United Nations
Office on Drugs and Crime

UNODC
Civil Society Unit

PUBLIC-PRIVATE PARTNERSHIPS ON CYBERCRIME

REGIONAL PERSPECTIVES ON BEST PRACTICES, CHALLENGES, AND OPPORTUNITIES FROM THE AMERICAS, AFRICA, AND ASIA

Some materials and terms used in this publication, including those that have legal interpretation in different national contexts, reflect only the opinion and understanding of those who provided them and sources attributed to them, and do not imply the expression of any endorsement on the part of the United Nations.

This publication has been made possible thanks to the financial contribution of the Government of the United States of America.

PUBLIC-PRIVATE PARTNERSHIPS ON CYBERCRIME

REGIONAL PERSPECTIVES ON BEST PRACTICES, CHALLENGES, AND OPPORTUNITIES FROM THE AMERICAS, AFRICA, AND ASIA

List of Selected Abbreviations

AHC	Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes
AI	Artificial Intelligence
ASEAN	Association of Southeast Asian Nations
AU	African Union
CoE	Council of Europe
CSAM	Child sexual abuse material
CSOs	Civil society organizations
EU	European Union
GBV	Gender-based violence
GFCE	Global Forum on Cyber Expertise
ICTs	Information and communication technologies
ISPs	Internet service providers
LAC	Latin America and Caribbean
LEAs	Law enforcement agencies
OAS	Organization of American States
OSCE	Organization for Security and Co-operation in Europe
MOU	Memorandum of understanding
NCIIS	Non-consensual intimate image sharing
NGOs	Non-governmental organizations
PPPs	Public-private partnerships
UN	United Nations
UNODC	United Nations Office on Drugs and Crime
UNODC CSU	UNODC Civil Society Unit

EXECUTIVE SUMMARY

This report collects best practices, challenges, and opportunities for strengthening PPPs on cybercrime. To gather insights from the multistakeholder community, expert interviews and surveys focused on organizations' knowledge of and experience with national and regional public-private collaboration to prevent and fight cybercrime. The guiding questions examined existing initiatives and further explored the topics, approaches, and resources that can contribute to developing new and strengthening existing collaboration, and how such programmes benefit from multistakeholder collaboration. Interview questions for specific projects and case studies zoomed in on public-private mechanisms, motivation for actors to participate in such partnerships, key aspects driving their effectiveness, and importantly, examples of success worth following. However, this is not a toolkit on combatting cybercrime, nor an exhaustive overview of all legal and ethical aspects of public-private models of cooperation. The report is an initial multistakeholder assessment of the PPPs on cybercrime designed to serve as a practical tool for raising awareness about this complex issue.

CONTENTS

Acknowledgements

This report was drafted by Pavlina Pavlova (independent consultant) under the direction of Mirella Dummar and the guidance of Anders Frantzen (UNODC Civil Society Unit) and the Alliance of NGOs on Crime Prevention and Criminal Justice, as part of the Cybercrime Stakeholder Engagement Initiative. It aims to provide a practical overview of best practices, challenges, and opportunities for strengthening public-private partnerships (PPPs) on cybercrime with regional perspectives from the Americas, Africa, and Asia.

We would like to acknowledge the work of the numerous government officials, experts from international and regional organizations, private sector representatives, and civil society organizations who shared their insights and feedback. This report is dedicated to all stakeholders involved in implementing PPPs on preventing and countering cybercrime. Your engagement is the driving force behind successful collaboration.

KEY FINDINGS

1 Fostering collaborative partnerships

The prevention and fight against cybercrime require fostering collaborative partnerships that leverage the expertise and resources of each actor and meaningfully engage governments, industry, civil society, academia, technical experts, and other relevant stakeholders. The report identifies a critical need to further develop PPPs on cybercrime in the Americas, Africa, and Asia while considering regional, national, and local perspectives.

2 Types of existing cooperation

Types of existing cooperation extend to information-sharing initiatives, enabling law enforcement agencies, the private sector and other partners to facilitate the exchange of threat intelligence and best practices, capacity-building programmes that contribute technical expertise, resources and training, policy development and implementation through consultative and multistakeholder processes, awareness-raising activities bolstering cybersecurity practices, and a range of tools, including those aiming at dismantling criminal behaviour online, policy and strategy toolkits, reporting mechanisms, and rankings.

3 Barries to effective collaboration

Barriers to effective PPPs and other forms of multistakeholder collaboration comprise the absence of trust among partners, weak rule of law, conflicting legislative and regulatory frameworks, limited resources such as funding, technology, legal and technical expertise, and human capital, as well as lack of coordination, alignment, and motivation among partners.

4 Areas of cooperation

Areas of cooperation that can contribute to developing new and strengthening existing public-private collaboration on cybercrime include streamlining data requests, catalysing systematic information sharing and operational collaboration, integrating subtopics of emerging technologies, facilitating policy dialogue and context-aware legislation and regulation, building evidence about cybercrime, addressing cybersecurity inequality and support under-resourced targets of cybercrime, reinforcing the linkage between human rights safeguards and economic and social growth, and supporting the synergies between cyber capacity building and sustainable development.

5 Effective approaches

Effective approaches to public-private collaboration on cybercrime should prioritise building trust and supporting demand- and need-driven initiatives, multistakeholder cooperation, and inclusive models of partnerships. They should incorporate human rights standards and safeguards and seek regional synergies. The report recommends partnerships based on voluntary cooperation and adaptive models that reflect the dynamic nature of cybercrime. Such PPPs are well-positioned to adopt flexible strategies and facilitate ongoing assessment and updating processes necessary for continuous improvement.

6 Establishing PPPs on cybercrime

Establishing PPPs on cybercrime necessitates due diligence that involves a systematic needs assessment, evaluation of existing initiatives, and review of legislative and regulatory frameworks. It emphasises upholding human rights standards and ensuring data protection and privacy. Key steps include implementing capacity-building programmes, developing robust information-sharing mechanisms, and engaging in consultative policy development. All actors embarking on a PPP must perform risk assessments as part of their due diligence to ensure the establishment of a PPP is feasible.

Introduction

UNODC Civil Society Unit (CSU), through the Cybercrime Stakeholder Engagement Initiative, has facilitated the participation of the multistakeholder community, including CSOs, academic institutions, and the private sector in the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes (AHC) and other related processes.

The initiative aims to create opportunities for regional networking and advocacy for relevant stakeholders, while fostering clarity and meaningfulness of their engagement in the AHC negotiations. This engagement has been achieved through side events organised in the margins of the AHC sessions and exchanges between member states and stakeholders. Going forward, the initiative aims to facilitate closer cooperation between competent national authorities and representatives of CSOs, academia, and the private sector at the regional level.

In particular, the initiative elaborates on the well-established regional stakeholder engagement networks in the Americas, Africa, Asia, and Europe, enhanced by the presence of Regional Focal Points, to coordinate technical inputs and expertise to further the dialogue on potential PPPs in the context of the AHC and other related process. The initiative benefits from strong multistakeholder partnerships from CSOs, technology companies, associations, and cybersecurity experts.

As part of this initiative, UNODC CSU seeks to strengthen the analysis and the constructive capacity of PPPs related to preventing and countering cybercrime by assessing the strengths and needs of such partnerships around the regional stakeholder engagement networks and expert groups. The purpose of this report is to distil best practices and lessons learned, highlighting the examples of established partnerships and areas of potential cooperation between the public and private sectors, CSOs, and academia relevant to the Cybercrime Stakeholder Engagement Initiative and broader stakeholder engagement on cybercrime.

Methodology

This mapping exercise combined expert interviews and surveys that gathered practitioners' views and insights. With support from the Alliance of NGOs on Crime Prevention and Criminal Justice, surveys were distributed to a broad network of CSOs working in the Americas, Africa, and Asia.[1] The organizations were requested to share experiences with PPPs on cybercrime at their national and regional levels. 57 NGOs provided relevant feedback through the surveys, from which 30 organizations are based in Africa, 13 organizations in the Americas, 11 organizations in Asia, and 3 organizations are based outside of this geographic scope but are otherwise involved in partnerships in the targeted regions. The work of these organizations extends to transnational organised crime, crime prevention, criminal justice, cybercrime, cybersecurity, human rights, as well as gender-related and environmental issues and migration. 18 organizations operate at an international level, 11 at a regional level, 21 at a national level, and 7 at a local level.

The expert interviews involved representatives from over 20 international and regional organizations, national agencies, private companies, and CSOs with an equal representation of each stakeholder group. The combination of interviews and surveys aimed to effectively map the positive practices in PPPs addressing cybercrime, explore avenues for further improvement, as well as to identify the obstacles experienced by various stakeholders. However, it is important to recognise that the views and case studies outlined in this report represent only a fraction of the collective efforts undertaken in this field. Further report limitations include potential bias in collected responses and their geographic representation.

1 These regions were identified as priority areas to seek regional perspectives in the margins of the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes process, which sessions took place in Vienna and New York between 2022-2024. More information: https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home

part

01

PUBLIC-PRIVATE **COLLABORATION** ON CYBERCRIME

What are public-private partnerships?

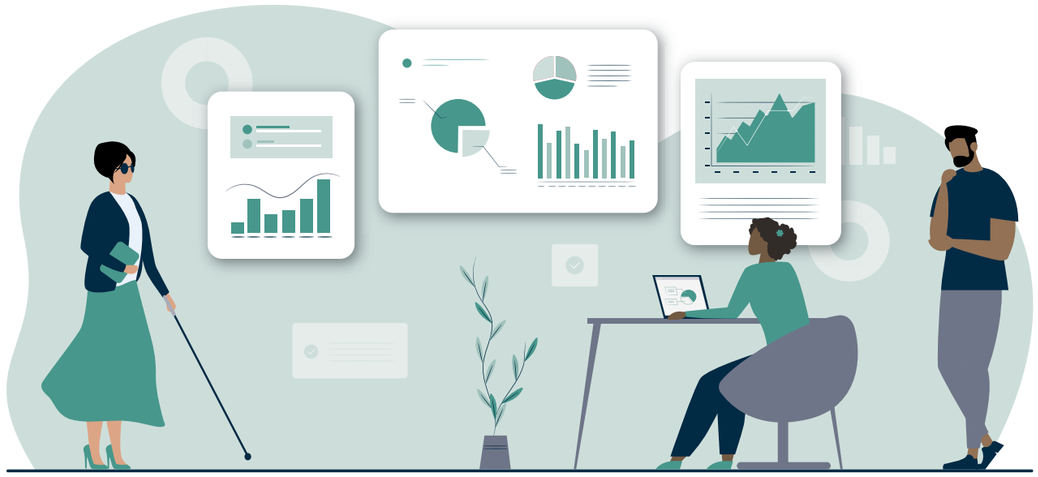
Over the past few years, cybercrime has increased in frequency, scale, and sophistication. Perpetrators target individuals, organizations, and critical sectors providing vital services. The complex and ever-changing nature of the cyber threat landscape requires collaboration across sectors to effectively address cybercrime and enhance cybersecurity. Cooperation with the private sector, including PPPs, plays a vital part in the fight against cybercrime, especially considering much of essential ICT infrastructure and digital services are owned, operated, and provided by privately owned entities.

From a government perspective, partnering with the private sector can provide substantial benefits. These include access to resources and expertise, a broader understanding of cyber threats, and collaboration to exchange information that improves defences and facilitates disruption efforts against cyber criminals. At the same time, private organizations have an interest in PPPs on cybercrime to protect their operations and customers. Public-private cooperation allows governments and stakeholders to leverage each other's strengths and address resource disparities and capacity gaps that may exist within individual stakeholder groups. Pooling resources and expertise from diverse sectors helps to maximise the impact and achieve common objectives more efficiently.

PPPs is an umbrella term that encompasses diverse models of cooperation, ranging from informal initiatives to contractual or mandated arrangements. They prominently serve as platforms for knowledge and information sharing, operational cooperation, capacity building, technical assistance, awareness raising, and designing practical tools such as reporting mechanisms. Public-private cooperation can be extended to other stakeholder groups. Civil society and academia in particular play vital roles in the effectiveness and sustainability of such partnerships. This report takes a broad view of public-private cooperation, including partnerships that are formed on an ad-hoc and informal basis, and those that are missing one of the public or private components but provide important examples for effective multistakeholder cooperations relevant to addressing cybercrime.

Who Are The Stakeholders?

Different stakeholders can be involved in different ways and at different stages of establishing PPPs. Stakeholders can include actors with a mandate, role, or responsibility in the process, as well as those with the resources and networks necessary to develop, implement, or review PPPs. Public-private collaboration can extend to organizations with the skills and expertise needed to inform the projects and their operationalisation, and those who are disproportionately impacted by the issue that the PPPs aim to tackle. Diverse groups of stakeholders can enhance partnerships on cybercrime. Each actor brings a unique blend of expertise, capacities, resources, and perspectives that can be developed and scaled in PPPs.



Governments provide regulatory frameworks, law enforcement capabilities, and access to intelligence. Their role is to draft and enforce laws, forming the legal basis for prosecuting cybercriminals and protecting citizens. LEAs bring expertise and authority to investigate and apprehend cybercriminals, often utilising specialised cybercrime units with advanced tools and training. These agencies collaborate with private sector partners to share intelligence and coordinate responses. Additionally, government agencies collect and analyse data on cyber threats, enhancing prevention and response strategies. The judiciary adjudicates cybercrime cases, ensuring justice and setting legal precedents that shape future enforcement practices.

Private sector partners can contribute to information sharing and threat analysis. Companies can host or have access to global datasets, including emerging threats, long-term or evolving trends, intelligence on criminal actors and groups, and their operations – all of which are necessary for law enforcement to carry out preventive action, investigations, prosecutions, or disruptions of cybercrime. The private sector can further support cybercrime prevention, detection, investigation, and disruption with targeted capacity building, innovative tools, technical expertise, and funding. The private sector generally includes ISPs, service providers, data custodians, and trade associations, as well as other private entities with specialised expertise, resources, technology, or services that enhance cybersecurity and the fight against cybercrime.

CSOs provide an array of functions that help to tackle cybercrime and its negative impacts and increase transparency of processes and partnerships. Many organizations assist governments with legal, regulatory, law enforcement, and judicial responses. They also support national authorities with collecting and analysing threat intelligence and employing open-source identifying techniques. Non-governmental stakeholders can provide knowledge and evidence of how cybercrime legislation and anti-cybercrime measures impact human rights and diverse communities. CSOs also work to build awareness about cyber threats, engage with communities to help them recognise threats to privacy and security online, and educate the public about their rights, as well as develop specific initiatives to protect vulnerable and targeted groups.

Relevant organizations from the non-governmental sector include, among others, those with expertise in transnational organised crime, crime prevention, criminal justice, cybercrime, cybersecurity, human rights, gender-related issues, migration, and environmental issues. Additionally, PPPs can include other organizations that engage with different groups and communities within society vulnerable to cybercrime, and organizations that work directly with the public on issues relating to cybercrime, cybersecurity and other related cross-cutting topics. These organizations can also encompass wider networks and umbrella groups.

Academia and researchers, such as university programmes, research entities, think tanks and independent experts and researchers whose expertise includes cybercrime play a part in the PPP ecosystem by contributing with research, knowledge, innovation, and critical insights. Academic institutions and research organizations also raise awareness through publications, conferences, training programmes, and toolkits. Moreover, technical experts, such as cybersecurity researchers, possess specialised knowledge and practical skills which enable them to conduct threat assessments, develop new technologies, and create innovative solutions to cybercrime.

International and regional organizations whose mandate or expertise include cybersecurity and cybercrime issues can facilitate cooperation and coordination among different stakeholders. These organizations provide frameworks for collaboration, set international standards, and offer platforms for information sharing and joint initiatives among trusted networks of stakeholders. Organizations such as the United Nations (UN), Interpol, Europol, the Council of Europe (CoE), the African Union (AU), the Organization of American States (OAS), the Association of Southeast Asian Nations (ASEAN), the Organization for Security and Co-operation in Europe (OSCE), and the World Bank provide technical assistance, capacity building, and funding support to bolster the efforts of national and local stakeholders in preventing and combating cybercrime, including through public-private models of cooperation.

What Are The Types of Public-private Collaboration?

PPPs can contribute to different activities related to cybercrime, encompassing prevention and detection, investigation, prosecution, and victim assistance. Areas of cooperation cover a wide range of activities, including but not limited to information sharing and threat analysis, joint operations to disrupt cybercrime, capacity building and technical assistance, policy development and implementation, awareness raising, development of tools and toolkits, or a combination of any of these components.

Information sharing initiatives provide general and ongoing support to improve and accelerate gathering, analysing, and acting on threat intelligence. Such partnerships between the public and private sectors enable and streamline access to data, allow sharing of information between different entities about the causes, incidents, and threats, as well as sharing broader experience, knowledge, and analysis. Operational collaborations form different but closely related types of partnerships in which companies are working to support LEAs or even directly disrupt criminal activities and infrastructures. This includes takedowns, which are happening in collaboration with the private sector, as well as providing concrete support for law enforcement and legal actions.

Capacity building encompasses a broad and varied set of activities providing assistance, resources, and training to enhance the capabilities to investigate and prosecute cybercrime or prevent, mitigate, and otherwise minimise its negative impacts. Collaboration to build capacities can take the form of technical assistance, joint training or exercises, and collaborative research, among others. Under technical assistance, partnering private sector entities provide tools and techniques to assist law enforcement in analysing or disrupting cyber threats. Joint training or exercises create platforms for the industry to upskill cybersecurity agencies and law enforcement. PPPs can also develop tools that increase capacity to prevent, disrupt, or otherwise respond to cybercrime, as well as toolkits, reporting mechanisms, and ranking platforms that help to assess cybersecurity readiness and posture.

Policy development and implementation involve collaboration between the public and private sectors to develop cybersecurity and cybercrime laws, regulations, strategies, or other policy and legal measures and instruments. Such consultative processes can take the form of established sector-specific or issue-driven advisory groups or ad hoc consultations focused on a particular piece of regulation or legislation.

Awareness raising programmes and initiatives can target the wider public as well as selected groups to educate and upskill individuals and communities. They can take on forms of educational events, training and workshops, media campaigns, public service announcements, community engagement programmes, and even industry-specific or issue-specific programmes such as healthcare or finance cybersecurity awareness or phishing and ransomware awareness programmes.

TIPS: Risk Assessment

Effective PPPs necessitate that all entities conduct a risk assessment of a partnership before it is embarked upon. This includes looking at contextual, programmatic and institutional risks. For more effective and impactful PPPs, the public sector should seek to share risks and rewards with the private sector and other partners. In addition, decision-making should be a collaborative process between the partnering entities, beginning in the planning phase, throughout the implementation of project goals, right through to monitoring and evaluation. A PPP strategy and expectations should be agreed upon and outlined to mitigate risks from the outset through due diligence and properly constructed partnership modalities and agreements.[2]

2 UNODC, Compendium of Promising Practices on Public-Private Partnerships (PPPs) to Counter Trafficking in Persons, https://www.unodc.org/documents/NGO/PPP/UNODC-PPP-Interactive.pdf

part

02

PUBLIC-PRIVATE PARTNERSHIPS **ON CYBERCRIME** IN THE AMERICAS, AFRICA, AND ASIA

Regional perspectives and selected examples from the Americas

At the regional level, the **Organization of American States (OAS)** seeks to build and strengthen cybersecurity capacity in the member states through technical assistance and training, policy roundtables, crisis management exercises, and the exchange of best practices related to ICTs. The OAS was the first regional body to adopt a regional cybersecurity framework, which addressed key areas such as public awareness, PPPs, and capacity building. To support the member states in their fight against cybercrime, the **Inter-American Committee against Terrorism (CICTE)** and the **Cybersecurity Program** develop and further the cybersecurity agenda in the Americas. The CICTE has done extensive work with PPPs on cybersecurity. The Cybersecurity Program, among other important initiatives, helps to establish national computer security incident response teams (CSIRTs). The CSIRTAmericas network provides threat intelligence and timely cybersecurity information among 29 CSIRTs from 20 OAS member states.[3] Finally, within the Meetings of Ministers of Justices, other Ministers, Prosecutors and Attorney Generals of the Americas (REMJA) framework, the OAS promotes international cooperation and exchange of information to increase the capacity of states to effectively fight cybercrime. Although REMJA does not currently have a PPP component, they engage with private enterprises through a working group and take the recommendations to the member states.[4]

PPP platforms can serve to gather government agencies, private companies, CSOs, and international and regional bodies to address both the prevention and responses to cybercrime. **InfraGard**[5] is a partnership connecting owners and operators within critical infrastructure to relevant state agencies. This initiative enhances the resilience of critical infrastructure against cyberattacks by fostering a community of informed and prepared stakeholders through education, information sharing, networking, and workshops. Complementing InfraGard is the **Internet Crime Complaint Center (IC3)**[6], the central hub in the United States for reporting cybercrime. IC3 offers the public a reliable and accessible reporting mechanism to submit information about suspected internet-facilitated criminal activity.

The **International Counter Ransomware Initiative (CRI)**[7] is the world's largest international cyber partnership, established by the United States. The CRI builds collective resilience to ransomware, disrupts the ransomware ecosystem, and designs policy approaches to combat ransomware. The **International Counter Ransomware Task Force (ICRTF)** brings together policy, law enforcement, and operational agencies from around the world to defend against and disrupt ransomware while building resilience against malicious cyber actors. While this is mainly an inter-governmental platform, it increasingly connects government agencies with industry partners for enhanced defensive and disruptive activities.

The **Europe Latin America Programme of Assistance against Transnational Organised Crime (EL PAcCTO)**[8] is an international cooperation programme funded by the **European Union (EU)** that supports the fight against transnational crime. The partnership on justice and security fights organised transnational crime through an integral approach to reinforce the rule of law in Latin America and the Caribbean (LAC). This initiative covers a range of different thematic crimes, including cybercrime. **EL PAcCTO 2.0**[9] further consolidates stable and direct relationships between European and Latin American and Caribbean justice, law enforcement and penitentiary institutions, addressing the entire criminal chain from an integral perspective through its work in three components: police, justice, and penitentiary.

The **EU CyberNet**[10] project focuses on strengthening capacity building through provisions of technical assistance to partner countries in areas of cybersecurity and countering cybercrime. The EU CyberNet also launched the **Latin American and Caribbean Cyber Competence Centre (LAC4)**[11], which serves as a training and knowledge hub for sharing expertise in cybersecurity and cybercrime, facilitating practical collaboration between the LAC region and the EU as well as other like-minded partners. The Centre is incorporated as an international NGO where countries and international organizations are encouraged to join. Membership in the organization includes the Dominican Republic, the Netherlands, Estonia, Panama, Honduras, El Salvador, Uruguay and organizations such as RedCLARA and Cyber 4.0 Competence Centre.

PPPs can target specific areas of cybercrime and issue-based cooperation, particularly on cross-cutting issues. This model is encouraged for developing innovative solutions to fight cybercrime. For instance, the **HEROES project**[12] works toward designing novel strategies to fight child sexual abuse and human trafficking crimes and protect victims. The project explores how to use the latest technological advances and strategies and supports investigation into these crimes and victims' protection. It develops an interdisciplinary, international, and victim-centred approach to establish a coordinated contribution with LEAs to address the specific needs of victims and provide protection, which can be limited due to a lack of coordination among stakeholders. Participating organizations include NGOs in Brazil, Colombia, Peru, and Uruguay.

3 Organization of American States (OAS), Cybersecurity Program, www.oas.org/ext/en/security/prog-cyber
4 Meetings of Ministers of Justices, other Ministers, Prosecutors and Attorney Generals of the Americas (REMJA), www.oas.org/en/sla/dlc/remja-en/remja.asp
5 InfraGard, www.infragard.org
6 Internet Crime Complaint Center (IC3), www.ic3.gov
7 International Counter Ransomware Initiative, https://counter-ransomware.org
8 EL PAcCTO, https://elpaccto.eu
9 EU CyberNet, *EL PAcCTO 2.0*, www.eucybernet.eu/project/el-paccto-2-0
10 EU CyberNet, *EU CyberNet – the bridge to cybersecurity expertise in the European Union*, www.eucybernet.eu
11 Latin America and Caribbean Cyber Competence Centre (LAC4), *The Bridge to cyber capacity building in the Americas*, www.lac4.eu
12 European Commission, *Novel Strategies to Fight Child Sexual Exploitation and Human Trafficking Crimes and Protect their Victims*, https://cordis.europa.eu/project/id/101021801

Many NGOs in the American region have a track record of engaging in public-private and broader multistakeholder partnerships. **SaferNet**[13] is a leading NGO focused on online safety that has worked in partnership with **Brazil's Federal Public Ministry**. They are recognised as the Safer Internet Center in Brazil and operate in three strategic arms, namely the National Cyber Crime Reporting Center (hotline), the National Guidance Channel on Internet Security and Brazil helpline and the Digital Citizenship Education actions. Together with Google, SaferNet Brasil has developed educational resources, awareness campaigns, and tools to combat cyberbullying, online child sexual abuse, and other cyber threats targeting and impacting children.

The **Electronic Frontier Foundation** is a non-profit digital rights group promoting Internet civil liberties globally. Their project **"Who Has Your**[14] aims to hold the private sector accountable to their users by analysing and comparing companies' privacy practices. The Latin American iteration **¿Quién defiende tus datos?** has cooperated with key digital rights groups to rate ISPs, holding them to account vis-à-vis privacy best practices and international human rights standards. The project does not include the private sector component directly in its design, but it has impacted the standards applied by technology companies and helped to improve privacy practices globally.

Regional perspectives and examples from Africa

The **African Union (AU)** is a regional organization with a key role in formulating policies and spearheading cyber initiatives in the region. The AU Convention on Cybersecurity and Personal Data Protection, also known as the **Malabo Convention**, covers a range of criminal activities and establishes procedures for investigating and prosecuting cybercrime. The **African Union Cyber Security Expert Group (AUCSEG)**[15] was established to provide advice to the African Union on technical, policy, legal, and other related cybersecurity matters at national, regional, and continental levels. This includes the dissemination of best practices in the fight against existing and emerging cybercrime. The Group consists of 10 members from across the five regions in Africa.

National authorities are pivotal for spearheading partnerships on cybercrime. The **Cyber Security Agency of Ghana (CSA)** has been collaborating with private companies to establish an industry forum[16] encompassing cybersecurity service providers, telecommunication network operators, civil society, and other relevant stakeholders. Its primary mandate is to provide a platform for industry players to discuss common interests, develop an industry code, and prepare a voluntary code to address issues outlined in the Cybersecurity Act, including the investigation and prosecution of cybercrime. Similarly, the **Joint Cybersecurity Committee of Ghana**[17] is an innovative mechanism with the authority to form subcommittees including private sector representatives. Both the Committee and the **Industry Forum** are set to be important platforms for promoting private sector participation in national cybercrime prevention measures.

The CSA has also been involved in ad hoc partnerships facilitating consultations on cybercrime legislation. Under the **Global Action on Cybercrime Extended (GLACY)+**[18], the Agency invited private industry stakeholders to the national conference on the Technical Implementation of the Council of Europe Convention on Cybercrime, also known as the **Budapest Convention**. This consultation gathered relevant national institutions, criminal justice authorities, and the private sector, and provided a platform for knowledge sharing among industry players. The Agency also held a public consultation for industry stakeholders on the Second Additional Protocol to the Budapest Convention on Enhanced Co-operation and Disclosure of Electronic Evidence to provide both public and private stakeholders with insights into the Protocol for improved operationalisation.

PPPs can take on the form of task forces, working groups, and other expert platforms for sharing information. The Technical Assistance to the **Uganda National Task Force Against Cybercrime**[19] includes an information-sharing function on regulatory mechanisms and rights-based law enforcement, as well as ways to enhance cooperation and provide mutual support in the management of cyber challenges. Core members of the national task force can reach out to other stakeholders and the public. The organizations making up the national task force include national agencies, but also non-state actors such as UNICEF and the Uganda Youth Development.

Two national initiatives in Togo outline diverse partnership models to build capacities on cybercrime. **Cyber Defense Africa**[20] is the national cybersecurity services company established from a strategic PPP between the Togolese Republic and a private company to support the country's operational security of information systems. Furthermore, the UN Economic Commission for Africa signed a MoU with the Government of Togo for the establishment of the **African Center for Coordination and Research in Cybersecurity (ACCR)**[21] to be situated in Lomé. The centre is set to provide expertise related to cybersecurity and the investigation of cross-border cybercrime. The partnership model with the private sector has been highlighted among the county's priorities in preventing and combatting cybercrime.[22]

13 SaferNet Brasil, https://new.safernet.org.br
14 Electronic Frontier Foundation, *Rating Internet Companies' Privacy Policies Around the World*, www.eff.org/qdtd
15 African Union, *African Union Cybersecurity Expert Group holds its first inaugural meeting*, https://au.int/en/pressreleases/20191212/african-union-cybersecurity-expert-group-holds-its-first-inaugural-meeting
16 Cyber Security Authority of Ghana, *CSA constitutes committee to facilitate the establishment of the Industry Forum*, www.csa.gov.gh/csa-constitutes-committee-to-facilitate-establishment-of-industry-forum.php
17 Cyber Security Authority of Ghana, *Fighting crime, a shared responsibility*, www.csa.gov.gh/fighting-cybercrime-a-shared-responsibility-csa-director-general
18 Council of Europe, *Global Action on Cybercrime Extended (GLACY)+,* www.coe.int/en/web/cybercrime/glacyplus
19 Cybil Portal, *Technical Assistance to the Uganda National Task Force Against Cybercrime*, https://cybilportal.org/projects/technical-assistance-to-the-uganda-national-task-force-against-cybercrime
20 Cyber Defense Africa, www.cda.tg
21 United Nations Economic Commission for Africa, *Lomé Declaration*, www.uneca.org/dite-for-africa/lomé-declaration
22 United Nations, *Togo and UN sign MoU to establish the African Cybersecurity Centre,* www.un.org/africarenewal/magazine/september-2022/togo-and-un-sign-mou-establish-african-cybersecurity-centre

The **Africa Cybersecurity Resource Centre (ACRC)**[23] exemplifies cybersecurity capacity collaboration between governments and private sector organizations in sector-specific areas. ACRC is led by a not-for-profit consortium of public and private partners to create an affordable shared platform for monitoring cyberattacks against financial service providers, facilitates information sharing and best practices, and provides incident response. The Centre also advises organizations on their cybersecurity posture and works on developing cybersecurity talent to meet Africa's growing demand for expertise.

NGOs can play a critical role in supporting national authorities to develop cybersecurity and anti-cybercrime capacities. For example, **Paradigm Initiative**, an NGO working to connect underserved young Africans with digital opportunities, trained Federal High Court Judges on internet governance and digital rights. The training sessions covered a spectrum of critical topics, including human rights and internet governance, national and regional cybercrime frameworks, and digital security for judicial officers.[24] **African Wildlife Foundation (AWF)** has partnered with the Ugandan government and a digital intelligence firm to train and certify wildlife law enforcement officers from the **Uganda Wildlife Authority** on mobile forensic investigations to enhance in-house capacity in the context of illegal wildlife trade.[25]

NGOs can be particularly well-positioned to implement advocacy and awareness-raising campaigns, reaching wider audiences and relying on trusted local networks. The UNODC supported the launch of the **Digital Ambassador program**[26] by **Cyber221**, an NGO promoting cyber security culture and digital education in Senegal. Awareness-raising programmes by Cyber221 also promote good practices on the internet, strengthen the protection of children online, and promote women in STEM and cybersecurity professions. **Spaces for Change (S4C)**, an NGO working to infuse human rights into social and economic governance processes in Nigeria, organises **Digital Security Clinics**[27] across West Africa building the capacity of activists and civil society organizations to navigate digital closures and cybersecurity threats. In addition, S4C trains judges on how to handle cases involving tensions between digital technologies and human rights as well as a digital literacy programme for students aimed at safeguarding the online safety of young people.

23 Africa Digital Financial Inclusion Facility, *Africa Cybersecurity Resource Centre (ACRC) for Financial Inclusion,* www.adfi.org/projects/africa-cybersecurity-resource-centre-acrc-financial-inclusion
24 Paradigm Initiative, *Nigeria: Paradigm Initiative Trains Federal High Court Judges on internet governance and digital rights*, https://paradigmhq.org/nigeria-paradigm-initiative-trains-federal-high-court-judges-on-internet-governance-and-digital-rights
25 African Wildlife Foundation, *Uganda Wildlife Authority to Benefit from Cybercrime Investigations Training*, www.awf.org/pressroom/uganda-wildlife-authority-benefit-cybercrime-investigations-training
26 UNODC, *Newsletter by the Global Programme on Cybercrime on its activities in Africa,* www.unodc.org/documents/Cybercrime/tools-and-resources/unodc_cyber_crunch_newsletter_issue01_sep2022.pdf
27 Spaces for Change, *S4C's digital literacy initiative is keeping 300+ young people safe on the internet*, https://spacesforchange.org/s4cs-digital-literacy-initiative-is-keeping-300-young-people-safe-on-the-internet

Regional perspectives and examples from Asia

Regional organizations like the **Association of Southeast Asian Nations (ASEAN)** offer a platform for the member states to share and offer regional perspectives, exchange information on emerging and existing threats and build capacity. The Cyber ASEAN Framework[28] has four pillars: international collaboration, international technical standards, information-sharing and incident or threat management, and inclusion, which are flexible and iterative to meet changing cybersecurity policy issues and priorities. ASEAN recently concluded a project **"Building Anti-Cybercrime Capacity in ASEAN Through Simulation"**[29] aimed at cyber resilience in ASEAN countries by fostering the understanding of the measures needed to fight cybercrime and build informal networks between ASEAN stakeholders. The project was implemented by **Chatham House** through two key components. The cybercrime capacity-building workstream looked at strategic approaches to cybercrime responses. The distilled recommendations were subsequently applied in the implementation of simulation exercises in the ASEAN region. The equality, diversity and inclusion (EDI) in cybercrime workstream produced a toolkit providing guidance on integrating gender and inclusion into cybercrime capacity-building projects. The toolkit **"Integrating gender in cybercrime capacity building"**[30] has been designed for practitioners to promote gender-sensitive design and implementation for a wide range of capacity-building activities.

Public-private collaboration can help forge a strategic alliance and advance national digital security through innovative features and education. The PPP between **Google Singapore** and the **Cyber Security Agency of Singapore**[31] includes launching a security feature in Google Play Protect to block harmful apps and enhance mobile security. The Agency also established separate cooperative efforts with **Microsoft** and **Google**[32] on national cyber defence and cybersecurity. Recognising that in cyberspace, multistakeholder cooperation is key, the partnerships are set to facilitate cyber threat intelligence sharing, joint operations to tackle cybercrime and malicious cyber activity, exchanges on emerging and critical technologies, such as artificial intelligence, as well as capacity-building efforts.

28 Cyber ASEAN Network, *Advancing Cyber Resiliency and Capacity in Southeast Asia*, https://downloads.ctfassets.net/corl1354p0t3/750MZKJ7tfh9NSwTdPviqG/9dec46e2d311f2f8b130c28600a55fba/CyberAsean_Report.pdf
29 Chatham House, *Building Anti-Cybercrime Capacity in ASEAN Through Simulation Exercises*, www.chathamhouse.org/about-us/our-departments/international-security-programme/building-anti-cybercrime-capacity-asean
30 Chatham House, *Integrating gender in cybercrime capacity-building*, www.chathamhouse.org/2023/07/integrating-gender-cybercrime-capacity-building/about-toolkit
31 Tech Wire Asia, *Google's commitment to security bolstered by partnership with the CSA,* https://techwireasia.com/02/2024/google-singapore-teams-up-with-csa-for-enhanced-mobile-security
32 Cyber Security Agency of Singapore, *CSA Collaborates with Microsoft and Google to Strengthen National Cyber Defence and Cybersecurity*, www.csa.gov.sg/News-Events/Press-Releases/2023/csa-collaborates-with-microsoft-and-google-to-strengthen-national-cyber-defence-and-cybersecurity

The **Australian Signals Directorate** and **Microsoft**[33] also announced a collaboration to improve the joint capability to identify, prevent and respond to cyber threats posed by malicious actors.

An example of capacity-building multistakeholder cooperation is the **Pacific Cyber Security Operational Network (PaCSON)**[34], which is an operational cyber security network of regional working-level cyber security experts in the Pacific. PaCSON coordinates activities benefiting the regional network of cyber security incident response professionals through encouraging collaboration on best practice, sharing information and developing incident response capability. The PaCSON network consists of technical experts from eligible governments across the Pacific and is supported by other partners including not-for-profit organizations and academia.

Under-resourced cyber-poor organizations deserve particular attention as they can easily fall victims to cybercrime. The Asia Foundation launched the **APAC Cybersecurity Fund**[35] to bolster the cyber capabilities of underserved micro and small businesses, nonprofits, and social enterprises. Sponsored by the **Google**'s philanthropic arm, the fund is working with implementing organizations and universities across the region. The Asia Foundation aims to equip local communities and students via upskilling tools and cyber clinics to protect against online risks. The initiative will span 13 locations, including Bangladesh, India, Indonesia, Japan, Korea, Malaysia, Pakistan, Philippines, Singapore, Sri Lanka, Thailand, and Vietnam.

Finally, to foster more inclusive multistakeholder partnerships, academia and researchers can not only provide objective research and input into regulatory and legislative initiatives, but also help to build capacities under PPPs. For example, the **Seven Centres of Excellence**[36], funded by the **Higher Education Commission of the Ministry of Education of Pakistan**, focus on technology research and forensics, as well as sharing technical resources and expertise.

The public-private and broader multistakeholder initiatives across Asia illustrate the diverse approaches and partnerships essential for enhancing capacities in the region. Furthermore, drawing from the examples of public-private cooperation in the Americas, Africa, and Asia, it is notable that while some PPPs such as those covering information sharing and operational cooperation can be strictly limited to fighting cybercrime, many other initiatives, particularly capacity-building collaboration can cover broader areas and extend to cybersecurity. Therefore, many cyber-PPPs do not have clear delineations and encompass various activities related to the prevention, disruption, mitigation, and investigation of cybercrime and strengthening cyber resilience. Through a combination of ad hoc, strategic, issue-based, sector-specific, informal and formalised strategic collaboration, these partnerships help to create a more secure and resilient digital landscape.

33 Australian Government, *Microsoft's investment in Australia's cyber security,* www.cyber.gov.au/about-us/news/microsofts-investment-in-australias-cyber-security
34 Pacific Cyber Security Operational Network (PaCSON), https://pacson.org
35 The Asia Foundation, *APAC Cybersecurity Fund*, https://asiafoundation.org/2023/10/09/apac-cybersecurity-fund
36 Higher Education Commission of Pakistan, *Centers of Excellence*, https://rfi.hec.gov.pk/coe/national-centers-established-psdp

Global public-private collaboration on cybercrime

The **Global Forum for Cyber Expertise (GFCE)**[37] is a multistakeholder international hub, gathering a community of over 200 members and partners, including governments, international organizations, private companies, and academics. The GFCE operates the **Cybil Portal**[38] providing a comprehensive database of projects, tools, and publications on cyber capacity building. The GFCE's Clearing House is a global mechanism that connects the member countries with cyber capacity needs with partners who can offer support, such as the Regional Hubs and African Cyber Experts (ACE) Community. The GFCE community shares information and best practices in thematic working groups, which also address cybercrime.[39]

Parties to the Budapest Convention can engage in PPPs targeting the treaty's operationalisation as well as capacity-building efforts. The **Octopus Project**[40] is a **Council of Europe** project based on voluntary contributions from state parties and observers to the Convention on Cybercrime and other public and private sector organizations, aiming to support the Convention's implementation. The **Global Action on Cybercrime Extended (GLACY)+**[41] is a joint project of the **European Union** and the Council of Europe that strengthens the capacities of states, such as Chile, the Dominican Republic, Ghana, Senegal, Sri Lanka, the Philippines, Mauritius, and Tonga to apply legislation on cybercrime and electronic evidence and to enhance their abilities for effective international cooperation in this area. The project's outcomes cover the reinforcement of policies and strategies, as well as relevant aspects of cybersecurity and partnerships with the private sector.

Information sharing, threat analysis, and incident response are among the key priorities incentivising PPPs on cybercrime globally. Examples such as the **Partnership against Cybercrime (PAC)**[42] by the **World Economic Forum** highlight how public-private cooperation can create a platform for sharing insights and continuous exploration of approaches to drive effective collaboration against cybercrime. The **Cyber Fusion Centre (CFC)**[43] is another successful initiative for sharing intelligence. This format brings together cyber experts from law enforcement and industry to gather and analyse information on cybercriminal activities to provide countries with coherent and actionable intelligence. Finally, hosted by the **World Economic Forum**, the **Cybercrime Atlas**[44] is a collaborative effort by leading companies.

37 Global Forum for Cyber Expertise, https://thegfce.org
38 Global Forum for Cyber Expertise, *Cybil Portal*, https://cybilportal.org
39 Global Forum for Cyber Expertise, *Cybercrime*, https://thegfce.org/theme-gfce/cyber-crime
40 Council of Europe, *Octopus Project,* https://rm.coe.int/2542-newoctopus-summary-v2/1680a02d03
41 EU CyberNet, *GLACY-e Project on Global Action on Cybercrime Enhanced*, www.eucybernet.eu/project/glacy-e
42 World Economic Forum, P*artnership Against Cybercrime*, www.weforum.org/projects/partnership-against-cybercime
43 Interpol, *Cyber Fusion Centre,* www.interpol.int/en/Crimes/Cybercrime/Cybercrime-threat-response
44 World Economic Forum, *Cybercrime Atlas,* https://initiatives.weforum.org/cybercrime-atlas/home

The Atlas is an open-source resource for members only that consists of a group of investigators open to discussions on a strategic level and facilitates joint investigations of criminal actors through a group of corporate volunteers. Its open-source investigators also research criminal actors. Finally, the **Forum of Incident Response and Security Teams (FIRST)**[45] is a successful model of partnership that enables incident response teams to respond to security incidents more effectively by bringing together a variety of computer security incident response teams from governmental, commercial, and educational organizations.

Cooperation between technology companies and LEAs can take many forms, including information sharing, threat analysis, and incident response, often channelled through specialised cyber units. **Google's Threat Analysis Group (TAG)** proactively identifies emerging cyber threats, including malware, phishing campaigns, and zero-day vulnerabilities and analyses the tactics, techniques, and procedures. The Group regularly shares information about emerging cyber threats, vulnerabilities, and attack trends with relevant government agencies and national emergency response teams. **Google Cloud's Mandiant Cybersecurity Consulting**[46] collaborates with government agencies and other security companies to respond to major cyber incidents. Similarly, **Microsoft's Digital Crimes Unit**[47] is an international team of technical, legal, and business experts that has been providing insights into online criminal networks as well as evidence used in criminal referrals to law enforcement. The Unit also shares information to assist with victim remediation and supports education campaigns and the development of technical countermeasures to combat cybercrime.

The **SIRIUS** project[48] helps both law enforcement and judicial authorities access cross-border electronic evidence for criminal investigations and proceedings. Co-implemented by **Europol** and **Eurojust**, in close partnership with the **European Judicial Network**, SIRIUS is a central reference point for regional knowledge sharing on cross-border access to electronic evidence. This project supports investigators' capacity to cope with both the complexity and volume of cybercrime by providing products such as standardised guidelines on cooperation processes between competent authorities and specific service providers, with emphasis on the critical area of cross-border requests to access electronic evidence.

PPPs can provide actionable assistance to people and organizations impacted by cybercrime. **No More Ransom**[49] is a public-private initiative by the **National High Tech Crime Unit of the Netherlands' police, Europol's European Cybercrime Centre**, and private companies with the goal of helping victims of ransomware retrieve their encrypted data without having to pay the criminals. Helplines are essential tools for assisting and supporting victims and witnesses of cybercrime. Such partnerships play a critical role in addressing the persistent problem of underreporting. The **Digital Security Helpline**[50] by **Access Now** is a member of the **Civil Society Computer Emergency Response Team (CiviCERT)**, an accredited CERT focused on improving the incident response capabilities of civil society groups and individuals around the world. CiviCERT is an initiative of **Rapid Response Network (RaReNet)**, bringing together non-governmental organizations, internet content and service providers, and individuals who contribute their time and resources to improve the security awareness of civil society groups.

Toolkits can help states and organizations to build capacities on PPPs. A critically important initiative in this area is the toolkit **"Combatting Cybercrime: Tools and Capacity Building for Emerging Economies"**[51] by the **World Bank**. The Assessment Tool in the report enables countries to evaluate their current capacity to respond to cybercrime and identify capacity-building priorities. The toolkit provides a comprehensive overview of PPPs on cybercrime, detailing the considerations when building PPPs, barriers to effective cooperation, and examples of cyber-PPPs. The recent report **"Public-Private Partnerships to Combat Ransomware"**[52] by the **Institute for Security and Technology** provides guidance for governments on how to set up or improve their fight against ransomware through PPPs, identifies existing partnerships, and offers a step-by-step guide on how to establish PPPs to mitigate ransomware and other cyber threats.

Rankings can support effective resource allocation and raise awareness among key partners. The **Global Cybersecurity Index (GCI)**[53] by the **International Telecommunication Union (ITU)** is an established reference measuring the commitment of countries to cybersecurity. Among its performance indicators, the Index measures the number of officially recognised national or sector-specific PPPs for sharing cybersecurity information and assets between the public and private sectors. The **World Cybercrime Index**[54] is a recent effort to rank countries by their cybercrime threat level. This partnership between the **University of Oxford** and the **University of New South Wales in Canberra** assesses the most significant sources of cybercrime at a national level to support early interventions in at-risk countries. By identifying major cybercrime hubs, the initiative aims to direct public and private sector funding towards high-risk areas, ensuring resources are allocated where they are needed most.

45 Forum of Incident Response and Security Teams, www.first.org
46 Google Cloud, *Mandiant Cybersecurity Consulting,* https://cloud.google.com/security/consulting/mandiant-services?hl=en
47 Microsoft, *Digital Crimes Unit: Leading the fight against cybercrime,* https://news.microsoft.com/on-the-issues/2022/05/03/how-microsofts-digital-crimes-unit-fights-cybercrime
48 Europol, *Sirius Project,* www.europol.europa.eu/operations-services-innovation/sirius-project
49 No More Ransom, www.nomoreransom.org/en/index.html
50 Access Now, *Digital Security Helpline*, www.accessnow.org/help/#community-resources
51 World Bank, Combatting Cybercrime: Tools and Capacity Building for Emerging Economies, https://documents.worldbank.org/en/publication/documents-reports/documentdetail/355401535144740611/combatting-cybercrime-tools-and-capacity-building-for-emerging-economies
52 Institute for Security and Technology, *Public Private Partnerships to Combat Ransomware: An inquiry into three case studies and best practices,* https://securityandtechnology.org/virtual-library/reports/public-private-partnerships-to-combat-ransomware
53 International Telecommunication Union, *Global Cybersecurity Index*, www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx
54 University of Oxford, *The World Cybercrime Index*, www.alumni.ox.ac.uk/article/mapping-global-cybercriminals

part

03

CHALLENGES TO PUBLIC-PRIVATE COLLABORATION **ON CYBERCRIME**

LACK OF TRUST

Lack of trust has been identified as a key challenge in fostering effective PPPs on cybercrime. Trust is vital for effective collaboration between public and private entities, and the level and quality of information sharing correlates with the level of trust between partnering entities. Trust impacts how requests are dealt with, and how timely. Lack of confidence can hinder the sharing of necessary information, threat intelligence, incident data, and best practices and prevent effectively combating cyber threats. The private sector can be reluctant to cooperate with government agencies if there are concerns relevant to data privacy, regulatory compliance, or fear of damaging their reputation. Similarly, government agencies may be hesitant to share sensitive information due to concerns about data security, potential misuse of shared information, and the risk of exposure to reputational damage.

WEAK RULE OF LAW

Weak rule of law undermines trust between partners and prevents effective collaboration. Partnering organizations must have a clear basis for cooperation with government agencies to prevent potential misuse of information or penalisation. Adhering to human rights frameworks and embedding robust safeguards into PPPs is a prerequisite for cooperation, especially for companies operating across jurisdictions and held to account to international standards. PPPs can be perceived negatively if they are mandated, imposed, or otherwise forced on private entities and operationalised in secrecy without the necessary transparency measures and oversight mechanisms.

CONFLICTING LEGISLATIVE AND REGULATORY FRAMEWORKS

Conflicting legislative and regulatory frameworks create hurdles to implementing PPPs. Given the transnational nature of cybercrime, evidence and resources are often scattered across different jurisdictions. Discrepancies or variations in applicable frameworks prevent efficient and streamlined cooperation. Divergent laws and regulations related to data protection, information sharing, and liability can create legal uncertainties and compliance challenges. For instance, differences in data protection regulations between countries can hinder cross-border information sharing and operational collaboration. As companies regularly operate across borders, they need to consider how to share data while respecting applicable legal provisions and regulatory requirements. If these frameworks conflict, the private sector is discouraged from cooperation and may refrain from voluntary disclosures or closer cooperation to avoid potential negative repercussions.

LIMITED RESOURCES

Limited resources, funding, technology, legal and technical expertise, and human capital impede the organizations' ability to actively participate in PPPs. Given the technical nature of cybersecurity and the complexities involved in investigating and prosecuting cybercrime, certain public and private stakeholders may lack the necessary expertise to effectively contribute to discussions on developing strategies to enhance cybersecurity and responses to cybercrime. Disparities in capacity and expertise among public and private sector entities translate into unequal access to resources, and certain sectors may face unique challenges due to their reliance on legacy systems or outdated technologies. Many organizations operate on limited budgets and with inadequate resources. Capacity gaps are experienced across the board and can be particularly pronounced in the public sector, as well as in micro-, small- and medium-sized enterprises and under-resourced NGOs. Multinational corporations and technology companies may face challenges in allocating adequate resources to their cybersecurity and anti-cybercrime efforts. Additionally, they might deprioritize cooperation with countries that are not considered key markets, or where language and cultural barriers hamper effectiveness and necessitate further investments.

LACK OF COORDINATION, ALIGNMENT, AND MOTIVATION

Lack of coordination, alignment, and motivation between partnering organizations can create challenges for establishing and sustaining PPPs. Diverse actors and stakeholder groups have varying priorities, interests, and approaches. Government agencies may prioritise defence and security objectives, while the private sector may focus on streamlining operations, protecting intellectual property, and maintaining customer trust. Overlapping or competing programmes and initiatives can duplicate existing efforts, splinter, and waste resources, frustrate partners, overwhelm the channels for reporting or communication, and consequentially hinder efficient collaboration.

part

04

OPPORTUNITIES FOR DEVELOPING PUBLIC-PRIVATE **COLLABORATION ON CYBERCRIME**

STREAMLINING DATA REQUESTS

Streamlining data requests has been identified as a top priority for public-private cooperation. About half of all criminal investigations include a cross-border request to access electronic evidence such as data from messaging or email services, or social media.[55] Despite a number of existing training programmes in this area, requesting electronic evidence from data custodians responding to these requests remains a hurdle in the effective investigation and prosecution of cybercrime. Both the public and private sectors have demonstrated a strong interest in supporting further initiatives to build capacities, trust, and understanding. PPPs such as training programmes and specialised tools could provide further guidance on how to streamline data requests and help to gather views on different legislative approaches. Compendiums of best practices, databases that allow for a search for relevant information, and other open-source tools could inform relevant entities about their obligations and guide them on how to proceed under different legal and regulatory regimes. A multistakeholder examination applying human rights principles to determine what constitutes a valid request can further help to close the capacity and trust gaps between actors. Such initiatives would be particularly beneficial for countries revising national cybersecurity and cybercrime legislation.

CATALYSING SYSTEMATIC INFORMATION SHARING

Catalysing systematic information sharing has been highlighted as a potential avenue for strengthened PPPs. Collaboration facilitating the timely exchange of threat intelligence and incident data oftentimes intensifies following a major incident and during operational cooperation but ceases afterwards. PPPs can overcome the ad hoc nature by creating and incentivising regular channels of communication for sharing intelligence, data, and trends. Ongoing and formalised exchanges can help to make informed decisions and enable timely responses and adaptation to the changing threat landscape, which are all essential components of the fight against cybercrime. Importantly, due to the risks involved in allowing data transfers between different entities both the transferors and transferees of that data must be diligent and careful within the information-sharing process. This includes ensuring full compliance with all national and regional data protection laws and regulations.[56]

55 Europol, *Sirius Project*, www.europol.europa.eu/operations-services-innovation/sirius-project
56 UNODC, *Compendium of Promising Practices on Public-Private Partnerships (PPPs) to Counter Trafficking in Persons*, www.unodc.org/documents/NGO/PPP/UNODC-PPP-Interactive.pdf

INTEGRATING SUBTOPICS OF NEW AND EMERGING TECHNOLOGIES

Integrating subtopics of new and emerging technologies such as artificial intelligence (AI), quantum computing, cryptocurrency tracing, blockchain solutions, dark web monitoring, and new developments and techniques relevant to the Cyber Crime Emergency Response Teams (C-CERTs) can increase the added value of existing PPPs and prompt new multistakeholder partnerships. Constructive collaboration between LEAs and technology companies can help build capacities and integrate new tools and innovative approaches, in areas such as identifying fake or synthetic illegal content, collecting and analysing threat intelligence, and supporting investigations through gathering, examining, and interpreting open-source intelligence.

CONSULTATIVE PROCESSES

Consultative processes on cyber-related legislation and regulation can create avenues for issue-based public-private cooperation and provide benefits for both governments and stakeholders. Through facilitating policy dialogue, governments can tap into the knowledge and expertise of the private sector, allowing for informed, streamlined, and context-awareness legislation and regulation and help to ensure meaningful and sustainable implementation of the agreed measures. Broader stakeholder engagement with NGOs and academia contributes to the diversity of views and expertise and helps to design frameworks that address cybercrime while upholding human rights and privacy standards.

BUILDING EVIDENCE ABOUT CYBERCRIME

Building evidence about cybercrime, its impact, perpetrators and victims through improved reporting, evidence-based and data-driven approaches, collection of testimonies, and support to cybercrime victims and witnesses that provides remedies and redress. Such PPPs can support community work with cybercrime victims, improve assistance and redress mechanisms, and raise awareness about the applicable cybercrime legislations, rights of cybercrime victims and witnesses, and effective remedies for individuals whose data was mishandled or unlawfully disclosed as part of the investigation.

ADDRESSING CYBERSECURITY INEQUALITY

Addressing cybersecurity inequality through PPPs can focus on helping under-resourced targets of cybercrime and closing the remaining capacity gaps in cybersecurity. Constraints can be particularly experienced by cybersecurity-poor organizations from among micro-, small- and medium-sized enterprises and NGOs. Concurrently, such entities have been targeted by cybercriminals with increasing scale and frequency. Scalable solutions need to ensure protection for vulnerable organizations and increase their capacity to meaningfully participate in multistakeholder partnerships combatting cybercrime. PPPs can identify and propel sustainable models for supporting entities involved in critical cybersecurity functions.

STRENGTHENING THE LINKAGE

Strengthening the linkage between human rights and economic and social growth can improve how companies approach data protection and privacy safeguards in their daily operations. Local companies often do not have the capacity to consider and apply international human rights standards in their daily operations. However, once these entities expand into foreign markets and need to store data or export technology across jurisdictions, they may encounter mounting costs of compliance. Public-private cooperation can address this problem by developing training programmes and disseminating cybersecurity toolkits tailored for diverse entities to integrate human rights standards and best practices in data protection into operations.

SUPPORTING THE SYNERGIES

Supporting the synergies between cyber capacity building and sustainable development, as well as other related issues, such as the importance of adhering to human rights standards, can improve holistic models of cooperation. Cyber threats can erode end-users' trust and discourage citizens from adopting digital solutions. Without effective cybersecurity measures and secure infrastructure in place, cybercrime may undermine the stability of digitalised societies, making innovative technologies a source of risk rather than a source of sustainable development. PPPs focused on cybersecurity maturity are essential preventive measures that can reduce the impacts of cybercrime and mitigate potential negative consequences.

part

05

EFFECTIVE APPROACHES TO STRENGTHENING PUBLIC-PRIVATE **COLLABORATION ON CYBERCRIME**

PRIORITISE BUILDING TRUST

Trust among the public and private sectors encourages information sharing, which remaining inefficiency creates a critical hurdle for facilitating cooperation on cybercrime. Public-private initiatives cannot properly function and fulfil their objectives without guarantees of protection, privacy, and other necessary safeguards for participating entities. Successful efforts rely on clear expectations, secure communication channels, active participation, and renewed commitment to agreed-upon norms and principles. Trust between governments and stakeholders can be strengthened when actors lead by example, deliver results, actively engage, and promote transparency. PPPs need to create trusted networks that facilitate meaningful participation and open exchanges, including through promoting person-to-person collaboration, in-person exchanges, and shared ownership. Regular meetings, interactive exchanges, joint exercises, and updated information-sharing platforms have been highlighted as best practices for building confidence between partners.

DEMAND-DRIVEN APPROACH

PPPs need to identify and address the actual needs on the ground, avoid duplication, and consider the local contexts and existing partnerships. The public-private design should respond to the national and regional realities to ensure sustainable outcomes. Prior needs assessment should also consider that different actors may be subject to different regulatory and compliance requirements. The type of operations and the size of companies also impact their resources, capacity, and motivation to engage in partnerships. Micro-, small- and medium-sized enterprises may prioritise capacity building to respond to cybercrime, for example, in the form of training, databases, or toolkits. International corporations and large companies may be interested in influencing policy decisions, adhering to standards in the supply chain, and making principles universal across jurisdictions to simplify their cross-border operations.

MULTISTAKEHOLDER APPROACH

PPPs can benefit from broader multistakeholder partnerships, facilitating the exchange of diverse expertise and perspectives as well as sharing established and trusted networks. By fostering partnerships across various stakeholder groups, such as NGOs, academia, and the technical community, PPPs can better reflect on how cybercrime legislation and anti-cybercrime measures impact individuals and communities, enhance threat intelligence by tracking malicious perpetrators and investigate the harm inflicted by cybercrime, and sensitise public-private collaboration by informing about the lived realities of cybercrime victims and witnesses. Multistakeholder networks are also well-positioned to work on issue-based and thematic partnerships, such as the fight against CSAM, NCIIS or GBV, and to drive cross-cutting and innovative solutions.

INCLUSIVE APPROACH

Several types of PPPs, including awareness-raising campaigns, advocacy initiatives, and policy development efforts benefit from reaching broader audiences and the public. Such partnerships should prioritise inclusive setups and open dialogue to foster diversity and ensure that the perspectives and experiences of affected individuals and communities are meaningfully considered. Engaging diverse groups helps to develop informed and equitable partnerships that are responsive to the unique challenges and needs of marginalised or underrepresented groups. Inclusivity should also extend to the participation of local organizations to ensure that solutions are tailored to the specific needs and context of the community, increasing their local ownership, effectiveness and sustainability. CSOs with a track record of engagement in specific areas bring valuable insights and knowledge about the community, fostering trust and engagement among stakeholders and the wider public. This collaboration enhances the legitimacy and relevance of initiatives, making them more likely to succeed and be supported by the recipients and target audience.

HUMAN RIGHTS-BASED APPROACH

PPPs that embed human rights standards can ensure that efforts addressing cybercrime respect and protect fundamental freedoms, thereby fostering trust and legitimacy among stakeholders and the public. Such cooperation emphasises accountability and transparency, both essential for building robust and ethical collaborative frameworks. By prioritising human rights, these partnerships can design more inclusive and sustainable solutions, ensuring that interventions are effective, socially responsible, and widely supported. Furthermore, incorporating human rights considerations can help mitigate potential negative impacts on vulnerable populations and promote equitable access to justice and protection. This approach can also enhance international cooperation by aligning with global human rights norms and standards, creating a unified front against cybercrime.

REGIONAL APPROACH

Partnering or otherwise closely engaging with regional organizations helps to ensure clarity on how new PPPs will complement, rather than duplicate, other existing anti-cybercrime initiatives. Many regional organizations boast established trust and a track record of successful partnerships, aiding both emerging and existing PPPs in the effective sharing of resources and enhanced sustainability. These organizations often have deep insights into regional specificities and challenges, allowing for tailored strategies. Furthermore, their established networks can facilitate smoother communication and coordination among stakeholders, leading to more cohesive and comprehensive PPPs.

VOLUNTARY APPROACH

Cross-border cooperation, information sharing, threat analysis, joint investigations, and technology transfers are common types of partnerships between the public and private sectors. PPPs established on a voluntary basis, rather than mandated, can incentivise proactive exchanges and enhance the effectiveness of cybercrime prevention, mitigation, investigation and enforcement measures. Additional incentives for cooperation, such as rewarding companies that actively contribute to these partnerships, can further support voluntary and proactive engagement, fostering a collaborative environment that benefits stakeholders and strengthens the overall resilience against cyber threats.

ADAPTIVE APPROACH

Recognising the dynamic nature of cybercrime, PPPs should adopt flexible strategies that facilitate continuous assessment and updating. These strategies should leverage emerging technologies and threat intelligence, while also adapting to evolving regulatory environments. As expectations, motivations, and constraints of partnering entities may change over time, PPPs should include regular re-assessment of alignment and contributions from partners. Effective communication and a “culture of collaboration” are essential for navigating hurdles within the partnership and encouraging feedback and input from all parties. Defining success metrics to measure the impact and success rate of joint efforts helps to refine partnership models, convening methods, and the overall structure and goals of PPPs as needed, ensuring they remain responsive and effective in preventing and combatting cybercrime.

AFTERWORD

This report has sought to provide an overview of some of the benefits, challenges, and considerations to be made in promoting public-private partnerships on cybercrime. Based on regional stakeholder dialogues, focused interviews, and surveys, stakeholders consistently acknowledged that effectively addressing cybercrime requires collaborative efforts among diverse actors. This necessitates joint partnerships between public agencies and the private sector, as well as broader outreach to civil society and academia. Leveraging the public-private model can contribute to facilitating systematic communication and exchanges and creating platforms that bolster and streamline collaboration.

As emphasised at the onset, this report is not a toolkit on combatting cybercrime, nor an exhaustive overview of all legal and ethical aspects of public-private models of cooperation. The report provides an initial multistakeholder assessment of the PPPs on cybercrime designed to serve as a practical tool to level the playing field among organizations across diverse regions.

Key findings suggest that creating effective public-private collaborations to prevent and combat cybercrime requires thorough needs assessments tailored to specific regional, national, and local contexts, as well as the resources and limitations of partnering organizations. This report offers preliminary insights to guide governments, private companies, civil society organizations, academic institutions, and other experts in forming structured collaborations to tackle common threats.

United Nations Office on Drugs and Crime
Civil Society Unit (CSU)
Vienna International Centre | P.O. Box 500 | A-1400 Vienna, Austria