European Commission

INTERNATIONAL CYBER CAPACITY BUILDING: GLOBAL TRENDS AND SCENARIOS

Annex 3
Notes on Cyber Capacity Building Funders

Manuscript completed in 2021

Prepared by

EUROPEAN
UNION
Institute for
Security Studies

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

This report was authored by Robert Collett and Nayia Barmpaliou. The project was coordinated by Dr Patryk Pawlak, Brussels Executive Officer for the EUISS and Ondrej Vosatka, Policy Officer for the European Commission (Service for Foreign Policy Instruments).

INTERNATIONAL CYBER CAPACITY BUILDING: GLOBAL TRENDS AND SCENARIOS

Annex 3
Notes on Cyber Capacity Building Funders

Robert Collett
Nayia Barmpaliou

September 2021

TABLE OF CONTENTS

ACRONYMS

ACCBP	Anti-Crime Capacity Building Program
AICCTP	Australia-India Cyber and Critical Technology Partnership
APISC	Asia Pacific Information Security Center
APNIC	Asia Pacific Network Information Centre
ASCCE	ASEAN-Singapore Cybersecurity Centre of Excellence
ASEAN	Association of Southeast Asian Nations
ASPI	Australian Strategic Policy Institute
CAMP	Cybersecurity Alliance for Mutual Progress
CARICOM	Caribbean Community
CCB	(International) cyber capacity building
CEABAD	Centro de Estudios Avanzados en Banda Ancha para el Desarrollo
CERT/CC	Computer Emergency Response Team Coordination Centre
CERT NZ	New Zealand Computer Emergency Response Team
CICTE	Organisation of American States' Inter-American Committee against Terrorism
CMM	Capacity Maturity Model for Nations
CNI	Critical National Infrastructure
CoE	Council of Europe
CSA	Cyber Security Agency of Singapore
CSIRT	Computer Security Incident Response Team
CSIS	Centre for Strategic International Studies
CSSF	Conflict, Stability and Security Fund
CTCBP	Counter-Terrorism Capacity Building Program
Cyber4Dev	Cyber Resilience for Development
DAP	Digital Access Programme
DCCP	Digital Connectivity and Cybersecurity Partnership
DCMS	Department for Digital, Culture, Media and Sport
DFAT	Department of Foreign Affairs and Trade
DFID	Department for International Development
DG	Directorate-General
DG INTPA	Directorate-General for International Partnerships
DG NEAR	Directorate-General for Neighbourhood and Enlargement Negotiations
DHS	Demographic and Health Surveys
DOJ	Department of Justice
EDF	European Development Fund
EEAS	European External Action Service
ENI	European Neighbourhood Instrument
ENISA	European Union Agency for Cybersecurity
EU	European Union

EU CyberNet	EU Cyber Capacity Building Network
FCO	Foreign and Commonwealth Office
FCDO	Foreign, Commonwealth and Development Office
FFRDC	Federally Funded Research and Development Center
FOC	Freedom Online Coalition
GAC	Global Affairs Canada
GCC	Geographic Combatant Command
GCCD	Global Cybersecurity Center for Development
GCFA	Global Cyber Forensics Advisor
GFCE	Global Forum on Cyber Expertise
GGE	Group of Governmental Experts
GIZ	Deutsche Gesellschaft für Internationale Zusammenarbeit
GLACY	Global Action on Cybercrime
GLACY+	Global Action on Cybercrime Extended
GLEN	U.S. Transnational and High-Tech Crime Global Law Enforcement Network
IADB	Inter-American Defense Board
ICHIPS	International Computer Hacking and Intellectual Property Advisors
IcSP	Instrument Contributing to Stability and Peace
IDB	Inter-American Development Bank
IfS	Instrument for Stability
ILEA	International Law Enforcement Academies
INL	Bureau of International Narcotics and Law Enforcement Affairs
INTERPOL	International Criminal Police Organisation
IPA	Instrument for Pre-Accession
ITU	International Telecommunication Union
JAIF	Japan-ASEAN Integration Fund
JICA	Japan International Cooperation Agency
JPCERT/CC	Japan CERT Coordination Center
KISA	Korea Internet & Security Agency
KrCERT/CC	Korean Computer Emergency Response Co-ordination Centre
LAC4	Latin America and the Caribbean Cyber Competence Centre
METI	Ministry of Economy, Trade and Industry
MFAT	Ministry of Foreign Affairs and Trade
MFF	Multi-Annual Financial Framework
MIC	Ministry of Internal Affairs and Communications
MOFA	Ministry of Foreign Affairs
NCA	National Cyber Agency
NCSC	National Cyber Security Centre
NCSP-I	National Cyber Security Programme - International

NDICI	Neighbourhood, Development, International Cooperation Instrument
NISC	National Center of Incident Readiness and Strategy for Cybersecurity
NIST	National Institute of Standards and Technology
NUPI	Norwegian Institute of International Affairs
NZ	New Zealand
OAS	Organization of American States
OCWAR-C	Organised Crime: West African Response on Cybersecurity
ODA	Overseas Development Assistance
OEWG	Open-Ended Working Group
OSCE	Organization for Security and Co-operation in Europe
PI	Partnership Instrument
PSOP	Peace and Stabilization Operations Program
RIA	Estonian Information System Authority
RRM	G7 Rapid Response Mechanism
RSIS	S. Rajaratnam School of International Studies
RTC	Regional Training Centers
S/CCI	Office of the Coordinator for Cyber Issues
SCP	Singapore Cooperation Programme
SEI	Software Engineering Institute
TAIEX	Technical Assistance and Information Exchange
TCTP	Third Country Training Programmes
UNIDIR	United Nations Institute for Disarmament Research
UNODC	United Nations Office on Drugs and Crime
UK	United Kingdom
UNSCP	United Nations-Singapore Cyber Programme (UNSCP)
UNTOC	UN Convention Against Transnational Organized
US	United States
USAID	United States Agency for International Development

1 INTRODUCTION

This Annex serves as an accompanying working document to the Report “International Cyber Capacity Building: Global Trends and Scenarios”. It provides additional information on countries and foundations funding cyber capacity building programmes. It is not an exhaustive account of all such organisations or their activities but provides contextual information from interviews and document search. It is intended to be a living document with updates and additions in regular intervals.

2 EUROPEAN COMMISSION

Building on a solid policy framework (see the EU section of the main report), the EU has been utilising its relevant thematic and geographic external financing instruments to finance global, regional and bilateral cyber-specific actions.

The main global financing instrument utilised since 2013 has been the **Instrument for Stability (IfS)**, that as of 2014 was renamed **Instrument contributing to Stability and Peace (IcSP)**, which included cybersecurity and cybercrime as priority areas since 2013 and has led the creation of global programmes. The IcSP has served as an incubator and test bed of niche thematic actions, including on cyber, allowing the definition of a methodological approach that has been taken up by geographical instruments subsequently targeting regional or country-specific programmes.

The EU's budget, known as the **Multi-Annual Financial Framework (MFF)**, is a seven-year long-term budgets, that is executed through different financing instruments. For the period of 2007-2013, the EU had committed approximately €10 million on its initial cyber-specific external cooperation. Most notably, that increased significantly during the 2014-2020 MFF to around €95 million.

	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021
EU's CCB						**EUR million**							
Instrument for Stability (IfS) / Instrument Contributing to Stability and Peace (IcSP)	-	-	-	4.5		9	0.3	11.25	3	4	6	5.2	5
Instrument for Pre-Accession (IPA)	-	2.25	-	1.35	-	5	-	3.5	1	1	4.45		
European Neighbourhood Instrument (ENI)	0.2	0.9	-	-	0.9	1.5	-	3	0.3	11.4	5.5	1.5	
European Development Fund (EDF)	-	-	-	-	-	-	-	-	9.3	-	-	-	
Partnership Instrument (PI)	n/a	n/a	n/a	n/a	n/a	-	-	-	2.5	-	2	3.5	
TOTAL	**0.2**	**3.15**	**0**	**5.85**	**0.9**	**15.5**	**0.3**	**17.75**	**16.1**	**16.4**	**17.95**	**10.2**	

For the next MFF covering 2021-2027, the EU has merged several of its earlier external financial instruments into the **'Neighbourhood, Development, International Cooperation Instrument – Global Europe (NDICI-Global Europe)'** to serve as the EU's main financial instrument for external action. The NDICI-Global Europe Regulation entered into force on 14 June 2021, with retroactive effect as of 1 January 2021. At a first stage after its adoption, the services of the Commission and the European External Action Service will develop multi-annual indicative programmes for each region, partner country and thematic programme, which will set the framework for the subsequent annual action programmes and the financial implementation of actions. Given this circumstance, it is therefore too early to anticipate the plans for the EU's 2021 spending on CCB.

The types of CCB projects financed up to 2020 by the EU can be systematised around four main priorities:

- Facilitating the development or reform of **appropriate legal frameworks in the fight against cybercrime** on the basis of international standards (Budapest Convention on Cybercrime) and in a manner that fosters greater international cooperation; as well as investing in **enhancing the capacities of criminal justice authorities**, such as law enforcement, prosecutors and judges, in order to enable them to effectively investigate, prosecute and adjudicate cases of cybercrime and other offences involving e-evidence.

- Supporting the development of a **comprehensive set of organisational, technical and cooperation frameworks and mechanisms that increase third countries' cyber resilience and preparedness**, for example: facilitating the development of national cybersecurity strategies and promotion of cyber culture; strengthening incidence management capabilities through the set up and training of functional national Computer Emergency Response Teams; promoting effective inter-institutional and international cooperation as well as public-private partnerships.

- Strengthening **international cyber policy cooperation** by supporting activities and exchanges that increase the convergence between partner countries and regional organisations standards, policies and best practices and those of the EU; and by fostering increased consensus in partner countries for an open, free, and secure cyberspace, through the promotion of existing international law, norms of state behaviour and confidence building measures in cyberspace.

Below is a mapping of projects financed by the EU's external financing instruments in the previous two MFFs (2007-2020) that have a cyber-specific focus or a distinct cyber-specific component in larger programmes. The table does not include projects that: have cybersecurity or cybercrime aspects as cross-cutting issues; that focus on ICT and loosely touch on cyber issues; address infrastructure and e-governance with embedded cybersecurity safeguards; or, more recently, respond to hybrid threats. The EU does not yet have a system for tagging cyber in such projects, nor for identifying the percentage of the allocation assigned to cyber components in them. Similarly, the table does not include activities of the Technical Assistance and Information Exchange (TAIEX) instrument because of their ad-hoc and short-term nature. Finally, any actions financed by internal financing instruments, even with an external outlook, were excluded. The table is therefore not an absolutely exhaustive account of every external cyber capacity building activity financed by the EU.

MAPPING OF EU-FUNDED PROJECTS WITH A CYBER-SPECIFIC FOCUS OR A CYBER-SPECIFIC COMPONENT PER YEAR AND EXTERNAL FINANCING INSTRUMENT:

Instrument for Stability (IfS) / Instrument Contributing to Stability and Peace (IcSP art.5)

	Budget Year AAP	Budget EUR	Budget Breakdown EUR	Project Name	Type
MFF 2007-2013	2012	4,500,000	3,000,000	Global Action on Cybercrime (GLACY)	Global
			1,500,000	Enhancing cyber security, protecting information and communication networks (ENCYSEC)	Regional
MFF 2014-2020	2014	9,000,000	9,000,000	Global Action on Cybercrime extended (GLACY+)	Global
	2015	300,000	300,000	EU-GFCE Research and Knowledge Management Initiative	Global
	2016	11,250,000	11,000,000	Cyber Resilience for Development (Cyber4Dev)	Global
			250,000	Operational Guidance for the EU's international cooperation on CCB	Global
	2017	3,000,000	3,000,000	GLACY+ top-up	Global
	2018	4,000,000	4,000,000	EU CyberNet	Global
	2019	6,000,000	1,000,000*	Countering Election-related Cyber Threats and Disinformation in Ukraine *Under Art.3 of IcSP Regulation, non-programmable	Bilateral
			5,000,000	GLACY+ top-up	Global
	2020	5,200,000	5,000,000	EU CyberNet top-up	Global
			200,000	Global mapping and trends of cyber capacity building (incl. pilot CCB training)	Global

Instrument for Pre-Accession (IPA)

	Budget Year AAP	Budget EUR	Budget Breakdown EUR	Project Name	Type
MFF 2007-2013	2010	2,250,000	2,250,000	CyberCrime@IPA	Regional
	2012	1,350,000	1,350,000	Strengthening Capacity Against Cybercrime in Turkey	Bilateral
MFF 2014-2020	2014	5,000,000	5,000,000	iPROCEEDS	Regional
	2016	3,500,000	3,500,000	Strengthening Capacity Against Cybercrime in Turkey	Bilateral
	2017	1,000,000	1,000,000	Serbia: Strengthened capacities (human and legal) of Criminal Police Department and Special Prosecutor's Office in combating cyber-crime and public awareness	Bilateral
	2020	1,000,000	1,000,000	EU 4 Fight Against Cybercrime in BiH	Bilateral
	2019	4,450,000	4,450,000	iPROCEEDS 2	Regional

European Neighbourhood Instrument (ENI)

	Budget Year AAP	Budget EUR	Budget Breakdown EUR	Project Name	Type
MFF 2007-2013	2009	200,000	200,000	Cybercrime Project in Georgia	Bilateral
	2010	900,000	900,000	Cybercrime@EAP I	Regional
	2013	900,000	900,000	Strengthening the capacity of the public administrations to combat cybercrime in the Hashemite Kingdom of Jordan	Bilateral

MFF 2014-2020	2014	1,500,000	800,000	Cybercrime@EAP II	Regional
			700,000	Cybercrime@EAP III	Regional
	2016	3,000,000	3,000,000	CyberSouth	Regional
	2017	300,000	300,000	Assessment of Ukraine's e-governance policy framework in the light of the Public Administration Reform Strategy and cybersecurity challenges	Bilateral
	2018	11,400,000	3,200,000	CEU4Digital – Improving Cyber Resilience in the EaP Countries	Regional
			3,800,000	CyberEast – Action on Cybercrime for Cyber Resilience in the EaP region	Regional
			1,300,000	Strengthening Cybersecurity Capacities in Georgia	Bilateral
			1,300,000	Strengthening Cybercrime and cyberterrorism investigative capabilities of law enforcement authorities and protection of critical infrastructure in Georgia	Bilateral
			1,500,000	Consolidation of the legislative framework in the field of cybersecurity in line with EU acquis and building institutional capacity within national cybersecurity system in Ukraine	Bilateral
			300,000	Cybersecurity of Elections in Ukraine	Bilateral
	2019	5,500,000	2,500,000*	EU4DigitalUA *Estimate of the cybersecurity component	Bilateral
			3,000,000*	E-governance and digital economy in Ukraine *Estimate of the cybersecurity component	Bilateral
	2020	1,500,000	1,500,000	CyberSouth top-up	Regional

European Development Fund (EDF)

	Budget Year AAP	Budget EUR	Budget Breakdown EUR	Project Name	Type
MFF 2014-2020	2017	9,300,000	1,800,000*	Capacity Development for CARIFORUM Member States on Financial Compliance, Asset Recovery and Cybercrime *Allocation for the cybercrime component only*	Regional
			7,500,000	Organised Crime: West African Response on Cybersecurity and fight against Cybercrime (OCWAR–C)	Regional

Partnership Instrument (PI)

	Budget Year AAP	Budget EUR	Budget Breakdown EUR	Project Name	Type
MFF 2014-2020	2016	2,500,000	2,500,000	EU Cyber Direct	Global
	2019	2,000,000	2,000,000*	Enhancing Security Cooperation in and with Asia *Estimate of the cybersecurity component*	Regional
	2020	3,500,000	3,500,000	EU Cyber Diplomacy Support Initiative	Global

3 COUNTRIES

3.1 Australia

Australia's 2016 Cyber Security Strategy resulted in the position of Ambassador for Cyber Affairs being established in the **Department of Foreign Affairs & Trade (DFAT)** and the creation of an international cyber capacity building programme. The initial commitment was for AUS$4m over 4 years. In 2017, a further AUS$10m was added to this at the launch of the International Cyber Engagement Strategy. Further announcements of new funding came in 2018 (AUS$1m) and 2019 (AUS$9m for the Pacific and AUS$10m for South East Asia). The programme is classified as ODA.

DFAT's programme started with a call for grant proposals under AUS$100,000. These annual calls for proposals continued until 2020, when DFAT ran its latest funding round. They increased the maximum proposal size of grant proposals to AUS$500,000 and including in its guidelines that new projects should complement existing efforts. DFAT issued 8 grants through that round. Other projects have been funded using a tender process to enter commercial contracts with Cardno – an external grant management and monitoring and evaluation support unit– and The Australian National University for the Cyber Bootcamp project.

DFAT partner with several other government agencies to deliver projects, including the **Australian Federal Police**, **Attorney General's Department**, **Office of the eSafety Commissioner** and the **Australian Cyber Security Centre**. Their non-governmental implementing partners have included the ABC International Development, Australian Human Rights Commission, Australian National University, Australian Strategic Policy Institute (ASPI), Cyber Law International, CyberCX, FireEye, FIRST, the Foundation for Media Alternatives, ICT4Peace Foundation, the Institute of Policy Research and Advocacy (ELSAM), the International Foundation for Electoral Systems (IFES), Ionize, Macquarie University, Monash University, Plan International Australia, Retrospect Labs, TAFE Queensland, UNIDIR, UNITAR, UNODC, Willyama Services and WithYouWithMe. They also support the PaCSON and PILON networks.

In 2021, DFAT announced that its programme would be renamed the **Cyber and Critical Tech Cooperation Program**, reflecting the expanded focus of its new International Cyber and Critical Tech Engagement Strategy. They also announced that Australia and the Australian Strategic Policy Institute (ASPI) would host a Sydney Dialogue in late 2021 on cyber and critical technology. In addition, Australia launched two new programmes in 2020: the $12.7 million Australia-India Cyber and Critical Technology Partnership (AICCTP); and the Quad Tech Network - a project with universities in Australia, Japan, India and US to support research and promote engagement on cyber and critical technology issues.

Australia's CCB	2016 AUD	2017 AUD	2018 AUD	2019 AUD	2020 AUD
DFAT	1m (€0.62m)	2.9m (€1.8m)	4.98m (€3.09m)	6.92m (€4.29m)	7.47m (€4.63m)

3.2 Canada

Global Affairs Canada (GAC) began its international security capacity building programming in 2005 with the Counter-Terrorism Capacity Building Program (CTCBP). They followed this with an **Anti-Crime Capacity Building Program (ACCBP)** in 2009. The ACCBP was created to enhance the capacity of beneficiary states to prevent and respond to threats posed by international criminal activity throughout the world, with a particular focus on the Americas. Since 2015, GAC has committed funding for cyber-specific projects through the ACCBP.

Since 2015 the ACCBP has invested $18.2M in cyber capacity building, with an additional $9.6M committed to be disbursed over the next 3 years. GAC's cyber capacity building projects deliver against the ACCBP's mandate to protect Canadians at home and abroad, as well as Canada's National Cybersecurity Strategy 2019-2024, and therefore it has the primary aim of increasing Canada's security. Their cyber capacity building expenditure is therefore not classified as ODA.

GAC has a strong preference for funding regional or multi-country projects over those that address issues in just one country. From 2015 to 2021, the ACCBP focused its programming, including cyber related projects, in the Latin America and Caribbean region and Southeast Asia. They have mainly worked through grant and contribution type funded partnerships with UNODC and INTERPOL to address cybercrime related challenges. INTERPOL's ACCBP-funded activities occur across the LAC region, while UNODC's are implemented in Southeast Asia and the northern triangle of Central America – starting with Guatemala, Honduras and El Salvador and most recently supporting Belize as well in the new phase.

The ACCBP's approach to cybercrime capacity building has been two-pronged: raising public awareness, so citizens know how to protect themselves online and crime is more likely to be reported; and technical training, which includes training police in cyber forensics and investigation, while also providing capacity building training for judges and prosecutors in cybercrime cases. Additionally, the UNODC and INTERPOL work with states to update and improve their legal frameworks related to cybercrime.

ACCBP has also provided significant support to the Organisation of American States' Inter-American Committee against Terrorism (CICTE), which is the OAS secretariat unit responsible for cyber programming. The support to the OAS seeks to improve cybersecurity capacities through the development of Cyber Security Incident Response Teams (CSIRTs) and national cybersecurity strategies. This work also regularly cross-supports GAC's counter-cybercrime activity. In several countries they found the same officials or units would have responsibility for both cybersecurity and cybercrime issues.

In 2019, the ACCBP programme team considered how their programme should evolve to meet the needs of the new national cyber strategy and their divisional mandate. They decided to maintain their commitment to Latin America and the Caribbean, while looking at opportunities to address transnational cybercrime threats from West and East Africa or Asia. Of these two, GAC decided to fund an exploratory project in ASEAN, implemented through Chatham House with the intention of increasing Cyber capacity building in the region. Additionally, Canada has recently launched another pilot project in Southeast Asia with the UNODC which seeks to improve state capacity to address the use of the dark web and cryptocurrencies in transnational criminal activity, with a particular focus on human smuggling.

ACCBP has also broadened the thematic issues it addresses within its programme related to cyber capacity building. In 2019, they began supporting cyber defence capacity through the Inter-Americas Defense Board's (IADB) new Cyber Defense Programme in order to support the development of a hemispheric cyber defence framework and seek to bring militaries into the larger regional discussion on cybersecurity and CSIRT development (Inter-American Defense Foundation 2020). This project has now been completed. Separately, to coincide with the latest round of UN Group of Governmental Experts (GGE) and Open-Ended Working Group (OEWG) negotiations, Canada has begun to fund projects that help government officials and civil society engage in the international debate on the governance of cyberspace. Complementing this, Canada has also recently started to fund projects that address the understanding and development of international law on cybersecurity: one with the Council of Europe and one with Cyber Law International.

The ACCBP also provided funding to the Global Forum on Cyber Expertise to support their research agenda which will produce valuable research and knowledge products that will help improve the impact and effectiveness of cyber capacity building around the world.

Other parts of the Canadian government have conducted cyber activities, including through GAC's support to the **G7 Rapid Response Mechanism (RRM)** which works to reinforce democracies and respond to foreign interference. The G7 RRM is mandated to identify and respond to foreign threats to democracy, including disinformation. In support of this mandate, RRM Canada shares information and analyses, coordinates action and develops strategies to help safeguard G7 democracies from foreign threats. Additionally, RRM Canada leverages its open source data analytics capability to monitor the digital information ecosystem in real-time and report on signs of foreign state sponsored disinformation related to Government of Canada domestic and foreign priorities.

Through the **Office of Human Rights Freedoms and Inclusion**, and its Promoting and Protecting Democracy Fund (PRO-DEM Fund), Canada has supported programming to address emerging and evolving threats to democracy and the promotion of equitable and participative civic engagement online. Pro-Dem programming has funded projects which seek to: combat disinformation and negative influence activities linked to elections; build societal and state resilience to targeted disinformation campaigns by nefarious external or domestic actors; support responsive action by public and private institutions when developing platforms, laws, and policies related to safe and effective civic engagement online; combat the misuse of emerging technologies and internet-facilitated trends which prevent the meaningful and inclusive participation of all individuals in public discourse and decision-making; protect critical internet users and social communicators and the free flow of information, and; strengthen information literacy and awareness within civic education curricula for students and educators.

The **Peace and Stabilization Operations Program (PSOPs)** provides technical and programmatic support in conflict affected scenarios and politico-security crises that impact Canadian interests abroad. In recent years PSOPs has supported information and cyber-related activities including countering disinformation and misinformation through social media and the digital space; building cyber-security capacity of civil society and governance actors in conflict and fragile settings; collection of digital evidence for transitional justice and accountability processes; and, using digital platforms to promote peacebuilding, reconciliation and legitimacy. PSOPs' technical advice and programming have supported Canadian efforts in countries and regions such as Colombia, Iraq, South Sudan, Syria, and Ukraine among others.

The **International Cyber Policy team within GAC** has a small pot of funding which can be used to support events and activities or fund research projects. Additionally, Canada, via the International Cyber Policy team, has been one of the donor countries (the others being Australia, the Netherlands, the UK and New Zealand) behind the Women in Cyber (WiC) fellowship program. This program seeks to promote the meaningful participation of women in UN cyber processes by funding the participation of female diplomats from the Global South in UN cyber OEWG meetings, providing targeted training and support to increase their engagement in international cyber discussion while also promoting digital inclusion and providing mentorship to support the career progression of these female diplomats. GAC's Peace and Stabilization Programme also supports some cyber projects related to election protection and misinformation specially in conflict-affected states. Canada currently has multiple interdepartmental working groups such as the Cyber Skills Work Force Development Working Group and Internet Child Exploitation Working Group which seek to coordinate both their domestic and international cyber activities.

Canada's CCB	2014/15 CAD	2015/16 CAD	2016/17 CAD	2017/18 CAD	2018/19 CAD	2019/20 CAD	2020/21 CAD
Global Affairs Canada (Anti-Crime Programme only)	2.10m (€1.41m)	2.25m (€1.51m)	1.21m (€0.81m)	2.74m (€1.84m)	2.59m (€1.74m)	3.97m (€2.67m)	1.22m (€0.82m)

3.3 Estonia

After the 2007 cyber-attacks on Estonia, the government made a significant investment in strengthening its cyber resilience, contributing to an international reputation as a country that transformed its cybersecurity readiness. This experience and reputation resulted in interest from other countries in learning from Estonia and provided lessons it could share with others through cyber capacity building.

Given the context of the politically motivated 2007 cyber-attacks, the Estonian approach to cyber capacity building was originally shaped by cyber defence and military considerations. Notably, Estonia began sharing expertise and knowledge with partners in NATO and neighbouring countries through intelligence, defence and military channels. This cooperation addressed the technical aspects of cyber defence, but also included a civilian dimension relating to the protection of critical infrastructure.

In May 2008, the **NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE)** was established in Tallin, with the cooperation of Estonia, Germany, Italy, Latvia, Lithuania, Slovak Republic and Spain (NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE) 2021). It serves as a multinational and interdisciplinary cyber defence hub that undertakes research [1], training and exercises. Many of these activities have a cyber capacity building dimension.

As Estonia moved quickly to develop its civilian cybersecurity capabilities, the **Estonian Information System Authority** (known as RIA) engaged with partner countries. RIA's international engagement included offering advice to low and middle income countries interested in establishing a national strategic framework, incident management, and relevant regulations. This pro bono activity is not part of a structured international cyber capacity building programme per se, but nonetheless contributes to creating trusted international relationships and improved capabilities in partner countries.

Estonia's national authorities, such as RIA, have embraced the role of cyber capacity building implementers to a unique extent. For example, RIA has led the implementation of several EU-funded TAIEX and Twinning projects primarily in the Eastern Partnership region. It is also a key delivery partner in the EU-funded 'Cyber Resilience for Development' (Cyber4Dev) project and the lead implementer of the EU CyberNet project. Officials from RIA and Estonian ministries of foreign affairs, defence and economy are closely engaged with the Organization of American States (OAS) in training decision makers on cyber-related strategic policy issues.

Another trusted implementor is the non-profit **e-Governance Academy (eGA)**, which was established in 2002 at the initiative of the Estonian Government in partnership with the Open Society Institute and the United Nations Development Programme (e-Governance Academy 2021). While

[1] Including the flagship Tallinn Manual on the International Law Applicable to Cyber Warfare (Schmitt 2013).

originally focused on national e-government and digital transformation projects [2], the eGA was quick to expand its scope to cybersecurity, both as an enabler of digital transformation and as a standalone issue in need of capacity building.

In addition to government-led activity, Estonia's investment, public-private partnerships and international outreach, have created the conditions for a strong ecosystem of Estonian cybersecurity companies that serve as cyber capacity building implementors or contractors in larger CCB projects.

The creation of the **office of the Cyber Ambassador at the Ministry of Foreign Affairs** (MFA) in September 2018 led to the consolidation of Estonia's cyber diplomacy activity, including cyber capacity building. In 2019, Estonia's MFA launched the **Tallinn School of Cyber Diplomacy**, which delivers a week-long course for diplomats and public sector officials from partner countries who are new to cyber foreign policy-making and strategic planning (Estonian Ministry of Foreign Affairs 2019). The Foreign Ministry also supports CCB activities by the e-Governance Academy and by the Estonian Ministry of Defence in Georgia and Ukraine. In August 2021, the Estonian MFA was one earliest donors to the World Bank's new Cybersecurity Multi-Donor Trust Fund (World Bank 2021).

3.4 Germany

Germany has conducted and funded CCB since at least 2014. Its activity can be summed in the following categories:

Supporting the implementation of regional Confidence Building Measures in cyberspace: Since 2017, the German Federal Foreign Office has funded exchanges that promote, assist and foster the implementation of cyber/ICT Confidence-Building Measures (CBMs) in OSCE member states. Their approach has been to support the identification of challenges states face in implementing CBMs, the creation of national CBM implementation roadmaps and customised capacity building plans. Germany also supports the operationalisation of the CBMs network of policy and technical Points of Contact.

Cyber Diplomacy: Since 2014, the German Federal Foreign Office has financed CCB activities to help public officials, diplomats, industry, and civil society representatives better understand the application of international law in cyberspace, and promote international norms and CBMs. A key objective of these activities has been to broaden the multi-stakeholder participation in the international debates and regional and global negotiations. The lead implementing partner in this effort has been the ICT4Peace Foundation (ICT4Peace Foundation 2019).

[2] For example, providing support for the formulation of a nation's interoperability strategies and the development of related legal and technical frameworks.

Enabling civil society to engage in cyber policy processes: Germany has funded small-scale projects with the aim at enhancing the capacity of civil society organisations to better engage in cyber policy processes both nationally and internationally.

Cybersecurity, Digitalisation and SDGs: Germany's Ministry for Economic Cooperation and Development (BMZ) and its implementing partner Gesellschaft für Internationale Zusammenarbeit (GIZ) have been systematically supporting digital transformation projects which integrate cybersecurity safeguards. For example in Tunisia, as part of the project 'Shaping Tunisia's digital transformation and creating jobs', GIZ implements an integrated approach that includes the development of cybersecurity skills as part of the action (Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) 2020).

In August 2021, Germany was among the first group of donors to contribute to the World Bank's Cybersecurity Multi-Donor Trust Fund (World Bank 2021).

Research and conferences: The German Federal Foreign Office has funded research on: integrating cybersecurity capacity building in the sustainable development agenda (2016-17 implemented by the Global Public Policy Institute, (Hohmann, Pirang, and Benner 2017)), and promoting gender approaches to cybersecurity (2020-21 implemented by UNIDIR, (Millar, Shires, and Tropina 2021)). It has also financed in the past UNIDIR's Cyber Stability Conference (2012, 2014) in order to support the identification of pragmatic steps (including on CCB) towards a more stable and predictable cybersecurity environment.

CCB Partnerships: Germany was a founding member of the Global Forum on Cyber Expertise and the Freedom Online Coalition. Its national experts are often mobilised to lead technical assistance activities in EU-funded TAIEX and Twinning projects. German ministries and agencies are members of the implementing consortia for EU CyberNet project (Federal Foreign Office) and the EU's Enhancing Security Cooperation in and with Asia initiative (GIZ). The Federal Criminal Police Office of Germany (BKA) and Federal Office for Information Security (BSI) have capacity building partnerships with counterpart agencies in partner countries for offering advice and peer-to-peer technical assistance.

3.5 Israel

The Isreali approach to international cyber capacity building has been developed based on its broader international cooperation objectives that relate to: enabling Israel's foreign policy objectives including both its international security and development agendas; contributing to the international agenda and policy discussions; fostering defence partnerships with partner countries; promoting market opportunities for Israeli cybersecurity industry; and developing technological partnerships with other governments to enhance Israel's nationally-oriented cutting-edge technologies in cybersecurity. The leading coordinating authority for all civilian aspects of cyber policy and operations in Israel, including on its international cyber capacity building efforts, is the **Israel National Cyber Directorate (INCD)**.

While Israel had been engaging for several years in CCB through the more traditional ODA-type of activities financed through its **Ministry of Foreign Affairs** with ad hoc training courses and consultative work, a pivotal moment for a more substantive involvement in CCB came in 2012-13 when the **Ministry of Economy** took charge of the engagement with IFIs and development banks from the National Bank of Israel. This shift in mandate allowed for a strategic analysis of all the IFIs in which Israel has membership in including a reflection on if and how they could work on cybersecurity through these IFIs. By 2015-16, the Ministry of Economy was able to identify cybersecurity as a strategic priority it could pursue through its IFI partnerships. Specifically, Israel set up its first donor fund in cybersecurity in 2016 with a 3million USD contribution to the Inter-American Development Bank focusing on South America, followed by contributions to the World Bank in 2017 to its Digital Development Partnership and another 1million USD in 2019 with a focus on CCB for Africa.

In addition to its financing of CCB through IFIs, Israel also engages in cybersecurity exchanges in its bilateral relations with partner countries. Its bilateral approach entails offering peer-to-peer knowledge exchange that could eventually lead to business partnership agreements with other governments whereby Israeli stakeholders and industry implement a comprehensive capacity building effort as contractors, financed by the partner country itself.

Finally, in 2019 the INCD invested in the establishment of a cyber capacity building-focused centre within the auspices of **the Blavatnik Interdisciplinary Cyber Research Center (ICRC) at Tel Aviv University**. The main objective of the centre is to support the development of CCB methodology, analytical frameworks and knowledge tools that can support action and resource-oriented CCB. One of the first tools it developed in partnership with the World Bank through 2019-20 has been the 'Sectoral Cyber-Capability Maturity Model: Promoting Global Cyber Resilience for Sectors and Society' (ProGReSS) which was designed for assessing and maturing cyber capabilities of critical infrastructure sectors, in complementarity with other existing maturity models that have a nation-wide scope.

Israel's CCB	**2016** **USD**	**2017** **USD**	**2018** **USD**	**2019** **USD**
Ministry of Economy	3m (€2.52m)	1m (€0.84m)	-	1m (€0.84m)*

*MFA figures not available.

3.6 Japan

A wide range of Japanese agencies are involved in cyber capacity building: the **Japan International Cooperation Agency (JICA)**; the **National Center of Incident Readiness and Strategy for Cybersecurity (NISC)**; the **Ministry of Economy, Trade and Industry (METI)**; the **Japan**

CERT Coordination Center (JPCERT/CC) within METI; the **Ministry of Foreign Affairs (MOFA)**; the **Ministry of Internal Affairs and Communications (MIC)**; the **National Police Agency**; and the **Japan-ASEAN Integration Fund (JAIF)**.

Japan's capacity building activities are coordinated by **NISC**, which started its capacity building activities in 2009. This coordination occurs through inter-agency meetings held four times a year. Japan produced a policy document for capacity building in 2014 that provides some structure to their national activity. NISC are considering updating this at the moment.

Although Japan has projects around the world, NISC's main capacity building focus is the ASEAN region. They are responsible for the ASEAN-Japan Cybersecurity Policy Meeting, which is held once a year, and the working groups three times a year and projects under it. There are ten collaborative activities under the Policy Meeting covering exercises, awareness raising working, metrics (an area of work that began in 2020) and the mutual notification programme. Projects under this ASEAN-Japan process are funded by NISC, METI and MIC. NISC also contributes by hosting joint cyber exercises with ASEAN. NISC's annual spend administering the process is around 50 million Yen (€390k) a year. This is not reported as ODA spend. NISC have four staff whose job description is 60 - 80% cyber capacity building.

JICA's ICT programme team started considering cyber capacity building in 2013 at the encouragement of METI, MIC and MOFA. Their first project was in 2014 in Indonesia. In a typical year their ICT programme will include one or two cyber projects, costing 60m Yen (€470k) in ODA funds. JICA prefer to manage a small number of projects to focus on quality and deploy Japanese experts to live and work in the partner country as part of a project team with locally hired staff. JICA run all aspects of their own projects rather than outsourcing this to implementing partners through contracts or grants. They have a close collaboration with the Asia Pacific Network Information Centre (APNIC).

JP's CCB*	**2013**	**2014**	**2015**	**2016**	**2017**	**2018**	**2019**	**2020**	**2021**
	JPY	**JPY**	**JPY**	**JPY**	**JPY**	**JPY**	**JPY**	**JPY**	**JPY**
JICA	-	43.2m (€0.34m)	61.7m (€0.48m)	60.2m (€0.47m)	6m (€0.05m)	2.9m (€0.02m)	62.6m (€0.49m)	unknown	unknown
NISC	40.1m (€0.31m)	66.7m (€0.51m)	47.7m (€0.37m)	47.7m (€0.37m)	47.7m (€0.37m)	47.7m (€0.37m)	36.5m (€0.28m)	37m (€0.29m)	211m (€1.63m)
MIC	-	-	18.5m (€0.14m)	31.1m (€0.24m)	15.3m (€0.12m)	10.7m (€0.08m)	48.8m (€0.22m)	89.3m (€0.69m)	55m (€0.42m)

*METI and MOFA figures not available.

3.7 South Korea

The **Korea Internet & Security Agency (KISA)**, under the Ministry of Science and ICT, contains a programme team that runs both the **Global Cybersecurity Center for Development (GCCD)** and the **Cybersecurity Alliance for Mutual Progress (CAMP)**. Also, within KISA is the national incident response team, **KrCERT/CC**, which delivers some international training, under the **Asia Pacific Information Security Center (APISC)** training programme, that is separate to these initiatives.

The **Global Cybersecurity Center for Development (GCCD)** was established in 2015 to support cyber capacity building activities benefiting government policymakers and staff in developing countries. The GCCD has three main lines of activity: training sessions that are timed to coincide with the CAMP annual conference; joint seminars, which are co-hosted with a partner country ministry; and grant-funded collaborations. Most training and seminars are delivered by experts from KISA and external organisations. The training focuses on incident response, but also covers strategy and public awareness.

GCCD has grant-funded collaborations with the World Bank and the Inter-American Development Bank (IDB). With the World Bank, they have funded the provision of national capacity assessments, delivered by the Global Cyber Security Capacity Centre in Oxford. KISA has then followed some of these up with targeted workshops to address issues identified in the assessment. Separately, since 2014, Korea has worked with IDB, through the GCCD, to set up and support the Centro de Estudios Avanzados en Banda Ancha para el Desarrollo (CEABAD) in Nicaragua. CEABAD provides ICT training to government officials in Latin America, including on cyber issues.

As of 2021, the annual GCCD budget is approximately 625 million won (€470k), reported as ODA. This does not include the resource cost of KISA staff used for the programme's management and training.

The **Cybersecurity Alliance for Mutual Progress (CAMP) network** is a mechanism for Korea to share its expertise with a large group of partner countries and help them share their knowledge with each other. It was launched in July 2016 40 organizations from 29 countries, and as of October 2020 has 61 organisation members from 46 countries. Its main activities are an annual meeting in Korea and regional forums. It does not have an equivalent of the Cybil Portal or GFCE magazine, but instead shares information between members through its meetings and by email. CAMP's running costs are covered by approximately 160 million Won (€120k) annually. CAMP's main activities consist of an Annual Meeting and Regional Forums.

In addition to the above KISA programmes:

- the **Korea International Cooperation Agency (KOICA)** and the **Ministry of Foreign Affairs** collaborate to deliver international cyber capacity building, such as a course in October 2019 for ASEAN partners on cyber policy (Indonesia, Bureau of Technical Cooperation Abroad 2019);
- the **National Police Agency** has hosted an annual International Symposium on Cybercrime Response since 2000; and
- the **Korean Supreme Prosecutors' Office** is working with the World Bank to establish an Asia-Pacific Cybercrime Hub that will assist with the coordination of projects and expertise sharing (Global Forum on Cyber Expertise 2020, 13).

South Korea's CCB	2015 KRW	2016 KRW	2017 KRW	2018 KRW	2019 KRW	2020 KRW	2021 KRW
GCCD	625m (€0.46m)	540m (€0.39m)	625m (€0.46m)	625m (€0.46m)	625m (€0.46m)	625m (€0.46m)	625m (€0.46m)
CAMP	-	-	220m (€0.16m)	220m (€0.16m)	210m (€0.15m)	160m (€0.12m)	160m (€0.12m)

3.8 New Zealand

New Zealand's **Ministry of Foreign Affairs and Trade (MFAT)** launched its first cyber capacity building programme in 2019, with a commitment to invest NZ$10m of ODA funding over 5 years. Their programme is exclusively for projects in the Pacific and consist of 4 pillars: strategy and governance; information security; e-safety (e.g. public awareness campaigns); and cybercrime. While the programme is led by MFAT, it is supported by **CERT NZ**, the **Department of Internal Affairs** and the **Cabinet Office**. These departments coordinate through a cross-government working group and programme steering group.

The MFAT programme delivers through a mix of government staff, contracted companies and grants. Of particular note is their use of a CERT NZ staff member as a Pacific Liaison, with a full-time role either implementing capacity building activity or coordinating it domestically and with other donors and implementers.

Several other programmes in New Zealand also directly support cyber capacity building activity:

- the police contribute directly to cybercrime projects, including Cybersecurity Pasifika;
- the Women and International Security Fellowship is funded from a new programme administered by the Cabinet Office; and
- and the ICT for Development programme includes activities that support cyber capacities.

3.9 Singapore

Singapore has funded cyber capacity building through its general Singapore Cooperation Programme and the specialist programmes of the **Cyber Security Agency of Singapore**.

The **Singapore Cooperation Programme (SCP)** was established in 1992 to serve as the primary platform through which Singapore offers technical assistance to other countries. It is administered by the Ministry of Foreign of Affairs and contains two types of programmes: bilateral; and Third Country Training Programmes (TCTP) that are supported jointly by Singapore and partner country or organisation. The SCP has funded cyber capacity building since at least 2015, when it supported with ICT4Peace's Capacity Building Program for International Cyber Security Negotiations. In October 2015, Singapore hosted the third cybersecurity policy and diplomacy workshop, for ASEAN countries, co-organized by ICT4Peace and The S. Rajaratnam School of International Studies (RSIS)

(ICT4Peace 2015; Cybil Portal 2021a). In 2016, Singapore and the US signed a Memorandum of Understanding on Cybersecurity Cooperation and began a series of annual TCTP workshops on cybersecurity (Cybil Portal 2021d). The 2020 round was held virtually with 30 participants from all ASEAN countries as well as Timor-Leste and the ASEAN Secretariat. Through separate partnerships with Canada and the UK, Singapore has respectively conducted online training on cyber diplomacy and incident response training for Commonwealth countries.

Since its formation in April 2015, the **Cyber Security Agency of Singapore (CSA)** has shared its experience with other countries. In 2016, CSA held the first of its annual Singapore International Cyber Weeks at which it announced a three-year S$900,000 grant to **CyberGreen** (Cybil Portal 2021b) and launched the S$10 million, five-year **ASEAN Cyber Capacity Programme (ACCP)**, which strengthens technical, policy and legislative capacity in the region (Cyber Security Agency of Singapore 2016). Delivery partners for ACCP training have included INTERPOL and RSIS (Singapore CSA 2017).

As an extension of the ACCP, Singapore launched the **ASEAN-Singapore Cybersecurity Centre of Excellence (ASCCE)** in 2019, with an initial investment of S$30 million over five years. The ASCCE is a multi-disciplinary research and training facility. It will:

- conduct research and provide training in areas spanning international law, cyber strategy, legislation, cyber norms and other cybersecurity policy issues;
- provide technical incident response training as well as facilitate the exchange of opensource cyber threat and attack-related information and best practices; and
- conduct virtual cyber defence trainings and exercises through a cyber range run in partnership with Temasek Polytechnic.

Initiatives of the ASCCE under the 2018 United Nations-Singapore Cyber Programme (UNSCP) include: the Senior Executive Cyber Fellowship with the United Nations Office for Disarmament Affairs (UNODA); and workshops on the Implementation of Norms and Confidence Building Measures for ASEAN (Cyber Security Agency of Singapore 2020). Prior to the launch of the UNSCP, CSA helped the United Nations Office for Disarmament Affairs (UNODA) develop an online training course on the use of ICTs in the context of international security (Cybil Portal 2021c).

3.10 The Netherlands

The **Netherlands' Ministry of Foreign Affairs (MFA)** began its programmatic engagement on cyber-related issues in 2011 with its leadership role in establishing the **Freedom Online Coalition (FOC)**, whose secretariat it funded. Today the FOC has 33 members, spanning from Africa to Asia, Europe, the Americas, and the Middle East.

In 2015, the Dutch Ministry of Foreign Affairs hosted the fourth Global Conference on Cyber Space (GCCS) in the Hague and used this as a launchpad for the **Global Forum on Cyber**

Expertise (GFCE). The MFA continues to fund the majority of GFCE Secretariat and event running costs. However, in 2020, the MFA transitioned the GFCE's administration to full independent status as a not-for-profit Foundation. The creation of the Foundation marked the 'internationalisation' of the GFCE leadership and also allows other funders to support the GFCE directly. As of August 2021, the GFCE has 90 members and 46 partners.

The Dutch MFA's cyber capacity building activities now include:

- Support to the **Global Forum on Cyber Expertise**, including funding its secretariat.
- Support to the **Freedom Online Coalition**, including funding its secretariat.
- **Cyber diplomacy**: financing the development of training curricula and training courses in areas of the application of international law in cyberspace, cyber norms and responsible state behaviour in cyberspace. A long-term implementing partner in this effort is Cyber Law International.
- **Support to civil society**: A worldwide programme to enhance the capacity of local civil society engage in national, regional and global cyber policy processes. A long-term implementing partner in this effort is Global Partners Digital.
- **Promoting research**: financing research in identifying policy responses to new cybersecurity and technological challenges. A key partner in this effort is UNIDIR.
- **Cybersecurity, Digitalisation and SDGs**: partnering with the World Bank and financing the Cybersecurity window of its Digital Development Partnership.
- **Women and International Security in Cyberspace Fellowship**: supporting greater participation of women in discussions at the United Nations on international security issues related to responsible state behaviour in cyberspace, in partnership with Australia, Canada, New Zealand and the United Kingdom (Cybil Portal 2021e).
- Being a **consortium partner** in the EU-funded 'Cyber Resilience for Development' (Cyber4Dev) programme, along with the UK and Estonia.

From 2019 to 2022, the Dutch MFA's annual budget for cyber capacity building has been approximately **€5 million per year**.

The Netherlands also supports the development of academic capacity through its Leiden Hague Norms programme, which is funded from a separate envelope to its main CCB programme.

3.11 United Kingdom

The UK's first international cyber capacity building programme - **National Cyber Security Programme - International (NCSP-I)** - was launched in 2012 to implement commitments in the 2011 UK Cyber Security Strategy. The programme was managed by the then Foreign and Commonwealth Office (FCO)[3], but in partnership with other ministries and with funding from the centralised

[3] The UK's Foreign and Commonwealth Office and Department for International Development would later merge in September 2020 to form the Foreign, Commonwealth and Development Office (FCDO).

National Cyber Security Programme. The primary purpose of NCSP-I was to work internationally to secure the UK, in line with objectives set in 2011 Strategy.

The NCSP-I started by developing a framework to understand the components and maturity indicators of national cybersecurity capacity. Oxford University won a competition among UK universities to complete this work, creating the Cybersecurity Capacity Maturity Model for Nations (CMM) and the launching a **Global Cyber Security Capacity Centre** to help countries apply the CMM and to generate research from the findings.

From 2012 and 2018, the UK held annual, open invitations for project proposals. The focus of these project was directed by the 2011 strategy and the UK's 2015 National Cyber Security Strategy Strategic Objective 12, which called for 'International Action' in building a free, open, peaceful and secure cyberspace. This resulted in the UK funding and supporting projects in more than 100 countries.

In 2018, the UK started and/or partnered in three new programmes:

- a two-year **Programme Supporting Cyber Security in the Commonwealth**, launched at the Commonwealth Heads of Government Meeting in London (CHOGM 2018), with in-kind sponsorship and support from Microsoft, Citi Bank and Templar Executives;
- the **Digital Access Programme (DAP)**, a partnership between the then FCO, Department of International Development (DFID) and Department for Digital, Culture, Media and Sport (DCMS) to support digital access in five partner countries (South Africa, Nigeria, Kenya, Brazil and Indonesia), with a dedicated Trust and Resilience pillar; and
- the **Cyber4Dev programme**, a partnership between the UK, The Netherlands, Estonia and the European Commission, managed by Northern Ireland Cooperation Overseas.

These new programmes were driven a by broadening of the UK's objectives and delivery approach. The UK prioritised development and economic outcomes, alongside tradition security outcomes in CCB programming. The UK further evolved its delivery model, moving away from an annual 'calls for grant' proposals process, to tendering for multiyear commercial implementer consortiums and aligning activities (via sponsorship and in-kind support) with private sector funders.

In 2019, the UK contributed to the cybersecurity window of the **World Bank's Digital Development Partnership** and proposed the creation of a new Multi-Donor Trust Fund specifically for cyber capacity building.

In 2020, the FCO secured funding for the first time from the UK's Conflict, Stability and Security Fund (CSSF). This was used to commission a **Cyber and Tech Programme**, with a focus on CCB in technology, global cyber awareness and CNI resilience.

Entering 2021, the UK is going through a period of refresh as it updates its National Cyber Strategy, merges the FCO and DFID, and conducts an Integrated Review of Security, Defence, Development and Foreign Policy.

UK's CCB	2012/ 13 GBP	2013/ 14 GBP	2014/ 15 GBP	2015/ 16 GBP	2016/ 17 GBP	2017/ 18 GBP	2018/ 19 GBP	2019/ 20 GBP	2020/ 21* GBP
National Cyber Security Programme: International	0.15m (€0.17m)	2m (€2.33m)	2.2m (€2.56m)	2.4m (€2.80m)	3.1m (€3.61m)	2.2m (€2.56m)	£2.59m (€3.02m)	£4.73m (€5.51m)	£5.35m (€6.23m)
Supporting Cyber Security in the Commonwealth	-	-	-	-	-	-	£2.2m (€2.56m)	£3.1m (€3.61m)	
Digital Access Programme: Trust and Resilience	-	-	-	-	-		£0.5m (€0.58m)	£0.86m (€1.00m)	£2.1m (€2.45m)
Cyber and Tech Programme	-	-	-	-	-	-			£5.6m (€6.53m)

*Subject to variation at FY end.

Since 2012 the UK has worked with numerous CCB implementing partners, including, among others: APMG, ASPI, British Standards Institution, Chatham House, Commonwealth Parliamentary Association, Commonwealth Secretariat, Commonwealth Telecommunications Organisation, Control Risk, Council of Europe, Cranfield University, CREST International, CyberGreen, Cysiam, Deloitte, Endcode, EY, FIRST, Geneva Centre for Security Sector Governance (DCAF), Get Safe Online, Global Partners Digital, ICT4Peace, Igarape, Institute for Technology & Society of Rio, International Association of Prosecution, INTERPOL, ITU, KPMG, Meridian Community, New Americas, Organisation of American States, Protection Group International, Rand Europe, Royal United Services Institute, Torchlight, UNODC, and the World Bank.

Since 2012, the UK has also allocated a portion of its annual CCB budget to the **National Cyber Agency (NCA) for cybercrime projects**, primarily delivered through serving officers providing training to partner countries. In 2018, the UK further expanded international CCB activity delivered by other UK Government Departments, including the **Home Office**, **Government Communication Service** and the **National Cyber Security Centre (NCSC)**.

3.12 United States

State Department's Office of the Coordinator for Cyber Issues (S/CCI) began its Cybersecurity Capacity Building Programme in 2014.

The US Cybersecurity Capacity Building Programme started by engaging **Federally Funded Research and Development Centers (FFRDC)** to develop frameworks and good practices for capacity building. FFRRDCs are public-private partnerships that have an exclusive and close relationship with the US Government. The first FFDRC that S/CCI engaged was the Software Engineering Institute (SEI) at Carnegie Mellon University. SEI had previously worked with the Department of Defence, in 1988, to pioneer the concept of cyber security incident response teams and establish the CERT Coordination Centre (CERT/CC). In 2014, State Department asked SEI to develop a good practice framework for cyber capacity building for national incident response, and a CSIRT maturity framework to accompany it.

In 2016, S/CCI engaged a second FFRDC – MITRE – to develop a good practice framework for national cybersecurity strategies. MITRE have since regularly updated this framework, which is now on its 4th version.

To accompany the two pillar-specific frameworks, S/CCI produced a third guide to national cyber capacities that could be used by its programme team and embassies when providing advice to partner countries and when designing projects. This toolkit plays a similar role to the EU's Operational Guidance on Cyber Capacity Building and includes a categorization of national cyber capacities into five building blocks, similar to the EU's pillars.

Since 2018, the US Cybersecurity Capacity Building Programme has been delivering against the updated US National Cyber Strategy. The fourth pillar of the US strategy is Advancing American Influence, under which is an action line to build international cyber capacity (United States Government 2018, 26).

S/CCI's implementing partners have included: SEI, MITRE, the George C. Marshall European Center for Security Studies, Department of Homeland Security, the National Institute of Standards and Technology (NIST), the Organization of American States (OAS), the Centre for Strategic International Studies (CSIS), and the Organization for Security and Co-operation in Europe (OSCE).

State Department capacity building projects are currently operating in all regions. Country partners of note include: in Africa, Ghana and Kenya; in Asia Pacific, Indonesia, Vietnam, Philippines and Thailand; and in Eastern Europe, Ukraine, Moldova and Georgia. Although some projects are in low- and middle-income countries, the US does not classify the funds as Overseas Development Assistance (ODA).

In addition to running their own programme, S/CCI are also responsible for coordinating US cyber capacity building across State Department and other government agencies. Among the programmes they coordinate are those of: State's regional bureaus; the Digital Connectivity and Cybersecurity Partnership (DCCP); the Bureau of International Narcotics and Law Enforcement Affairs (INL); USAID; and the Department of Defence. This coordination is achieved through regular cross-agency meetings in Washington and, where appropriate, Embassy-drafted country cyber engagement strategies.

Since around 2017, **regional bureaus within State Department** have begun to fund CCB projects. Principal among these are the Bureau of East Asian and Pacific Affairs and Bureau of European and Eurasian Affairs. They use the implementer partnerships formed by S/CCI and have formed some of their own. For example, the European bureau is working with the Department of Energy to deliver assistance. By 2020, the combined spend of State Department's regional bureaus had overtaken that of S/CCI.

The **Digital Connectivity and Cybersecurity Partnership** is a whole of government effort to support the development of open communications infrastructure, transparent regulatory policies and partner cybersecurity capacity. It was launched in July 2018, with cyber capacity building being one of its four activity areas. Approximately a third of the total DCCP spend ($25m in 2019; $18m in 2020; $10m in 2021) has been on cyber projects. The first year of activity, in 2019, was focused upon the Indo Pacific and the second upon Latin America and the Caribbean. The programme is co-chaired by USAID and State Department's Economic Bureau. US Embassies bid for programme funding, so there is a lot of variety among its country activities. DCCP cyber capacity building implementing partners include DAI, SEI, MITRE, NIST, OAS and DHS.

The **Bureau of International Narcotics and Law Enforcement Affairs (INL)** leads U.S. State Department capacity building efforts on cybercrime and intellectual property (IP) rights. While foreign assistance for these topics had existed previously in limited forms, the programme began to expand starting in 2004 (U.S. Department of State 2004, 92), with an initial emphasis on combating intellectual property theft that has since steadily expanded to include cybercrimes. It has seen a steady increase in its approved funding by Congress in the years since, from $1m/year at the beginning to $5m/year in 2010-11 and reaching $10m/year in 2019. These allocations only capture the financing of the global programmes that are centrally managed. It is complemented by separate cybercrime and IP capacity building delivered through INL regional and bilateral programming, as well as the INL-funded International Law Enforcement Academies (ILEAs) and Regional Training Centers (RTCs).

The flagship of the INL centrally-managed programmes is the **U.S. Transnational and High-Tech Crime Global Law Enforcement Network (GLEN)**, an adaptive initiative that deploys experienced U.S. law enforcement experts abroad to deliver sustained training to foreign counterparts with a view to enhance local capacities and deliver near-term operational success. The GLEN features U.S. Department of Justice (DOJ) International Computer Hacking and Intellectual Property Advisors (ICHIPs) mainly posted at US Missions abroad; DOJ Global Cyber Forensics Advisors (GCFAs) operating out of the DOJ Cyber Lab; and long-term U.S. federal agent mentors. The GLEN is funded by INL and managed in partnership with DOJ. Recent examples of capacity building by the GLEN network include online training sessions in law enforcement in combating COVID-19 related crimes and criminal misuse of cryptocurrencies (US Department of Justice 2021).

In addition to the GLEN, INL funds cybercrime and IP law enforcement capacity building efforts implemented by other partners such as: the U.S. Department of Homeland Security (DHS); the Council of Europe (CoE); the United Nations Office on Drugs and Crime (UNODC); and the Organization of American States (OAS). A key goal of State Department programmes is to enable more countries to become parties to the CoE Convention on Cybercrime, known as the Budapest Convention. U.S.

training promotes effective use of existing tools like the Budapest Convention, the UN Convention Against Transnational Organized Crime (UNTOC) and the G7 24/7 Network Points of Contact.

The **US Agency for International Development (USAID)**'s Digital Development 2020-24 strategy contains several references to cybersecurity and commits to connecting USAID's activities to the national cyber strategy and the DCCP in particular. Furthermore, the 2018–2022 State-USAID Joint Strategic Plan mandates international cooperation to "secure an open, interoperable, reliable, and stable cyberspace and strengthen the capacity of the United States and partner nations to detect, deter, rapidly mitigate, and respond to international cyber threats and incidents". Their primary concern is mitigating the cybersecurity risks to their projects and implementing partners.

The **Department of Defense (DOD)** has been conducting cyber capacity building, as a form of security cooperation, since at least 2009. The department drafted its first International Cyberspace Security Cooperation Guidance in 2013 and revised this in 2019, following issuance of a new Defense Cyber Strategy in 2018. Their approach has been mainstream cybersecurity within its security cooperation relationships fostered and maintained by, with, and through DOD's Geographic Combatant Commands (GCCs). The department provides guidance that is then applied by the GCCs in the development and execution of Significant Security Cooperation Initiatives they run with individual country partners in their assigned global area of responsibility. In addition to bilateral cooperation, the DOD also run multi-country projects, such as those delivered by the George C. Marshall Center. The total, non-ODA, spend on cyber capacity building under the United States Code Title 10, Section 333 - covering foreign assistance ("authority to build capacity") by the armed forces – was approximately $10.3m in Financial Year 2021. In addition to this, GCCs can use Operation & Maintenance (O&M) funds to conduct capacity building. The DOD implement directly and through contracted implementers, including the aforementioned FFRDCs, as well as its geographically-aligned Regional Centers (e.g. the Marshal Center).

US’s CCB*	2005 USD	2006 USD	2007 USD	2008 USD	2009 USD	2010 USD	2011 USD	2012 USD	2013 USD
State Dept Cyber-crime Programme (INL)	1m (€0.84m)	1m (€0.84m)	1m (€0.84m)	1m (€0.84m)	1m (€0.84m)	5m (€4.19m)	5m (€4.19m)	5m (€4.19m)	5m (€4.19m)

US’s CCB*	2014 USD	2015 USD	2016 USD	2017 USD	2018 USD	2019 USD	2020 USD	2021 USD	2022 USD
US Cyber Security Capacity Building Programme	1.4m (€1.17m)	0.48m (€0.4m)	0.4m (€0.34m)	2m (€1.68m)	0.89m (€0.75m)	1m (€0.84m)	3m (€2.52m)	5m (€4.19m)	7m (estimate) (€5.87m)
DCCP (approximation)	-	-	-	-	-	10m (€8.39m)	7m (€5.87m)	1.5m (€1.26m)	
State Dept Cybercrime Programme (INL)	5m (€4.19m)	5m (€4.19m)	5m (€4.19m)	5m (€4.19m)	5m (€4.19m)	10m (€8.39m)	10m (€8.39m)	10m (€8.39m)	10m (estimate) (€8.39m)
Department of Defense (Section 333)	-	-	-	-	-	1.1m (€0.92m)	4.1m (€3.44m)	10.3m (€8.64m)	12.3m (estimate) (€10.31m)

* US State Department Regional Bureaus figures not available.

4 FOUNDATIONS

In the last three years several Foundations have started to fund cyber capacity building.

APNIC, the Internet address registry for the Asia-Pacific region, spends a quarter of its budget on capacity building projects, such as the APNIC Academy and the Information Society Innovation Fund (ISIF). In 2016 they created the separate, but connected, **APNIC Foundation** as a way to raise and disburse additional funding for projects. The Foundation raises around $1m a year from grants and uses these to support projects in the Pacific, especially in Papua New Guinea and Vanuatu (Macintosh 2019; Magan 2020).

The **Asia Foundation** has supported cybersecurity projects in Asia and the Pacific since at least 2017. They have previously partnered with the APNIC Foundation. For example, both supported, with Australia and New Zealand, the 2020 Pacific Cyber Dialogue and they collaborated to help Papua New Guinea secure the APEC Summit in 2018.

In the last couple of years, the **Bill and Melinda Gates Foundation**’s interest in financial services for the poor has led it to start supporting cybersecurity capacity building projects. In 2019, they gave a grant of $1.4m (€1.2m) to the standards certification organisation CREST International to enable local markets to address the growing cyber-risk in digital financial services (Bill and Melinda Gates Foundation 2019). The projects supports pen testing, local regulation on standards and the capacity of local cybersecurity companies to deliver managed services in accordance with global standards. Its priority countries are Bangladesh, Ethiopia, Indonesia, Kenya, Nigeria, Pakistan, Tanzania and Uganda (Scroxton 2020). In 2020, the Gates Foundation gave a grant worth over one million Euros to a new project, co-delivered by the GFCE and African Union, that will help AU members identify capacity building requirements, access training and strengthen the community of cybersecurity policy experts across the continent.

Since 2017, **Citi Foundation** has funded the Creating a Career Path in Digital Security project through the Organisation of American States' cyber programme, and the OAS-affiliated Young Americas Business Trust. The project, now in Phase II, is preparing Latin America's low-income urban youth for careers in cybersecurity. The project directly trained several hundred young people in Colombia, Costa Rica, the Dominican Republic, Peru and Brazil and reached over 5,000 more through an online course (Global Forum on Cyber Expertise 2017, 13; Organization of American States (OAS) 2019, 3) In November 2020, the Citi Foundation, Cisco and the OAS opened applications for a $200,000 (€165,000) Cybersecurity Innovation Fund to finance innovation projects in Latin America (Organization of American States (OAS) 2020).

The **Hewlett Foundation** has provided 213 cyber grants, several of which touch upon international cyber capacity building. These include large grants to the Carnegie Endowment for International Peace's Cyber Policy Initiative and grants to the Global Cyber Alliance, New America and the Centre for Internet and Society (CIS) in India.

The **Ford Foundation** supports research and organisations that contribute to technology developing to meet the needs of people in a rights-respecting and inclusive way. They have produced several tools that could be useful for cyber capacity building, including a guide to managing digital security risks in non-technical grant making (Brennan et al. 2017) and a cybersecurity assessment tool for organisations (Ford Foundation 2020).

Bibliography

Bill and Melinda Gates Foundation. 2019. “Grant to CREST International.” Bill and Melinda Gates Foundation. November 2019. https://www.gatesfoundation.org/How-We-Work/Quick-Links/Grants-Database/Grants/2019/11/INV-001323.

Brennan, Michael, Elizabeth Eagen, Bryan Nuñez, John Scott-Railton, and Eric Sears. 2017. “Digital Security Grantcraft Guide.” https://www.fordfoundation.org/media/3334/digital-security-grantcraft-guide-v10-final-22317.pdf.

Cyber Security Agency of Singapore. 2016. “Key Partnerships Established at the Inaugural Singapore International Cyber Week 2016.” Government Organisation. Cyber Security Agency of Singapore. October 18, 2016. https://www.csa.gov.sg/news/press-releases/key-partnerships-established-at-the-inaugural-sicw-2016.

———. 2020. “United Nations - Singapore Cyber Programme: Senior Executives Cyber Fellowship and Workshop on Implementation of Norms and Confidence Building Measures.” https://www.csa.gov.sg/-/media/csa/documents/sicw_2019/amcc/factsheet---unscp.pdf.

Cybil Portal. 2021a. “Capacity Building Program International Cyber Security Negotiations.” Cybil Portal. 2021. https://cybilportal.org/projects/capacity-building-program-international-cyber-security-negotiations/.

———. 2021b. “CyberGreen Initiative - A Global Community to Measure and Improve Cyber Health (*GFCE Initiative).” Cybil Portal. 2021. https://cybilportal.org/projects/cybergreen-initiative-a-global-community-to-measure-and-improve-cyber-health-gfce-initiative/.

———. 2021c. “Online Training Course on Cyber Diplomacy.” Cybil Portal. 2021. https://cybilportal.org/projects/online-training-course-on-cyber-diplomacy/.

———. 2021d. “Singapore-United States Third Country Training Programme (TCTP) Cybersecurity Workshops.” Cybil Portal. 2021. https://cybilportal.org/projects/singapore-united-states-third-country-training-programme-tctp-cybersecurity-workshops/.

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

Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ). 2020. “Shaping Tunisia’s Digital Transformation and Creating Jobs.” https://www.giz.de/en/downloads/giz2020-en-digitalzentrum-tunesien.pdf.

e-Governance Academy. 2021. “E-Governance Academy.” 2021. https://ega.ee/about-us/.

Estonian Ministry of Foreign Affairs. 2019. “Tallinn School of Cyber Diplomacy.” July 2019. https://vm.ee/en/summerschool.

Ford Foundation. 2020. “Cybersecurity Assessment Tool.” Ford Foundation. November 2020. https://www.fordfoundation.org/work/our-grants/building-institutions-and-networks/cybersecurity-assessment-tool/.

Global Forum on Cyber Expertise. 2017. “GFCE Magazine Volume 4.” https://thegfce.org/wp-content/uploads/2020/04/GlobalCyberExpertiseMagazine_issue4.pdf.

———. 2020. “GFCE Magazine Volume 7.” https://thegfce.org/presentation-of-the-global-cyber-expertise-magazine-vol-7-special-edition/.

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.

ICT4Peace. 2015. “ICT4Peace Capacity Building Program for International Cyber Security Negotiations in Singapore.” NGO. ICT4Peace. October 27, 2015. https://ict4peace.org/activities/ict4peace-capacity-building-program-for-international-cyber-security-negotiations-in-singapore/.

ICT4Peace Foundation. 2019. “International Cyber Security Policy and Diplomacy Capacity Building Program.” December 2019. https://www.un.org/disarmament/wp-content/uploads/2019/12/cybersecurity-policy-and-diplomacy-capacity-building-december-2019.pdf.

Indonesia, Bureau of Technical Cooperation Abroad. 2019. “Korea International Cooperation Agency (KOICA) Training 2019.” Indonesia, Bureau of Technical Cooperation Abroad. October 8, 2019. https://ktln.setneg.go.id/info_pelatihan_koica_2019.html.

Inter-American Defense Foundation. 2020. “Programs Cyber Defense.” Inter-American Defense Foundation. 2020. https://www.iadfoundation.org/cyberdefense/.

Macintosh, Duncan. 2019. “APNIC Foundation Reports Fund Raising Successes and Major Project Impacts.” Foundation. APNIC Foundation. July 11, 2019. https://blog.apnic.net/2019/07/11/apnic-foundation-reports-fund-raising-successes-and-major-project-impacts/.

Magan, Bhadrika. 2020. “Event Wrap Cyber Pacific Dialogue.” Intergovernmental Organisation. APNIC Blog. December 16, 2020. https://blog.apnic.net/2020/12/16/event-wrap-cyber-pacific-dialogue/.

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

NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE). 2021. “NATO Cooperative Cyber Defence Centre of Excellence.” 2021. https://ccdcoe.org/about-us/.

Organization of American States (OAS). 2019. “2018 Annual Report of the Inter-American Committee Against Terorism (CICTE) to the 49th Regular Periof of Sessions of the General Assembly.” http://www.oas.org/en/sms/cicte/session_2019.asp.

———. 2020. “OAS, Cisco and the Citi Foundation Open Applications for the Cybersecurity Innovation Fund.” https://www.oas.org/en/media_center/press_release.asp?sCodigo=E-108/20.

Schmitt, Michael N. 2013. *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge University Press.

Scroxton, Alex. 2020. “Bill Gates Backs Crest Fintech Security Scheme for Africa and Asia.” News Site. Computer Weekly. March 9, 2020. https://www.computerweekly.com/news/252479741/Bill-Gates-backs-Crest-fintech-security-scheme-for-Africa-and-Asia.

Singapore CSA. 2017. “Factsheet for Singapore’s ASEAN Cyber Capacity Programme.Pdf.” https://www.csa.gov.sg/-/media/csa/documents/sicw2016/amcc/factsheet_accp_final.pdf.

United States Government. 2018. “National Cyber Strategy of the United States of America.” https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

US Department of Justice. 2021. “The Department of Justice’s Office of Overseas Prosecutorial Development, Assistance and Training (OPDAT) Provides COVID-19 Related Technical Assistance to Partner Countries.” January 20, 2021. https://www.justice.gov/archives/criminal-opdat/blog/department-justice-s-office-overseas-prosecutorial-development-assistance-and.

U.S. Department of State. 2004. “The Fiscal Year 2005 Performance Summary U.S. Department of State.” https://2009-2017.state.gov/documents/organization/29325.pdf.

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