinationals with SMEs, there have been efforts to create alliances, such as the Cybersecurity Tech Accord and the Paris Call for Trust and Security in Cyberspace. Microsoft has played a key role in both. Companies in these alliances typically commit to a safer cyberspace and, inter alia, promote awareness-raising campaigns addressing cyber risk and threats.

The emergence of companies specialising in delivering international cyber capacity building projects is a positive sign for the field. It indicates that there has been a large and reliable enough flow of funding for such specialism to develop. It also means that there is a career path for cybersecurity professionals wanting to work in capacity building. Yet, there has been slow progress on involvement of traditional development consultancies in CCB.

An opportunity and challenge for the field created by the greater engagement of companies is that they bring a different perspective and culture. For example, some companies have said [37] that the field's progress is too slow and that it is too focused on putting in place the foundational building blocks of capacity, such as basic incident response teams and legislation, as opposed to the higher-level capabilities needed to meet advanced threats.

While the private sector is not a monolith, the technology-focused companies play a significant role in shaping cyberspace through the technological solutions and services they provide, while they are also the largest seekers of cyber talent. This influences their priorities in cyber capacity building and their approach. They are keen to strengthen relationships with corporate, government and individual customers, to foster availability of local talent and encourage stability and predictability in cyberspace and its regulation.

Why does this trend matter?

The fact that cyber capacity building has organically grown within distinct, and sometimes siloed, parent communities is important because it affects what actions are needed to ensure CCB grows in an efficient and coordinated way in the future. As our scenarios explore, there are futures in which CCB is conducted with competing approaches and objectives and there are futures in which there is alignment, coordination, shared goals and common practices between the parent communities.

The inhomogeneity of the cyber capacity building community is both a strength and a weakness. The parent communities have a variety of knowledge, methods, tools and funding sources that they can bring to the table. However, this diversity also creates inherent fragility and the need to invest more energy in efforts to ensure alignment and coordination. It is also significant that the majority of potential funding for CCB lies in the communities in the less-integrated group, especially the international development community.

The strengthening of the core community is a long-term process that will require breaking through horizontal and vertical silos between and within parent communities. Agreeing to and implementing

[37] This insight comes from remarks made by private sector representatives during GFCE meetings attended by the authors.

principles of cyber capacity building can assist by building trust and creating common frameworks and terminology that aid coordination and collaboration between and within the parent communities and with the core community. The Open-Ended Working Group's 2021 final report proposes 10 principles for the field and follows an earlier set of principles agreed in the GFCE's 2017 Delhi Communique. This a useful start, but further work must be done to communicate the principles-based approach to all parent communities and to a wider group of stakeholders outside of the UN process in a way that will gain wide support for their implementation (Pawlak and Barmpaliou 2017; Collett 2021, 14–16).

Recommendations

***For the EU*:**

- In the process for the development of the EU External Cyber Capacity Building Agenda, capture the EU's CCB lessons to date and reflect on concrete actions for better embedding different parent communities, including bringing the EU Member States' development agencies on board with CCB.
- Use the EU Cyber Capacity Building Board to systematically bring together line Directorates-General (DGs) experts in CCB programming discussions and coordination.
- In light of the leading role of several EU Member States' development cooperation agencies globally, consider convening an informal meeting with the relevant EU services and bring together the representatives of the Council Horizontal Working Party on Cyber Issues (HWP) and the Working Party on Development Cooperation for a hands-on awareness raising discussion on prioritising and/or mainstreaming CCB into development cooperation based on the examples of the EU's experience since 2013.
- Update the EU Operational Guidance with concrete examples that demystify cybersecurity for EU Member State development agencies. Consider using the EU CyberNet Annual Conference to bring different parent communities together with the core stakeholders engaged in EU-funded capacity building activities to strengthen the network and knowledge exchange.
- Ensure the EU engages systematically with the core CCB community represented at the GFCE and consider assigning thematic experts as points of contact for each WG with an overall coordinating PoC.

***For the whole CCB community*:**

- Countries and large companies and organisations should shift from ad hoc inter-agency, inter-service or inter-departmental meetings on cyber capacity building to regularised processes that bring together all relevant teams to discuss strategy and progress.
- The UN and any other actors organising events to follow up the Open-Ended Working Group and Group of Government Expert 2021 recommendations on cyber capacity building principles and coordination should use this as an opportunity to involve all the parent communities in the process.

- Step up efforts to connect cyber capacity building with the international development community, especially those running digital projects. Actions to achieve this have been recommended in several reports and should be implemented [38].

***For the GFCE*:**

- Use the GFCE's proposed conference in 2022, co-hosted with the World Bank, World Economic Forum and Cyber Peace Institute, to bring together parent communities. The mix of co-hosts lends itself to engaging ICT for development practitioners and researchers in particular. Action-orientated outcomes could be achieved through dedicated sessions, side events, a communiqué and a Sherpa process to prepare these.
- Design an outreach strategy for each parent community.

TREND 4. CYBER CAPACITY BUILDING IS GRADUALLY PROFESSIONALISING

Many cyber capacity building programmes are maturing, by which we mean they are applying good practices from the established fields of programme management and development. These include having a needs-based approach to project duration, having stronger programme management teams, managing human rights risks, using monitoring and evaluation, using research, mainstreaming gender and adapting implementation methods.

Strengthening programme management teams

Several programme teams have strengthened their own capacity in the last couple of years and have plans to continue doing so. This has occurred through a combination of adding staff, creating specialist roles or training.

The UK Foreign Commonwealth and Development Office (FCDO) programme team operated with a staff of about three from 2012 to 2018, when it expanded to over ten. From 2018 to 2020, two of the team members were economists, brought in to strengthen metrics, monitoring and evaluation processes. The team started to more proactively encourage team members to take programme management courses in 2019. Australia's Department of Foreign Affairs and Trade (DFAT) programme team started with one and a half people in 2017 and now consists of three programme staff and two to three people in its managing contractor support unit. The use of such a unit was a lesson applied from DFAT's management of its development programmes. In 2020, the US State Department began the process of expanding their S/CCI programme team, with plans to increase its size from three people to eight, including communications and strategy specialists.

[38] Reports with recommendations or insights on mainstreaming cyber capacity building into international development include EUISS's Cyber Capacity Building in Ten Points (Pawlak 2014a), NUPI's 'Teach a Person How to Surf: Cyber Security as Development Assistance' (Schia 2016), New America's 'Securing Digital Dividends: Mainstreaming Cybersecurity in International Development' (Morgus 2018) and the World Bank's 'Digital Dividends' (World Bank Group 2016).

Singapore Cyber Security Agency's international programme team began by using part of the time of a few staff in 2015 and has since grown to have three full-time positions.

The strengthening of programme teams is also occurring outside of governments. In 2020, the World Bank restructured their Digital Development Department, increasing the number of staff with a concentration in cybersecurity to around 10. They also took the step of providing their cyber programming staff the opportunity to take a three-month part-time course in cybersecurity at Harvard.

The growth of programme teams has not, however, been universal. For example, the Japan International Cooperation Agency (JICA) and Korea Internet & Security Agency (KISA) programme teams have remained at a consistent size since they were established.

Managing human rights risks

Cyber capacity building projects can give rise to, or be used to address, a range of human rights risks including privacy, freedom of expression, freedom of association, discrimination, the right to a fair trial, the right to life and access to online services and information.

The human rights risk landscape for projects is becoming more complicated. Awareness of the risks among programme teams is improving, and there are some signs of increased action to understand and mitigate risks. The human rights landscape is becoming more challenging with each new case of governments putting human rights principles at risk, or contravening them, through problematic cybercrime legislation or the misuse of powers and data (Calandro and Berglund 2019, 2). Beneficiaries are also more frequently requesting capacities that generate human rights risks, such as tools and training that could be used for offensive cyber capabilities or social media monitoring. Some interviewees noted that these tools are readily available from other sources, so even if their projects did not provide them, countries would probably still acquire them.[39]

The EU's operational human rights guidance for cyber capacity building recommends integrating human rights principles and safeguards at all stages of the project management cycle (European Commission, Nicole, and Hansen 2015, 25). During our interviews, we heard few examples of this end-to-end integration. However, several programme managers said their teams were giving greater consideration to human rights risks and they typically described taking at least one of the following assessment or mitigation measures:

- **Pre-project risk assessments**. The World Bank use Environmental and Social System Assessments. The UK conducts Overseas Security and Justice Assistance risk assessments. JICA conduct project Environmental and Social Assessments.
- **Regular reports from embassies**. US embassies submit annual human rights reports, while Australia's produce them every two years.

[39] Interviews with private sector representatives on 18 December 2020 and 1 February 2021.

- **Selection of implementing partners**. Australia manages risk by working with a small number of trusted implementing partners and making use of the due diligence process they go through when selected.
- **The closeness and length of their relationship with beneficiary countries**. New Zealand works with a small number of regional partners which gives them a strong understanding of the risks and influence over them.
- **Restricting the types of support provided**. The World Bank will only finance civilian, defensive capabilities and bank-executed funding is not used to purchase equipment. FireEye decline requests for social media monitoring tools and provide a fixed list of trainings. US cyber capacity building will not assist offensive cyber capabilities.

There is also increasing investment in projects with a rights-focus or strong rights component. One implementer estimated the funding for this type of work had doubled within the last couple of years – a faster rate of growth than for cyber capacity building overall. Examples of such projects include: the Australian Human Rights Commission providing technical training in Vietnam; Plan International helping Solomon Islands youth stay safe online; and GIZ assisting civil society to engage on cyber issues at the African Union.

The strategic framework pillar has received particular attention for integrating a human-centric and rights respecting approach. For example, Global Partners Digital has published two good practice guides to involving stakeholders in national cybersecurity strategy development (Global Partners Digital 2020; Shears, Schnidrig, and Kaspar 2018). They have supported the application of these approaches in the strategy development processes of several countries including Ghana, Mexico, Belize and Sierra Leone. This has contributed to human rights language being included in national cyber strategies, although it is too soon to assess if this has influenced how rights are respected during the implementation of those strategies.

Some programme managers expressed concern that they, or their peers, did not sufficiently understand the risks or have the tools they needed to mitigate them. They recognised that there was a positive trend towards awareness of human rights risks, and to a lesser extent mitigating action, but they felt it was too slow and may be not sufficient to keep pace with the growth in risks. The cyber capacity building community needs to catch up with the development community. As an example, in 2009 the UN Secretary General established the UN Development Group's Human Rights Working Group to mainstream efforts within the UN development system. Although funder programme teams are bringing in more specialists in monitoring and evaluation, cybersecurity and strategic communication, we did not find any creating positions for human rights specialists.

Monitoring and evaluation

Cyber capacity building has suffered from a lack of supporting evidence for the effectiveness of its activities (European Commission et al. 2018, 103). Measurement challenges have created problems across the spectrum of cybersecurity activity, including such key areas as risk management methodologies, the performance of national cybersecurity programmes and the effectiveness of the cyber insurance market (Hubbard and Seiersen 2016; UK National Audit Office 2019, 24; Dambra, Bilge, and Balzarotti 2020). It has also spurred interest among the cyber capacity building community in improving the frameworks, indicators and data they have for monitoring and evaluation (M&E) and in being more robust in their application. In response to the challenge, programme teams are strengthening their M&E approaches.

Organisations typically start approaching the challenge of evaluating and measuring their CCB programmes by deciding if there are any **organisation-wide evaluation frameworks** they should apply. We found several examples of programmes that had orientated their evaluation around such frameworks. These include New Zealand's Ministry of Foreign Affairs and Trade, Japan's JICA and the World Bank. All of these are organisations that use Overseas Development Assistance and therefore their organisation-wide frameworks draw upon the Organisation for Economic Co-operation and Development's Development Assistance Committee (OECD DAC) evaluation criteria: relevance; efficiency; effectiveness; and sustainability.

The European Commission has several organisation-wide frameworks that can be applied to cyber capacity building depending upon which funding instrument is being used. These include: the EU Result Framework used by DG International Partnerships (DG INTPA); the EU Partnership Instrument Monitoring System used by the Service for Foreign Policy Instruments; or the Better Regulation Guidelines used by the DG for Neighbourhood and Enlargement Negotiations (DG NEAR).

Organisation-wide frameworks are by necessity quite generic, which has left a space, and created a demand, for **cyber-specific capacity frameworks** that can be used for M&E. Several organisations have made use of national cybersecurity capacity maturity models to measure improvements in national-level **outcomes** that projects aimed to contribute to (Weisser Harris et al. 2021) [40].

While there are frameworks programmes one can use to measure national-level outcomes, there is less supporting literature on how they can measure the **impact** of these capacity outcomes on improving indicators of cybersecurity vulnerability or harm, or an open, free, secure and peaceful cyberspace. Work that could be applied to impact evaluation includes: models of cyber harm; national cyber risk assessment methodologies; Oxford University's research to quantify the link between cybersecurity capacity and positive indicators of security and digital access (Agrafiotis et al. 2016; Dutton et al. 2019; Creese et al. forthcoming); and the recent 'Literature Review: Guide for Criminal Justice Statistics on Cybercrime and Electronic Evidence' .

[40] Examples mentioned in interviews include the UK using the Capacity Maturity Model in the measurement of programme outcomes, FireEye using their own National Cybersecurity Assessment Methodology and South Korea looking for improvements in the ITU Global Cybersecurity Index.

Ten examples of CCB programmes strengthening their M&E approach

1. The ITU is moving from activity-based reporting to results-based reporting, which prompted them to redesign their planning and delivery process.

2. The US State Department intends to improve the M&E in its foreign assistance, with additional, multi-million-dollar investment in M&E activities. As a consequence, the S/CCI cyber programme team are hiring an M&E specialist.

3. The World Bank have recently created a Global Analytics Department and are preparing the ground for a research project that could contribute to better metrics for the community.

4. Australia's DFAT amended the latest version of their grant form to include more robust M&E and clearer milestones.

5. The UK brought two economists into their programme team from 2018 to 2020 and have begun using logframes. Their Digital Access Programme could break new ground by using three sets of metrics: development goal outcomes; improvements in the national capacity maturity assessment; and reductions in cyber harms.

6. Japan's JICA is developing a cyber capacity framework and indicators to inform their project design and M&E.

7. The EU's Operational Guidance made a useful contribution to the tools for designing and measuring outputs by sharing templates for each capacity pillar (European Commission et al. 2018, 63, 87, 91, 110, 118, 126, 134).

8. The EU's Capacity4Dev platform publishes on its website practical guidance on indicators and results chain across different sectors of intervention, including on cybersecurity (European Commission 2018).

9. Several programme managers have commissioned independent or semi-independent evaluation reports of their projects. At least two have been published (World Bank, Dutton, and Bauer 2019; UK Foreign Commonwealth and Development Office 2021).

10. Singapore has commissioned research on how to better measure the outcomes of CCB training projects.

Use of research

The development community places greater emphasis upon conducting and using research to inform programme and project design than the cyber capacity building community, but the gap has been narrowing. The shift from smaller, shorter projects to larger, longer programmes has contributed to the demand, and time available, for research. This research takes several forms. It is relatively common for programmes to review and use existing literature; for example New Zealand drew upon several regional cyber reports covering the Pacific when designing its new programme. It is also becoming more common for programmes to build in time for national capacity assessments or surveys before their projects; for example all JICA projects are preceded by a country study mission and the UK commissioned capacity assessments at the start of its Digital Access Programme. The story with regard to producing and commissioning fresh research is a little more complicated.

Cyber capacity building programmes have routinely produced or commissioned tools and research reports that were shared with others, either on their own or in collaborative efforts. However, there was a period of especially high interest and investment in research at the start of cyber capacity building, as the new field was setting itself up. Commissions and funding supported new cyber capacity building researchers in knowledge centres such as Oxford University, MITRE, Software Engineering Institute (SEI), Australian Strategic Policy Institute (ASPI), DiploFoundation, the e-Governance Academy, EUISS and NUPI.

There are signs that we are at the start of a second wave of interest and investment in research. In 2020, the GFCE responded to member demand by launching a research agenda that prioritises research requests from its working groups and connects them to funding, initially from Canada. In Spring 2020, the World Bank Digital Development Global Practice established a Global Analytics Department that will produce and commission research. Australia included encouragement to submit research proposals in its last call for grants – although the absence of proposals was a sign of the gap between research supply and demand. Singapore is commissioning research, especially on evaluating what works, to support its ASEAN Singapore Cybersecurity Centre of Excellence (ASCCE). In Africa, there has been recent investment in the Cybersecurity Capacity Centre for Southern Africa and the Africa Cybersecurity Resource Centre Consortium (ACRC). This fits a pattern of investment in regional centres that can conduct capacity building and have expertise that could be used for research and education (Perrier and Baur-Yazbeck 2020). Interviewees encouraged funders to explore supporting existing research and regional centres before creating new ones.

Gender mainstreaming

Our focus groups and interviews identified gender as an emerging issue. Some cyber capacity building projects with a gender component, such as the Women and International Security in Cyberspace Fellowship (Cybil Portal 2021b), are well known among the community, but the total number of projects in the Cybil Portal is still quite low [41]. In the last two years, driven by the Women, Peace and Security agenda, there has been a move to start including gender within CCB. The coronavirus pandemic has accelerated this with remote working and services creating greater opportunities for

[41] At the time of writing, the Cybil Portal contained seven projects with an explicit gender component.

exposure and exploitation [42]. However, cyber capacity building has not yet moved beyond considerations of gender equality to deliver gender-sensitive prevention, mitigation and response.

Although hard to measure accurately, in line with the trend and critique of feminist-foreign policy (Jezierska 2021), there could be a larger volume of gender-informed cyber capacity building occurring within the programmes of other communities. In particular, the Women, Peace and Security agenda – built upon UN Security Council Resolution (UNCSR) 1325 – plays a significant role. This agenda has mainstreamed gender considerations into international security programming. That security programming is beginning to address cybersecurity issues and thereby connect gender considerations with cyber capacity building 'from the outside' [43]. The UNCSR 1325 Women, Peace and Security agenda is reflected within the normative discussions in the UN Open-Ended Working Group and UN Group of Government Experts, but is less prominent in the GFCE.

Those national cybersecurity strategies that include gender primarily do so from the perspective of women's participation, as do at least a third of the gender-related international cyber capacity building projects in the Cybil Portal. Gender equity addresses the issue of increasing the representation of all genders in cyber and narrowing the gender gap [44]. Gender equality is also the primary concern of the GFCE's Women in Cyber Capacity Building initiative (Global Forum on Cyber Expertise 2020b).

While gender equality is important, it is essential to also consider how gender interacts with cyber risk, policy and operational effectiveness. This has received less attention from cyber capacity building, partly because it is more difficult and politically sensitive to address culturally rooted concepts of which groups are acknowledged as victims and the dynamics of masculinity within government cybersecurity structures (Sharland and Smith 2019).

Where gender sensitivity considerations are addressed by projects, it is mostly at the civil society level, in the feminist or human rights space focused on providing safeguards for cyber-related harms to fill gaps where the state is unable to offer protections. The beneficiary countries for these projects tend to be those where there have been conflict-related shifts in the human rights context, such as Egypt, Thailand and Jordan. The UN Women's Violence Against Women in Politics (VAWP) project is an exception to this: it will study and address how 'cyber violence' is used by state and non-state actors to discourage women from entering politics and to undermine them after they have (UN Women 2021).

[42] For example, see advice for mitigating online risks in Canada's Gender Equality Guide for Covid-19 Related Projects (Global Affairs Canada 2021, 4).

[43] For example, the Women's International League for Peace and Freedom (WILPF) submitted a report, with the support of donor funding, to the UN Working Group On The Use Of Mercenaries on the international services of 'cyber mercenaries' and their human rights impact (Women's International League for Peace and Freedom 2021).

[44] The International Information System Security Certification Consortium 2017 indicated that 24% of cybersecurity professionals worldwide are women and 51% of those had experienced discrimination, compared to 15% of men (Help Net Security). See also (Global Forum on Cyber Expertise 2020b).

Organisations and initiatives seeking to advance the field's work on gender sensitivity include UNIDIR, in their report on 'Gender Approaches to Cybersecurity'(Millar, Shires, and Tropina 2021), the Council of Europe's Cyberviolence project and knowledge portal (Council of Europe 2021c) and a new Chatham House project on Equity, Diversity and Inclusion in cybercrime programming.

Project design

The way cyber capacity building projects are being implemented is maturing and has been changed considerably by the coronavirus pandemic.

Early cyber capacity building projects were critiqued for relying upon 'fly-in fly-out' training and mentoring. This was poorly suited to building the interpersonal relationships and accumulating the knowledge of local context that enables capacity building. Learning from this, and good practices in development, security assistance and private sector projects, the field has deployed several other ways of delivering projects.

One alternative to flying international experts in and out for short visits has been to deploy experts in the beneficiary counties for long periods, up to a year or occasionally longer. JICA regularly use a combination of Japanese experts who live in the project country for its duration, working in small teams with locally hired experts. With a World Bank loan, Ghana contracted an Israeli company to deploy experts into their national incident response team who worked as part as the unit, and as trainers, until the Ghanaian staff were capable of operating without them (Ghana, Ministry of Communications 2019). New Zealand has pioneered using secondments and reverse-secondments between the CERT NZ and their counterpart teams in some Pacific partner countries. The EU is also investing in the creation of a Latin America and the Caribbean Cyber Competence Centre (LAC4) to be hosted in the Dominican Republic, with the aim to serve as a hub for sharing EU's collective expertise and building up local and sustainable capacities in the LAC region.

Another alternative to flying in international experts has been to use or build up local consultants and organisations who can deliver the project, alone or with an international partner. Recognising that local implementing capacity often needs strengthening to achieve this, some programmes have included the need to partner with and assist local organisations within contracts or have grant funded new local CCB initiatives, such as the Cybersecurity Capacity Centre for Southern Africa [45] and the Africa Cybersecurity Resource Centre Consortium.

Lastly, projects have experimented with remote activities as an alternative delivery method, an experiment accelerated by the travel restrictions created by the coronavirus pandemic. During the pandemic, the ITU moved more of its ITU Academy courses, including those for cybersecurity,

[45] Although the Cybersecurity Capacity Centre for Southern Africa was launched as a new initiative in March 2020, it emerged from pre-existing work at the University of Cape Town, Research ICT Africa and the Global Cyber Security Capacity Centre at the University of Oxford.

online. The ITU also offer an online cyber range and have delivered virtual cyber exercises. New Zealand has shifted to remote mentoring delivered by its CERT NZ staff. APNIC adapted to the pandemic restrictions by moving its training courses, lasting a full week, online. They found this allowed them to continue capacity building, but the drop-out rates in their online training were five times higher than in their offline training. They also found both implementers and trainees missed the valuable exchanges and networking that occurred during the breaks.

Another way in which project delivery is evolving is that the length of the average project is increasing. In 2010, the average span of a project was roughly one calendar year; by 2015 it had risen to two calendar years. Our interviews and literature review confirmed there has been a push for projects that have the flexibility to last longer if they need to. Where internal rules place a limit, often three years, on project duration, some programmes have used multi-phased projects to extend the duration to six years or more [46].

Finally, the scope of the typical project is deepening. The earliest projects tended to focus on a single pillar of capacity and, within that, a single aspect of that pillar. It is now common for projects to take a more holistic and ambitious approach, addressing several capacity pillars at once.

Why does this trend matter?

Professionalising CCB by adopting lessons from related fields of practice, especially international development, matters because it will result in more effective projects and give confidence to funders and beneficiaries. Programmes are more likely to be effective when they are commissioned and overseen by funder teams with sufficient staff, with relevant experience and specialist expertise. Strong risk management is not only the responsible approach to take, but is also important for the practical reasons that projects achieve better outcomes when they have fewer negative impacts for citizens and the capacities they build are resistant to misuse.

For a young field like CCB, evaluation and an evidence base to demonstrate impact will be essential to identify what works and attract investment. The better use of research can support such evidence gathering and, when used to inform programme design, can improve outcomes and make project management easier. The integration of gender equity and sensitivity considerations into programming is necessary to deliver upon United Nations Security Council Resolution 1325 on Women, Peace and Security, and to deliver projects that serve all targets and victims of cyber threats. Finally, cyber capacity building needs ways to implement projects that are effective, efficient, scalable and sustainable. Longer projects provide the time needed to build the strong relationships and understanding of local context that underpin effective capacity building. The fly-in fly-out delivery method was necessary in the early years of the field when there were few people

[46] Interviews with a government official on 9 December 2020, an EU official on 14 December 2020 and two project implementers on 15 December 2020 and 21 January 2021, respectively.

with experience delivering international cyber training and projects had small budgets. However, these conditions are changing, other models have been tried and the coronavirus travel restrictions have emphasised the limitations of not having local implementing partners.

Recommendations

For the EU:

- Compare the results indicators and results chains of existing programmes to look for lessons and potential efficiencies in collecting data. This exercise could be done as part of the updating of the EU's Operational Guidance.
- A concerted effort should be made to mobilise and utilise research at pre-programming stages and inform an evidence-based prioritisation of capacity building efforts.
- Review how the EU's CCB actions are integrating a rights-based approach both at the design stage and during implementation to manage risks, and whether the key points that related to cyber issues from the 2015 Operational Human Rights Guidance for EU external cooperation actions addressing Terrorism, Organised Crime and Cybersecurity could be updated and transformed into 'how to' factsheets for the EU programme managers and the implementers.
- Create EU guidance for gender sensitivity in cyber programming, adapting the principles of the 2004 toolkit on mainstreaming gender equality in EU development cooperation.
- Strengthen the involvement of the EU agencies and bodies such as the European Union Agency for Cybersecurity (ENISA), the European Cybercrime Centre (EC3) at Europol, the EU Agency for Law Enforcement Training (CEPOL) and Eurojust in the delivery of cyber capacity building, either as project leads or as project partners, in line with their respective mandates on international engagement.
- Ensure that all implementers of EU-funded projects on CCB get an information session after contract signature, at the latest at the beginning of the inception phase, on the EU's overall project cycle management methodology and the Operational Guidance on CCB. A specific training course on the EU's international cyber policy, related issues and CCB approach could be developed.

For the whole CCB community:

- Funder programme teams and larger implementers should look for applicable lessons in the approaches their peers are using to strengthen their own capacity, such as training, specialist roles and additional staff.
- Programmes could make use of experts in human rights risk management and conflict sensitivity to review their current approaches and advise on improvements.
- Share project evaluations online and, ideally, by linking to them from Cybil project pages. If necessary, publish redacted versions.
- Hold an academic conference on cyber capacity building with an open invitation for presentations by researchers working in the field from both academia and think tanks.
- Apply lessons from Women, Peace and Security programmes on how to manage gender-related risks when domestic legal protections fail and social norms are harmful.

- Funders should find ways to make it easier for locally based implementers to compete in contract tendering processes and create incentives for bidding consortia leaders to include locally based implementing partners.

***For the GFCE*:**

- Consider whether the GFCE Foundation could offer training courses for cyber capacity building managers and implementers, if members agree this fits its mandate and does not compete with any service offerings of GFCE members.
- If the Cybil Portal decides to add a section on capacity building metrics data, then include human rights as a dimension, for example using the Freedom on the Net factsheets.
- Include research to support impact measuring research (especially indicators and data sources) in the GFCE Research Agenda.
- GFCE members should support the coordination and prioritisation of research by feeding their requirements and suggestions into the GFCE Research Agenda process.
- Run a session on the application of gender sensitive approaches in cyber capacity building programmes at a future Annual Meeting and include an article on gender sensitivity in an issue of the GFCE magazine.
- Use the GFCE magazine to raise the profile of local implementers and their contribution to cyber capacity building.

TRENDS AND EMERGING ISSUES SPECIFIC TO THE EU'S EXTERNAL CYBER CAPACITY BUILDING

Increased use of cyber capacity building as a mechanism for the EU's international cooperation

The role of external cyber capacity building as a mechanism in the EU's international cyber cooperation toolkit has increased over time. Building on its internal experience, the EU commenced financing a few projects since 2009, with a focus on cybercrime mainly in the accession and neighbourhood countries. The first EU Cybersecurity Strategy defined cyber capacity building as a key pillar of the EU's international cyber policy, coupled with the call to utilise different external assistance financing instruments to this end (European Union 2013, 16). Since then, the EU has started a comprehensive cyber-specific capacity building engagement at a global level, which has been growing as a mechanism for its external cooperation, mirroring the global trend identified in this report.

The increased use of capacity building as part of the EU's international cyber engagement is a broad trend shaped by three main elements.

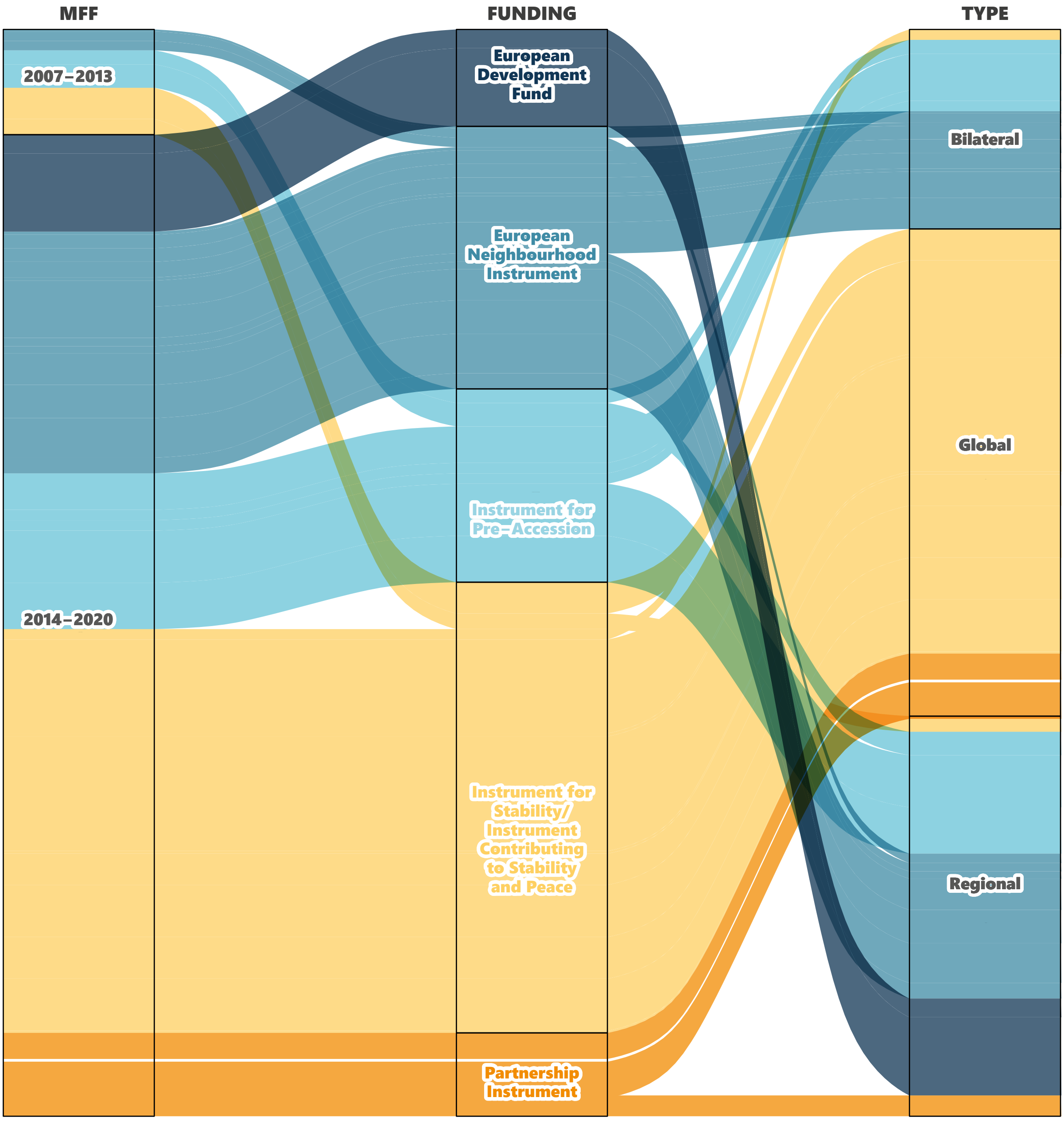
First, **the EU has increased its financial commitment for CCB**. From the initial investment of €10 million for its cyber-specific external cooperation actions in the 2007-2013 budget, known as Multi-Annual Financial Framework (MFF), it reached the significantly higher commitment of almost

€95 million during the 2014-2020 MFF.[47] This has naturally resulted in an increase in the number of financed projects with a cyber-specific objective, from one project in 2009 to a cumulative total of about 40 projects by mid-2021.

It is noteworthy that the EU **has been one of the few international donors to systematically link its international cyber capacity building activities with its development and international cooperation funds** from the early 2010s, in contrast to several other donors that have mainly used foreign assistance financing. This approach has been promulgated in key EU policy

FIGURE 8. **EU CCB FUNDING**

2007-2020



Data: Authors' compilation from interviews and open-source information

[47] See Annex 3 for a detailed list.

documents, most notably the Council Conclusions on Cyber Diplomacy (Council of the European Union 2015, 9–11) and the Digital4Development framework which recognised cybersecurity as a transversal issue cutting across development cooperation (European Commission 2017, 12–13). As a result, the connection of CCB with the EU's sustainable development commitments of the 2030 Agenda [48] has played a pivotal role in shaping the EU's increased financing for CCB and this trend overall, underscoring the intersection between cyber resilience, development and the role of capacity building in third countries (European Union 2017, 19).

Second, the evolution of the EU's approach from the technical assistance objectives of its early cybercrime legislation projects to recognising "**the importance of cyber capacity building in third countries as a strategic building block of the evolving cyber diplomacy efforts of the EU**" (Council of the European Union 2015, 9) further showcases how capacity building has been increasingly recognised as a mechanism that can serve multiple policy objectives as part of the EU's international cooperation toolbox. On the one hand, this can be seen in the expanded scope of the available financing to include activities and projects beyond traditional CCB on cybercrime and cyber resilience, such as aspects of cyber diplomacy and ICT standards. On the other hand, there is growing interest in connecting cyber capacity building activities with fostering strategic alliances and promoting "relevant EU cyber diplomacy policies and standards" as called for in the latest EU Cybersecurity Strategy (European Union 2020, 23). A few interviewees noted that this approach does not imply conditionality, but rather a clear line that the EU's cyber capacity building cannot be value-free, as the EU's core values and principles on fundamental rights, democracy and the rule of law also translate to cyberspace. [49] The case of the GLACY+ project is indicative of this trend, as the project is designed to support any country's development of national cybercrime legislation, yet the 15 priority countries that benefit from the full suite of its capacity building activities, primarily for law enforcement and the judiciary, include only countries that have been invited to accede or have signed or ratified the Budapest Convention on Cybercrime. This trajectory is likely to continue in the future, considering the geopolitical ambitions of the von der Leyen Commission. [50]

Finally, this trend can also be traced in the **overall increased political priority the EU has been placing over time on capacity building as a building block of its international cyber policy**. It is a theme that has gained prominence in the EU's cybersecurity strategic frameworks of 2013, 2017 and 2020. It has also been highlighted in vertical policies, with the most notable example being the need to prioritise the use of external assistance in the fight against cybercrime

[48] The external cyber capacity building financed by the EU have been linked most notably with SDG 9a on resilient infrastructure; SDG 16.4 on combatting all forms of organised crime; and SDG 16.6 on effective, accountable and transparent institutions as indicated in the respective Commission Implementing Decisions (Action Documents) for each project.

[49] Interviews with EU officials on 11 December 2020 and 6 January 2021, and a government official on 11 March 2021.

[50] This is reflected also in the revised mission and revamping of the Directorate General for International Cooperation and Development (DEVCO) into the new Directorate for International Partnerships (INTPA) in 2020 with the objective to ensure the European model of development, inter alia, contributes to the EU's wider political priorities (President of the European Commission 2019).

recognised in the European Agenda on Security (European Commission 2015) and the EU Security Union Strategy (European Commission 2020b). The adoption of the EU External Cyber Capacity Building Guidelines by Member States in June 2018 was a milestone in this respect. It provided overarching political guidance on the scope, objectives and principles for the EU's international capacity building and cooperation efforts (Council of the European Union 2018). Similarly, CCB has been a topic systematically included in the EU's official Cyber Dialogues with its strategic partners for exchanging lessons learnt, improving coordination and agreeing on priority actions.[51]

Overall, we expect cyber capacity building to continue to grow as a mechanism for the EU's engagement with its partners. On the one hand, we see cyber capacity building placed at the centre of several discussions in major international fora including at the UN. On the other hand, partner countries and regional organisations also seem to be increasingly interested in working with the EU, either through traditional capacity building partnerships or to address cyber-related issues broadly, as the requests for starting new official cyber dialogues and having peer-to-peer exchanges would indicate.

Looking ahead: key challenges and opportunities

Despite the EU's use of external cyber capacity building to achieve multiple mutually reinforcing objectives, an **overarching narrative for cyber capacity building is still missing.** The EU uses CCB to contribute to an improved global digital ecosystem, to foster strategic alliances consistent with the EU's core values and principles, promote cooperation frameworks with partner countries and regions and support the implementation of the 2030 Agenda (Council of the European Union 2018, 6). But several interviewed EU officials underlined the lack of a clear articulation regarding how CCB can serve these different objectives while consistently supporting the EU's digital, technological, development, security and strategic autonomy agendas.[52] While they agreed that cyber capacity building is low hanging fruit as a mechanism for strengthening international cooperation with partners, they expressed divergent visions and expected outcomes of such actions, which at times could end up being at odds with each other.

Reflecting on the 2020-2024 Commission's objectives for "a stronger Europe in the world" and the external dimension of the objectives for "a Europe fit for the digital age" and "promoting our European way of life" (von der Leyen 2019), there is an opportunity for the newly launched EU Cyber Capacity Building Board to expand on the existing cyber policy frameworks and use the Strategic

[51] As of July 2021, the EU has established formal Cyber Dialogues that are coordinated by the External Action Service with the United States, China, Japan, Republic of Korea, Brazil, India and Ukraine.

[52] Interviews with EU officials on 10 December 2020, 11 December 2020, 17 December 2020 and 6 January 2021.

Plans of the relevant Commission services [53] to shape an **all-encompassing, coherent EU External Cyber Capacity Building Agenda** that recognises and integrates the different objectives. Such an Agenda can also help the EU make better informed and coordinated decisions on its funding in order reinforce its responsible global leadership and translate its investment into soft power. CCB, at its heart, is about supporting the cyber culture development of partner countries based on common values that make cooperation easier. Nevertheless, the EU's CCB to date has had little normative and policy influence, as the actions have rarely been designed with that in mind [54]. Amidst growing geopolitical tensions over cyberspace issues and governance, it will be necessary to pay more attention in aligning CCB with the EU's cyber diplomacy objectives.

Linked to this is the reality that cyber-related issues, and related capacity building, cannot be seen in a vacuum apart from the digital transformation, especially in light of a new wave of policy priorities relating to digital and data technologies. In the past year, the EU has adopted a comprehensive strategic policy framework, with its 'digital decade' vision (European Commission 2020a) and the '2030 Digital Compass' (European Commission 2021c), that has a strong international dimension, incorporates cybersecurity elements and sets the EU's ambition for global influence. Through '**international digital partnerships**' the EU intends to promote alignment or convergence with its regulatory norms, inter alia, on cybersecurity and trust, and shall support these partnerships with developing and emerging economies through 'digital economy packages' (European Commission 2021c, 19). It is therefore a great opportunity to ensure the **mainstreaming of cybersecurity** as part of this large exercise that has a significant digital capacity building component, both in terms of policy and infrastructure, and could help pivot cybersecurity from a niche to a mainstream theme of international cooperation.

Cybersecurity is a cross-cutting issue in the foundation of the digital economy and should be considered the 'invisible mile' for the integrity of the digital infrastructure value chain (Broadband Commission 2019, 36, 42). While at the strategic policy level, the overarching narrative of the EU's international digital cooperation exists and nominally weaves in the cyber dimension, on the ground it will be a challenge to translate these prerogatives into capacity building actions that practically incorporate and/or mainstream cybersecurity without concrete guidance. Without a clear mainstreaming strategy, there is also a risk that cyber capacity building, along with its nuances and distinct policy objectives, will be entirely subsumed by the large digital envelopes. There is also a risk of incoherence with key cyber policy objectives. Past shortfalls where EU-financed projects on ICT policy and legislation harmonisation led to the promotion of cybercrime model laws that were largely incompatible with the EU-supported Budapest Convention on Cybercrime as the

[53] See the Strategic Plans 2020-2024 of the Directorate-General for International Cooperation and Development (European Commission 2020e, 23–25, 31–32); of the Directorate-General for Neighbourhood and Enlargement Negotiations (European Commission 2020c, 24–25); and of the Service for Foreign Policy Instruments (European Commission 2020d, 15, 22–23).

[54] The case of joint EU-CoE projects against cybercrime is an outlier; they have woven in the promotion of the Budapest Convention on Cybercrime as the global framework of reference for cybercrime legislation.

global framework of reference (Pawlak and Barmpaliou 2017, 12–13) can serve as useful lessons to anticipate and avoid such risks of policy incoherence in the future.

Progressing maturity in the EU's cyber capacity building programming, design and delivery

The recognition of external cyber capacity building as a policy priority of the EU's international cyber engagement since 2013 (European Union 2013) launched a gradual yet steady momentum towards shaping a consistent approach to CCB and the maturing of the EU's programming efforts in this new field of activity. Yet, cyber issues were not a distinct priority in the complex architecture of the EU's external geographical and thematic financial instruments subject to their own medium- to long-term planning ('programming'). [55] While the EU did identify opportunities for funding regional programmes addressing cybercrime in accession and neighbourhood countries under the rule of law objectives of the related financing instruments, the maturing trajectory of the EU's cyber capacity building received a boost in 2013 with the increased use of the Instrument for Stability (IfS). [56]

IfS, and its successor Instrument contributing to Stability and Peace (IcSP), is an external financing instrument with a global scope to address, inter alia, global and trans-regional threats and, as such, has served as an incubator and testbed of niche thematic actions against global threats at the heart of the security-development nexus. In anticipation of the adoption of the EU Cybersecurity Strategy in 2013, **cybersecurity and cybercrime were spelled out as priority areas for action under IfS** in its 2012-2013 Strategy Paper and its accompanying Multiannual Indicative Programme, which allowed the launch of the joint EU-Council of Europe 'Global Action on Cybercrime' (GLACY) and the pilot project 'Enhancing cybersecurity, Protecting information and Communication networks' (ENCYSEC) in 2013. These two areas have remained priorities under IcSP, allowing the scaling up of global programmes, most notably with the projects GLACY+ in 2016 and Cyber Resilience for Development (Cyber4Dev) in 2018. The existence of this distinct financing instrument, untied to specific geography, **allowed the EU to develop a general methodological approach to cyber capacity building programming**, integrate development cooperation practices in the design of projects and test what works and what doesn't in an iterative process. This experience has informed the design of subsequent projects financed by geographical instruments both for

[55] In the EU's previous MFF covering the years 2014-2020, external action spending was linked to 11 financing instruments.

[56] CyberCrime@IPA started in 2010, covering the Western Balkan countries and Turkey, and CyberCrime@EAP I commenced in 2011 in the countries of the Eastern Partnership, both joint regional projects of the EU and the Council of Europe, implemented by the latter (Council of Europe 2021b; 2021a).

cyber-specific initiatives with a regional and/or country-specific focus [57] and for the integration of cybercrime components in actions with a broader rule of law reform objective. [58]

The maturing of the EU's cyber capacity building programming can be also seen in **institutional efforts to create methodological tools to support EU staff** in charge of cyber capacity building actions. Notably, the operational guidance on 'Integrating the rights-based approach in EU external cooperation actions addressing Terrorism, Organised Crime and Cybersecurity' (European Commission, Nicole, and Hansen 2015) offers practical advice on how to incorporate human rights safeguards across the project cycle of cyber-related actions. Moreover, the development of the 'Operational Guidance for the EU's international cooperation on cyber capacity building' (European Commission et al. 2018) articulates a comprehensive, systematic methodology to ensure the cyber-related projects are consistent with EU policies, values and principles. However, while many interviewees referred to the tools as a welcome effort to help further professionalise the EU's work in this field, they noted a gap between awareness of them and actual use, suggesting that an outreach and training effort would be opportune. [59] The impetus for creating a systematic and methodological EU CCB approach is linked to an extent to the **organisational structure** of the Commission services at the time. The unit in charge of the management of the 'global and trans-regional threats' priority of the IfS/IcSP in DG DEVCO served until 2020 as the natural central point for offering thematic expertise on cyber capacity building to EU Delegations and geographical units and connecting with relevant teams across other Commission services, as well as the European External Action Service (EEAS).

As the available financing for external cyber capacity building increased, the EU considered all the **methods of implementation** it could employ. The project approach is traditional in the case of such new fields of cooperation, and allowed the EU to start by financing pilot projects – in particular through regional and global thematic envelopes of its relevant external financing instruments – only to soon move to more mature iterations of larger programmes with multiple strands of

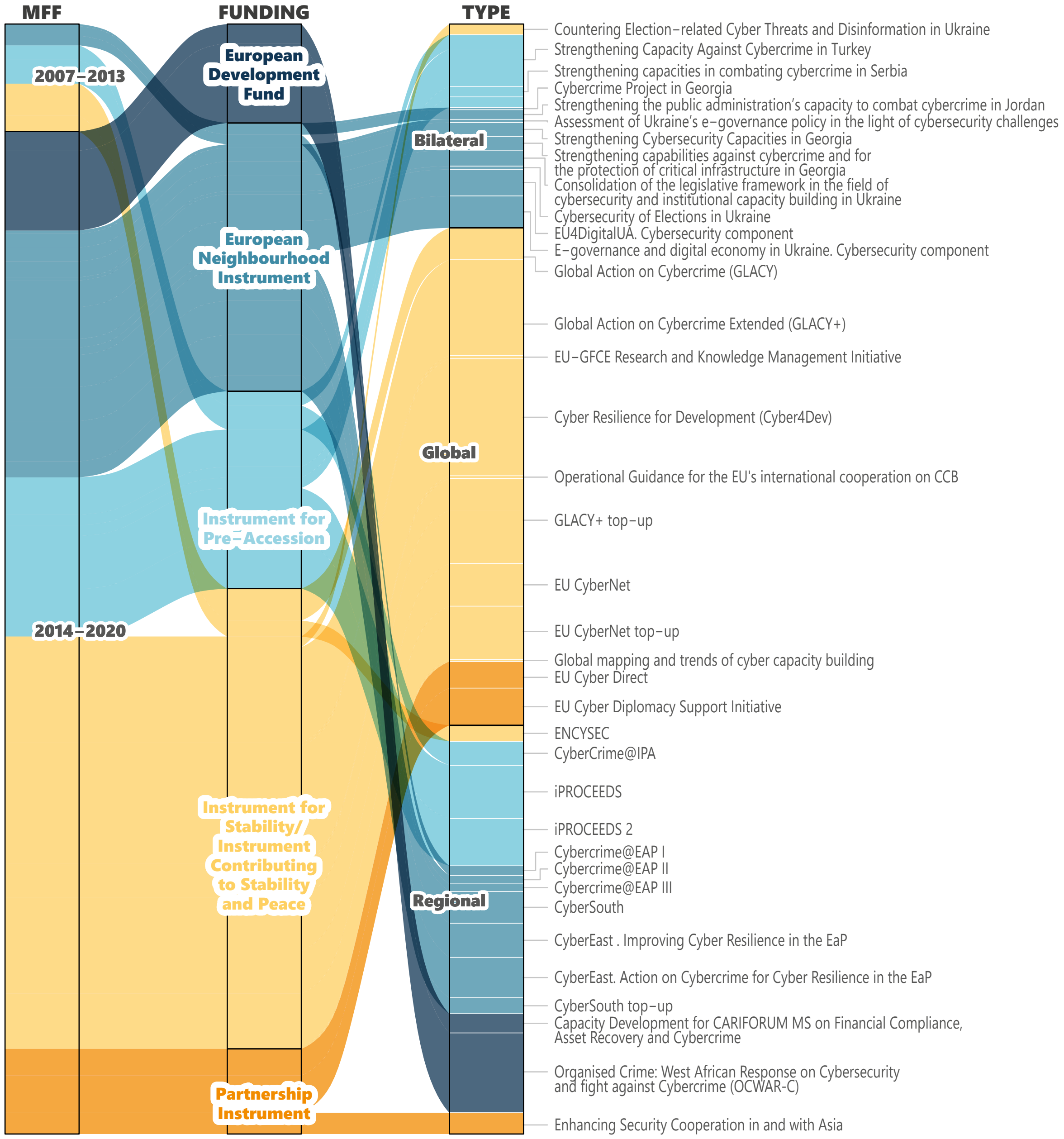
[57] Key examples of ongoing cyber capacity building projects financed through geographical envelopes include: CyberEast, CyberSouth and iProceeds 2, implemented by the Council of Europe in the Eastern Partnership, Southern Neighbourhood and Western Balkans regions, respectively, building on previous iterations (Council of Europe 2021e); the regional project 'West African Response on Cybersecurity and Fight against Cybercrime' (OCWAR-C) under a Financing Agreement between the EU and the ECOWAS Commission that is implemented by Expertise France (Expertise France 2021); and the 'Capacity Building for CARIFORUM Member States on Asset Recovery and Cybercrime' project implemented by CARICOM IMPACS (CARICOM IMPACS 2021).

[58] Indicative examples of EU-funded programmes with a cyber component or cyber-related activities include: 'EL PAcCTO' that aims to provide technical assistance to 18 Latin American states to help to enhance the Rule of Law and Citizen Security where cybercrime is identified as a priority cross-cutting issue as part of the larger criminal justice reform objectives (FIIAPP and Expertise France 2021); and 'EuroMed Police' (CEPOL 2021) and 'EuroMed Justice' (Eurojust 2021) that aim, respectively, to enhance the operational capacities of South Partner countries to fight serious and organised crime, and to foster sustainable cross-border judicial cooperation in criminal matters between the South Partner Countries and with the EU Member States.

[59] Interviews with EU officials on 10 December 2020, 11 December 2020, 14 December 2020, 6 January 2021 and 22 January 2021.

FIGURE 9. **EU CCB FUNDING**

2007-2020



Data: Authors' compilation from interviews and open-source information

work, higher complexity and longer duration. [60] [61] Linked to this is the **choice of implementing partners and available expertise for the delivery of CCB actions**. Given that the EU's original focus was on cybercrime-related actions, it built a strong partnership with the Council of Europe to finance joint programmes that strengthen the capacities of partner countries to apply

[60] Examples include the expanded scope of GLACY in 2013 to GLACY+ in 2014 that was further financed in 2017 and foreseen to get a top-up in 2021, and the continuation of projects in their next phases, such as CyberCrime@EAP I, II and III, as well as iPROCEEDS and iPROCEEDS2.

[61] To a lesser extent, the EU has been using the Technical Assistance and Information Exchange instrument (TAIEX) to offer short-term, needs-driven, tailor-made expertise on cyber issues through workshops, expert missions and study visits.

legislation on cybercrime and improve their abilities for effective international cooperation. While it also finances other implementing partners, the EU's investment in capacity building addressing cybercrime has been primarily through the Council of Europe. Since 2009, the EU has co-financed twelve projects implemented by the Council of Europe – four of which are still ongoing as extended and expanded programmes of earlier iterations. This has been possible chiefly thanks to the Council of Europe's own scaled up capacity to implement projects since the establishment of its Cybercrime Programme Office (C-PROC) in Bucharest, Romania in 2013. Over time, the EU has also developed projects with the involvement of the EU agencies and bodies as partners in CCB where their respective mandates allow for such engagement, most notably EC3 at Europol and CEPOL.

In the field of cybersecurity, the EU did not have a single obvious partner, and its approach has been to rely primarily on consortia led by EU Member State entities. This aimed to ensure projects were aligned with EU values and policies and relied upon the mobilisation of EU experts. Nevertheless, a few interviewees noted the limitations of this approach, considering that the EU's programming for cybersecurity capacity building has been piecemeal, due to a large extent to the lack of available expertise for delivering large-scale programmes. [62] In accession countries, however, where the main objective of cooperation is linked to supporting the transposition, implementation and enforcement of the EU legislation and policies, the 'Twinning' approach is a key tool. Twinning projects entail peer-to-peer institutional cooperation between EU Member States' public administrations and accession countries through the placement of resident Twinning advisors to competent ministries and authorities to strengthen their cybercrime and cybersecurity legal and institutional frameworks in line with EU standards. This instrument is also available to neighbourhood countries with the aim of approximating their national laws, regulations and quality standards to those of the EU. It is currently being used in Georgia and Ukraine.

In light of the global polarisation over cyber issues and in recognition of the limited number of implementing organisations available in the field, **the EU pushed for the creation of an EU Cyber Capacity Building Network** (European Union 2017) to bring together relevant organisations within the EU (Member States' national cyber authorities, development agencies, academia, think tanks and NGOs with cybersecurity expertise as well as relevant EU agencies) that have the EU policy and operational expertise to be utilised for EU external assistance purposes and respond to increasing capacity building needs. The network, **EU CyberNet**, (Estonian Information System Authority 2021) was launched in 2019 and is another indication of the EU's trajectory towards maturity as it tries to further build its own capacity to deliver CCB.

Looking ahead: key challenges and opportunities

This gradual maturing has not come without challenges that may extend into the future if not addressed. Markedly, several interviewees in charge of EU project design and management pointed to

[62] Interviews with EU officials on 17 December 2020, 6 January 2021 and 22 January 2021.

the fact that, in recent years, various cyber-related or adjacent policy and intervention areas, such as connectivity and digitalisation – including infrastructure, privacy and data governance, hybrid threats and online disinformation – are often bundled up together in discussions with partner countries and organisations.[63] However, the multiplication of objectives for cooperation on cyber issues is not combined with a narrative that makes the EU's value-add explicit and connects the dots with these adjacent policy fields. In their experience, **this missing overarching chapeau impacts project identification and formulation**, making it more challenging to identify opportune synergies across themes and, even more so, pre-empt potential project design pitfalls regarding the actions' policy coherence. The fast pace of the policy directions from headquarters, along with the scarcity of available external expertise, make things more challenging.[64] The EU External Cyber Capacity Building Agenda mentioned in the previous trend and foreseen in the latest EU Cybersecurity Strategy provide an opportunity to address these issues in a comprehensive manner.

The recent consolidation of six of the EU's previously stand-alone external financial instruments into the unified 'Neighbourhood, Development, International Cooperation Instrument – Global Europe' (NDICI-Global Europe) (European Commission 2021d) as the main financial instrument for the EU's external action in 2021-2027[65] is an important moment to improve the programming process overall, and to **reflect on how to leverage the opportunities this single instrument offers for pursuing more holistic and complementary cyber capacity building programming** by exploring methods of implementation and synergies that were not possible before. Tapping into these opportunities, however, requires a shift in working culture to break through silos.[66] On the one hand, as cybersecurity gains more prominence, it is likely that there will be more interest from partner countries in bilateral programmes on cybersecurity or with a cyber component, while, on the other, there is a chance to be more ambitious and explore an expanded model of cyber capacity building, including through the use of the External Investment Plan. In addition, there are potentially more opportunities for scaled-up cyber-related cooperation programmes, especially as part of digital initiatives, under the 'Team Europe' approach that is integral to the NDICI-Global Europe programming (European Commission 2021b). The 'Team Europe' approach is based on the principle of joint programming, pooling all of the EU resources by bringing together the EU and its Member States – including their implementing agencies and public development banks – as well as the European Investment Bank and the European Bank for Reconstruction and Development.

At a practical level, one challenge that persists is the **limited pool of implementing partners for cybersecurity capacity building**. The current status quo of a handful of implementers limits the EU's options for scaling up CCB funding. This is further aggravated by the difficulty implementers

[63] Interviews with EU officials on 17 December 2020, 6 January 2021 and 22 January 2021.

[64] Interviews with EU officials on 17 December 2020, 6 January 2021 and 22 January 2021.

[65] Except for pre-accession beneficiaries and overseas countries and territories, which are subject to specific instruments. The NDICI-Global Europe Regulation entered into force on 14 June 2021, with retroactive effect as of 1 January 2021.

[66] Interviews with EU officials on 14 December 2020, 6 January 2021 and 22 January 2021.

have in combining the expertise of cyber policy/legal frameworks and technical knowledge with development methodologies. As a result, this puts an extra burden on the EU programme managers for oversight, but the implications of this shortcoming, if not addressed decisively, could be more far-reaching. With CCB placed at the centre of international cyber processes at the UN and the Group of 77 that highlight the need for technical assistance, it will be a significant pitfall if the EU, along with like-minded partners, do not offer the requisite expertise for CCB, while other global players are on the ground offering large infrastructure projects.[67] Moving beyond the traditional project modality and focusing on more sustainable models of creating local and regional ecosystems of expertise may partly address this issue. Options include the pilot idea of the EU-funded LAC4, or using funding to support the development of local public-private cybersecurity hubs and ecosystems aimed at developing the requisite capabilities, skills and services at a local level.

Finally, it should not be underestimated that digitalisation and even more so **cyber issues remain relatively new areas of engagement in the EU's external action, and neither can yet claim a strong institutional capacity** or knowledge base, especially in EU Delegations. Even in EU headquarters, there has been no increase since 2015 in staff with thematic expertise in cyber capacity building across the three main Commission services managing external funds (INTPA, NEAR, FPI). While there are ongoing plans to set up relevant expert support facilities, relying extensively on outsourcing the requisite expertise could be a risk in ensuring the EU cyber diplomacy policies are appropriately reflected in relevant external programmes. For this reason, the role of the EU Cyber Capacity Building Board will be critical in enabling a joined-up approach to cyber capacity building programming, design and delivery, and could facilitate coordination and positive feedback loops that, combined, can help the EU keep up the positive trajectory of its progressive maturity in this area.

Increased commitment to improving coordination of cyber capacity building

Mirroring the global trend towards increased desire for coordination of cyber capacity building actions, the EU has shown increasing commitment to strengthening coordination efforts at the global level as well as internally, albeit with limited success. For the EU, **the coordination conundrum can be categorised into three main dimensions, which have also guided its responses to date:** First, coordination with other donors to avoid duplication of efforts that hinder efficiency and can also perpetuate the 'donor darlings' phenomenon. Second, coordination with the EU Member States and their financed initiatives. Third, internal coordination within the EU among the different services that program and manage different financing envelopes and its policy line DGs.

In an ideal world, better coordination at the strategic level before financing decisions are made, both with other donors and EU Member States, would solve a lot of the secondary coordination

[67] Interviews with EU and government officials as well as private sector representatives on 10 December 2020, 22 January 2021, 11 March 2021 and 1 February 2021, respectively.

difficulties at the stage of implementation. Yet, partner countries have shown little interest in centrally steering CCB discussions with donors, while each donor has its own financing cycle and political agendas. The knock-on effect on coordination efforts is that they largely get pushed to the stage of implementation, putting the burden mainly on implementing partners. [68]

From the outset of its systematic engagement in cyber capacity building, the EU has called for improved international coordination – namely for the development of “donor coordination for steering capacity-building efforts” (European Union 2013, 16), as well as for “streamlining and prioritising funding” (Council of the European Union 2015, 10), committing itself to “work together with other donors in this field to avoid duplication of effort and facilitate more targeted capacity building in different regions” (European Union 2017, 19). Indicative of its increased interest in this area is the **progressively elevated importance the EU has placed on cyber capacity building and its coordination** in its official Cyber Dialogues with its strategic partners. This political commitment also translated into the active support of the European Commission and the EEAS in the process that led to the creation of the GFCE in April 2015 as a CCB coordinating platform with global aspirations, of which the EU is a founding partner. Several interviewees noted that the GFCE itself has shown good potential for networking and knowledge sharing amongst stakeholders of the CCB community, while pointing to the Cybil Portal as a good starting point for setting a baseline for mapping activities globally. [69] Nevertheless, the majority of the interviewed EU staff pointed out that coordination even with like-minded donors most often stops at information sharing, not necessarily attributed to bad faith but rather to the complexity of the workings of each funder. [70]

On the internal front, the EU originally used its existing mechanisms to monitor and coordinate the financing of its cyber capacity building financing – notably the quality control consultations for the identification and formulation of new projects as well as the formal inter-service consultation, along with informal working level coordination meetings. However, several interviewees commented that the consultation and coordination dimension of the programming process was not designed to enable meaningful coordination, nor is it built around assurances for thematic experts of line DGs to input. [71]

With the increased number of CCB projects from different parts of the Commission engaged in external action, there was recognition of a need to have a **mechanism that would “support effective coordination of EU-funded external cyber capacity building activities**” (Council of the European Union 2018, 10). This has led to the mandating of the EU Cyber Capacity Building Network (European Union 2017, 19) that was launched in 2019.

[68] Interviews with project implementers on 10 and 15 December 2020 and 23 March 2021.

[69] Interviews with EU officials on 10, 11 and 14 December 2020; and with government officials on 22 and 27 January, and 11 March 2021.

[70] Interviews with EU officials on 10, 11 and 14 December 2020.

[71] Interviews with EU officials on 10, 11, 14 and 17 December 2020 and 22 January and 24 June 2021.

While the EU CyberNet has focused on bringing together the implementing partners of EU-funded cyber capacity building projects to enable coordination and knowledge exchange amongst them, many interviewees expressed frustration over the lack of an **internal central function that would enable a more efficient, streamlined and effective coordination of the EU's cyber capacity building**. [72] In response to this fragmented institutional structure, the 2020 EU Cybersecurity Strategy has called for the institutional solution of an EU Cyber Capacity Building Board "to encompass relevant EU institutional stakeholders, and to monitor progress, as well as the identification of further synergies and potential gaps […] support enhanced cooperation with Member States, as well as with public and private sector partners and other relevant international bodies to ensure coordination of efforts and avoid duplications". While the Board is yet to be fully operational, it further demonstrates the EU's increasing commitment to find ways to address the challenge of CCB coordination at multiple levels.

Looking ahead: key challenges and opportunities

Digital transformation is a growing international cooperation priority not only for the EU but also for other actors, both like-minded and non-like-minded, who are already rallying to push their agendas with their partners globally, including through capacity building initiatives. Organic growth of the CCB ecosystem makes capacity building coordination among donors and stakeholders more challenging. These challenges are only made more complex by adding the layer of increased digital cooperation across the board with 'hidden' cyber components, or the growing spill over of cyber-related activities of adjacent areas. The creation of the EU Cyber Diplomacy Network could play a significant role to this end, while the use of existing global mapping tools such as the GFCE's Cybil Portal will be very useful as a starting point, especially if its members and partners see the value in contributing.

Internally, the organisational structure of the Commission services and their respected mandates along with the EEAS and the EU Delegations are not set up for effortless internal coordination. Yet, there are opportunities to learn from good practice and tools used by other fields of the EU's activity. For example, the project CT Morse has been a great resource in supporting coordination and monitoring in the areas of counterterrorism and preventing and countering violent extremism.

Recommendations

Pivot to a next generation 2.0 international cyber capacity building

- The upcoming EU External Cyber Capacity Building Agenda foreseen in the 2020 EU Cybersecurity Strategy should reflect on the scope and objectives of the EU's future cyber capacity building in line with its leading geopolitical ambitions as a global player. It would be necessary to

[72] Interviews with EU officials on 10, 11, 14, 17 and 22 December 2020, 6 and 22 January 2021 and 24 June 2021; as well as with a project implementer on 15 December 2021.

start with mapping the EU's lessons learnt from CCB to date to enable a positive feedback loop for the Agenda's development. Building on these, and guided by existing strategies, the Agenda should create a holistic, harmonised narrative that elaborates on the different objectives that external cooperation on cyber issues can play with clear deconflicting guidance.

- The Agenda should consider the objectives and requirements of each available financing stream to be able to match overarching priorities with the potential funding across key themes: cybercrime, cyber resilience, cyber diplomacy, cyber mainstreaming in digital and international cooperation and cyber defence in light of the new European Peace Facility.

Enable smart cyber capacity building programming and implementation

- Invest in knowledge tools to enable better programming, identification, formulation and implementation of CCB actions. Notably, update and digitalise the EU Operational Guidance to reflect the changes and additions in the relevant pillars of CCB activity, and also elaborate concrete methods and tools on how to integrate and mainstream cybersecurity across digital programming. In addition, develop guidance on how to address the cross-cutting issues of gender and environment in CCB programming.

- Create a modular training programme for EU staff in HQ and EU Delegations on cyber policies, CCB design and the connection with other policies. Involve senior management to improve awareness and understanding of CCB.

- Develop a training programme for implementing partners to ensure the design and delivery activities are aligned with EU values and policies in cyber-related themes.

- Consider how to integrate more strategically the role of the private sector in CCB and create a framework of available engagement options for the private sector in CCB to increase awareness, transparency and boost public-private cooperation. For example, given that any cybersecurity ecosystem relies heavily on private-sector infrastructure and services, for external cooperation programmes, the EU could reflect on lessons learnt from areas of development that deal with investment climate and private sector development, and integrate these in the next generation of CCB. This could be pursued by creating synergies with methods of implementation that had not been pursued before, such as utilising the European External Investment Plan (EIP) especially for combining infrastructure development.

- Expand the use of implementing partners by leveraging more EU Executive Agencies, fostering stronger cooperation with regional organisations and more systematically integrating civil society organisations and local partners in the implementation of CCB actions.

Untie the cyber capacity building coordination knot

- Invest in a systematic mapping of its cyber-related external actions that will improve the EU's own situational awareness about its financing and enable better internal coordination and synergies. This can expand to the creation of guidance or a reporting key for tagging projects with a cyber dimension, distinguishing between (a) mainstreaming cybersecurity in digital projects and (b) cyber-specific components. The EU Cyber Capacity Building Board can advise to this end, while the EU CyberNet could serve the mapping function.

- Use the Board to connect with the network of EU MS Cyber Attaches of the Horizontal Working Party on Cyber Issues (HWP) of the Council of the EU in order to have a better visibility of Member State-funded projects.

- Continue engagement with the GFCE and support its mission to strengthen international collaboration in CCB. Consider assigning PoCs with the relevant expertise for each GFCE Working Group; and use the existing projects, such as the EU CyberNet, to feed information on the EU projects into the Cybil Portal.

- Systematise working-level exchanges on CCB with key partners, especially with larger donors and those countries with which the EU has bilateral Cyber Dialogues.

PART II: SCENARIOS

Scenario narratives are a future studies tool to help policymakers think through choices, opportunities and challenges. The strength of a scenario is in its ability to help users consider how variables could interact in the future and what their role in that future might be. They are hypothetical narratives that unfold in different directions, rather than an attempt to predict a single future.

When developing each scenario, we considered how the cyber capacity building trends would interact with seven megatrends: the changing nature of work and the workforce, managing technological change (including AI), power shifting between states and away from states, the changing security paradigm (proliferation of advanced weapons), individual empowerment and education, a chaotic information space / fake news and the challenge to the rules-based international system (which is related to the shifting power megatrend).

Although there may be some short-term positive moves in US-China relations, the overall trend is one of increasing strategic competition. Global economic power is shifting Eastwards and Southwards. The rules-based international system is under pressure, with new international governance structures and alliances emerging to fill the gap. Non-state actors are growing in influence. There is increased risk of conflicts within states and between states and non-state actors. The shifts in power and end of hegemony create an atmosphere of political uncertainty and concern.

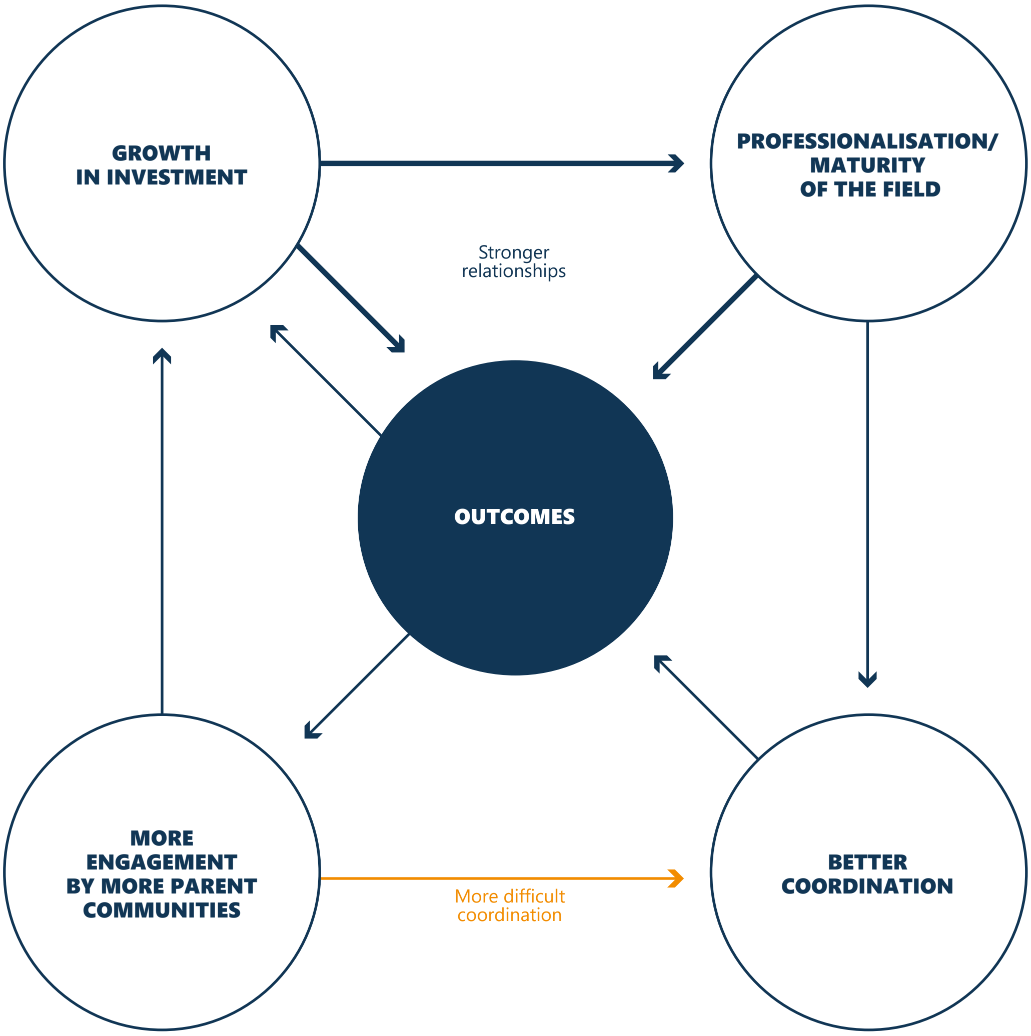
In high income countries, the fourth industrial revolution is well established. Individuals, companies and governments are regularly using what we currently describe as emerging tech: machine learning, powerful cloud computing, cyber-physical systems and the Internet of Things. With this comes easier access to spyware and offensive cybersecurity capabilities for state and non-state actors. Although three-quarters of the world's population are online, the digital divide in terms of how tech is used has widened. Furthermore, advancing technology exacerbates global challenges such as job losses to automation, the ease of making high-quality deep fakes and more invasive surveillance. These disbenefits will contribute to a popular and regulator 'techlash' that seeks tighter regulation and larger fines for tech firms.

Advancing technology will drive changes in work, education and individual empowerment. It will enable a continuation of the remote working trend that was accelerated by the coronavirus pandemic. This in turn will fuel greater diversification of the workforce, with inclusion of more women and people with physical impairments and greater international hiring. New learning models will emerge, facilitated by online education. People will have more opportunities for monitoring their own health and disease susceptibility.

INTERACTION BETWEEN CYBER CAPACITY BUILDING TRENDS

When developing the scenarios, we created a simple model for how the four trends of cyber capacity building interact with one another. Growth in investment – our proxy for the growth of the

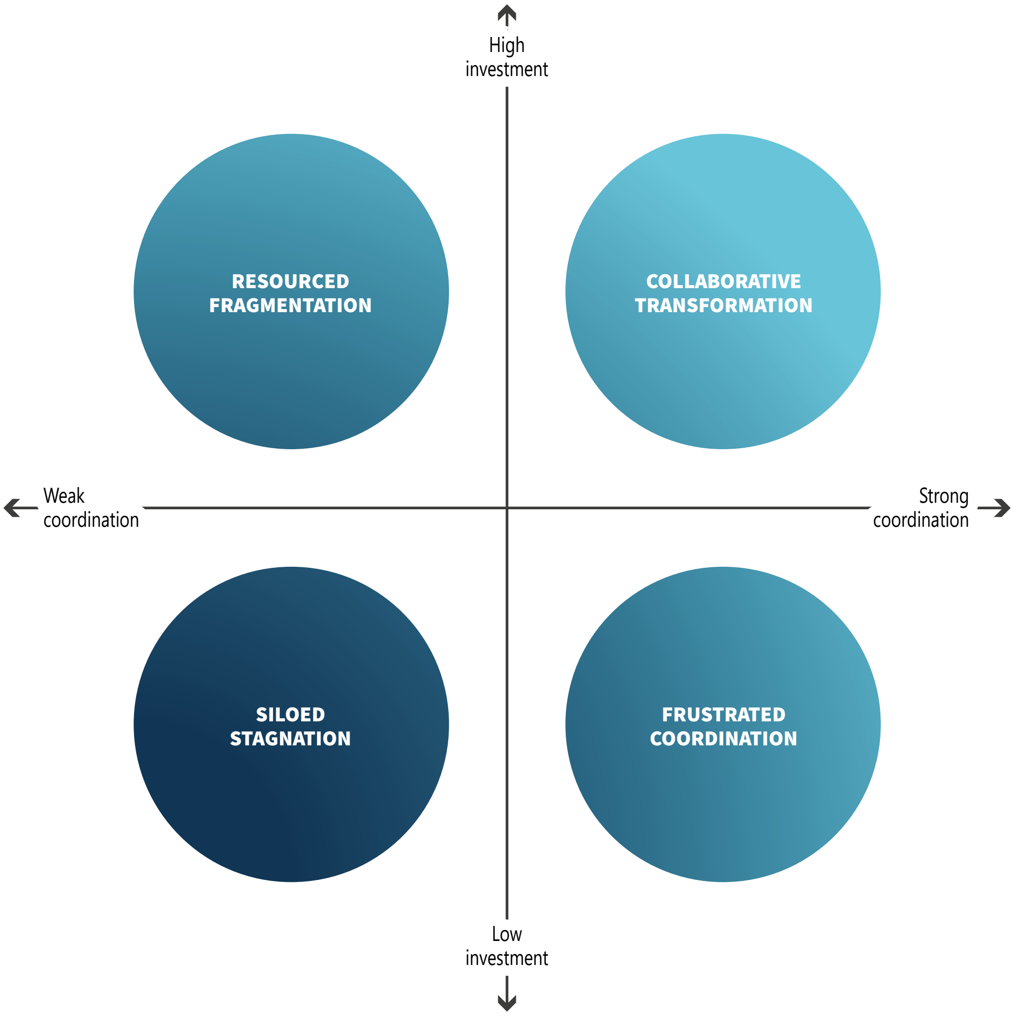
FIGURE 10. **INTERACTION BETWEEN CYBERCAPACITY BUILDING TRENDS**



field – improves overall project outcomes and professionalisation. Professionalisation improves outcomes and coordination. Coordination improves outcomes. Deeper engagement by more parent communities leads to more investment, but it also makes coordination more difficult. More positive outcomes attract more communities to engage in cyber capacity building, leading to more investment.

As mentioned in the introduction, the two trends we selected for our axes were the growth of the field and the level of coordination. We used investment in capacity building as a proxy for the field's growth. In selecting these two trends we considered the factors that are within the control of the EU and how trends relate to each other. By combining the two trends we generated the four scenario permutations, which we call Siloed Stagnation, Resourced Fragmentation, Collaborative Transformation and Frustrated Coordination.

FIGURE 11. **FUTURE SCENARIOS GRID**



SCENARIO 1: SILOED STAGNATION

Our first scenario is called ***Siloed Stagnation*** because it is marked by little new investment and weak coordination. This results in negligible change in professionalisation and parent community involvement in CCB. The field looks much as it does today, grappling with the same challenges and having the same conversations.

Siloed Stagnation implies that the fast pace of investment increase that cyber capacity building has experienced over the past ten years will slow. This is likely to happen if funding from the foreign policy community hits a ceiling. Foreign ministries had sufficient resources to give the early years of cyber capacity building a boost, but their budgets are not large enough to fund the next phase of expansion. In the *Siloed Stagnation* world other communities are not sufficiently engaged to bring in a new wave of funding. The growth momentum of the early years has stalled.

Turning to the megatrend context, the good news is that in this scenario there has not been a global cybersecurity disaster of sufficient size to spur a new wave of interest and investment in cyber capacity building. The bad news is that the political and technological megatrends have resulted in a steady increase in cyber risks. The conditions for a cyber incident with negative global impact are all present, and growing each year, but politicians have not taken any greater interest in cooperating internationally to change this.

The cyber capacity gap between countries, and within countries, widens fastest in the Siloed Stagnation scenario. This contributes to the growing disquiet about the downsides of advancing technology. There is a global movement that pushes back against the pace of technological change, which it argues has widened divisions within society and left people unhappy, unsafe and unemployed. Governments come under pressure to respond to this movement and turn to regulation as a visible sign of action and way to slow the shift of power from states to global companies. Cyber capacity building is barely mentioned by political leaders as a solution, because there has been little evidence published to show it works, and regulation gets more attention than behind-the-scenes risk mitigation.

SCENARIO 2: FRUSTRATED COORDINATION

The ***Frustrated Coordination*** scenario has many similarities to *Siloed Stagnation*, because growth in investment is at the same low level and this is the most significant driver of change. However, in this future there is a high level of coordination. This coordination has occurred without the direction or assistance of organisation heads and politicians, as their involvement is only triggered in the high investment scenarios. Instead, the coordination has been driven from the bottom up, by cyber capacity building practitioners motivated by maximising the effectiveness of their work and eliminating duplication.

In the *Frustrated Coordination* world there has been some improvement in professionalisation, because practitioners who are highly committed to coordination are also taking other steps to improve their working methods and apply lessons from other communities. However, this improvement is limited by low growth in investment. With low investment, there is low growth in the number of staff working on cyber capacity building and the present state of overstretch continues. The overstretch means there is little time for personal development, going the extra mile to ensure good coordination and volunteering to assist coordination processes.

The mix of communities in cyber capacity building, and the depth of their involvement, in *Frustrated Coordination* are very similar to those in *Siloed Stagnation*. The fact that there has been no change in this mix helps a little with the improved coordination, because there is no need to adapt to additional diversity. Lessons can be learnt from the current situation that will still apply in the *Frustrated Coordination* world.

The relationship between the cyber capacity building trends and the megatrends is the same as in the *Siloed Stagnation* scenario, and this is the cause of the frustration. The practitioners of cyber capacity building have put in the effort to improve the efficiency and effectiveness of their field, but it has not resulted in a narrowing of the cyber capacity gap, because of the low investment growth. They have built and refined an engine for better global cyber capacity, but it is not being provided with fuel.

Frustrated Coordination is not a stable scenario, because it is built upon a large number of individuals volunteering and going above and beyond what their managers expect. When people who go the extra mile for coordination move on, there is a significant chance their successors will be not exhibit the same commitment to it. A stable scenario could be achieved if there were sufficient resources for international coordinating mechanisms to have secure funding and a high enough staff-to-projects ratio to allow teams to do more than the bare minimum of coordinating, communicating and knowledge sharing. The quantity of investment needed for this is not present in the *Frustrated Coordination* world. Over time, *Frustrated Coordination* is likely to either fall back to the *Siloed Stagnation* or progress to *Collaborative Transformation*.

SCENARIO 3: RESOURCED FRAGMENTATION

The ***Resourced Fragmentation*** scenario is one in which there has been considerable growth in investment, but little improvement in coordination. This investment has come from deeper engagement in cyber capacity building by a range of communities, but primarily by those concerned with defence and stability. The level of coordination in this scenario is low because these communities work in silos, pursuing their own goals. There is also active competition and interference between rival states.

Looking at how individual communities act in the *Resourced Fragmentation* scenario, we start with defence. The leaders of several countries have responded to the global uncertainties and tensions by instructing their militaries to speed preparations for their own and their allies' readiness to face cyber threats. The defence community step up their international cybersecurity assistance and exercising accordingly. They start taking a more active interest in the resilience of civilian-governed areas such as critical national infrastructure. Speed is the order of the day and they conclude they could work faster on their own or with just a few close allies. A few countries are experimenting with using private military companies and volunteer units in their international cybersecurity assistance. Nobody is sure what they are doing or if they are effective. However, rumours about them are rife and they make it harder to attribute and understand opponent intent.

The development community follow what is happening in the political and security space closely, worried that their projects, almost all of which are now ICT-dependent, are at greater risk from insecurity and cyber threats. They invest more in conflict prevention and securing the ICT systems their projects have developed or are dependent upon. They are concerned by the securitisation of ICT issues by the defence community.

Ministries of foreign affairs are increasing their spending on projects that either strengthen the rules-based international system or help them gain influence at a critical time for international diplomacy. As concern about state-backed cybersecurity attacks rises, cyber capacity building assistance becomes one of the most frequently offered and requested types of bilateral assistance. Many countries want to remain neutral and receive assistance from all camps, but they are under pressure to pick a side.

Global tech companies share the concerns of the other communities, but they are benefitting from being an increasingly important part of any solution. Power is shifting their way. Politicians feel their power slipping away and suspect that the private sector's 'move fast and break things' approach has contributed to the current climate of social and geopolitical tension. They respond with tighter regulation. Companies increase investment in cyber capacity building activity to demonstrate corporate social responsibility, win allies in resisting regulation and gain influence in whatever new international political structures and alliances might emerge should the old rules-based systems break down.

Civil society and the technical community try to be a voice for peace in uncertain times and warn against the signs of zero sum thinking and bellicose rhetoric. They more actively engage in international campaigns and people-to-people networks and projects. They are wary of receiving international support for capacity building given the political backdrop of international mistrust. Several governments tighten the rules on NGOs receiving foreign funding.

The projects of different communities often cut across each other and, as described, their approaches and unintended consequences are causes of concern. At its worst, some communities see others as part of the problem and certainly not as potential partners for cooperation.

This world is also fragmented in that divisions between the US and Russia/China, and their respective like-minded groups, have grown rapidly. The memory of joint projects that worked across this divide has been forgotten. The groups now actively seek to undermine each other's programmes, for example by discouraging middle ground countries from working with the other side or by publishing sensitive or fake information about each other's projects. Furthermore, the secrecy around cyber capacity building and the military's increasing role in it contributes to the megatrend of political mistrust.

The combined effect of this lack of alignment and coordination is that there are duplication, conflicting activities and a lower return on investment. There is also a high concentration of projects in 'donor darling' countries that are considered important because they are threatened by state actors, have political importance as a middle-ground countries or are the beneficiary of large 'digital for development' programmes.

The weak coordination mechanisms that exist are unable to do much to mitigate any of these coordination challenges and bring communities or rivals together. In the Resourced Fragmentation scenario, there was not a sustained period of investment in global coordination mechanisms. By the time senior decision makers spot the problematic fragmentation of cyber capacity building, it is too late to do much about it. It would have taken years of work to firmly establish the sort of principles and relationships that could, for example, limit the use of private military companies in cyber capacity building, create a common international curriculum for digital forensics training or keep companies and governments aligning their projects even when they are in the midst of fierce disputes about regulation. In the *Resourced Fragmentation* scenario this was a missed opportunity.

Reaching a *Resourced Fragmentation* world only required two things: a small shift in the level of strategic mistrust resulting from geopolitical megatrends, and for there to be no mechanisms or well-established cooperative norms that stop this cascading down to the attitudes and actions of the capacity building communities and actors.

SCENARIO 4. COLLABORATIVE TRANSFORMATION

In our final scenario, ***Collaborative Transformation***, there has been both significant growth in investment and much improved coordination. Professionalisation improves as a result of increased funding and in line with the improved coordination. A broad range of communities deepen their engagement in capacity building, and the development community in particular engages more.

In *Resourced Fragmentation*, concern about cyber threats associated with growing geopolitical mistrust and uncertainty drove the increased investment, in a ‘security from’ paradigm. In contrast, in *Collaborative Transformation*, investment growth is driven primarily by the goal of making the benefits of technology and digital development safe, resilient and accessible, in a ‘security for’ paradigm.

Global public concern about digital equity and safety – the techlash – is responded to by a handful of politicians, philanthropists and activists with a positive vision for safe digital access for all. This agenda is far from new, but there is greater public interest in its aims and researchers have built an evidence base that allows effective types of intervention to be identified and the enabling role of cyber capacity building to be understood. The conditions exist for high-profile change leaders to work with development agencies, international financial institutions, philanthropists and corporate social responsibility funds to put renewed effort behind digital access and equity, with an emphasis on people-centred safety and resilience.

The megatrend of political instability and mistrust is still present, and the defence community increase their engagement in capacity building. However, the centre of gravity and majority of funding for cyber capacity building lean towards the development community. Principles of cyber capacity building gain traction and influence the design of most projects. A large part of the cyber capacity building community signs up to a set of global goals.

The communities and most actors involved in cyber capacity building see the benefits in coordination. They support and participate in coordinating mechanisms and forums. Although there is heightened global mistrust, cyber capacity building is seen as mostly serving goals that have wide international support. Therefore, while coordination is closer within like-minded groups of countries, it also spans across them.

Most coordination occurs among specific types of projects, for example, the policing and justice community coordinate their cybercrime training. However, there are also coordinating events that bring together the whole cyber capacity building community and adjacent communities, such as ICT4Development. It is also common to find cyber workshops and side events happening within the events of adjacent communities. The funding and interest are present to build up a supporting ecosystem of conferences, publications, academics and implementers.

There is nothing inherently unstable about the *Collaborative Transformation* scenario, as there was in Frustrated Coordination, but it is vulnerable to shifts in the megatrends: too little global concern about the state of digital equity and safety and funding may dry up; too much and ambitious international digital projects could become too controversial to attempt. Securing investment is also dependent upon achieving impact, being able to measure that impact and building an evidence case around it. Public and political desire to tackle a problem will only drive investment if cyber capacity building can offer demonstrably effective solutions. As investment goes up, so must the measurable benefits. In the *Collaborative Transformation* world this has been achieved, but it will need to be sustained.

CONCLUSIONS

This report has shown that although international cyber capacity building is a relatively young field, it has accumulated a sufficient track record to identify trends. There has been little published on these trends and busy practitioners have limited time to reflect upon them holistically. We therefore believe that this trend analysis, and its potential to form the basis of a scenarios exercise, could make a valuable contribution to strategic planning. Such strategic planning is currently taking place within the EU following publication of the EU's Cybersecurity Strategy in the Digital Decade. However, we also encourage other members of the cyber capacity building community to use the trends and scenarios in their own planning.

The main conclusion we draw from our findings is that a broad range of communities with an interest in a trusted, open and resilient digital future should be investing in cyber capacity building. And with part of that investment, we recommend supporting coordination of the field. The pace of the field's growth, and the gap between the aspiration for coordination and the implementation, suggest there is a narrowing window of opportunity to ensure that international cyber capacity building has a coherent architecture, with principles and coordinating processes that connect and serve all its parent communities. Without coordination we may be on a path to a future of *Resourced Fragmentation* and the negative consequences that could accompany this.

Any investment in cyber capacity building should be based upon an informed expectation of what this will achieve. We heard from all our interviewees examples of successful projects strengthening a free, open, peaceful and secure digital future. However, anecdotal evidence will not be a sufficiently strong foundation for the next phase of cyber capacity building's growth. For better evidence-based programming, and a compelling narrative for investment, the field will need more studies of project impact. As described in the monitoring and evaluation section of the report, there is a strong interest in collecting this evidence of impact, and we suggest this is the next priority for research by the EU and other funders. We also see a need for further research into cyber capacity building within each parent community and into the experience and perspectives of low- and middle-income countries.

ANNEX 1. LIST OF INTERVIEWS

A total of 59 interviews were conducted between November 2020 and August 2021 with representatives of the following 50 organisations.

	Organisation
1	Africa Cybersecurity Resource Centre (ACRC)
2	African Union Commission
3	APNIC Foundation
4	Australian Department of Foreign Affairs and Trade
5	Council of Europe
6	Cyber Security Agency of Singapore (CSA)
7	Cybersecurity Capacity Centre for Southern Africa
8	DAI
9	Dutch Ministry of Foreign Affairs
10	Estonian Ministry of Foreign Affairs
11	EU CyberNet
12	European Commission, Directorate-General for Migration and Home Affairs (DG HOME)
13	European Commission, Directorate-General for International Partnerships (DG INTPA)
14	European Commission, for Neighbourhood and Enlargement Negotiations (DG NEAR)
15	European Commission Service for Foreign Policy Instruments (FPI)
16	European External Action Service (EEAS)
17	FireEye
18	Forum of Incident Response and Security Teams (FIRST)
19	German Federal Foreign Office
20	Global Affairs Canada
21	Global Cyber Security Capacity Centre (GCSCC)
22	Global Forum on Cyber Expertise (GFCE)
23	Global Forum on Cyber Expertise Pacific Hub
24	Global Partners Digital
25	Hewlett Foundation
26	Indian Ministry of Economy, Trade and Industry

27	Inter-American Development Bank
28	International Telecommunication Union (ITU)
29	INTERPOL
30	Israel National Cyber Directorate
31	Japan International Cooperation Agency (JICA)
32	Japan National Center of Incident Readiness and Strategy for Cybersecurity (NISC)
33	Kaspersky
34	Korea Internet & Security Agency
35	KPMG
36	Microsoft
37	North Atlantic Treaty Organization (NATO)
38	New Zealand Ministry of Foreign Affairs and Trade
39	New Zealand CERT
40	Organization of American States
41	Palo Alto Networks
42	Sberbank/BiZone
43	South African Department of International Relations and Cooperation
44	Swiss Federal Department of Foreign Affairs
45	The World Bank
46	UNIDIR
47	United Kingdom Foreign, Commonwealth & Development Office
48	UNODC
49	US Department of Defence
50	US State Department

ANNEX 2. MEGATRENDS COMPARED

Theme	UK DCDC (16 Focus Areas)	US NIC (4 Megatrends)	EU Foresight (1 4 Megatrends)
Climate change	Increasing disruption and cost of climate change: The cost of climate change to governments and societies will increase and, as time passes, mitigation measures will become increasingly complex and expensive to implement.		Climate change and environmental degradation: Anthropogenic greenhouse gas emissions are continuously increasing, largely driven by economic and population growth.
Resources	Increasing demand and competition for resources: Increasing world population and rising living standards are increasing demand on all resources, including food and water, energy and rare earth materials.	Food, Water, Energy Nexus. Demand for these resources will grow substantially owing to an increase in the global population. Tackling problems pertaining to one commodity will be linked to supply and demand for the others.	Aggravating resource scarcity: Global demand for materials has increased ten-fold during the 20th century and is set to double again by 2030, compared to 2010. Demand for water, food, energy, land and minerals will continue to rise substantially.
Demographics	Managing demographic change: Rates of migration are likely to increase as transport becomes easier and cheaper to use and populations in many parts of the developing world grow. The rate of urban growth is likely to outstrip the capacity of governments in many developing countries. An ageing population is likely to be a key issue in Europe and East Asia as current models of employment, health/social care and retirement may become unsustainable.	Demographic Patterns. The demographic arc of instability will narrow. Economic growth might decline in 'ageing' countries. Sixty percent of the world's population will live in urbanised areas; migration will increase.	Increasing demographic imbalances: By 2030, the world's population is estimated to reach 8.5 billion, while getting older and increasingly urban. Change will be uneven across regions, with rapid population growth in many still-developing economies, but stalled, or shrinking, populations in many developed countries Continuing urbanisation: By 2030, urban population share is expected to reach 60% and 68.4% by 2050. Much of the urban population growth is expected to take place in Asia and Africa.

Nature of work and workforce	Greater automation and an increasingly diverse workforce: By 2050, machines will play an increasing role in the workplace. The workforce, particularly in developed countries, is likely to include more women, older people and people with physical impairments or cognitive differences, such as autism. In militaries, there may be a shift in the balance between the components of fighting power with an increased use of machines in many combat functions previously performed by humans.		Changing nature of work: Digitalisation and hyperconnectivity, new generations entering the workforce and older generations working longer are changing the forms of employment, career models and organisational structures.
Inequality	Rising inequality, reducing social cohesion and fragmented societies: Whilst inequality between countries has declined, inequality within countries has increased, with the gap between the haves and have-nots increasing in terms of income, wealth, education, social mobility, prosperity and political advantage. If left unchecked, inequality could lead to instability.		Diversifying inequalities: Income inequality among countries has been decreasing, while that within countries is increasing.
Crime and extremism	Increasing threat from crime and extremism: There is a strong correlation between violence and extremism, and corruption, organised crime and state fragility. The network of organised criminal groups is global, fuelling conflict and connecting conflict areas to our home countries.		
Information space / Fake News	An expanded and unregulated information space: An increasingly expanding, unregulated information space (blurring between fact and opinion, and between real and virtual), where there is little or no quality control, combined with the echo chamber effect, will make individuals more susceptible to misinformation and/or radicalisation. Ultra-high speed, ultra-agile networks of interacting smart devices will present societal, organisational and personal challenges, which could potentially be exploited by malign actors.		
Managing technological change (including AI)	Managing technological change: The rate and impact of technological change will be in part cultural (societies' capacity to absorb, and demand for, technological change) and in part technological. The interplay and layering of rapid technological advancements make prediction extremely challenging and the spread of technology will make it harder to preserve a competitive advantage. Harnessing artificial intelligence. As more devices and people are connected through the Internet, the volume and variety of data created and the speed at which it is gathered and analysed will increase. This will be important for developing and using artificial intelligence and machine-learning algorithms. Applications of artificial intelligence will enable machines to develop perception and reasoning, solve problems, learn and plan. Artificial intelligence will also improve the management and verification of data, data analysis and data integration.		Accelerating technological change and hyperconnectivity: Advancements in genetics, nanotechnology, robotics and artificial intelligence, photonics, quantum and other emerging technologies and the synergies among them are accelerating.

Human enhancement	Understanding human enhancement: Human enhancement technologies, including gene editing, physical and cognitive prostheses and pharmaceutical enhancement, are nascent now and their development over the next 30 years is likely to offer profound expansion of the boundaries of human performance.
Affordability / Prices	The challenge of affordability: Competing priorities will make the affordability challenge ever starker and necessitate harsh choices. Economic growth could become ever more elusive and countries are likely to spend less on defence unless there is a clear and present threat to the state. Sectors of fast technological change (such as defence) will require an increased share of funding due to rapid obsolescence and high replacement costs.
Rules-based international system	Adaptation of the rules-based international system: The world order is changing and current rules, norms and institutions are being increasingly challenged, as many believe the current system is biased in favour of the West. Interstate competition (and potentially conflict) may be more about defending old or new 'rules' as if they were a strategic interest in themselves.
Competition in global commons	Increasing competition in the global commons: Nations are becoming increasingly reliant upon capabilities and infrastructure that are dependent upon access to the global commons (cyberspace, the oceans, polar regions and space). Maintaining freedom of action in the global commons will thus be a vital objective for governments. Governance will continue to be a contentious issue as increasing levels of activity in the global commons could lead to a rise in competition, and possibly conflict.

Power shifting between states and away from states	Erosion of state sovereignty: The nation state is expected to remain the primary actor in shaping societies and in global politics for at least the next 30 years. However, state authorities may struggle to cope with the rate of change, level of uncertainty and the growing demands of their increasingly diverse populations. States will face increased competition in the provision of public services that have traditionally been the responsibility of governments and will be confronted by emerging non-state actors both domestically and internationally. An expanding competitive space: As the balance of power shifts, competition between states and other actors is likely to intensify and become ever more persistent. Conflict will be most likely where relative power differentials are greatest or when power is contested or redistributed. The number of intra-state and non-state conflicts is increasing and the boundary between war and peace is becoming increasingly blurred. However, the level of interconnectedness and dependencies could increase the cost of armed conflict. Actors will, increasingly, use a hybrid approach to warfare and confrontation below the threshold of armed aggression, going beyond military and economic activities and opening up new arenas of conflict, including space, cyberspace, sub-oceanic and, potentially, augmented and virtual reality.	Diffusion of Power. There will not be any hegemonic power. Power will shift to networks and coalitions in a multipolar world.	Increasing influence of new governing systems: The expanding influence of non-state actors, the emergence of a global conscientiousness, the prominence of social media platforms and internationalisation of decision making are forming new, multi-layered governing systems over traditional decision-making structures. Expanding influence of the East and South: The shift of global economic power from the established advanced economies in North America, Western Europe and Japan towards the emerging economies in the East and South is set to continue.
Changing security paradigm (proliferation of advanced weapons)	Increasing proliferation of weapons of mass effect. The number of nuclear-armed states could rise and increasing investment in tactical nuclear weapons and electromagnetic pulse weapons will increase the risk that nuclear weapons are used. The cost of developing chemical, biological and radiological weapons is likely to decline and advances in genetics and biological sciences have increased the risk of their use through new delivery mechanisms that will make detection hard.		Changing security paradigm: The emerging security paradigm is framed by new asymmetrical warfare, increasingly easy access to increasingly powerful weapons, violent extremism, conflicting motivations and a relatively chaotic organisation of the parties involved
Individual empowerment and education		Individual Empowerment. Individual empowerment will accelerate owing to poverty reduction, growth of the global middle class, greater educational attainment, widespread use of new communications and manufacturing technologies, and health care advances.	Diversification of education and learning: New generations and hyperconnectivity are rapidly changing both educational needs and modes of delivery.

Health gains and challenges	Shifting health challenges: Advancements of science and better living standards have increased the opportunity to live longer and healthier lives and reduced the incidence of infectious diseases. However, obesity, malnutrition, antimicrobial resistance and non-communicable diseases are increasingly becoming the health burden of our century.
Migration	Increasing significance of migration: While the share of international migrants in the world population has not grown significantly over the past decades, the significance of migration as a social and political concern has intensified significantly.
Consumerism	Growing consumerism: By 2030, the global middle class is expected to reach 5.3 billion people. This means an additional more than 2 billion people with increased purchasing power. Most of this growth will be in Asia.

ANNEX 3. NOTES ON CYBER CAPACITY BUILDING FUNDERS

Annex 3 is contained in an accompanying working document.

REFERENCES

Africa Cybersecurity Resource Centre. 2021. 'Africa Cybersecurity Resource Centre (ACRC) for Financial Inclusion'. Africa Digital Financial Inclusion Facility. 9 March 2021. http://www.adfi.org/projects/africa-cybersecurity-resource-centre-acrc-financial-inclusion.

Agrafiotis, Ioannis, Maria Bada, Paul Cornish, Sadie Creese, Michael Goldsmith, Eva Ignatuschtschenko, Taylor Roberts, and David M. Upton. 2016. 'Cyber Harm: Concepts, Taxonomy and Measurement'. *Saïd Business School WP* 23 (August).

Aiken, Klée, and Cherie Lagakali. 2019. 'Mapping Cyber Capacity Building in the Pacific'. https://www.kleeaiken.com/blog/2019/12/9/mapping-cyber-capacity-building-in-the-pacific.

Australia, Department of Foreign Affairs and Trade. 2021. 'Meet Our Partners'. Government Organisation. Department of Foreign Affairs and Trade. 2021. https://www.dfat.gov.au/international-relations/themes/cyber-affairs/cyber-cooperation-program/Pages/meet-our-partners.

Barbero, Fabio, and Nils Berglund. 2021. 'Cybersecurity Capacity Building and Donor Coordination in the Western Balkans'. https://www.dcaf.ch/sites/default/files/imce/Events/CybersecurityConference_DiscussionPaperPanel%203_CapacityBuildingDonorCoordination.pdf.

Broadband Commission. 2019. 'Connecting Africa Through Broadband: Digital Moonshot for Africa'. https://www.broadbandcommission.org/Documents/working-groups/DigitalMoonshotforAfrica_Report.pdf.

Calandro, Enrico, and Nils Berglund. 2019. 'Unpacking Cyber-Capacity Building in Shaping Cyberspace Governance: The SADC Case'. In *GIGAnet Annual Symposium*. Berlin. https://researchictafrica.net/wp/wp-content/uploads/2019/11/33_Calandro_Berglund_Unpacking-Cyber-Capacity-Building-1.pdf.

CARICOM IMPACS. 2021. 'Capacity Building for CARIFORUM Member States on Asset Recovery and Cybercrime'. 2021. https://caricomimpacs.org/11th-edf-project/.

CEPOL. 2021. 'EUROMED Police'. CEPOL. 2021. https://www.cepol.europa.eu/projects/euromed.

Collett, Robert. 2021. 'Understanding Cybersecurity Capacity Building and Its Relationship to Norms and Confidence Building Measures'. *Journal of Cyber Policy* 0 (0): 1–20. https://doi.org/10.1080/23738871.2021.1948582.

Collett, Robert, Lea Kaspar, and Carolin Weisser Harris. 2021. 'Catalog of Project Options for the National Cybersecurity Strategy (NCS) Cycle'. Global Forum on Cyber Expertise. https://cybilportal.org/wp-content/uploads/2021/06/GFCE-catalog-of-project-options-NCS_edited10June.pdf.

Council of Europe. 2001. *Convention on Cybercrime*. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185.

———. 2021a. 'CyberCrime@EAP I'. Council of Europe. 2021. https://www.coe.int/en/web/cybercrime/cybercrime-eap-i.

———. 2021b. 'CyberCrime@IPA'. Council of Europe. 2021. https://www.coe.int/en/web/cybercrime/cybercrime-ipa.

———. 2021c. 'Cyberviolence'. Council of Europe. 2021. https://www.coe.int/en/web/cyberviolence/home.

———. 2021d. 'Global Project on Cybercrime Phase I'. Council of Europe. 2021. https://www.coe.int/en/web/cybercrime/global-project-phase-i.

———. 2021e. 'Worldwide Capacity Building against Cybercrime'. Council of Europe. 2021. https://www.coe.int/en/web/cybercrime/capacity-building-programmes.

Council of Europe, Committee of Ministers. 1989. 'Recommendation R(89)9 on Computer-Related Crime'. 13 September 1989.

———. 1995. 'Recommendation R(95)13 on Problems of Criminal Procedure Law Connected with Information Technology'. 11 September 1995. https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804f6e76.

Council of the European Union. 2015. ‘Council Conclusions on Cyber Diplomacy’. 6122/15. https://data.consilium.europa.eu/doc/document/ST-6122-2015-INIT/en/pdf.

———. 2018. ‘EU External Cyber Capacity Building Guidelines - Council Conclusions (26 June 2018)’. 10496/18. Brussels: European Union. https://data.consilium.europa.eu/doc/document/ST-10496-2018-INIT/en/pdf.

Creese, Sadie, William H. Dutton, Patricia Esteve-Gonzalez, and Ruth Shillair. forthcoming. ‘Cybersecurity Capacity Building: Cross-National Benefits and International Divides’. *Journal of Cyber Policy*.

Cybil Portal. 2021a. ‘CMM Review Somalia’. Cybil Portal. 2021. https://cybilportal.org/projects/cmm-review-somalia/.

———. 2021b. ‘Women and International Security in Cyberspace Fellowship’. Cybil Portal. 2021. https://cybilportal.org/projects/women-and-international-security-in-cyberspace-fellowship/.

Dambra, Savino, Leyla Bilge, and Davide Balzarotti. 2020. ‘SoK: Cyber Insurance–Technical Challenges and a System Security Roadmap’. In *2020 IEEE Symposium on Security and Privacy (SP)*, 1367–83. IEEE.

Deibert, Ron. 2011. ‘Towards a Cyber Security Strategy for Global Civil Society?’ *Global Information Society Watch 2011 Report*, Global Information Society Watch, December, 6.

Duijnhoven, Hanneke, Bram Poppink, Tom van Schie, and Don Stikvoort. 2021. ‘Getting Started With A National CSIRT’. TNO. https://cybilportal.org/wp-content/uploads/2021/06/TNO-2021-Getting_started_with_a_national_CSIRT_FINAL.pdf.

Duru Aydin, Deniz. 2015. ‘Global Conference on Cyber Space Heavy on “Cyber,” Light on Solutions’. Access Now. 23 April 2015. https://www.accessnow.org/global-conference-on-cyber-space-heavy-on-cyber-light-on-solutions/.

Dutton, William H., Sadie Creese, Ruth Shillair, and Maria Bada. 2019. ‘Cybersecurity Capacity: Does It Matter? (2019)’. *Journal of Information Policy* 9: 280–306. https://doi.org/10.5325/jinfopoli.9.2019.0280.

Estonian Information System Authority. 2021. ‘EU CyberNet’. 2021. https://www.eucybernet.eu/.

Eurojust. 2021. ‘EuroMed Justice’. 2021. https://www.euromed-justice.eu/.

European Commission. 2015. ‘Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: The European Agenda on Security’. https://ec.europa.eu/home-affairs/sites/default/files/e-library/documents/basic-documents/docs/eu_agenda_on_security_en.pdf.

———. 2017. ‘Commission Staff Working Document: Digital4Development: Mainstreaming Digital Technologies and Services into EU Development’. https://ec.europa.eu/transparency/documents-register/detail?ref=SWD(2017)157&lang=en.

———. 2018. ‘Results and Indicators for Development: Cybersecurity’. https://europa.eu/capacity4dev/system/files/documents/sector/sectorpresentation41.pdf.

———. 2020a. ‘Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Shaping Europe’s Digital Future’. https://ec.europa.eu/info/sites/default/files/communication-shaping-europes-digital-future-feb2020_en_4.pdf.

———. 2020b. ‘Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the EU Security Union Strategy’. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0605&from=EN.

———. 2020c. ‘Strategic Plan 2020-2024, Directorate-General for Neighbourhood and Enlargement Negotiations (DG NEAR)’. https://ec.europa.eu/info/system/files/near_sp_2020_2024_en.pdf.

———. 2020d. ‘Strategic Plan 2020-2024, Service for Foreign Policy Instruments’. https://ec.europa.eu/info/system/files/fpi_sp_2020_2024_en.pdf.

———. 2020e. ‘Strategic Plan 2020-2024, Directorate-General for International Cooperation and Development (DG DEVCO)’. https://ec.europa.eu/info/sites/default/files/devco_sp_2020_2024_en.pdf.

———. 2021a. ‘Joint Letter of Intent to Foster a “Team Europe” Approach Implementing Digital4Development (D4D) in Partner Countries’. https://toolkit-digitalisierung.de/app/uploads/2020/12/MoU-D4D-Hub.pdf.

———. 2021b. ‘Working Better Together as Team Europe Guidance’. https://europa.eu/capacity4dev/wbt-team-europe.

———. 2021c. ‘Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: 2030 Digital Compass: The European Way for the Digital Decade’. https://eur-lex.europa.eu/resource.html?uri=cellar:12e835e2-81af-11eb-9ac9-01aa75ed71a1.0001.02/DOC_1&format=PDF.

———. 2021d. ‘Factsheet on Global Europe: Neighbourhood, Development and International Cooperation Instrument’. https://ec.europa.eu/international-partnerships/system/files/factsheet-global-europe-ndici-june-2021_en.pdf.

European Commission, Sylvie Nicole, and Abigail Hansen. 2015. ‘Operational Human Rights Guidance for EU External Cooperation Actions Addressing Terrorism, Organised Crime and Cybersecurity’. European Commission. https://ec.europa.eu/international-partnerships/system/files/manual-hr-guidance-ct-oc-cyber-november-2015_en.pdf.

European Commission, Patryk Pawlak, Directorate-General for International Cooperation and Development, and France) Institute for Security Studies (Paris. 2018. *Operational Guidance for the EUs International Cooperation on Cyber Capacity Building*. https://www.iss.europa.eu/sites/default/files/Operational%20Guidance%20for%20the%20EU%E2%80%99s%20international%20cooperation%20on%20cyber%20capacity%20building%20%E2%80%93%20A%20Playbook.pdf.

European Union. 2013. ‘Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace’. JOIN(2013) 1 final. https://ec.europa.eu/digital-single-market/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security.

———. 2017. ‘Joint Communication to the Parliament and the Council: Resilience, Deterrence and Defence: Building Strong Cybersecurity for the EU.Pdf’. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017JC0450&from=en.

———. 2020. ‘The EU’s Cybersecurity Strategy for the Digital Decade’. https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0.

Expertise France. 2021. ‘OCWAR-C – Organised Crime West African Response to Cybersecurity and Fight against Cybercrime’. 2021. https://www.ocwarc.eu/.

Ferrari, Verónica, and Sheetal Kumar. 2020. ‘A Human-Centric Approach to International Cybernorms: Civil Society Feedback on the UN Open-Ended Working Group on ICTs Proposals | Association for Progressive Communications’. Association for Progressive Communications. 1 December 2020. https://www.apc.org/en/news/human-centric-approach-international-cybernorms-civil-society-feedback-un-open-ended-working.

FIIAPP and Expertise France. 2021. ‘EL PAcCTO, Europe Latin America Programme of Assistance against Transnational Organised Crime’. EL PAcCTO. 2021. https://www.elpaccto.eu/en/about-el-paccto/what-is-el-paccto/.

Forum of Incident Response and Security Teams. 2019. ‘Statement Regarding Huawei’s Suspension from the Forum of Incident Response and Security Teams (FIRST)’. FIRST — Forum of Incident Response and Security Teams. 18 September 2019. https://www.first.org/newsroom/releases/20190918.

———. 2021. ‘FIRST Members around the World’. FIRST - Forum of Incident Response and Security Teams. 2021. https://www.first.org/members/map.

Frickenstein, Judith, and Silvia Baur-Yazbeck. 2020. ‘Risk Alert: Development Community Support Needed for Cybersecurity’. Not For Profit. CGAP. 14 January 2020. https://www.cgap.org/blog/risk-alert-development-community-support-needed-cybersecurity.

G8, Birmingham Summit. 1998. ‘1998 Drugs and International Crime’. 16 May 1998. http://www.g8.utoronto.ca/summit/1998birmingham/drugs.htm.

Gates, Bill, and Collins Hemingway. 1999. *Business @ the Speed of Thought: Using a Digital Nervous System*. New York, NY: Warner Books.

Ghana, Ministry of Communications. 2019. ‘Implementation of the Operational Cyber Security Infrastructure for the National Cyber Security Centre’. Ministry of Communications. 12 August 2019. http://www.moc.gov.gh/implementation-operational-cyber-security-infrastructure-national-cyber-security-centre.

Global Affairs Canada. 2021. ‘Gender Equality Guide for COVID-19 Related Projects’. https://www.international.gc.ca/gac-amc/publications/evaluation/2021/empowerment-pouvoir.aspx?lang=eng.

Global Forum on Cyber Expertise. 2020a. ‘GFCE Annual Meeting 2020 Working Groups Report’. https://thegfce.org/wp-content/uploads/2020/12/Annual-Report-GFCE-Working-Groups-2020.pdf.

———. 2020b. ‘Report on the “Women in Cyber Capacity Building” Session – Global Forum on Cyber Expertise’. 2 May 2020. https://thegfce.org/report-on-the-women-in-cyber-capacity-building-session/.

Global Partners Digital. 2020. ‘Involving Stakeholders in National Cybersecurity Strategies: A Guide for Policymakers’. https://www.gp-digital.org/wp-content/uploads/2020/08/NCSS-guidance-doc_gpd.pdf.

Gray, Catriona, and Lea Kaspar. 2018. ‘Human Rights Based Cybersecurity Capacity Building in International Cooperation: Trends, Lessons Learned, Recommendations’, 32.

Hameed, Faisal, Ioannis Agrafiotis, Carolin Weisser, Michael Goldsmith, and Sadie Creese. 2018a. ‘Analysing Trends and Success Factors of International Cybersecurity Capacity-Building Initiatives’. https://ora.ox.ac.uk/objects/uuid:50e9c5aa-4f3d-40f0-a0a0-ff538b735291.

Hohmann, Mirko, Alexander Pirang, and Thornston Benner. 2017. ‘Advancing Cybersecurity Capacity Building: Implementing a Principle-Based Approach’. Global Public Policy Institute (GPPi). https://www.gppi.net/media/Hohmann__Pirang__Benner__2017__Advancing_Cybersecurity_Capacity_Building.pdf.

Hubbard, Douglas W., and Richard Seiersen. 2016. *How to Measure Anything in Cybersecurity Risk*. Wiley Online Library.

Inter-American Defense Foundation. 2020. ‘Cyber Defense Program - Inter-American Defense Foundation (IADF) One Pager’. https://www.iadfoundation.org/wp-content/uploads/2020/09/one_page_final.pdf.

International Telecommunication Union. 2008. *ITU Global Cybersecurity Agenda (GCA) High Level Experts Group (HLEG) Global Strategic Report*. https://ccdcoe.org/uploads/2018/10/ITU-080801-HLEGreport.pdf.

———. 2021. ‘Global Cybersecurity Index 2020’, June, 172.

International Telecommunication Union (ITU). 2014. ‘World Telecommunication Development Conference (WTDC-14) Final Report’. https://www.itu.int/en/ITU-D/Conferences/WTDC/Documents/D-TDC-WTDC-2014-PDF-E.pdf.

Iversen, Jonas Svava. 2005. ‘Futures Thinking Methodologies - Options Relevant for “Schooling For Tomorrow”’. OECD. http://www.oecd.org/education/ceri/35393902.pdf.

Jezierska, Katarzyna. 2021. ‘Incredibly Loud and Extremely Silent: Feminist Foreign Policy on Twitter’. *Cooperation and Conflict*, March, 00108367211000793. https://doi.org/10.1177/00108367211000793.

Kaspar, Lea, and Matthew Shears. 2018. ‘Framework for Multistakeholder Cyber Policy Development’. Global Partners Digital. https://www.gp-digital.org/wp-content/uploads/2018/03/framework_cyberpolicy.pdf.

Korea Internet & Security Agency. 2019. ‘Global Cybersecurity Center for Development (GCCD) 2019 Report’. https://www.kisa.or.kr/jsp/common/downloadAction.jsp?bno=264&dno=16&fseq=1.

Lagakali, Cherie, and Klée Aiken. 2020. ‘The GFCE Meets the Pacific’. Organisation Blog. Pacific Online. 16 February 2020. https://pacificonline.org/portfolio-item/the-gfce-meets-the-pacific/.

Lea Kaspar. 2017. ‘GCCS2017: A Cyberspace Free, Open and Secure (but Mostly Secure) | Global Partners Digital’. 29 November 2017. https://www.gp-digital.org/gccs2017-a-cyberspace-free-open-and-secure-but-mostly-secure/.

Leyen, Ursula von der. 2019. ‘Political Guidelines for the next European Commission 2019-2024’. https://ec.europa.eu/info/sites/default/files/political-guidelines-next-commission_en_0.pdf.

Lipson, Howard F. 2002. ‘Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues’, November, 85. https://doi.org/10.1184/R1/6585395.v1.

‘London Conference on Cyberspace: Chair’s Statement’. 2011. https://www.gov.uk/government/news/london-conference-on-cyberspace-chairs-statement.

Malekos Smith, Zhanna, Eugenia Lostri, and James A. Lewis. 2020. ‘The Hidden Costs of Cybercrime’. https://www.csis.org/analysis/hidden-costs-cybercrime.

Millar, Katharine, James Shires, and Tatiana Tropina. 2021. ‘Gender Approaches to Cybersecurity’. UNIDR. https://unidir.org/publication/gender-approaches-cybersecurity.

Morgus, Robert. 2018. *Securing Digital Dividends: Mainstreaming Cybersecurity in International Development*. New America.

North Atlantic Treaty Organization. 2002. ‘Vulnerability of the Interconnected Society’. https://www.nato.int/science/publication/nation_funded/doc/262-VIS%20Final%20Rep-Oct%202002.pdf.

Nye, Joseph. 2014. 'Global Commission on Internet Governance: The Regime Complex for Managing Global Cyber Activities'. https://www.cigionline.org/sites/default/files/gcig_paper_no1.pdf.

OECD. 1992. 'OECD Guidelines for the Security of Information Systems'. 1992. https://www.oecd.org/digital/ieconomy/oecdguidelinesforthesecurityofinformationsystems1992.htm.

Organization of American States (OAS). 2019. 'Summary of Cybersecurity Activities Implemented by the OAS/CICTE Secretariat.Pdf'. http://scm.oas.org/IDMS/Redirectpage.aspx?class=X.2.19%20CICTE/Inf&classNum=1&lang=t.

Painter, Chris. 2020. 'GFCE Submission of Comments on Discussion Questions for the Third Round of Informal OEWG Meetings'. https://ceipfiles.s3.amazonaws.com/pdf/CyberNorms/UNGGE/GFCE+Comments+on+Discussion+Questions+for+the+Third+Round+of+Informal+OEWG+Meetings.pdf.

Pawlak, Patryk. 2014a. 'Cyber Capacity Building in Ten Points'. https://www.iss.europa.eu/sites/default/files/EUISSFiles/EUISS_Conference-Capacity_building_in_ten_points-0414.pdf.

———. ed. 2014b. *Riding the Digital Wave: The Impact of Cyber Capacity Building on Human Development*. EUISS Reports 21. Paris: European Union Institute for Security Studies (EUISS). https://www.iss.europa.eu/content/riding-digital-wave-%E2%80%93-impact-cyber-capacity-building-human-development.

———. 2016a. 'Confidence-Building Measures in Cyberspace: Current Debates and Trends'. *International Cyber Norms: Legal, Policy & Industry Perspectives*, 129–53.

———. 2016b. 'Capacity Building in Cyberspace as an Instrument of Foreign Policy'. *Global Policy* 7 (1): 83–92. https://doi.org/10.1111/1758-5899.12298.

Pawlak, Patryk, and Panagiota-Nayia Barmpaliou. 2017. 'Politics of Cybersecurity Capacity Building: Conundrum and Opportunity'. *Journal of Cyber Policy* 2 (1): 123–44. https://doi.org/10.1080/23738871.2017.1294610.

Pawlak, Patryk, and Antonio Missiroli. 2019. 'Introduction: Trends, Patterns and Challenges for International Cooperation in Cyberspace'. *European Foreign Affairs Review* 24 (2). https://kluwerlawonline.com/journalarticle/European+Foreign+Affairs+Review/24.2/EERR2019008.

Perrier, Jean-Louis, and Silvia Baur-Yazbeck. 2020. 'Regional Centers Can Help Low-Income Countries Build Cyber Resilience'. 8 July 2020. https://www.cgap.org/blog/regional-centers-can-help-low-income-countries-build-cyber-resilience.

Portnoy, Michael, and Seymour Goodman. 2008. *Global Initiatives to Secure Cyberspace: An Emerging Landscape*. Springer Science & Business Media.

President of the European Commission. 2019. 'Mission Letter: Commissioner for International Partnerships', 1 December 2019.

Radunović, Vladimir, and David Rüfenacht. 2016. 'Cybersecurity Competence Building Trends'. DiploFoundation. https://www.rcc.int/p-cve/download/docs/Cybersecurity%20Competence%20Building%20Trends%20in%20OECD.pdf/9be68dfd9a803a0bcfcf76347d894916.pdf.

Raymond, Mark, and Laura DeNardis. 2015. 'Multistakeholderism: Anatomy of an Inchoate Global Institution'. *International Theory* 7 (3): 572–616. https://doi.org/10.1017/S1752971915000081.

Sabillon, Regner, Victor Cavaller, and Jeimy Cano. 2016. 'National Cyber Security Strategies: Global Trends in Cyberspace'. *International Journal of Computer Science and Software Engineering* 5 (5): 67.

Seger, Alexander. 2013. 'Capacity Building on Cybercrime: Discussion Paper'. Discussion Paper. Strasbourg: Council of Europe. https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa3e6.

Sharland, Lisa, and Hannah Smith. 2019. 'Cyber, Technology and Gender: What Are We Missing?' Think Tank. ASPI The Strategist. 12 June 2019. https://www.aspistrategist.org.au/cyber-technology-and-gender-what-are-we-missing/.

Shears, Matthew, Daniela Schnidrig, and Lea Kaspar. 2018. 'Multistakeholder Approaches to National Cybersecurity Strategy Development'. Global Partners Digital. https://www.gp-digital.org/wp-content/uploads/2018/06/Multistakeholder-Approaches-to-National-Cybersecurity-Strategy-Development.pdf.

Singer, Peter W., and Allan Friedman. 2014. *Cybersecurity and Cyberwar: What Everyone Needs to Know®*. What Everyone Needs To Know®. Oxford, New York: Oxford University Press.

Skierka, Isabel, Robert Morgus, Mirko Hohmann, and Tim Maurer. 2015. 'CSIRT Basics for Policy-Makers', May, 28.

Tanczer, Leonie Maria, Irina Brass, and Madeline Carr. 2018. 'CSIRTs and Global Cybersecurity: How Technical Experts Support Science Diplomacy'. *Global Policy* 9 (S3): 60–66. https://doi.org/10.1111/1758-5899.12625.

UK Foreign Commonwealth and Development Office. 2020. 'UK Commonwealth Cyber Security Programme. A Selection of Six Case Studies'. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/971015/UK_Commonwealth_Cyber_Security_Programme_six_case_studies.pdf.

———. 2021. 'Cyber and Tech Security Programme: Building on a Modest Investment to Design Catalytic Intent into a New Programme'. GOV.UK. 22 March 2021. https://www.gov.uk/government/publications/cyber-and-tech-security-programme-case-study-building-on-a-modest-investment-to-design-catalytic-intent-into-a-new-programme/cyber-and-tech-security-programme-case-study-building-on-a-modest-investment-to-design-catalytic-intent-into-a-new-programme.

UK National Audit Office. 2019. 'Progress of the 2016-2021 National Cyber Security Programme', March, 53.

UN Women. 2021. 'Conduct a Study on the Dimensions of Violence against Women in Politics (VAWP) in Five Countries of the Arab States Region (Tender Notice)'. https://www.ungm.org/Public/notice/120784.

United Nations. 1991. 'Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, Havana, 27 August-7 September 1990: Report Prepared by the Secretariat.' A/CONF.144/28/Rev.1. New York. https://digitallibrary.un.org/record/142947?ln=en.

United Nations, General Assembly. 2015. 'Transforming Our World: The 2030 Agenda for Sustainable Development'. A/RES/70/1. https://documents-dds-ny.un.org/doc/UNDOC/GEN/N15/291/89/PDF/N1529189.pdf?OpenElement.

United Nations Group of Governmental Experts. 2021. 'Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security'. A/76/135. https://front.un-arm.org/wp-content/uploads/2021/08/A_76_135-2104030E-1.pdf.

United Nations Open-Ended Working Group. 2021. 'Final Substantive Report of the Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security'. https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf.

U.S. Department of Defense. 2019. '5 Things to Know About the U.S.-Ukraine Defense Relationship'. U.S. Department of Defense. 7 November 2019. https://www.defense.gov/Explore/News/Article/Article/2011746/5-things-to-know-about-the-us-ukraine-defense-relationship/.

Viatchaninova, Ievgeniia, Felix Gonzalez, Antonio Garcia, and Natalija Gelvanovska. 2013. 'Role of Multilateral Organizations in Cyber Security'. http://www.intgovforum.org/cms/wks2013/workshop_background_paper/104_1382306664.docx.

Weisser Harris, Carolin, Ian Wallace, James Boorman, Orhan Osmani, Marwan BenRached, Melissa Hathaway, Francesca Spidalieri, Radu Serrano, and Kerry-Ann Barrett. 2021. 'Global Overview of Existing National Cyber Capacity Assessment Tools'. Global Forum on Cyber Expertise. https://cybilportal.org/wp-content/uploads/2021/07/Global-Overview-of-Assessment-Tools_CLEAN_07July.pdf.

Women's International League for Peace and Freedom. 2021. 'Submission to the UN Working Group On The Use of Mercenaries Regarding "cyber Mercenaries" and Their Human Rights Impact'. https://reachingcriticalwill.org/images/documents/Publications/cyber-mercenaries.pdf.

World Bank. 2019. 'Global Cybersecurity Capacity Program: Lessons Learned and Recommendations towards Strengthening the Program'. World Bank Group. http://documents.worldbank.org/curated/en/947551561459590661/pdf/Global-Cybersecurity-Capacity-Program-Lessons-Learned-and-Recommendations-towards-Strengthening-the-Program.pdf.

———. 2021. 'Cybersecurity Multi-Donor Trust Fund'. Text/HTML. World Bank. 2021. https://www.worldbank.org/en/programs/cybersecurity-trust-fund.

World Bank, William Dutton, and Johannes Bauer. 2019. 'Global Cybersecurity Capacity Program : Lessons Learned and Recommendations towards Strengthening the Program'. Working paper. World Bank. https://documents.worldbank.org/en/publication/documents-reports/documentdetail/947551561459590661/Global-Cybersecurity-Capacity-Program-Lessons-Learned-and-Recommendations-towards-Strengthening-the-Program.

World Bank Group. 2016. *World Development Report 2016: Digital Dividends*. World Bank Publications.

Zamfir, Ionel. 2017. 'Understanding Capacity-Building/Capacity Development: A Core Concept of Development Policy, European Parliamentary Research Service, April 2017'. https://www.europarl.europa.eu/RegData/etudes/BRIE/2017/599411/EPRS_BRI(2017)599411_EN.pdf.

Getting in touch with the EU

In person

All over the European Union there are hundreds of Europe Direct information centres. You can find the address of the centre nearest you at: https://europa.eu/european-union/contact_en

On the phone or by email

Europe Direct is a service that answers your questions about the European Union. You can contact this service:

– by freephone: 00 800 6 7 8 9 10 11 (certain operators may charge for these calls),

– at the following standard number: +32 22999696 or

– by email via: https://europa.eu/european-union/contact_en

Finding information about the EU

Online

Information about the European Union in all the official languages of the EU is available on the Europa website at: https://europa.eu/european-union/index_en

EU publications

You can download or order free and priced EU publications at: https://op.europa.eu/en/publications. Multiple copies of free publications may be obtained by contacting Europe Direct or your local information centre (see https://europa.eu/european-union/contact_en).

EU law and related documents

For access to legal information from the EU, including all EU law since 1952 in all the official language versions, go to EUR-Lex at: http://eur-lex.europa.eu

Open data from the EU

The EU Open Data Portal (http://data.europa.eu/euodp/en) provides access to datasets from the EU. Data can be downloaded and reused for free, for both commercial and non-commercial purposes.

QN-01-21-158-EN-C

Publications Office
of the European Union