



INTERPOL

**INTERPOL's contribution to the elaboration of a
Comprehensive International Convention on Countering
the Use of Information and Communications Technologies
for Criminal Purposes**



OCTOBER 2021

1. INTRODUCTION

The use of information and communications technologies (ICTs) for criminal purposes is a global challenge and a serious threat which takes advantage of the increased reliance on the digital environment. Its impact goes far beyond what is being reported or detected, with a recent shift in targets to governments, businesses, key infrastructure and even hospitals. This criminal use of ICTs poses a formidable challenge to security worldwide and inhibits the potential of digital economies. Recognizing the magnitude of this problem, INTERPOL plays a key role in addressing cybercrime on a global scale in support of its 194 member countries.

INTERPOL has been analysing a broad range of cyber threats since the inception of its Global Cybercrime Programme in 2015. Its most recent assessment underlined that the COVID-19 pandemic has opened up new avenues for cybercriminals to carry out various forms of online crime regardless of the region.¹ The prominent threats include ransomware-based extortion, Business E-mail Compromise, illegal data-harvesting operations, misinformation and the re-emergence of older types of malware repurposed to take advantage of the global pandemic.

With the escalation of cybercrime worldwide, the need for a global law enforcement response has never been more acute. In this context, this Position Paper proposes INTERPOL's strategic priorities on the issues concerning the current development of a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes (hereafter, the Convention). Rooted in a global law enforcement perspective, the priorities underline the importance of international police cooperation in addressing cybercrime, how INTERPOL is supporting member countries in this respect, and how these can underpin the objectives of the Convention.

2. CYBER THREAT LANDSCAPE

In the past year, INTERPOL has witnessed an exponential growth in the scale and impact of cyber threats as criminals and fraudsters have been exploiting fundamental social needs and anxieties in the cyberspace during the COVID-19 pandemic. Since March 2020, INTERPOL has been receiving requests from member countries to address **ransomware attacks** against hospitals and other institutions on the front lines in the fight against the coronavirus.² By attacking these critical infrastructures, criminals have been showing their will and power to maximize both the damage for their targets and their own financial gain.

While ransomware attacks are not new, they are the fastest growing form of cybercrime. Ransomware provides a highly enticing and lucrative business model for cybercriminals, with the use of double extortion and Ransomware-as-a-Service model. INTERPOL has also identified that such attacks are not geographically limited, suggesting that criminals are expanding their focus to target any institution across the globe. For instance, the same ransomware strain which shut down a hospital in Europe was also used in Asia.

In addition, we have seen complex **cyber frauds** hitting victims in Europe, and proceeds being routed as far as West Africa and South East Asia within hours. Massive **data breaches** also continue to occur, causing significant financial losses to businesses worldwide. At the same time, cybercriminals are

¹ COVID-19 Cybercrime Analysis Report (August 2020)
<https://www.interpol.int/en/content/download/15526/file/COVID-19%20Cybercrime%20Analysis%20Report-%20August%202020.pdf>

² <https://www.interpol.int/en/News-and-Events/News/2020/Cybercriminals-targeting-critical-healthcare-institutions-with-ransomware>

hiding in the **Darknet** that provides anonymous and untraceable access. This heightens the importance and relevance of INTERPOL's Notices³, particularly the Purple Notice, which is a tool for member countries to share information about the modus operandi of these fraudulent schemes. The goal is to disseminate this critical information before the next attack occurs.

Furthermore, the **convergence between cyber and financial crime** is posing a complex challenge. This entails multiple phases, ranging from cyberattacks to data exploitation, and then to money laundering phases of layering and eventual cashing-out. The use of cryptocurrency in this process also hinders an effective and timely threat response. Given the complexity, a joint operating model is required, combining capabilities of different specialized units in law enforcement to better combat cyber-enabled fraud and money laundering. To offer the full array of operational and analytical support in this regard, INTERPOL launched the INTERPOL Global Financial Crime Task Force at the end of 2020.

3. STRATEGIC PRIORITIES

INTERPOL is an inter-governmental organization with the vision of connecting police for a safer world. Its mandate is to facilitate cross-border law enforcement cooperation and, as appropriate, support governmental and intergovernmental organizations, authorities and services whose mission is to prevent or combat crime – within the limits of the laws existing in the different countries and in the spirit of the Universal Declaration of Human Rights.⁴ INTERPOL's Constitution, in particular Article 3, stipulates the strict neutrality of INTERPOL, and that it is forbidden "to undertake any intervention or activities of a political, military, religious or racial character".

Providing a range of expertise and services to our member countries, INTERPOL can play a key role in the exchange of information, and the transmission of international cooperation requests such as for provisional arrest and Mutual Legal Assistance (MLA). INTERPOL also manages 19 police databases with information on crimes and criminals, accessible to member countries in real-time. Its investigative support includes forensics, analysis, and assistance in locating fugitives around the world. Specifically on cybercrime, INTERPOL has established the 24/7 Contact Points on Computer-related Crime with national cybercrime units, and a legal framework to share information with the private sector. Provision of capacity building to law enforcement, analysis of cybercrime threats and operational responses are also INTERPOL's core function.

Due to their global reach, proven operational value, and the widely recognized data processing legal framework, INTERPOL's existing capabilities can be readily mobilized to **offer a direct law enforcement implementation vector** to the Convention.

The UNODC's Draft Comprehensive Study on Cybercrime (2013) recognizes INTERPOL's pivotal role in facilitating police-to-police cooperation.⁵ As a neutral and global organization, INTERPOL is uniquely positioned to help coordinate the global law enforcement response to cybercrime in cooperation with its member countries and partners. INTERPOL's role was also recognized in the final recommendations adopted by the UN Open-ended Intergovernmental Expert Group (IEG) to Conduct a Comprehensive Study of the Problem of Cybercrime at its seventh session held in April 2021.⁶

³ <https://www.interpol.int/en/How-we-work/Notices/About-Notices>

⁴ INTERPOL's Constitution, Article 2: "[INTERPOL's] aims are:

- (1) To ensure and promote the widest possible mutual assistance between all criminal police authorities within the limits of the laws existing in the different countries and in the spirit of the "Universal Declaration of Human Rights";
- (2) To establish and develop all institutions likely to contribute effectively to the prevention and suppression of ordinary law crimes."

⁵ https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf

⁶ https://www.unodc.org/documents/organized-crime/cybercrime/Cybercrime-April-2021/Working-documents/EGM_Cybercrime_Agreed_paragraphs_Status_7_April_6_PM.pdf

In particular, the INTERPOL Global Cybercrime Programme is working closely with the UNODC in the framework of a Joint Action Plan on Cybercrime in line with the UNODC's Strategy and INTERPOL's Strategic Framework (2022-2025). One of the key areas of collaboration includes INTERPOL's contribution to UN policy processes on cybercrime to share its views on the threat landscape and provide recommendations to member countries to help achieve effective international cooperation in combating cybercrime.

Taking the partnership to the next level, the second biannual review of the UN General Assembly Resolution on cooperation between the UN and INTERPOL was unanimously adopted on 23 November 2020⁷, with new language on cybercrime as one of the key areas for cooperation. This reinforces the role of INTERPOL and provides greater legitimacy for further collaboration between the two organizations in this field.

To this end, INTERPOL has established four strategic priorities to be promoted during the process of developing the Convention. Under each strategic priority, this Position Paper provides the context analysis and specific capabilities through which INTERPOL is supporting member countries **as a neutral interlocker**, which can be reflected in the Convention's language as determined by the Parties.

Building on the language from the United Nations Convention against Transnational Organized Crime and the Protocols Thereto (UNTOC),⁸ the United Nations Convention against Corruption (UNCAC),⁹ as well as the IEG's agreed and final recommendations,¹⁰ this Position Paper provides recommendations from the global law enforcement perspective.

⁷ UN General Assembly Resolution A/RES/75/10, entitled "Cooperation between the United Nations and the International Criminal Police Organization (INTERPOL)"

⁸ <https://www.unodc.org/documents/treaties/UNTOC/Publications/TOC%20Convention/TOCebook-e.pdf>

⁹ https://www.unodc.org/documents/brussels/UN_Convention_Against_Corruption.pdf

¹⁰ <https://www.unodc.org/documents/organized-crime/cybercrime/Cybercrime-April-2021/Report/V2102595.pdf>

[Strategic Priority 1] Enhance international law enforcement cooperation for a timely and effective global response to cybercrime

– in line with INTERPOL Strategic Goal 1 (2022-2025): Serve as the trusted global law enforcement hub for the exchange of actionable information and analysis

(1) Context analysis and challenges

Cybercrime knows no borders. While cybercriminals exploit borderless playing fields in the digital world, law enforcement structure is limited to its national borders. The transnational nature of cybercrime underlines the importance of international police cooperation. In the face of the continued evolution of cyber threats, there is a need for enhanced cooperation and coordination of timely transnational law enforcement response on a national, regional and global scale. The secure and swift exchange of actionable information is crucial in locating evidence, suspects and victims in multiple jurisdictions simultaneously.

(2) Recommendations for the way forward

- (a) [IEG Recommendation] “Countries are called upon to join, make wider use of and strengthen authorized networks of practitioners to preserve and exchange admissible electronic evidence, including 24/7 networks, specialized networks on cybercrime and INTERPOL channels for prompt police-to-police cooperation, as well as networking with strategically aligned partners, with a view to sharing data on cybercrime matters and enabling rapid responses and minimizing loss of critical evidence. The use of police-to-police cooperation and other methods of informal cooperation before using mutual legal assistance channels was also recommended”.
- (b) Countries should cooperate closely with one another, consistent with their respective domestic legal and administrative systems, to enhance the effectiveness of law enforcement action to combat cybercrime. Each country should, in particular, adopt effective measures to establish channels of communication between their competent authorities, agencies and services in order to facilitate the secure and rapid exchange of information concerning all aspects of cybercrime.
- (c) Countries should explore ways to help to ensure that information is exchanged among investigators and prosecutors handling cybercrime in a timely and secure manner, including by strengthening networks of national institutions that may be available 24/7 and through INTERPOL channels.
- (d) The efficiency of international cooperation should be improved by establishing rapid response mechanisms for international cooperation, as well as channels of communication between national authorities using INTERPOL's channels and platforms.
- (e) Countries should cooperate in criminal matters, assisting each other in investigations of and proceedings in civil and administrative matters relating to cybercrime.
- (f) Countries are encouraged to establish joint investigative teams with other countries at the bilateral, regional or international levels to enhance enforcement capabilities.

- (g) Effective international cooperation requires national laws which create procedures that enable international cooperation. Thus, national laws should permit international cooperation among law enforcement agencies.

(3) How can INTERPOL assist member countries in implementing these recommendations?

- Global information sharing and criminal data analysis are the cornerstone of all operational activity coordinated by INTERPOL. INTERPOL offers a secure global police communications system called **I-24/7**. It connects law enforcement officers in all INTERPOL member countries, enabling authorized users to share sensitive and urgent police information securely, and is available in INTERPOL's four working languages: Arabic, English, French and Spanish. INTERPOL offers an innovative all-in-one translation service called "**Translation as a Service**" (TAAS) available to all member countries via the INTERPOL Secure Cloud to enhance multilingual communication, which is crucial for police cooperation. I-24/7 also allows investigators to access INTERPOL's **19 global police databases** which contain over 110 million records to search and cross-check data in real time. In 2020 alone, these databases were searched by law enforcement across the world over 3.9 billion times.
- In addition, INTERPOL **Notices** are international requests for cooperation or alerts allowing police around the globe to share critical crime-related information. INTERPOL's well-established Notices system has also been combined with the UN sanctions regime into an effective law enforcement tool called the **INTERPOL-United Nations Security Council Special Notice**. This Special Notice alerts global police to individuals and entities that are subject to sanctions imposed by the United Nations Security Council.
- Member countries may also request cooperation from each other through another alert mechanism known as a "**diffusion**", targeting only recipient countries selected by the source, as demanded by criminal case scope and operational security needs. At all moments, information shared through INTERPOL channels remains in the control of the source, in line with INTERPOL's Constitution.
- The regulated exchange of police information lies at the core of INTERPOL's mandate and the centrality of data to INTERPOL's work is reflected in its longstanding commitment to privacy and data protection.¹¹ The **Commission for the Control of INTERPOL's Files (CCF)** is a key piece in INTERPOL's Information System safeguards, and is an independent, impartial body that ensures that all personal data processed through INTERPOL's channels conform to the rules of the Organization.
- Moreover, INTERPOL's data protection rules are updated continually to keep pace with technological developments and evolving international data protection standards. INTERPOL's current **set of data processing rules – the Rules on the Processing of Data (RPD)** – governs all data processing in the INTERPOL Information System. This robust set of rules ensures the efficiency and quality of international cooperation between criminal police authorities through INTERPOL channels as well as due respect for the basic rights of the individuals who are subjects of this cooperation.

¹¹ For further information, please see the "Background Note on INTERPOL's Information System Safeguards for the Processing of Personal Data" at https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwii5ff1gtvzAhVLLBoKHR_NDJwQFnoECAQQAQ&url=https%3A%2F%2Fwww.interpol.int%2Fes%2Fcontent%2Fdownload%2F15292%2Ffile%2FINTERPOL%2520Background%2520Note%2520-%2520Information%2520System%2520Safeguards%2520for%2520the%2520Exchange%2520of%2520Personal%2520Data.pdf%3FinLanguage%3Deng-GB&usg=AOvVaw11podvySBdmaAvUDrYai4A

- INTERPOL maintains a list of **INTERPOL 24/7 Contact Point for Computer-related Crime** to ensure that the information exchanged through the appropriate INTERPOL channels reaches the national cybercrime units with the least possible delay. The Contact Points are an essential prerequisite for the establishment of the early warning system. These Contact Points can also be activated through the INTERPOL Global Cyber Incident Response Team (I-CIRT) framework when coordinating global law enforcement responses to major cyber-incidents.
- There is a growing consensus within the global law enforcement community that police organizations are facing numerous challenges arising from a lengthy Mutual Legal Assistance (MLA) process with regard to cybercrime investigation and prosecution given the fast-evolving nature of cyberspace. In 2018, INTERPOL proposed the **e-MLA** Initiative to foster international cooperation in criminal matters by providing a secure, electronic transmission capability for requests seeking judicial assistance in cross-border cases. This initiative was adopted by INTERPOL's General Assembly ¹² with a set of rules approved by the Membership. It now requires financial support to be applied on a global scale.
- Access to critical domain name registration information (**WHOIS data**) is limited for law enforcement in the current regulatory environment. To support law enforcement worldwide in this key challenge, INTERPOL has designed and launched the pilot testing of a new restricted portal, providing automated access to domain registration information to vetted law enforcement entities. Following the successful completion of the pilot phase of the system, INTERPOL is integrating this solution into its global police capabilities with the necessary legal agreements in place to expand the pool of private operators involved and open the system to the member countries.

¹² <https://www.interpol.int/en/content/download/5905/file/GA-2018-87-RES-04%20The%20e-MLA%20Initiative.pdf>

[Strategic Priority2] Reduce duplication of effort to optimize the use of existing mechanisms, channels and platforms in addressing cybercrime

– in line with INTERPOL Strategic Goal 4 (2022-2025): Be an organization of excellence that is accountable, transparent and agile

(1) Context analysis and challenges

Without a clear vision of the various efforts at the national, regional and international levels, there are duplication of effort and uncoordinated responses. A number of recommendations suggested by member countries during the meetings of the UN IEG can be implemented with the use of the existing global mechanisms, channels and platforms to combat cybercrime. In this way, the international community can work together to optimize existing resources and increase their effectiveness without further investment in developing new instruments.

(2) Recommendations for the way forward

- (a) Countries should identify capacity-building efforts at the national, regional and global levels in combating cybercrime in collaboration with international organizations such as INTERPOL and the UNODC to avoid duplication and create synergies in the best interests of practitioners and stakeholders. In the case of existing bilateral and multilateral agreements or arrangements, countries should, to the extent necessary, strengthen efforts to streamline operational and training activities with international organizations such as INTERPOL as a deconfliction hub for on-going efforts.
- (b) Member countries should encourage complementarity of actions between international organizations, capitalizing on their respective strengths to build the most effective response against cybercrime. As the central repository for criminal data, INTERPOL is uniquely placed to enable law enforcement to exchange cybercrime data on a global scale.
- (c) The UNODC should continue to collaborate with INTERPOL in providing technical assistance, sharing of best practices, and upon request, to prevent and counter cybercrime.
- (d) The *modi operandi* of contemporary cybercriminals should be carefully studied by means of intelligence analysis and criminological research in order to deploy existing resources more effectively and to identify vulnerabilities, with the use of INTERPOL's analytical capabilities.
- (e) Regular advisories on incident prevention should be issued and shared through INTERPOL channels with users, organizations and other stakeholders to enable them to prevent cyber-incidents that could potentially lead to criminal activities.
- (f) National and regional prevention experiences should be brought together to create a multilateral repository on INTERPOL platforms that would allow the dissemination of best practices in diverse contexts.

(3) How can INTERPOL assist member countries in implementing these recommendations?

- INTERPOL serves as **a single focal point** for law enforcement across its 194 member countries. Leveraging this network, INTERPOL can help reduce the duplication of effort **through effective coordination**. In particular, given the cross-regional nature of cyberattacks and threat vectors, deconfliction is necessary to reduce the likelihood of investigators looking at the same group

or incident in different regions. **INTERPOL can be a global coordinator and act as a neutral deconfliction hub** to fuse information on on-going cases and clarify status to support law enforcement action where appropriate to increase efficiency.

- INTERPOL puts at the disposal of its 194 member countries services and platforms that support global efforts to fight cybercrime. More specifically, **INTERPOL's Global Cybercrime Programme** delivers policing capabilities to all member countries in preventing, detecting, investigating and disrupting cybercrime. With the mandate of reducing the global impact of cybercrime and protecting communities for a safer world, the Programme focuses on three core pillars of (1) cybercrime operations, (2) cybercrime threat response and (3) cyber strategy and capabilities development. Partnership is at the heart of all these areas and activities.
- The Programme also takes a regional approach for global coordination of operations targeted against cybercrime threat actors and groups undertaking criminal activities online. Reflecting on the unique challenges and needs within the regions, it provides tailored operational support to member countries through the "**Regional Cybercrime Operations Desk**" model to coordinate joint operations against cybercrime. There are currently the ASEAN Joint Cybercrime Operations Desk¹³ and the Africa Cybercrime Operation Desk¹⁴ based in INTERPOL's Cybercrime Directorate. Given its regional and global presence, INTERPOL is able to coordinate various efforts at the regional and global level to create synergies amongst police forces and with other actors in the global cybersecurity ecosystem.
- INTERPOL conducts strategic intelligence analysis of a specific crime threat or trend, or of criminal behaviour in a particular environment. Based on this capability, INTERPOL develops global and regional assessments on cybercrime. These assessments are produced based on member country surveys and data from private partners. They help prioritize and devise strategic and operational measures in anticipation of the development of threat landscapes and crime trends.

¹³ <https://www.interpol.int/en/Crimes/Cybercrime/Cybercrime-operations/ASEAN-Cybercrime-Operations-Desk>

¹⁴ <https://www.interpol.int/en/Crimes/Cybercrime/Cybercrime-operations/AFJOC-African-Joint-Operation-against-Cybercrime>

[Strategic Priority 3] Close gaps and bridge divides in capabilities, capacity and information sharing across the globe to overcome the challenges of investigating cybercrime

– in line with INTERPOL Strategic Goal 3 (2022-2025): Advance the global law enforcement community through research and innovative solutions

(1) Context analysis and challenges

Cybercrime investigation features a number of challenges that are not experienced in the physical realm. For law enforcement, it is difficult to know first-hand that an attack has occurred, and even then, reporting rates are low. This problem of underreporting limits law enforcement's ability to accurately assess threats and effectively respond to them. This consequently often leads to an absence of cybercrime prioritization within many law enforcement agencies worldwide, which further exacerbates the situation. Investigating cybercrime also requires specific skills and technology, which is not universally available. The gaps in law enforcement cyber capability or capacity across regions can be a fundamental enabler of criminal networks and activities.

(2) Recommendations for the way forward

- (a) Countries should jointly identify the existence of the “digital gap” among countries as some countries lack the capacity and capability to prevent, detect and combat cybercrime and are more vulnerable in the face of cybercrime challenges.
- (b) Countries are called upon to collect and share cybercrime statistics and criminal data with INTERPOL to help understand trends that can inform and shape cybercrime policies and operational responses to combat cybercrime.
- (c) Countries should consider developing analytical expertise concerning cybercrime and sharing it with each other through international organizations such as INTERPOL. For that purpose, common definitions, standards and methodologies should be developed and applied as appropriate.
- (d) Countries may develop or enhance their national cybercrime strategy on a regular basis to overcome the challenges of combating cybercrime.
- (e) Countries are encouraged to undertake surveys to measure the impact of cybercrime on organizations and individuals – including counter-cybercrime measures implemented, types of cyber incident that affect the countries, and the costs associated with recovering from and preventing cyber-incidents – to develop valuable insights and a clearer vision of the global problem.
- (f) Countries should consider monitoring their policies and actual measures to combat cybercrime and making assessments of their effectiveness and efficiency to narrow the gap between countries.
- (g) Each country should, to the extent necessary, initiate, develop or improve specific training programmes for its law enforcement personnel charged with the prevention, detection and investigation of cybercrime. Such programmes may include secondments to INTERPOL.

- (h) The UNODC and INTERPOL should actively engage in law enforcement capacity-building for all countries in need of assistance. Such capacity-building activities should be politically neutral and free from conditions, should result from thorough consultations and be voluntarily accepted by the recipient countries. Countries are encouraged to continue to provide the UNODC and INTERPOL with the necessary mandates and financial support with a view to delivering tangible results in capacity-building projects for law enforcement.
- (i) Sustainable capacity-building and technical assistance to increase capabilities across operational areas and strengthen the capacity of national authorities to respond to cybercrime should be prioritized and increased, including through networking, joint meetings, training, and the sharing of best practices and training materials with the use of INTERPOL's capabilities and platforms.
- (j) Countries should foster efforts to build the capacity of law enforcement personnel, including those working in specialized law enforcement structures, so that such personnel possess at least basic technical knowledge of electronic evidence and are able to respond effectively and expeditiously to requests for assistance in the tracing of communications and undertake other measures necessary for the investigation of cybercrime.
- (k) Countries are encouraged to increase their sharing of experiences and information, including national legislation, national procedures, best practices on cross-border cybercrime investigations, information on organized criminal groups, and the techniques and methodology used by those groups.
- (l) Domestic procedural laws should keep pace with technological advances and ensure that law enforcement authorities are adequately equipped to combat cybercrime. Relevant laws could take into account the practical needs of cybercrime investigators, especially in the areas of international cooperation, consistent with due process, privacy, human rights and fundamental freedoms.

(3) How can INTERPOL assist member countries in implementing these recommendations?

- INTERPOL enables law enforcement worldwide to share information on cybercrime and threat actors, and offers a wide range of expertise, and technical and operational support. For instance, INTERPOL maintains the **Regional Working Groups of Heads of Cybercrime Units** and **INTERPOL Global Cybercrime Expert Group** networks to understand the challenges in each country and region, and to share solutions and best practices on both strategic and operational levels.
- Furthermore, INTERPOL delivers **capacity building projects and training courses** to support member countries to enhance their cyber skills, knowledge and technical capabilities, and which are customized to their needs, in line with INTERPOL standards. The ongoing projects include ASEAN Cyber Capacity Development Project (ACCDP) and Global Action on Cybercrime Extended (GLACY+) Project. The ACCDP project published a **National Cybercrime Strategy Guidebook**¹⁵ to support member countries in developing or updating their national Cybercrime Strategies. The GLACY+ project developed the **Guide for Criminal Justice Statistics on Cybercrime and Electronic Evidence**¹⁶ to assist member countries in developing cybercrime statistics and measuring the impact of cybercrime.

¹⁵ <https://www.interpol.int/content/download/16455/file/National%20Cybercrime%20Strategy%20Guidebook.pdf>

¹⁶ <https://www.interpol.int/en/content/download/15731/file/Guide%20for%20Criminal%20Justice%20Statistics%20on%20Cybercrime%20and%20Electronic%20Evidence.pdf>

- As cybercriminals' techniques and tactics are being replicated around the world, it is essential to have a platform for law enforcement to keep pace by exchanging knowledge and information securely and rapidly. With the aim of supporting police in obtaining, exchanging and disseminating actionable criminal intelligence on cybercrime, INTERPOL has created the **Cybercrime Knowledge Exchange** and **Cybercrime Collaborative Platform – Operations** for secure communication and operational exchanges dedicated to cybercrime.
- INTERPOL has also developed the **Lynx: Cyber Fusion Platform**, which is designed to enhance cybercrime analytical capabilities in an accessible, adaptable and intuitive manner. It delivers a new data dimension complementing other data enriching tools which provide knowledge into malware, malicious infrastructure, Dark Web and cryptocurrencies. INTERPOL can leverage this fusion capability to support all member countries irrespective of their level of national infrastructure or data processing capacity, underpinned by a clear legal framework and secure data processing environment.
- Regardless of a country's level of digital enforcement capabilities, all INTERPOL member countries, as actors and participants in INTERPOL's Information System, operate under the **RPD**. The RPD ensure the legality and quality of information, and the protection of personal data.

[Strategic Priority 4] Maximize prevention efforts through Public-Private Partnerships for proactive disruption of cyber threats and their ecosystem

– in line with INTERPOL Strategic Goal 2 (2022-2025): Maximize resources, knowledge and operations through cooperation and strategic partnerships

(1) Context analysis and challenges

In the face of continuously growing cyber threats, enforcement itself is not a complete solution: prevention is key. Prevention efforts can reduce harm by neutralizing cybercrime attempts and dismantling related infrastructure before perpetrators succeed in committing offences online. The partnership element is fundamental to successfully preventing these cyber threats given the prominent role that the cyber security industry, computer emergency response teams (CERTs) and non-governmental organizations (NGOs) play in the digital arena. Collaborating with these various actors in the global ecosystem of cybersecurity is therefore of paramount importance to successfully prevent and disrupt cybercrime.

(2) Recommendations for the way forward

- (a) Prevention of cybercrime requires participation by various stakeholders, including governments, law enforcement authorities, the private sector, international organizations, non-governmental organizations, academia, in addition to the general public.
- (b) Countries should consider implementing mechanisms for cooperating with industry, including on referrals to competent national authorities and takedowns of harmful criminal material such as child sexual exploitation and other abhorrent violent material.
- (c) Each country should, in accordance with the fundamental principles of its legal system, develop and implement or maintain effective and coordinated prevention and disruption measures against cybercrime.
- (d) In accordance with fundamental principles of their domestic law, countries should endeavour to develop projects and collaboration with international organizations such as INTERPOL to establish and promote best practices and policies aimed at the prevention of cybercrime.
- (e) Countries should endeavour to promote public awareness regarding the existence, causes and gravity of and the threat posed by cybercrime. Information may be disseminated, where appropriate, through the mass media and should include measures to promote public participation in preventing and combating cybercrime in collaboration with international organizations such as INTERPOL.
- (f) Countries should invest in raising awareness of cybercrime among the general public and private industry in order to address the lower rates of reporting of cybercrime compared with other types of crime that hinders understanding of the threat.
- (g) Countries are encouraged to continue to include effective prevention measures at the national and international levels and to focus on proactive activities, such as raising awareness about the risks of cybercrime. Such campaigns should target *modi operandi* such as phishing or malware (“ransomware”) and the likelihood of prosecution and punishment for offenders, and efforts to prevent further crime by identifying and disrupting ongoing illicit online activities.

- (h) Countries should support businesses and communities in raising awareness of cybercrime risks, mitigation strategies and enhancing cyber hygiene, as these can have significant downstream preventive benefits.
- (i) The collective capabilities of competent institutions should be built and the prevention culture should be changed from reactive to proactive. A robust mechanism is needed to stimulate and facilitate the sharing of intelligence on potential criminal *modi operandi*, using INTERPOL's channels.

(3) How can INTERPOL assist member countries in implementing these recommendations?

- In 2019, INTERPOL's General Assembly endorsed a legal framework entitled "**Gateway**", which enables INTERPOL to share information with private sector companies with which it has signed legal arrangements.¹⁷ This decision was based on the understanding that law enforcement needs to work closely with the private sector where the majority of data and expertise lies in relation to cybercrime. Under this framework, INTERPOL is able to receive up-to-date cybercrime data from private partners from different sectors. These partners also share their expertise on recent trends and provide technical assistance for law enforcement agencies.
- In line with the United Nations Guidelines for the Prevention of Crime highlighting the importance of public education and awareness¹⁸, INTERPOL focuses on prevention of cybercrime by raising awareness through a series of **global awareness campaigns**, jointly with the public and private partners. INTERPOL is also collaborating with the World Economic Forum to build an alliance for the Partnership Against Cybercrime initiative, which gathers law enforcement, private sector and civil society.¹⁹
- Going forward, law enforcement needs to position itself as a willing partner in a global effort between member countries, and between the public and private sectors. **Partnerships** based on trust within the global ecosystem of cybersecurity will be a deciding factor in formulating timely and effective response to cybercrime. In addition to the collaboration with private-sector partners, INTERPOL plans to further engage with national cybersecurity agencies within INTERPOL's networks.

¹⁷ <https://www.interpol.int/en/News-and-Events/News/2019/INTERPOL-s-General-Assembly-sets-roadmap-for-global-policing>

¹⁸ United Nations Guidelines for the Prevention of Crime, Economic and Social Council resolution 2002/13, Annex. Para.6 and 25.

¹⁹ <https://www.weforum.org/reports/partnership-against-cybercrime>

4. CONCLUSION

With nearly every country being connected to the Internet, a new paradigm has developed for global law enforcement. The ambiguity in its role in cyberspace – not as first responders – should be turned into an opportunity to excel in being collaborative, inclusive and open. Going beyond national borders and sectors, law enforcement should be a trusted partner for all. This holistic approach will help devise the most effective policies and operational responses to cybercrime. It will also allow us to pool our wisdom to be resilient and agile, especially in times of uncertainty.

As criminal actors, infrastructure and victims transcend national borders and jurisdictions, combating cybercrime requires full participation and cooperation of both public and private sectors in all member countries. Recognizing that the international community is equally exposed to threats and risks in cyberspace, INTERPOL's strategic priorities support the shared responsibility of member countries.

As highlighted in these strategic priorities, enhanced international law enforcement cooperation can formulate an effective response in a timely manner. When gaps in capacity and capability are filled, our weakest link will be removed. Proactive prevention of cybercrime alongside key partners is also instrumental in reducing the harm. At the same time, all these efforts should be well coordinated to avoid duplication and better utilize existing mechanisms in order to optimise the scarce resources in combating cybercrime.

Having a neutral and internationally recognized network governed by a legal framework, INTERPOL is able to serve as a global mechanism and provide a variety of services, platforms and tools to address cybercrime. Keeping in mind that national solutions or even regional solutions are no longer sufficient, INTERPOL will continue to foster international law enforcement cooperation as a neutral interlocker. INTERPOL stands ready to support the member countries alongside the UN and to contribute to the successful development of the Convention.



INTERPOL



WWW.INTERPOL.INT



[INTERPOL_HQ](https://www.instagram.com/INTERPOL_HQ)



[@INTERPOL_HQ](https://twitter.com/INTERPOL_HQ)



[INTERPOLHQ](https://www.facebook.com/INTERPOLHQ)



[INTERPOLHQ](https://www.youtube.com/INTERPOLHQ)