COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

www.coe.int/cybercrime

Strasbourg, 13 July 2020 T-CY (2020)16

T-CY(2020)16_BC_Benefits_rep_Prov_1.docx

Cybercrime Convention Committee (T-CY)

The Budapest Convention on Cybercrime:

benefits and impact in practice

Contents

Contact

Council of Europe
Secretariat of the Cybercrime Convention Committee
Strasbourg, France
Cybercrime@coe.int

Executive summary

The purpose of this report is to illustrate the benefits and impact of the Budapest Convention on Cybercrime in view of facilitating dialogue with States and stakeholders interested in cooperation on cybercrime. It is largely based on information provided by practitioners in Parties to this treaty.

The report provides evidence of the impact of the Budapest Convention on:

- domestic legislation on cybercrime and electronic evidence worldwide;
- domestic investigations based on such legislation;
- international cooperation, including of serious and organised cases of cybercrime;
- public/private cooperation;
- the strengthening of criminal justice capacities.

Practical experience shows that the Budapest Convention is more than a legal document providing for the criminalisation of cybercrime, procedural powers to secure electronic evidence and a legal basis for international cooperation.

Backed up by the Cybercrime Convention Committee (T-CY) and the C-PROC specialised Cybercrime Programme Office for global capacity building, it is a framework that permits hundreds of practitioners from all over the world to share experience and create relationships that facilitate cooperation in specific cases, including in emergency situations, beyond the specific provisions foreseen in this Convention.

While any country may make use of the Convention as a guideline for domestic legislation, becoming a Party provides additional benefits:

- it serves as a legal basis for international cooperation;
- Parties contribute to the further evolution of the Convention through guidance notes or additional protocols;
- membership in the Convention means membership in networks of practitioners, in particular the 24/7 Network of contact points established under this treaty;
- Parties experience improved cooperation with the private sector;
- Parties and States having requested accession to this treaty may become priority countries and hubs for capacity building.

As membership in this treaty keeps increasing, as related capacity building programmes are expanding and as the Convention is further evolving through the future 2nd Additional Protocol on enhanced international cooperation and access to evidence in the cloud, the framework of the Budapest Convention is likely to remain highly relevant and make a difference worldwide for years to come.

1 Introduction

The Convention on Cybercrime, opened for signature in Budapest, Hungary, in November 2001, is considered the most relevant international agreement on cybercrime and electronic evidence.

The Budapest Convention provides for (i) the criminalisation of conduct ranging from illegal access, data and systems interference to computer-related fraud and child pornography; (ii) procedural law tools to investigate cybercrime and secure electronic evidence in relation to any crime; and (iii) efficient international cooperation.

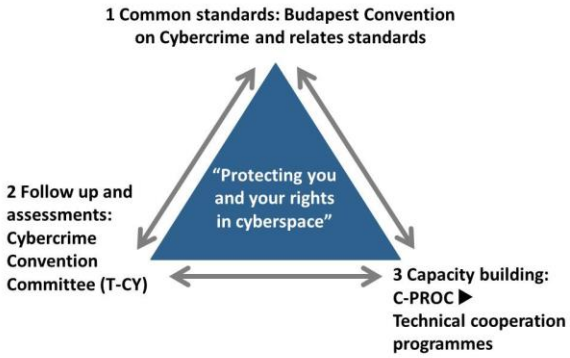
It reconciles the vision of a free Internet, where information can freely flow and be accessed and shared, with the need for an effective criminal justice response in cases of criminal misuse. Restrictions are narrowly defined; only specific criminal offences are investigated and prosecuted, and specified data that is needed as evidence in specific criminal proceedings is secured subject to human rights and rule of law safeguards.

The Convention is supplemented by an Additional Protocol covering the criminalisation of acts of a racist and xenophobic nature committed through computer systems (CETS 189). Negotiation of a second Additional Protocol on enhanced international cooperation and access to evidence in the cloud is underway.

While this treaty was negotiated by members of the Council of Europe as well as Canada, Japan, South Africa and USA, it is open for accession by any State, and an increasing number of countries of Africa, the Americas, and the Asia/Pacific region are making use of this opportunity in the interest of effective criminal justice action on cybercrime.

States that are Parties or that have signed it or been invited to accede, participate as members or observers (signatories or invitees) in the Cybercrime Convention Committee (T-CY). The T-CY, among other things, assesses implementation of the Convention by the Parties, adopts Guidance Notes or prepares additional legal instruments.

The Convention is furthermore backed up by capacity building projects – managed by the specialised Cybercrime Programme Office of the Council of Europe (C-PROC) in Romania – that assist countries worldwide to create the necessary capacities for the investigation, prosecution and adjudication of cybercrime and other cases involving electronic evidence, in line with the Convention and recommendations of the T-CY.



The Budapest Convention, therefore, is more than a legal document; it is a framework that permits hundreds of practitioners from Parties to share experience and create relationships that facilitate cooperation in specific cases, including in emergency situations, beyond the specific provisions foreseen in this Convention.

The purpose of the present paper is to illustrate the benefits and impact of this treaty in practice in view of facilitating dialogue with States and stakeholders interested in the Budapest Convention.

It is a snapshot that was prepared following a decision by the T-CY in 2019 and is primarily based on information received by Parties by June 2020. It is not meant to represent a detailed evaluation nor to replace assessments carried out by the T-CY. The report was validated by the T-CY in July 2020.

2 Domestic legislation and use for investigations and prosecutions

2.1 Improvements to and impact of domestic legislation

The Budapest Convention requires States to ensure that the offences against and by means of computers of Articles 2 to 12 are criminalised in their domestic law, and that their criminal justice authorities have the powers prescribed in their procedural law not only to investigate cybercrime but any offence where evidence is in electronic form. Domestic legislation consistent with the Budapest Convention further facilitates international cooperation in that it helps meet the dual criminality requirement. Some of the domestic procedural powers of the Convention also have a corresponding provision in the chapter on international cooperation.

Substantive criminal law: offences	Procedural law to secure evidence and investigate	International cooperation
Art. 2 – Illegal access Art. 3 – Illegal interception Art. 4 – Data interference Art. 5 – System interference Art. 6 – Misuse of devices Art. 7 – Computer-related forgery Art. 8 – Computer-related fraud Art. 9 – Child pornography Art. 10 – IPR offences Art. 11 – Attempt, aiding, abetting Art. 12 – Corporate liability	Art. 14 – Scope of procedural provisions Art. 15 – Conditions and safeguards Art. 16 – Expedited preservation Art. 17 – Expedited preservation and partial disclosure of traffic data Art. 18 – Production order Art. 19 – Search and seizure Art. 20 – Real-time collection traffic data Art. 21 – Interception of content data	Art. 23 – General principles Art. 24 – Extradition Art. 25 – General rules Art. 26 – Spontaneous information Art. 27 – MLA in absence of treaty Art. 28 – Confidentiality Art. 29 – Expedited preservation Art. 30 – Partial disclosure traffic data Art. 31 – MLA accessing data Art. 32 – Transborder access Art. 33 – MLA collection traffic data Art. 34 – MLA interception content Art. 35 – 24/7 point of contact

By May 2020, 76 States (39%) were either Parties (65 States) to the Budapest Convention or Signatories (3) or had been invited to accede (8). For example, Guatemala and Niger were invited in April 2020, and they now need to complete their domestic procedures to become Parties. All of these States have either already reformed their domestic legislation or are in the process of doing so in line with this treaty.

However, the impact of the Budapest Convention in terms of legislation is not limited to these States. A recent survey on the global state of cybercrime legislation concluded that by February 2020:

- some 177 States (92%) worldwide were in the process of reforming their legislation, or had done so in recent years;
- not only Parties have drawn on the Budapest Convention when reforming their legislation, but some 153 (79%) members of the United Nations had used it as a guideline or as a source for their reforms;
- some 106 States (55%) seem to have adopted specific domestic provisions corresponding broadly to the substantive criminal law articles of the Budapest Convention. An additional one third of States had adopted at least some specific substantive criminal law provisions in line

with this treaty. During the last seven years, progress in this sense was made in particular in Africa;

- some 82 States (42%) had specific procedural powers largely in place while many States still rely on general procedural law provisions to investigate cybercrime and secure electronic evidence. Obviously, reforming procedural law and enacting specific procedural powers to secure electronic evidence for use in criminal proceedings (corresponding to Articles 16 to 21 of the Budapest Convention and subject to the safeguards of Article 15) is a more complex undertaking.

Much of this progress is due to the Budapest Convention and related capacity building programmes.

Given the impact of the Budapest Convention as a guideline for domestic legislation worldwide, it is only possible to provide some examples for illustration.

- **Cabo Verde** in 2017 adopted Law n°8/IX/2017, which establishes substantive and procedural penal procedures as well as international cooperation dispositions regarding cybercrime and the collection of electronic evidence. This law was developed in line with the National Strategy on Cybersecurity and the provisions of the Budapest Convention.

- **Costa Rica** has carried out an extensive national examination of its laws in the process of joining the Budapest Convention with the support of Council of Europe experts. In particular, Costa Rican officials analysed and made suggestions regarding a new draft law on combating cybercrime. This statute would modify and reform certain articles of the penal code, the criminal procedure code, and a third law addressing criminal procedure and investigative measures. Further, Costa Rican officials have carried out comprehensive work to criminalise child sexual exploitation in line with the Budapest Convention and other international conventions, as well as to address numerous other forms of sexual exploitation and trafficking of vulnerable persons.

- **Croatia** in 2013 brought its substantive and procedural law fully in line with the Budapest Convention when new Criminal and Criminal Procedure Codes entered into force.

- The **Dominican Republic** is among the few countries in Latin America and the Caribbean with an independent law to investigate, prosecute and sanction cybercrime. Law No. 53-07 on Crimes and High Tech Crime (Ley No. 53-07 sobre Crímenes y Delitos de Alta Tecnología), in force since 23 April 2007, together with the Criminal Code, the Criminal Procedure Code and other legislation provides the legal framework on cybercrime and electronic evidence.

- **Finland** amended its Criminal Code in view of implementing its obligations vis-a-vis the Budapest Convention, while additional procedural powers were introduced in line with this treaty through the Coercive Measures Act in 2011 (in force – 2014).

- **France** enacted multiple amendments to its legislation to adapt to the evolution of cybercrime. The Law on the Confidence in the Digital Economy of 2004 (Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique) in particular subsequently permitted ratification of the Budapest Convention on Cybercrime.

- **Germany** amended its Penal Code in 2009 to cover all the substantive law provisions of the Budapest Convention while its procedural powers are covered by the Criminal Procedure Code.

- **Ghana** adopted the Electronic Transactions Act 772 ("ETA") in 2008. ETA is a comprehensive piece of legislation that provides for many cybercrime offences and procedural powers with respect to handling of electronic evidence in line with the Budapest Convention. Other legislation such as the Economic and Organised Crime Act, 2010 ("EOCA"), and Security and Intelligence Agencies Act 526, 1996 ("SIAA"), also provide procedural powers with respect to investigation of cybercrime.

- **Italy** carried out several amendments of criminal legislation related to cybercrime and related procedural powers. Additional rules were introduced in 2008 in line with the Budapest Convention.

- **Mauritius** passed the Computer Misuse and Cybercrime Act in 2003 which follows the Budapest Convention. The Act provides for criminal offences relating to cybercrime and the related rules for investigations and procedures. The Act also covers issues regarding prosecutions, jurisdiction, extraditions and forfeitures.

- **Peru** adopted and then updated its substantive cybercrime law in 2013 and in 2014. Its law now covers crimes against data and information systems, including illegal access and attacks on the integrity of data and systems; child exploitation offences; illegal trafficking in data and interception of data; electronic fraud; and crimes relating to identity theft and abuse of devices. The law covers both crimes against computers and the use of computers to commit crimes. In conjunction with that law, a regulation was issued facilitating Peru's signing and ratification of multilateral treaties that would guarantee cooperation with other states in pursuing cybercrime. A later regulation established that definitions in the 2014 law are to be understood as conforming to the meanings in Article 1 of the Budapest Convention.

- **Portugal** adopted its Law on Cybercrime in 2009 (Law 109/2009). This act follows in general the structure of the Budapest Convention and fully transposes into the domestic legal framework all its provisions on substantive penal law, penal procedural rules and international cooperation.

- **Romania** – with Law 161/2003 (Title III - Prevention and combating cybercrime), implemented fully the Budapest Convention into its legislation. In 2004, Romania ratified the Convention on Cybercrime (Law no 64/2004) and in 2009 the Additional Protocol concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems. In 2012 and 2013, these provisions were then integrated into the new Criminal and Criminal Procedure Codes which entered into force in 2014.

- **Slovakia** in 2005 adopted two acts that amended the Criminal Code and the Criminal Procedure Code to meet the requirements of the Budapest Convention.

- **Spain** carried out several amendments of substantive legislation related to cybercrime and related procedural powers to meet the requirements of the Budapest Convention. In 2015, Spain adopted additional amendments through its Organic Laws 1 and 2/2015 on definition of cybercrimes and through its Organic Law 13/2015 (Ley Orgánica 13/2015), inter alia to provide for expedited preservation of stored computer data, production orders, and search and seizure of stored computer data. Spain noted in particular that it uses the Budapest Convention as a resource beyond making alterations to its statutes for domestic legal guides and training materials. It uses both the treaty text and the Explanatory Report in training activities for criminal justice officials, including police forces (see discussion below), and for interpreting the substantive crimes and procedural tools in the Spanish law that derives from

Budapest. Such interpretation comes in the form of Circulars of the Spanish State Prosecutor General's Office establishing the criteria to be followed by prosecutors in understanding and applying legal norms. The Budapest Convention and its Explanatory Report constitute essential bases for several of these Circulars:

- Circular 1/2019 FGE on common provisions and assurance measures for technological research proceedings;
- Circular 2/2019 FGE on interception of telephone and telematic communications;
- Circular 5/2019 FGE on registration of devices and computer equipment;
- Circular 3/2017 on the reform of the Criminal Code in relation to crimes of discovery and disclosure of secrets and crimes of computer damage.

► **Sri Lanka** in 2007 adopted the Computer Crimes Act No 24 of 2007 which is largely based on the Budapest Convention. In addition, the Payment Devices Frauds Act No. 30 of 2006, the Intellectual Property Act No. 36 of 2003 and a number of general Penal Code articles and amendments are applicable to cybercrime offences. The Penal Code, amended by the Prisons Amendment Act No. 22 of 2005, Penal Code Amendment Act No. 16 of 2006 and No. 10 of 2018 is in place to deal with some issues relating to indecent images of children. In 2018, Sri Lanka furthermore adopted amendments to the Mutual Assistance in Criminal Matters Act (No. 24 of 2018) which now comprises specific provisions related to mutual legal assistance in matters related to cybercrime and electronic evidence, including the expedited preservation of data, in line with the Budapest Convention.

In addition to these and other States that are Parties to the Budapest Convention, many others have adopted domestic legislation in line with the Budapest Convention or are in the process of doing so – often with the technical assistance of the Council of Europe – such as Belize, Benin, Côte d'Ivoire, Burkina Faso, the Gambia, Guatemala, Fiji, Kenya, Niger, Nigeria and others.

2.2 Domestic investigations

When giving examples of the use of the legislation based on the Budapest Convention in domestic investigations and prosecutions, the following will need to be taken into account:

- In States that have adopted legislation based on the Budapest Convention any investigation making use of such legislative provisions may be attributed to this treaty. However, prosecutions and court decisions will refer to the articles of domestic law and not to the Budapest Convention except for instances where evidence has been obtained through international cooperation provisions.

- Public authorities can only share limited information as details may be confidential or investigations are ongoing.

Nonetheless, here are some examples submitted by Parties:

► The Prosecutor's Office of **Bosnia and Herzegovina** reported that:

- In at least three cases it used the mechanisms in Articles 29 and 30 of the Budapest Convention to seek data preservation from foreign providers. In two other cases, requests were sent for subscriber data in accordance with Article 31 of the Convention.
- The Prosecutor's Office of Brčko District indicted a suspect in 2013 for illegal use of another person's account to access a private Internet page and to change passwords

and the source code of the page. This led to automatic erasure of all data, which constituted the crime of damage of computer data and programmes.

- In another case, the defendant had repeatedly purchased goods and services via the Internet, conducted unauthorised monitoring of the computer activities of third parties, and forged documents via computers. The defendant was convicted of computer fraud and other cybercrimes and of thereby damaging individuals and businesses, receiving a prison sentence and fine.
- Procedural changes pursuant to the integration of the Budapest Convention (Article 26 on spontaneous information) in domestic legislation assisted the Republika Srpska in a 2019 investigation. Defendants were charged with misuse of copyrights – the unauthorised creation of an Internet web site to distribute movie content. Investigative mechanisms based on Articles 29 and 32 of the Convention were also used in the case.
- Another 2019 case used other mechanisms based on the Convention – investigators received information from a US Internet service provider (ISP) about the distribution of child pornography from Republika Srpska. The investigation identified a target in Banja Luka which resulted in the confiscation of 1000 items of storage media, 42 hard discs, computers, mobile phones and other equipment used to store child pornography.
- A 2018/2019 case used the Budapest Convention's mechanisms for cooperation with foreign ISPs for the preservation and disclosure of data identifying certain social network users. Finally, such methods were used in 2019 for investigations related to endangering the security of officials in Republika Srpska. In that case, a US ISP provided data to identify a target.

► **Costa Rica** became a Party to the Budapest Convention in January 2018. In the five year period from 2014 to 2019, more than 7,000 cases of cybercrime have been recorded, out of which the vast majority (6342) were related to fraud. Ninety-four of these fraud cases led to criminal prosecutions. Following accession to the Budapest Convention Costa Rica established an Anti-Cybercrime Unit at the Public Prosecutor's Office in what now is called the "Deputy Prosecutor's Office for Fraud and Cybercrime," which closely cooperates with the judicial police in investigating cybercrime. As a result, two organised crime groups involved in computer-related fraud have been dismantled and searches and seizures have been carried out. The organised crime groups had a complex set up with one unit targeting victims through phishing, pharming and other social engineering techniques, a second unit responsible for recruiting money mules, a third organising the transfers of criminal proceeds, and a fourth collecting information on potential victims.

► **Finland** carried out a remote search based on the Budapest Convention in a case involving multiple serious distributed denial of service attacks on several Finnish "Authoritative Services" in 2017 and 2018. The suspect had used a mobile device to launch the distributed denial of service (DDoS) attacks using Stresser (Crime as a Service) services (botnets) to automate the attacks. The police remotely searched data in the suspect's email and Stresser accounts to find evidence of the suspect having used those services via a certain device on the days when attacks occurred. The results of the remote searches were crucial, as there was basically no other way to get hard evidence that the suspect was behind the attacks.

► **France** stated that their cybercrimes services use regularly the framework of the Budapest Convention as a tool for the investigation of cyberattacks. France offered three examples of domestic cases based on Budapest-related legislation:

- In the first case, the public health authorities in Marseille investigated the importation and sale of a product containing glyphosate that was unauthorised for sale and

distributed under the counterfeited brands of GALLUP 360 and LUTESATE 360 (the products are dangerous for human consumption). The four defendants received suspended prison sentences and fines.

- In the second case, the same authorities investigated a counterfeit production network for the drugs PLAVIX and ZYPREXA that were also dangerous for human consumption. The preliminary investigation began with the seizure of 40,000 containers of the two medications, which apparently originated in Singapore and were sold mostly in Europe (the UK, France, and Switzerland). The three defendants were convicted in 2017 of the illegal practice of pharmacy, fraud involving a product posing a danger to persons or animals, and importation of products under a counterfeited brand that presented a danger to human health. The two defendants who were natural persons received varying prison sentences, had their property confiscated or a fine. One was barred for five years from the management of a business. The legal person was fined 15,000 euro.
- In the third case, a preliminary investigation led to the seizure of 6,000 cartons of counterfeit MAYFAIR cigarettes with a value of 387,000 euro. They had apparently been imported from Spain and were intended for sale in Italy. The danger to the health of consumers consisted in the complete lack of knowledge of the origin of the cigarettes and of how they had been manufactured. The defendant was convicted in 2018 of several offences relating to illegal possession and distribution of products lacking the necessary documents and organised-crime-related offences. He received a suspended sentence and a fine of 300,000 euro.

► **Hungary** supplied a number of examples of domestic investigations facilitated by criminal procedure changes based on the Budapest Convention's Article 32. Article 32 (a) permits a Party to access publicly available (open source) stored computer data without the authorisation of another Party, regardless of where the data is stored geographically. Article 32 (b) enables the trans-border access to stored computer data – in carefully delimited circumstances – with the lawful and voluntary consent of someone who has the authority to disclose that data:

- In the first case, two perpetrators boarded a bus heading to town X together with the underage victim. S/he was visibly under the influence of sedatives and alcohol and asked the perpetrators for a cigarette. The perpetrators told the victim that they would give him/her a cigarette if s/he got off the bus with them at town X. The victim got off the bus and they walked together to the bank of X river where the perpetrators gave the victim a cigarette. After having smoked it, s/he became disoriented and the perpetrators, taking advantage of the situation, sexually assaulted the victim. The investigating authority seized and analysed footage from the surveillance camera installed on the bus, allowing them to establish the identity of the perpetrators. The investigators also used public data, photos and relationships on Facebook, in accordance with Article 32 (a) of the Convention.
- In the second case, the accused suffocated his/her mother with a pillow in his/her home and disposed of it in the septic tank located in the yard behind the house. The investigating authority seized the accused's iPhone V and iWatch 3. It was necessary for the success of the investigation to obtain data stored in the cloud operated by the US-based service provider (Apple Inc.). During the interrogation, the investigating authority asked the accused's consent to access his/her account data remotely, since it was stored outside Hungary. The accused consented, logged into his/her account and provided the authorities with the password. With regard to this case, Hungary noted, "without the use of Article 32 (b), obtaining the data would only have been possible through a time-consuming legal assistance procedure."

More generally, Hungary commented that, "without the use of Budapest Convention, request for legal assistance had to be sent to service providers in the framework of judicial cooperation in order to access data stored in a server located in another country. This was time consuming and cumbersome, especially with regards to data stored in the territory of the US … With voluntary consent, the data stored abroad is accessible and recordable to the investigating authorities and thus becomes part of the evidence."

► **In Japan** multiple defendants operated a so-called leech site that gathered links to websites containing data of manga and other books that had been uploaded illegally. The defendants were convicted of violation of the Copyright Act. In another case, the defendant created a mining programme and uploaded it to the Internet, disguising it as an online games programme. The defendant earned rewards through the mining carried out when the programme was installed on the device of someone who downloaded the programme without knowing that it was actually a mining programme. The prosecution secured evidence through the use of search and seizure and extraction of evidence from seized computers. The defendant was convicted of operating an electromagnetic record giving an unauthorized command.

► The **Republic of Moldova** had adopted its Law on Cybercrime no. 20/2009 which permitted it to become a Party that year. The law was applied in a number of cases. For example:

- In one case, a defendant had travelled abroad to procure a skimmer to illegally obtain information from payment cards. He was convicted for being the organiser of an attempt to make available the technical means for the purpose of committing the crime provided for in article 259 of the Criminal Code of the Republic of Moldova and articles 26, 42 para. (2), article 259 para. (2) lit. b) and e) of the Criminal Code of the Republic of Moldova, and for being an author in the preparation of illegal access to computer data, committed by two or more persons, using special technical means.
- In another case, a defendant entered the territory of the Republic of Moldova with the plan of installing in Chisinau – in cooperation with other defendants –skimmers at ATMs to illegally access and steal information from payment cards. These acts were criminal offences under articles 237 and 259 of the Criminal Code.

► In **Romania**, cybercrime has evolved over the last 17 years from individual offences committed by skilled offenders to a more sophisticated modus operandi by organised crime groups specialised in different forms of fraud over the internet or in illegal activities related to electronic payment instruments.

- A Decision of the High Court of Cassation and Justice stated in 2013 that Article 6 of the Budapest Convention ("misuse of devices") is applicable when an offender mounts reading/writing device on an ATM with the purpose of collecting sensitive information from an electronic payment instrument. The Decision also stated that the illegal use at an ATM by a genuine or a counterfeited electronic payment instrument with the purpose of withdrawing cash is criminalised under Article 2 (Illegal access) in conjunction with the special provisions on fraudulent operations with electronic payment instruments. In addition, Romania encountered various attacks against computer systems or networks targeting the financial system materialised in different schemes of "jackpotting" that are criminalised under national legislation implementing the Budapest Convention.
- In a case in 2016, a "jackpotting" scheme that compromised more than 20 ATMs in less than 90 minutes, led to fraudulent cash withdrawals of 800,000 Euro. A defendant was

caught "red-handed" with 17.000 Euro cash withdrawn and sentenced to four years of imprisonment for computer fraud (Article 8 of the Budapest Convention) and participation in an organised crime group. Unfortunately, due to the complexity of the scheme that included the deployment of a phishing attack that compromised an official's email account, the intrusion (Article 2 of the Budapest Convention) and the alterations made to the system file of the ATMs that led to an overriding the commands of the systems (Article 4 and 5 of the Budapest Convention), remained unsolved.

► **Spain** provided selected examples in which the Convention itself was referenced in Spanish cases between 2015 and 2019:

- In numerous cases from 2015 to 2019, the Budapest (and also the Lanzarote) Convention were cited for the purposes of criminalisation of child pornography and child grooming crimes. They were also used to identify the facts necessary to prove crimes of child pornography or to define the concepts of child pornography and pornographic material. Other judgments cited Budapest and Lanzarote and their respective explanatory reports to assess the crime of possession of child pornography and to interpret what constitutes material of pornographic character or sexually explicit conduct.
- In a case involving illegal access to computer systems, a 2015 judgment used the Budapest Convention in interpreting and applying the crime of illegal access to systems. This case was decided before the relevant Spanish criminal statute was amended. The decision thus analyses the pre-amendment concept against Article 2 of the Convention.
- And in cases involving attacks on the integrity of data and systems, two judgments relied on the Budapest Convention. In the first, the court that convicted defendant of computer damage expressly cited Article 1 of the Convention to define the concept. In the second, also a prosecution for computer damage, the court cited Articles 2 to 6 of the Budapest Convention in interpreting the relevant articles of the Spanish criminal code
- Finally, in a case involving the physical removal of computer equipment, a 2015 judgment of the Provincial Court of Madrid referred to the concept of computer data in Article 1 of the Budapest Convention.

Spain furthermore commented that the expedited preservation of stored computer data pursuant to Article 16 of the Convention (and provided for in Spanish law) is used very frequently in practically all technology-related investigations, both when the information to be preserved is held by national providers and abroad. Spain also offered an example of the use of several Budapest criminal procedure tools. In June 2019, a complaint was filed by the Prosecutor's Office after an investigation of a computer attack with access to the internal network of an important Spanish institution, with effects on systems and devices located in different locations in Spain and in other countries. The Public Prosecutor's report charged illegal access to the systems and computer damage (based on articles in the Spanish code that derive from the Budapest Convention). This on-going investigation involves numerous transnational actions and the use of the Budapest Convention's investigative tools of preservation of data, production orders, and search and seizure of computing devices.

3 International cooperation

International cooperation
Art. 23 – General principles
Art. 24 – Extradition
Art. 25 – General rules
Art. 26 – Spontaneous information
Art. 27 – MLA in absence of treaty
Art. 28 – Confidentiality
Art. 29 – Expedited preservation
Art. 30 – Partial disclosure traffic data
Art. 31 – MLA accessing data
Art. 32 – Transborder access
Art. 33 – MLA collection traffic data
Art. 34 – MLA interception content
Art. 35 – 24/7 point of contact

The benefits of the Budapest Convention with regard to international cooperation stem from:

- the fact that it represents a legal framework for criminal justice cooperation on cybercrime and any other crime where evidence is on a computer. The chapter on international cooperation contains general provisions on international cooperation that may also be found in other treaties on cooperation in criminal matters as well as provisions that are specific to the collection of electronic evidence. The 2nd Additional Protocol that is currently under negotiation is to provide for additional tools, including for cooperation in emergency situations;

- the large network of practitioners participating in the Cybercrime Convention Committee (T-CY) and in capacity building activities who can call and rely on each other when needed in the investigation and prosecution of cases that more often than not are transnational in nature. The benefit of these relationships is immeasurable;

- the promotion of reforms and the strengthening of laws, procedures and mechanisms for international cooperation by the T-CY and capacity building activities. For example, in 2014 it carried out an assessment of the functioning of the mutual legal assistance provisions of the Budapest Convention and adopted a set of recommendations. In 2017, the Committee then reviewed the follow up given by Parties to these recommendations and documented good practices but also encouraged further efforts.

The following examples provided by Parties illustrate how the Budapest Convention is helping in practice.

3.1 Examples of mutual assistance in practice

All States recognise the limited effectiveness of mutual assistance and the need to improve the process when investigating transnational cybercrime and securing volatile electronic evidence. Although the Convention has not solved all problems, it helped improve the situation and has contributed to successful cooperation. One Party has remarked that, as a small, poor country, it could not possibly find the resources to negotiate all the bilateral agreements it would need to obtain electronic data rapidly from every country from which it might need assistance. However, once it acceded to the Convention, dozens of partner countries were instantly bound to provide assistance. This prospect of immediate connections to possible assistance was a crucial factor in this country's decision to seek accession. Another Party, Malta, added that, "since the majority of cybercrime attacks are of transnational nature, the Budapest Convention is indispensable in order to investigate perpetrators effectively, especially for countries such as Malta, which do not have international service providers based within their own jurisdiction."

In this vein, numerous Parties have described improvements to their ability to obtain formal and informal mutual assistance after they became Parties, and they provided statistics[1] and examples accordingly.

[1] It should be noted that statistics on the use of the offences of the Budapest Convention and its tools are not complete or fully reliable – in fact, they may be presumed chronically to understate actual use. Some countries don't keep

► **Bosnia and Herzegovina** commented that the best example of international cooperation lies in the specially-created platforms of service providers – for example, that of Facebook. These platforms, intended for representatives of law enforcement, allow the fast exchange of operational information. Thus, in investigations of illegal use of copyrights and endangerment of an official involved in security affairs, the Prosecutor's Office of Bosnia and Herzegovina used Convention provisions when it requested data preservation and disclosure of subscriber data from foreign service providers.

Most of the prosecutors' offices in Bosnia and Herzegovina reported that they had investigated or were investigating cases that involved Convention-based crimes. Overall, in 2019, about 110 such investigations were started, many of which resulted in prosecutions. Further, in 2019, the Ministry of Interior of Republika Srpska reported 115 high-tech crimes, twelve involving crimes against the security of computer data and 103 related to other high-tech crimes.

International police cooperation via INTERPOL in Sarajevo is very intensive in exchanging data regarding child pornography (per Article 9 of the convention) and breaking its distribution chains. In 2019, INTERPOL in Sarajevo opened thirty new child pornography cases. Five originated with domestic law enforcement and twenty-five were opened on the request of national contact bureaux in other countries.

The Ministry of Interior of Republika Srpska collaborated in several international actions in 2015 and 2016. These included Darkode (with the US; production and use of a computer virus and computer fraud); Odisej (with Germany; computer fraud, unauthorised access to a computer, computer network, telecommunication network and electronic data processing, etc.); and PLEJADE with the United Kingdom, US, Switzerland, Austria, Germany, Japan, Canada, Ireland, and Monaco on the extortion and prevention of, and limiting access to, a public computer network.

► **France** is the sender or receiver of many requests for assistance to obtain electronic data. These requests are based both on bilateral instruments, especially the agreement with the US, and multilateral instruments, including the agreement between the European Union and the US and the Budapest Convention. France notes that the Budapest Convention's provisions (especially Articles 29 and 35) and its community of trust are particularly important for preservation of data prior to formal requests.

In a 2018 example involving the kidnapping and murder of a minor and associated crimes, France made a request for electronic data. The requested state replied that its evidentiary standard had not been met and denied the request. However, a formal MLA request was transmitted to the requested state and was executed.

In a 2018 incoming request investigating a legal person for a complex of cybercrimes, including conspiracy and electronic fraud (sale of tools and programs to disable antivirus programs), France was asked to preserve the data in an account as well as data relating to an IP address. This request was executed in June 2019.

---

statistics; countries with federal systems may keep separate, unretrievable statistics; many countries don't keep statistics in a way that tracks the substantive crimes in the Convention (they may use general terms such as "fraud" rather than a statutory reference that relates to the Budapest Convention); and countries normally keep statistics by substantive crime, not by whether certain procedural tools were used in an investigation. For some of the same reasons, statistics relating to the 24/7 system (discussed below) also understate the use of the system. Conversely, where statistics exist, they sometimes mix requests that use different mechanisms or networks (such as the so-called G7 network), not solely the 24/7 network of the Budapest Convention.

In 2019, France sent fifty outgoing mutual legal assistance requests from French services for electronic data based on the Convention and handled twenty such incoming requests.

► **Georgia** has only a few mutual assistance agreements with countries beyond Europe. In the absence of agreements, the Budapest Convention has served as an important tool for Georgia with non-European partners in serious multinational investigations. In several cases, spontaneous information shared on the basis of Article 26 of the Convention led to successful investigations at an unprecedented scale for Georgia. Here are two examples:

- GozNym Malware Case. In 2019 Georgia participated in a largescale multinational law enforcement operation in which a complex, globally operating organised cybercrime network was dismantled. The criminal network used the GozNym malware to steal an estimated $100 million from more than 41 000 victims, primarily businesses and their financial institutions. The criminal network was led by a Georgian national and composed of members mostly from Eastern Europe. The operation culminated in the initiation of criminal prosecutions against members of the network in four different countries as a result of cooperation between Georgia, the United States, Ukraine, Moldova, Germany, Bulgaria, Europol and Eurojust. Georgia successfully prosecuted the leader of the syndicate and his associate who were sentenced to 7 years and 5 years in prison, respectively. Georgian prosecution heavily relied on the evidence shared by the international partners of the operation. More information can be found here, here, here and here.
- International Child Pornography Case. In 2019, Georgian police arrested Australian, Georgian and US nationals on child sexual exploitation and child pornography charges. In the multinational operation police dismantled a child-trafficking ring that exploited girls as young as 8 years to produce pornography. The pornographic materials were sold both locally and internationally mostly through the dark web. The police operation was preceded by intensive cooperation between Georgian, Australian and the United States authorities as well as Europol. Three have been convicted by a Georgian court and sentenced to 19 years in prison each, while 21 others are still on trial.

► **Hungary** supplied several examples of improved mutual assistance and noted, "using the Convention as the basis of mutual assistance results in expedited, more professional and direct procedure compared to mutual legal assistance between judicial authorities." It provided the following examples:

- In a case related to terrorism, Hungary learned that the subject had servers operating in another Party to the Convention. It requested assistance from that Party through the 24/7 network. Hungary also used trans-border access to stored computer data pursuant to Article 32 of the Convention because the suspect was using a virtual private server physically located in the requested Party.
- In a second case, the unknown subject regularly and illegally changed the subscriber identity module lock of iPhone 6 phones that were sold by Company X at a discount if a buyer purchased a new phone plan. On request from buyers of the phones, the subject unlocked the phones, which allowed buyers to use them with any network provider or to sell them at a higher price than the original purchase price.
  The lawful changing of the SIM lock can be initiated by Company X from Apple Inc. through a programme installed on the computers of Company X. After the subject infected the computers of Company X with a Trojan, the virus allowed the subject to use the program through a remote server. Thus, the subject had illegal access to the program that would be legally used by Company X to unlock phones.

The perpetrator unlocked 707 mobile phones and was prosecuted for the breach of an information system and of a large number of data. In accordance with Article 29 of the Convention, the Hungarian investigating authority requested the US Department of Justice to preserve stored computer data regarding the SIM unlock requests sent by Company X to Apple. A request for legal assistance, based partly on Articles 4, 23, 25, 29 and 31 of the Convention and partly on a bilateral mutual legal assistance treaty, was subsequently sent to the American authorities to obtain the disclosure of data preserved by Apple. This data was necessary to establish the facts of the case and identify the actual users of the unlocked phones, and thus helped to identify the subject(s).

- In its final example, Hungary requested disclosure of data from the Ukrainian authorities in a case involving breach of data and information systems. The CEO of a company had reported to the police that an unknown person had illegally accessed the company's telephone server and made a large number of calls to the Seychelles Islands and Guinea Bissau, amongst other countries, resulting in a loss of 7,500,000 HUF. The unknown subject used a phone number belonging to the company by first calling the number from a Ukrainian number. The Ukrainian authorities responded to the request.

► **Italy** provided the following international cooperation case example:

On 14 June 2013, the office of the Italian contact point received an urgent request for cooperation from the Norwegian contact point. Italy was informed that an Afghan national residing in Norway had stabbed his wife to death two days earlier.
The subject had then gone off the grid with his two-year-old daughter and had arrived in Italy, according to the information entered into the "Schengen Information System-SIRENE" by the Norwegian authorities. The Norwegian authorities provided physical details and a description of the suspect.
The analysis of Skype connections and the mobile phone number provided by the Norwegian police revealed two Italian IP addresses. In the meantime, the Prosecutor's Office obtained an order for real-time tracking and positioning with a view to locating the device.
As a consequence, between the night of 15 June and the following morning, the mobile phone was geolocated in a specific area of Rome. In that area, on 16 June, Italian officers noticed a young man in the company of a little girl whose age was consistent with the girl's age as reported by the Norwegian police.
Italian officers examined the man's seized personal effects, carried out checks, and were able to ascertain the identity of the man, who was then arrested. Photos of the arrested person and the child were sent to the Norwegian authorities, who confirmed the identities.
The subject was extradited and the child was returned to Norway, where a programme for her protection had been implemented and relatives were present to welcome and house her.

► **Panama** reported that it had been able to obtain the support in January 2020 of agencies in other countries, such as the UK's National Crime Agency, for a DDoS investigation.

► **Romania's** most relevant unit for international cooperation on cybercrime – the Service for Combating Cybercrime within Directorate for Investigating Organised Crime and Terrorism Offences (DIICOT) – which is also the 24/7 Point of Contact for the network established by Article 35 of the Convention, for 2019 reported 144 incoming requests for stored computer data preservation and 39 outgoing requests, as well as 407 mutual legal assistance requests in cybercrime cases (321 active requests and 86 passive requests). Apart of this, the prosecutors from the above-mentioned unit initiated and participated in 3 Joint Investigation Teams.

► In **Serbia**,

- the Serbian Special Prosecutor's Office for High-Tech Crime and the High-Tech Crime Department of the Ministry of Interior have been conducting an ongoing operation, "Armageddon," since 2011 relating to sexual abuse of children on the Internet. In line with the Lanzarote Convention, these cases are considered urgent. In most of these cases international cooperation is used for gathering evidence.
  Serbia underlined that, in the following case, it received effective and efficient mutual assistance: not only was all requested evidence gathered rapidly, but the Hungarian liaison officer in Serbia personally brought the evidence to the Serbian prosecutor.
  In this case, preliminary proceedings were initiated based on information from a Hungarian authority received via INTERPOL. The Hungarian authorities had received a criminal complaint from a minor victim who had been in communication with an unknown person on a social network registered in Hungary. After gaining the victim's trust, the target threatened her and forced her to send him pictures of herself without clothing and performing sexual activities in front of the camera.
  The Hungarian authorities sent to Serbia the IP logging records for the accounts that defendant had used on the social network, which belonged to a Serbian internet provider. The Special Prosecution Office obtained a court order and located the communication. The office then obtained a search *warrant*, and expert opinion found evidence of the crime on electronic devices belonging to defendant that were seized by the police.
  Simultaneously, the Special Prosecution Office submitted a request for mutual assistance and received from the competent prosecutor's office in Hungary statements from the victim and other witnesses as well as copies of the victim's electronic communications.
  The indictment alleged that defendant, on many occasions over a period of two years, used the minor victim to produce pornographic photographs and audio-visual items. He threatened that he would *post* on the Internet pictures of her in her swimsuit, her pictures without clothing, and the above video materials. Those threats and orders were sent via a social network and Skype. Defendant kept all the pictures and video material in his computer.
  The defendant was convicted of the offences of showing, procuring and possession of pornographic material and juvenile pornography and of coercion and given a prison sentence.
- In another case, in Spring 2020, **Serbia** – together with Austria, Bulgaria and Germany and with the support of Eurojust – participated in successful operations against two organised crime groups suspected of large-scale investment fraud in cyber-trading. On an action day on 2 April 2020, four suspects were arrested in Bulgaria. In Germany, EUR 2.5 million were frozen in the bank account of a company involved in the fraud scheme. The Serbian authorities arrested five suspects and searched nine places, seizing five apartments, three cars, a considerable amount of cash, and IT equipment. Additionally, more than 30 bank accounts were put under surveillance. Based on the information gathered during the action day, authorities engaged in another operation against a company in Belgrade on 4 April, arresting one suspect and seizing servers, other IT equipment, and documents. In this case, the Serbian authorities, inter alia, made use of Article 26 Budapest Convention (Spontaneous information) to share information with other partners.

- The **Slovak Republic** often requests mutual assistance for which the Convention provides it a legal basis. The Convention's articles 23, 25, and 31 are most often used (in addition to Article 29 for preservation). Outgoing requests seek various forms of evidence, including subscriber, traffic and content data. The majority of Slovak requests are sent to the major US providers and services (such as Microsoft, Google, Facebook, and Instagram) as well as other major or even small services.

- The majority of requests sent to **Spain** are for transactional data and, to a lesser extent, content data. The vast majority of requests come from the USA. The most recent request from the USA described a botnet scheme in which different countries and companies were involved. The request sought, among other measures, transactional data related to an IP address associated with the company responsible for the botnet.

- **Sri Lanka** reported previously that it had made 37 international requests and received replies to thirty. It was able to identify several phone numbers used to create fake Facebook accounts, which led to successful criminal investigations.
  In April 2019, Sri Lanka suffered serious terrorist attacks (known as "2019 Sri Lanka Easter bombings") during which more than 250 people were killed and hundreds injured. It was a national emergency where electronic evidence was required from a range of service providers instantly. There was immediate international assistance from a number of countries, including State Parties to the Convention, and Sri Lanka was able to successfully gather electronic evidence, including account details, correspondence and contents in some cases. Electronic evidence was furthermore obtained through joint investigations, based on the amendments to laws carried out since becoming a Party to the Budapest Convention. There were also many instances of spontaneous information shared through law enforcement agencies locally under Article 26 of the Convention.

- Most outgoing **Swiss requests** relating to cybercrime are addressed to the US to obtain information from Facebook, Google and other US Internet service providers. In the last two years, requests addressed to Turkey, Ghana, and non-Parties Hong Kong and Nigeria have increased. In general, Swiss requests are for identification of suspects by disclosure of traffic data. Interception of content data is not often requested – it is sought only in complex investigations that are accompanied by other technical surveillance measures in Switzerland and/or third countries. Computer fraud, such as romance scams; extortion by ransomware; child pornography and similar criminal acts are the main foci of Swiss investigations. Switzerland said that it frequently uses transborder access based on Article 32.
  Switzerland commented that the most used Budapest provision is Article 29, requests for preservation of data, indicating that it receives virtually no requests for mutual legal assistance without a prior Article 29 preservation request. Switzerland is seeing an increase in incoming requests for mutual assistance, usually seeking traffic data. Since several providers in Switzerland offer encrypted communication and this can be abused by criminals, the number of related requests to Switzerland is constantly increasing. Cryptocurrency trading offered by Swiss providers is also a main factor in requests for mutual legal assistance.

- **Turkey** provided several examples:

  - In the first Turkish case example, the Turkish National Police's Online Notice System received a notice saying that there was going be a bomb attack in a town in the south of Turkey. The system automatically captures the source IP, which resolved to a communications company in the US. After Turkey telephoned and emailed the company, it disclosed that the IP was resolving to an American cruise company. The

cruise company determined that the IP was resolving to one of its vessels, which was in another country at that time. Officials on board the ship checked security camera records and located the suspect, a Turkish man. After initially refusing to speak, he admitted that he had sent the notice when he was drunk. He was fired, his visa was cancelled, and he was arrested at the airport on return to Turkey.

- In another case, Turkey received information about a possible ISIS attack in Turkey and obtained subscriber information to prevent the attack.
- In its final example, Turkey received from a source a screenshot of a conversation between two Kurdistan Workers' Party (PKK) terrorists saying that they were in Paris and were planning to explode a bomb in Schiphol Airport the next day. Turkey passed on the notice to the Netherlands authorities so that they could take precautions.

3.2 Use of 24/7 contact points

Parties use the 24/7 network extensively and they supplied statistics and examples to illustrate this.

► **Belgium** in 2019 received 10 requests from the Netherlands, the USA, Lithuania, France and Switzerland and sent 27 requests to twelve different Parties, that is, Canada, France, Germany, Hungary, Latvia, Netherlands, Poland, Switzerland, Turkey, Ukraine, UK and USA

► The 24/7 point of contact in **Bosnia and Herzegovina** mainly sent requests for preservation of e-mail account data to ISPs in other countries; it has sometimes obtained subscriber data. Most requests went to the US 24/7 point of contact, and this "can be characterized as very successful cooperation." Cooperation has also been established with the points of contact in Germany, France, Netherlands, Latvia, etc., and in non-Parties. The Prosecutor's Office of Bosnia and Herzegovina has sent at least three requests for data preservation, per Article 29 of the Convention. Requests were sent in investigations of blackmail, damage to or unauthorised access to computer data and programs, computer fraud, child exploitation, unauthorised usage of copyrights, and other types of cases.
In one case example, the Prosecutor's Office of Brčko District made a preservation request for the data relating to a certain IP address through the 24/7 point of contact. The recipient of the request replied that a virtual private network (VPN) was involved and provided information on the service and service provider. Freezing the data was not possible, but the target's identity was determined based on the information that was disclosed.
In 2019, there were twenty-one requests by domestic institutions and three by other cybercrime points of contact. Eighty-six cybercrime cases were opened using INTERPOL channels on the request of domestic institutions and twenty-one on the request of foreign national contact bureaux.

► **Chile** reported using the 24/7 network nineteen times in the three months between mid-October 2019 and late January 2020 to make requests of three countries.

► The **Czech Republic** successfully resolved a case with the assistance of the 24/7 network. A Czech psychologist received several emails containing suicidal thoughts from a person using the seznam.cz portal. IP logs of the email box were obtained. As soon as the provider of the email service (Deutsche Telekom) was identified, immediate co-operation was requested via the German contact point, which established the endpoint of the user of the IP address. The user who had sent the emails was a Czech citizen living in Germany.

► **The Dominican Republic** between 2016 and 2019 sent 34 preservation requests and 3 requests under the three 24/7 networks (Budapest Convention, G7 and INTERPOL).

► **France** makes extensive use of the Budapest Convention's 24/7 network not only for computer-related crime but for all matters in which electronic evidence is necessary. France used the network at the time of the Charlie Hebdo attacks to obtain information on foreign forums about possible new terrorist attacks.

In practice, requests seek preservation pending a formal mutual assistance request. Beyond its essential rôle in preservation of data, the point of contact can provide initial technical or legal advice to the service making the requests. The channel can also transmit requests for immediate assistance in cases in which a person's physical safety is in question (kidnapping, threats, etc).

In 2019, the French point of contact handled 268 Budapest Convention-related requests, all for the preservation of data. These included 130 incoming requests (from 24 countries) and 138 outgoing requests. In several terrorism matters, this practice permitted the urgent preservation of essential data.

► **Israel** reported four significant cases involving the use of the 24/7 network.

- During April and May 2019, three requests to freeze data and obtain information concerning a business email compromise (BEC) fraud, in real time, were received from three European Parties. The IP addresses led to an Israeli suspect. During the real time investigation, several prepaid Israeli cell phones were located that were being used to commit the crime (most likely as "net sticks"). Several of the persons linked to these cases have a record of fraud offences and business email compromise frauds. Following the location of this base of operations, the European Parties are expected to send MLA requests regarding the case in order to open an Israeli investigation. Throughout the real time management of these events, a direct connection was maintained between Israel's 24/7 centre and the other 24/7 contact points in order to obtain additional information necessary to advance the investigation.
- A request for preservation was received from one European Party concerning a suspicious IP address involved in an attempt to hack into local governmental systems of that Party. The IP led to an Israeli storage provider. Investigative activities relating to that provider turned up a citizen of a Latin American country as a suspect. A complete copy of the server was made, and information was conveyed to the national CERT and as background/leads to counterparts.
- The Israeli national police unit for economic offences received a report concerning a suspect in death threats and witness tampering through Telegram. The unit provided support in this emergency to exhaust all leads to the suspect. After suspicious IP addresses were detected that led to communication companies in a non-Party in South Asia, as well as two Parties in the Americas and Europe, emergency requests were made to those countries. Considering all the evidence, it appears that the suspect is sophisticated and utilises multiple encryption measures (Telegram and VPN). Moreover, details were received from the country in South Asia regarding the suspect, who possesses an account linked to the Telegram account from which the threatening messages were sent.

- In September 2019, threatening comments directed at the Prime Minister and the President of Israel were made on an Israeli news website from several different profiles. Information obtained from the news website indicated that two of the threatening profiles were linked to one IP address, which led to an American communications company. An emergency request was made to the US' 24/7 contact point in order to immediately locate the suspect. From counterpart investigations, it emerged that the

suspect is an Israeli citizen residing illegally in the US. Consequently, the US started a deportation process and the suspect will be arrested upon arrival in Israel.

- **Italy** commented that the 24-7 network was and is basically being used to send and receive requests for the preservation of electronic evidence (logs, records, etc.). In many cases, the Italian point of contact also sent and received requests for basic subscriber information that can be disclosed immediately on a police-to-police basis when applicable.
  In addition to this, Italy found that the network proved helpful in conveying information and alerts on cyberattacks and cyber threats concerning critical infrastructures in other countries and in providing indicators of compromise if available.
  In 2018, Italy received 39 incoming requests and sent 69 requests. These involved 28 other countries.

- **Luxembourg** became a Party to the Convention in July 2014 and set up a 24/7 contact point. The contact point has handled 75 requests since then, including 25 in 2019. It commented that the use of the network has been growing quickly.

- **Panama** reported that, "covered by articles 16 and 17 of the Budapest Convention, we have succeeded in assisting nations such as Israel, Switzerland and Australia, through their contact points."

- The **Slovak Republic** in 2019 had 321 outgoing 24/7 messages to thirteen Parties in 2019, of which most to the USA (193) followed by Germany (34), the Czech Republic (29) and the UK (14). Slovakia received 380 messages, of which most from the USA (264), followed by the Czech Republic (39), Germany (22) and the UK (15).

- In February 2019, **Spain** received a request from the UK point of contact for the preservation of the NetFlow traffic of an IP address (this protocol stores information about IP and source/destination port for statistical and network management purposes). This information from a Spanish ISP was necessary for an ongoing investigation. This information had never been used in Spain; operators store it for no more than two days. The Spanish point of contact requested the preservations every other day and successfully ensured that the data would be available when the MLA request was received.
  In May 2019, in an investigation about an intrusion into a private network in Spain, the Spanish point of contact sent a content preservation request to a service provider hosted in Israel. The service turned out to be a virtual private server, and the point of contact not only preserved the data but provided basic subscriber information, which was very useful for pursuing the investigation.

- In the last four years, **Turkey** received 43 preservation requests, leading to twenty-one preservations and five requests still in progress. The remainder were refused because the data was no longer available or because of technical difficulties - for instance, the use of NATs (Network Address Translation).

- For the period of January to September 2019, **the UK** reported 77 incoming preservation requests from eighteen Parties and 169 outgoing preservation requests to twenty-seven Parties.[2]

[2] These statistics also include requests via the G7 network.

3.3 Improvements to cooperation with the private sector due to membership in the Convention

Most Parties emphasise two powers that provide a significant benefit: the ability to directly request preservation from US providers (or to have US government officials rapidly send preservation requests on their behalf) and the ability to request subscriber information directly from US providers. These powers are not tied solely to the Budapest Convention. However, some countries have been more willing to use them, or have been more successful with providers, since becoming Parties.

Moreover, in March 2017, the T-CY adopted a Guidance Note on Production orders for subscriber information (Article 18 Budapest Convention) which shows how Article 18.1.b of the Convention may serve as a legal basis for requesting subscriber information from a service provider offering its service in the territory of a Party.

Cooperation with US-based providers is especially significant for investigations by countries other than the US because desired data is frequently held in the US or controlled by US-based providers. Many countries are aware that, if the requested data is covered by US law, the provider has the discretionary authority to disclose certain types of that data to non-US officials without formal mutual legal assistance. Countries are also aware that, when the largest US providers decide whether to fulfil such discretionary requests, the providers explicitly consider whether a requesting country is a Party.

Thus, transnational cooperation with the private sector, not solely domestic cooperation, is important.

- **Bosnia and Herzegovina** commented that, in general, its law enforcement agencies have signed memoranda of cooperation with local telecommunications providers, which allows BiH law enforcement access to certain databases. Law enforcement agencies also organise and participate in roundtables, workshops and conferences where they exchange information and experience with telecommunications providers, financial institutions and information technology companies.
  The Ministry of the Interior of Republika Srpska reported that cooperation with the domestic and international private sector has been greatly advanced by the Convention. Most companies have set up contact lines for representatives of law enforcement agencies so that they can obtain the information necessary for further action.
  In a case involving the unauthorised use of copyrights, the Prosecutor's Office of Bosnia and Herzegovina authorised a police agency to send a request for voluntary disclosure of data, based on Article 18.1.b of the Budapest Convention, directly to a US service provider.

- **Chile** explained that its cooperation with the private sector, particularly cooperation with non-Chilean Internet service providers, had improved after it acceded to the convention. Based on Article 18 of the convention, Chile has received subscriber information, including IP information, via direct cooperation with private companies, including Facebook, Instagram, Uber, Google, Microsoft, and others. Before its accession, Chile obtained less cooperation; ISPs did not respond to its requests.

- **France** supports the Cybercrime Convention Committee (T-CY) in its broad interpretation of Article 18 of the Convention (rapid production of subscriber data by service providers). In France's view, the T-CY understanding of Article 18 (1) (b) offers a legal basis for obtaining – directly from service providers – data that is indispensable to criminal investigations. Obtaining quick disclosure of data held by foreign service providers remains a challenge.

Data available show that almost all Parties make use of the possibility of US service providers to discuss subscriber information voluntarily and that the level of cooperation has increased considerably in the five-year period between 2014 and 2019, even if not all Parties engage in such cooperation to the same extent.

One of the features envisaged for the future 2nd Additional Protocol to the Budapest Convention is to put direct cooperation with service providers in other Parties for the disclosure of subscriber information on a clearer legal basis. Direct cooperation would then not only be possible with US-service providers.

	Requests for account information received/disclosed by Facebook, Google/YouTube and Microsoft/Skype					
	In 2014			**In 2019**		
From Parties	**Received**	**Disclosed**	**%**	**Received**	**Disclosed**	**%**
Albania	19	4	21%	30	20	67%
Andorra	Not a Party			3	2	67%
Argentina	Not a Party			6,648	5,292	80%
Armenia	10	2	20%	27	15	56%
Australia	5,482	3,796	69%	8,046	6,494	81%
Austria	231	64	28%	843	449	53%
Azerbaijan	0	0	0%	0	0	0%
Belgium	1,789	1,313	73%	2,836	2,379	84%
Bosnia and Herzegovina	13	8	62%	111	83	75%
Bulgaria	4	3	75%	73	41	56%
Cabo Verde	Not a Party			0	0	0%
Canada	742	436	59%	4,266	3,407	80%
Chile	Not a Party			1,253	798	64%
Colombia	Not a Party			836	465	56%
Costa Rica	Not a Party			101	60	59%
Croatia	45	34	76%	114	90	79%
Cyprus	38	21	55%	40	23	58%
Czech Republic	332	204	61%	737	573	78%
Denmark	343	221	64%	306	163	53%
Dominican Republic	54	30	56%	326	161	49%
Estonia	35	19	54%	327	241	74%
Finland	143	102	71%	417	346	83%
France	19,184	12,098	63%	33,020	24,121	73%
Georgia	1	0	0%	20	13	65%
Germany	20,696	12,348	60%	43,372	28,094	65%
Ghana	Not a Party			3	0	0%
Greece	Not a Party			1,614	1,023	63%
Hungary	338	159	47%	810	347	43%
Iceland	3	2	67%	5	2	40%
Israel	Not a Party			1,755	1,354	77%
Italy	7,434	3,913	53%	8,917	4,907	55%

	Requests for account information received/disclosed by Facebook, Google/YouTube and Microsoft/Skype					
	In 2014			In 2019		
Japan	1,000	786	79%	883	634	72%
Latvia	2	2	100%	91	45	49%
Liechtenstein	Not a Party			0	0	0%
Lithuania	35	22	63%	377	307	81%
Luxembourg	143	112	78%	248	76	31%
Malta	367	196	53%	495	237	48%
Monaco	Not a Party			14	8	57%
Morocco	Not a Party			262	182	69%
Mauritius	0	0	0%	0	0	0%
Moldova	13	7	54%	35	9	26%
Montenegro	7	1	14%	41	32	78%
Netherlands	1,063	851	80%	2,664	2,083	78%
North Macedonia	0	0	0%	147	69	47%
Norway	342	235	69%	525	332	63%
Panama	88	68	77%	38	11	29%
Paraguay	Not a Party			43	15	35%
Peru	Not a Party			152	100	66%
Philippines	Not a Party			58	23	40%
Poland	1,742	548	31%	11,399	6,659	58%
Portugal	2,203	1,355	62%	4,023	2,102	52%
Romania	79	40	51%	515	297	58%
San Marino	Not a Party			1	0	0%
Senegal	Not a Party			7	0	0%
Serbia	16	9	56%	396	286	72%
Slovakia	104	36	35%	48	17	36%
Slovenia	10	6	60%	98	63	64%
Spain	3,892	2,255	58%	7,442	4,198	56%
Sri Lanka	0	0	0%	99	42	42%
Switzerland	396	270	68%	1,917	1,290	67%
Tonga	Not a Party		%	1	1	100%
Turkey	8,016	5,621	70%	9,740	6,071	62%
Ukraine	5	2	40%	91	60	66%
United Kingdom	16,599	12,557	75%	31,644	26,424	84%
USA	64,591	50,026	77%	136,101	114,127	84%
Total excluding USA	**93,158**	**59,756**	**64%**	**190,350**	**132,633**	**70%**
Total including USA	**157,749**	**109,782**	**70%**	**326,451**	**246,760**	**76%**

4 Capacity building

4.1 The rationale

Strengthening the capabilities of practitioners to investigate, prosecute and adjudicate cybercrime and other offences involving electronic evidence is probably the best way towards an effective criminal justice response to these challenges.

While the international community has been divided for decades on how best to address the question of cybercrime at international levels, there has always been broad agreement on capacity building. This was also an interim outcome of the UN Intergovernmental Expert Group on Cybercrime in February 2013.

The Council of Europe, therefore, decided in October 2013 to strengthen its own capacities for more effective capacity building by setting up the Cybercrime Programme Office (C-PROC) in Bucharest, Romania. C-PROC supported about one thousand activities worldwide since it became operational in April 2014. It currently manages projects with a volume of some EUR 40 million; these are joint projects with the European Union or are funded by voluntary contributions.

Project title	Duration	Budget	Funding
Cybercrime@Octopus	Jan 2014 – Dec 2020	EUR 4 million	Voluntary contributions (Estonia, Hungary, Japan, Monaco, Netherlands, Romania, Slovakia, UK, USA and Microsoft)
GLACY+ project on Global Action on Cybercrime Extended	Mar 2016 – Feb 2024	EUR 19 million	EU/CoE JP
iPROCEEDS-2 project targeting proceeds from crime on the Internet in South-Eastern Europe and Turkey	Jan 2020 – June 2023	EUR 5 million	EU/CoE JP
EndOCSEA@Europe project against Online Child Sexual Exploitation and Abuse	July 2018 – June 2021	EUR 1 million	End Violence against Children Fund
CyberSouth on capacity-building in the Southern Neighbourhood	July 2017 – Dec 2021	EUR 5million	EU/CoE JP
CyberEast project on Action on Cybercrime for Cyber Resilience in the Eastern Partnership Region	June 2019 – June 2022	EUR 4.2 million	EU/CoE JP

These projects may assist any country or territory upon request in the development of domestic legislation on cybercrime in a pragmatic manner on request through desk studies, advice, in-country or online workshops or similar activities. Recent examples include Burkina Faso, Republic of Congo, Fiji, Gambia, Guatemala, Liberia, Papua New Guinea, Namibia or Niger.

Experts from many countries also participate in regional events on different topics related to cybercrime organised by C-PROC or in partnership with other national, regional or international organisations.

However, for the full menu of activities – including sustainable training programmes for police, prosecutors and judges; specialised cybercrime units; cybercrime reporting systems; measures to enhance public/private, interagency and international cooperation; protecting children against sexual violence online – priority is given to States having requested accession to the Budapest Convention.

The rationale is that if a State requests accession to the Budapest Convention, this represents the necessary political commitment justifying support to the development of domestic legislation in line with this treaty and the strengthening of capabilities of criminal justice authorities to apply this legislation in the investigation, prosecution and adjudication of cybercrime and other offences involving electronic evidence.

This is not limited to Europe but is applicable to any country or region. The examples of countries such as the Philippines and Sri Lanka in Asia, of Ghana, Mauritius, Morocco or Senegal in Africa, of the Dominican Republic in Latin America or Tonga in the Pacific illustrate this correlation. These and other countries had decided to base their domestic laws on the Budapest Convention and to seek accession to this treaty. Therefore, they were eligible to participation in a wide range of activities in addition to assistance on legislation.

4.2 Examples of capacity building carried out

A full listing of activities supported in recent years in more than 100 countries worldwide would run over hundreds of pages and a full assessment of the impact of all of these activities is not feasible here.[3] The following snapshots should simply serve as examples illustrating that for States committed to joining the Budapest Convention, consistent multi-year support is available to permit such States to apply this treaty in practice and to engage in effective international cooperation.

It should also be underlined that not only the Council of Europe, but also other organisations and governments launched a wide range of capacity building initiatives from 2013 onwards.[4]

4.2.1 Africa: Senegal

Following several legislative reforms, the Senegalese government adopted the Law 2008-11 of 25 Jan 2008 on cybercrime, which is directly inspired by many of the provisions of the Budapest Convention. In November 2016, new amendments were introduced to the Penal Code and Criminal Procedure Code to create to further improve the legal framework regarding cybercrimes and facilitating the collection of electronic evidence.

---

[3] A full list of activities can be provided on request. For details of projects and their impact see www.coe.int/cybercrime

[4] Examples include: United Nations Office on Drugs and Crime with its Global Programme on Cybercrime; the European Union adopted a cybersecurity strategy calling for capacity building in 2013 and this engagement continues as reflected in the Council Conclusions on EU External Cyber Capacity Building Guidelines of June 2018; Government of the United States – in particular through the State Department and the Department of Justice – is assisting other countries through training and other means; the United Kingdom's Foreign and Commonwealth Office is funding the Global Cyber Security Capacity Centre (GCSCC) and has set up a Cyber Security Capacity Building Programme; the Government of the Netherlands in 2015 initiated and is funding the Global Forum on Cyber Expertise (GFCE); the World Bank in 2016 developed a toolkit on "Combatting Cybercrime – Tools and Capacity Building for Emerging Economies"; the Organisation of American States supports its member States in the strengthening of capacities on cybercrime and cybersecurity; INTERPOL has set up a Global Cybercrime Expert Group and provides targeted training in different regions of the world, often in cooperation with other organisations such as the Council of Europe; UNCTAD continues to support countries in the development of their regulatory framework on ICTs, including cybercrime.

In 2011, Senegal had requested accession to the Budapest Convention and was invited to accede. In 2017, Senegal became a Party to the Budapest Convention.

From 2013, Senegal was a priority country of the GLACY project on Global Action on Cybercrime, and in 2016 also became a regional hub under the GLACY+ project on Global Action on Cybercrime Extended. Senegal has benefitted from the following activities:

Date	Place	Title
Multiple	Strasbourg, France	Octopus Conferences 2009, 2013, 2015, 2016, 2018, 2019
10-14 Feb 2014	Dakar, Senegal	National situation report and country assessment in Senegal
24-27 March 2014	Dakar, Senegal	Launching conference of the GLACY project combined with workshops on international cooperation and statistics/ reporting systems
12-16 May 2014	The Hague, Netherlands	International workshop on Law Enforcement Training Strategies
2-3 June 2014	Bucharest, Romania	International workshop to reach agreement on concept for judicial training, held at the National Institute of Magistracy of Romania
17-18 June 2014	Strasbourg, France	11th T-CY Plenary
7-18 Sep 2014	Brussels, Belgium	Law Enforcement Training for Senegal and Moroccan representatives (Part 1)
1-3 Oct 2014	Singapore	Participation in the INTERPOL-Europol Cybercrime Conference
13-17 Oct 2014	Brussels Belgium	Law Enforcement Training for Senegal and Moroccan representatives (Part2)
Nov 2014	-	Contribution of a Senegalese expert to the Analysis report on the draft amendment of the legislation of the Kingdom of Morocco with regard to the requirements of the Convention on Cybercrime of the Council of Europe
2-3 Dec 2014	Strasbourg, France	12th T-CY Plenary
8-12 Dec 2014	Dakar, Senegal	Introductory Judicial ToT Course
26-27 March 2015	Colombo, Sri Lanka	International workshop on cybercrime strategies for all GLACY countries
15-19 June 2015	Strasbourg, France	13th T-CY Plenary and Octopus Conference
7-11 Sept 2015	Dakar, Senegal	Introductory cybercrime course for law enforcement for the Police
14-18 Sept 2015	Dakar, Senegal	Introductory cybercrime course for law enforcement for the Gendarmerie
23-24 Nov 2015	Dakar, Senegal	Meeting of the African Gendarmeries
30 Nov – 2 Dec 2015	Strasbourg, France	14th T-CY Plenary
8-11 Feb 2016	Dakar, Senegal	Support to national delivery of Introductory Judicial Course
21-23 March 2016	Port Louis, Mauritius	Second international workshop on adaptation and update of the Electronic Evidence Guide through development of the Standard Operating Procedures for digital forensics (with participation of all GLACY countries)
30 March – 1 April 2016	Dakar, Senegal	Advisory mission on cybercrime reporting systems, combined with workshop on reporting systems and interagency cooperation

11-13 April 2016	South Africa	International workshop on judicial training curricula integration (with participation of all GLACY countries)
25-27 April 2016	Colombo, Sri Lanka	International workshop and training for 24/7 points of contact of the GLACY countries (with participation of all GLACY countries)
2-4 May 2016	Dakar, Senegal	Advanced Judicial Training Course
9-11 May 2016	Dakar, Senegal	Improving international cooperation on cybercrime and electronic evidence in West Africa (GLACY Project)
23-26 May 2016	Strasbourg, France	15th T-CY Plenary
1-3 June 2016	Dakar, Senegal	In-country workshop on law enforcement training strategies and awareness raising on CY issues for the national police
27-28 July 2016	Rabat, Morocco	International Workshop on Effectiveness of legislation on cybercrime and electronic evidence measured through statistics
15-18 Aug 2016	Dakar, Senegal	Progress review meetings and updated situation reports for the country's participation the GLACY/GLACY+ projects
28-30 Sep 2016	Singapore	4th INTERPOL-Europol Cybercrime Conference
26-28 Oct 2016	Bucharest, Romania	GLACY Closing Conference to discuss the results of the project and adopt the Declaration on Strategic Priorities and Launching Event for the GLACY+ project
14-18 Nov 2016	Strasbourg, France	16th T-CY Plenary and Octopus Conference
16-17 Jan 2017	Dakar, Senegal	Advisory mission and workshop on Cybercrime Policies
25-26 Jan 2017	Nairobi, Kenya	Participation in the ICANN Capacity Building Workshop for African LEAs
27 Feb – 1 March 2017	Singapore	INTERPOL Joint training workshops for cybercrime units, prosecution, central authorities for mutual legal assistance and strengthening 24/7 POCs and International workshop on cooperation with Internet Service Providers
14-17 March 2017	Dakar, Senegal	CoE-ECOWAS joint Regional introductory judicial training on Cybercrime and e-evidence for West African countries and Mauritania (GLACY+ project)
29-31 March 2017	Accra, Ghana	International workshop on criminal justice statistics on cybercrime and electronic evidence, with participation of all GLACY+ countries
10-13 April 2017	Vienna, Austria	Participation in the 3rd meeting of the UN Intergovernmental Expert Group on Cybercrime (UNIEG)
7-9 June 2017	Strasbourg, France	17th T-CY Plenary
19-23 June 2017	Dakar, Senegal	First Responders Training of Trainers Course for the Gendarmerie
21-23 Aug 2017	Dakar, Senegal	In-country workshops on data protection and INTERPOL Tools and Services combined with support on how to set-up and how to strengthen the 24/7 points of contact for cybercrime and electronic evidence
11-13 Sep 2017	Abuja, Nigeria	Joint regional conference CoE-ECOWAS on the Harmonization of legislation on Cybercrime and Electronic Evidence with rule of law and human rights safeguards (GLACY+ project)
11-13 Oct 2017	Port Louis, Mauritius	4th African Working Group Meeting on Cybercrime for Heads of Cybercrime Units
20-24 Nov 2017	Singapore	INTERPOL Instructor Development Course
27-29 Nov 2017	Strasbourg, France	18th T-CY Plenary

11-13 Dec 2017	Cebu, Philippines	International Workshop on Judicial Training Strategies on Cybercrime and Electronic Evidence
7-8 March 2018	The Hague, Netherlands	CoE/Eurojust joint International conference on Judicial Cooperation in Cybercrime Matters
26-27 March 2018	Dakar, Senegal	Advice on the streamlining of procedures for mutual legal assistance related to cybercrime and electronic evidence
5-7 May 2018	Dakar, Senegal	AfriNIC Government Working Group (AfGWG) and ICANNs Capacity Development Workshop for African GAC members Law Enforcement and Consumer Protection Agencies
7-11 May 2018	Dakar, Senegal	Regional Basic Law Enforcement Training of Trainers on Cybercrime and Electronic Evidence for African Officers of Gendarmerie
14-18 May 2018	Vienna, Austria	UN Commission for Crime Prevention and Criminal Justice
18-22 June 2018	Singapore	INTERPOL Instructor Development Course
9-13 July 2018	Strasbourg, France	19th T-CY Plenary and Octopus Conference
4-7 Sep 2018	Strasbourg, France	Underground Economy Conference
18-20 Sep 2018	Singapore	6th INTERPOL-Europol Cybercrime Conference
16-18 Oct 2018	Addis Ababa, Ethiopia	African Forum on the policies on cybercrime capacity building by international/regional organisations organized in collaboration with the African Union Commission
12-15 Nov 2018	Dakar, Senegal	Advanced Judicial Training on cybercrime and electronic evidence for Judges, Prosecutors and Lawyers with participation of Francophone and Lusophone countries from the ECOWAS Region
27-30 Nov 2018	Strasbourg, France	20th T-CY Plenary and Protocol Drafting Plenary
4-6 Dec 2018	Accra, Ghana	5th INTERPOL African Working Group Meeting on Cybercrime for Heads of Cybercrime Units
17-21 Dec 2018	Dakar, Senegal	ECTEG Course: Cybercrime and digital forensics specialized training for law enforcement officers
24-30 March 2019	Vienna, Austria	UN Intergovernmental Expert Group on Cybercrime
4-5 April 2019	Cotonou, Benin	Contribution of an expert from Senegal to the Awareness Workshop on the Budapest Convention
15-16 April 2019	Brussels, Belgium	EU Cyber Forum
15-17 May 2019	Bucharest, Romania	FREETOOL showcase workshop in co-operation with University College Dublin
3-7 June 2019	Dakar, Senegal	Regional training of trainers for first respondents on cybercrime and electronic evidence to the African gendarmeries
24-27 June 2019	Accra, Ghana	African Region Data Protection and Privacy Conference
25-27 June 2019	Singapore	Workshop on Channels and Avenues for International Cooperation in Cybercrime
8-11 July 2019	Strasbourg, France	21st T-CY Plenary and 4th Protocol Drafting Plenary
10-12 July 2019	Strasbourg, France	International Conference of Judicial Trainers on Cybercrime and Electronic Evidence
3-6 Sep 2019	Strasbourg, France	Underground Economy Conference

23-26 Sep 2019	Lagos, Nigeria	African Regional Workshop on Cybercrime, National Cybersecurity and Internet Policy
21-23 Oct 2019	Dakar, Senegal	Advisory mission on CERT capacities, digital forensics lab and public-private cooperation
24-25 Oct 2019	Dakar, Senegal	Advisory mission on cybercrime reporting and workshop on collection and monitoring of criminal justice statistics on cybercrime and electronic evidence
30 Sep - 1 Oct 2019	The Hague, Netherlands	Eurojust-CoE International conference on online investigations: Darknet and online sexual violence against children
9-11 Oct 2019	The Hague, Netherlands	Europol-INTERPOL Cybercrime Conference
18-20 Nov 2019	Strasbourg, France	22nd T-CY Plenary and 5th Protocol Drafting Plenary
2-4 Dec 2019	Nairobi, Kenya	6th INTERPOL African Working Group Meeting on Cybercrime for Heads of Cybercrime Units

4.2.2 Asia: Sri Lanka

Sri Lanka adopted its Computer Crime Act in 2007. This Act was largely modelled on the Budapest Convention. In 2008, a first workshop was supported in Colombo and in the following years, experts from Sri Lanka participated on several other activities.

In 2015, however, Sri Lanka was invited to accede to the Budapest Convention and became a Party to this treaty. This permitted the implementation of a large number of activities with a particular focus on the training of law enforcement, prosecutors and judges in Sri Lanka.

By 2020, Sri Lanka is not only a priority country receiving support, but it serves as a hub through which it shares its experience and experts from Sri Lanka are now training practitioners in other countries in the Asia/Pacific region.

Date	Place	Title
27-28 Oct 2008	Colombo, Sri Lanka	Workshop on cybercrime for judges, prosecutors and investigators in Sri Lanka
5-6 April 2011	Colombo, Sri Lanka	Regional workshop on cooperation against cybercrime in South
4-5 Oct 2013	Colombo, Sri Lanka	Workshop on cybercrime capacity building: judicial and law enforcement training
Multiple	Strasbourg, France	Octopus Conferences 2008, 2009, 2010, 2011, 2013, 2015, 2016, 2018, 2019
26-27 March 2015	Colombo, Sri Lanka	Assessing the threat of Cybercrime Conference for Decision Makers
26-27 March 2015	Colombo, Sri Lanka	International workshop on cybercrime strategies (during Colombo conference)
26-27 March 2015	Colombo, Sri Lanka	International workshop on criminal justice statistics and reporting systems (during Colombo conference)
30 Sep – 2 Oct 2015	The Hague, Netherlands	Participation in the INTERPOL-Europol Cybercrime Conference
4-8 Nov 2015	Colombo, Sri Lanka	First Responders Course: Training of Trainers
30 Nov – 2 Dec 2015	Strasbourg, France	14th T-CY Plenary

12-14 Jan 2016	Colombo, Sri Lanka	Scoping mission on cybercrime reporting systems, combined with workshop on reporting systems and legal basis for interagency cooperation
8-10 Feb 2016	Colombo, Sri Lanka	Live data forensics training for law enforcement & CERT
11-12 Feb 2016	Colombo, Sri Lanka	Study visit of Tonga to SL-CERT
21-23 March 2016	Port Louis, Mauritius	Second international workshop on adaptation and update of the Electronic Evidence Guide through development of the Standard Operating Procedures for digital forensics (with participation of all GLACY countries)
31 March-3 April 2016	Colombo, Sri Lanka	Introductory Judicial ToT Course for Judges
5-6 April 2016	Colombo, Sri Lanka	Introductory Judicial ToT Course for Prosecutors
11-13 April 2016	South Africa	International workshop on judicial training curricula integration (with participation of all GLACY countries)
25-27 April 2016	Colombo, Sri Lanka	International workshop and training for 24/7 points of contact of the GLACY countries (with participation of all GLACY countries)
23-26 May 2016	Strasbourg, France	15th T-CY Plenary
27-28 July 2016	Rabat, Morocco	International Workshop on Effectiveness of legislation on cybercrime and electronic evidence measured through statistics
8-11 Aug 2016	Colombo, Sri Lanka	Progress review meetings and updated situation reports for the country's participation the GLACY/GLACY+ projects
31 Aug – 2 Sept 2016	Colombo, Sri Lanka	Advanced judicial training with participation of judges from Tonga and adaptation of revised advanced judicial course materials
24-25 Sep 2016	Colombo, Sri Lanka	Support to national delivery of introductory judicial course
28-30 Sep 2016	Singapore	4th INTERPOL-Europol Cybercrime Conference
26-28 Oct 2016	Bucharest, Romania	GLACY Closing Conference to discuss the results of the project and adopt the Declaration on Strategic Priorities and Launching Event for the GLACY+ project
14-18 Nov 2016	Strasbourg, France	16th T-CY Plenary and Octopus Conference
27 Feb – 1 March 2017	Singapore	INTERPOL Joint training workshops for cybercrime units, prosecution, central authorities for mutual legal assistance and strengthening 24/7 POCs and International workshop on cooperation with Internet Service Providers
29-31 March 2017	Accra, Ghana	International workshop on criminal justice statistics on cybercrime and electronic evidence, with participation of all GLACY+ countries
10-13 April 2017	Vienna, Austria	Participation in the 3rd meeting of the UN Intergovernmental Expert Group on Cybercrime
5-8 June 2017	Madrid, Spain	Participation in the INTERPOL Eurasian Working Group on Cybercrime for Heads of Units and in the Operational side-meeting on Business Email Compromise
7-9 June 2017	Strasbourg, France	17th T-CY Plenary

14-16 June 2017	Brussels, Belgium	International workshop for cybercrime units and law enforcement training institutions on training strategies (technical level) and access to ECTEG training materials
28-30 July 2017	Colombo, Sri Lanka	Residential workshop for High Court Judges on cybercrime and electronic evidence
9-13 Aug 2017	Colombo, Sri Lanka	Support to the residential workshop on cybercrime for intake of new judges
16-20 Aug 2017	Kathmandu, Nepal	Special training on cybercrime for Nepal judicial officers with trainers from Sri Lanka Judges' Institute, in partnership with Nepal Judicial Academy
22-24 Sep 2017	Colombo, Sri Lanka	Residential workshop for District Judges and Magistrates on cybercrime and electronic evidence (Batch 1/4)
13-15 Oct 2017	Colombo, Sri Lanka	Residential workshop for District Judges and Magistrates on cybercrime and electronic evidence (Batch 2/4)
20-24 Nov 2017	Singapore	INTERPOL Instructor Development Course
27-29 Nov 2017	Strasbourg, France	18th T-CY Plenary
11-13 Dec 2017	Cebu, Philippines	International Workshop on Judicial Training Strategies on Cybercrime and Electronic Evidence
18-19 Dec 2017	Colombo, Sri Lanka	Annual Conference for Judges organized by the Sri Lanka Judges' Institute
19-21 Feb 2018	Colombo, Sri Lanka	Advisory mission on the set-up of the Cybercrime Division at the CID
7-8 March 2018	The Hague, Netherlands	CoE/Eurojust joint International conference on Judicial Cooperation in Cybercrime Matters
12-16 March 2018	Hong Kong	Participation in the Cyber Command Course organized by the Hong Kong Police
13-15 March 2018	Dhaka, Bangladesh	Participation in the Workshop on Cybercrime and Cybersecurity for BIMSTEC Member Countries
16-18 March 2018	Colombo, Sri Lanka	Residential workshop for District Judges and Magistrates on cybercrime and electronic evidence (Batch 3/3)
27-30 March 2018	Chisinau, Moldova	Participation in the Regional Meeting: Cybercrime Cooperation Exercise organized under Cybercrime@EAP 2018
4-6 April 2018	Colombo, Sri Lanka	Integration of ECTEG materials in the training strategy for law enforcement officers
8-10 May 2018	Tehran, Iran	Participation in the INTERPOL Eurasian Working Group on Cybercrime for Heads of Units
14-18 May 2018	Vienna, Austria	UN Commission for Crime Prevention and Criminal Justice
18-22 June 2018	Singapore	INTERPOL Instructor Development Course
27-29 June 2018	London, UK	Participation in the 3rd INTERPOL Digital Forensics Experts Group
9-13 July 2018	Strasbourg, France	19th T-CY Plenary and Octopus Conference
4-7 Sep 2018	Strasbourg, France	Underground Economy Conference
29 Oct – 2 Nov 2018	Colombo, Sri Lanka	ECTEG Course: Cybercrime and digital forensics specialized training for law enforcement officers
14-16 Nov 2018	Colombo, Sri Lanka	In-country workshops on data protection and INTERPOL Tools and Services combined with support on how to set-up and how to strength the 24/7 points of contact for cybercrime and electronic evidence

27-30 Nov 2018	Strasbourg, France	20th T-CY Plenary and Protocol Drafting Plenary
2-3 March 2019	Colombo, Sri Lanka	Support to the workshop on cybercrime for intake of new judges
18-22 March 2019	Hong Kong	Participation in the Cyber Command Course organized by the Hong Kong Police
24-30 March 2019	Vienna, Austria	UN Intergovernmental Expert Group on Cybercrime
15-16 April 2019	Brussels, Belgium	EU Cyber Forum
15-17 May 2019	Bucharest, Romania	FREETOOL showcase workshop in co-operation with University College Dublin
22-24 May 2019	Seoul, Korea	Participation in the 20th International Symposium on Cybercrime Response (ISCR 2019)
25-27 June 2019	Singapore	Workshop on Channels and Avenues for International Cooperation in Cybercrime
8 July 2019	Brussels, Belgium	Study visit of Sri Lankan judges to Belgium and workshop on cybercrime and electronic evidence
16-27 July 2019	Leon, Spain	Participation in the Cybersecurity Summer BootCamp 2019
8-11 July 2019	Strasbourg, France	21st T-CY Plenary and 4th Protocol Drafting Plenary
10-12 July 2019	Strasbourg, France	International Conference of Judicial Trainers on Cybercrime and Electronic Evidence
28 July 2019	Bucharest, Romania	Review of the Framework for a Proposed Personal Data Protection Bill in Sri Lanka
2-6 Sep 2019	Manila, Philippines	Participation in the INTERPOL Malware Analysis Training
3-6 Sep 2019	Strasbourg, France	Underground Economy Conference
30 Sep - 1 Oct 2019	The Hague, Netherlands	Eurojust-CoE International conference on online investigations: Darknet and online sexual violence against children
8 Oct 2019	The Hague, Netherlands	Meeting of the 24/7 CPs of the Parties to the Budapest Convention
9-11 Oct 2019	The Hague, Netherlands	Europol-INTERPOL Cybercrime Conference
30 Oct - 1 Nov	Suva, Fiji	Participation of one expert from Sri Lanka in the Advisory mission on cybercrime legislation in Fiji
18-20 Nov 2019	Strasbourg, France	22nd T-CY Plenary and 5th Protocol Drafting Plenary
26-28 Feb 2020	Tbilisi, Georgia	International Meeting on Cooperation with Foreign Service Providers

4.2.3 Europe: Serbia

In 2005, the Council of Europe launched the "PACO Serbia Project on Economic Crime" which included a component on cybercrime. This was the first project of the Council of Europe that covered specifically this topic, apart from an Octopus Conference on Cybercrime held in 2004. Serbia signed the Budapest Convention in the same year, and in 2009 became a Party.

Between 2009 and 2013, Serbia was a priority country under the Cybercrime@IPA project on regional cooperation on cybercrime in South-eastern Europe.

In 2016, a new regional project was launched in this region. The iPROCEEDS project from 2016 to 2019 focused on the proceeds from crime online. Serbia was again a priority country, and the same is true for the follow up project iPROCEEDS 2 which commenced in January 2020.

The following table only lists the activities under the iPROCEEDS project in which experts from Serbia participated:

Date	Place	Title
14-15 April 2016	Belgrade, Serbia	Country Assessment Visit on the initial situation
24–25 May 2016	Strasbourg, France	15th plenary session of the Cybercrime Convention Committee (T-CY)
13-14 June 2016	Ohrid, North Macedonia	Regional workshop on private/public information sharing and intelligence exchange mechanisms between financial sector institutions, cybercrime units and other stakeholders (combined with the Opening Conference of the iPROCEEDS project)
7-8 Sep 2016	Belgrade, Serbia	Advisory Mission and workshop on Reporting Mechanisms
13-15 Sep 2016	Helsinki, Finland	Participation of cybecrime units in the Regional Internet Security Event (RISE) - Finland 2016 (Team Cymru)
28-30 Sep 2016	Singapore	INTERPOL-Europol Annual Cybercrime Conference
11-12 Oct 2016	Zagreb, Croatia	Regional workshop to review the current state of judicial training curricular on cybercrime, electronic evidence and online crime proceeds
24-25 Oct 2016	Dublin, Ireland	International meeting on private/public cooperation
25 Nov 2016	Tirana, Albania	Regional Workshop on Reporting Mechanisms: International Good Practices
14-15 Nov 2016	Strasbourg, France	The 16th plenary session of the Cybercrime Convention Committee (T-CY)
16-18 Nov 2016	Strasbourg, France	Participation in the Octopus Conference 2016
12-13 Dec 2016	Bucharest, Romania	Regional workshop on Money Laundering Risks related to New Technologies
16-17 Jan 2017	Belgrade, Serbia	Workshop on Online Financial and Credit Card Fraud
28 Feb-3 March 2017	Bucharest, Romania	Regional training for cybercrime units, economic crime units, financial investigators and specialised prosecutors on virtual currencies and the dark web (EMPACT)
19-20 April 2017	Belgrade, Bucharest	Workshop on inter-agency and international cooperation for search, seizure and confiscation of online crime proceeds
24-28 April 2017	Tbilisi, Georgia	Regional case simulation exercise on cybercrime and financial investigations
10 April 2017	Belgrade, Serbia	Meeting on Public-Private Cooperation
10-13 April 2017	Vienna, Austria	UN Intergovernmental Expert Group on Cybercrime
12-13 June 2017	Luxembourg	International workshop for cybercrime units, economic crime units, financial investigators, FIUs and specialised prosecutors on techniques to search, seize and confiscate proceeds from crime online in cooperation with FIU Luxembourg (combined with 3rd meeting of the Project Steering Committee)
15-16 June 2017	Brussels, Belgium	International workshop on cybercrime training strategies for law enforcement agencies and access to ECTEG materials in cooperation with INTERPOL and ECTEG

20-24 June 2017	Budva, Montenegro	Regional Training of trainers on delivery of the basic training module on cybercrime, electronic evidence and online crime proceeds for judges and prosecutors
22-23 June 2017	Belgrade, Serbia	Assessment mission of guidelines to prevent and detect/identify online crime proceeds
5-8 Sep 2017	Barcelona, Spain	Underground Economy Conference 2017 (organised by Team Cymru)
27-29 Sep 2017	The Hague, The Netherlands	The 5th INTERPOL/Europol Cybercrime Conference
4-5 Oct 2017	Ljubljana, Slovenia	Regional workshop to share experience on indicators and guidelines for financial sector entities to prevent money laundering in the online environment in cooperation with FIU Slovenia
9-11 Oct 2017	Baku, Azerbaijan	Regional conference on cybercrime and money laundering in cooperation with the Global Prosecutor's E-Crime Network (GPEN) and Government of Azerbaijan
12-13 Oct 2017	Bucharest, Romania	Study visit of representatives from CERTs to CERT-RO
30-31 Oct 2017	Sofia, Bulgaria	South-eastern Europe Regional Forum on Cybersecurity and Cybercrime in cooperation with the Ministry of Interior of Bulgaria
2-3 Nov 2017	Bucharest, Romania	Regional workshop to assess the national regulatory framework for obtaining and using electronic evidence in criminal proceedings
27-29 Nov 2017	Strasbourg, France	The 18th Plenary of the T-CY and 1st Protocol Drafting Plenary
4-7 Dec 2017	Belgrade, Serbia	National delivery of the Introductory Training Module on Cybercrime, Electronic Evidence and Online Crime Proceeds
11-15 Dec 2017	Dublin, Ireland	Long-distance master programme
20-21 Dec 2017	Skopje, North Macedonia	Regional workshop for sharing good practices on reporting mechanisms existent in IPA region (combined with the 4th meeting of the Project Steering Committee)
7-8 March 2018	The Hague, The Netherlands	Joint International Conference on Judicial cooperation in cybercrime matters in cooperation with EUROJUST
3-5 April 2018	Vienna, Austria	UN intergovernmental expert group meeting on cybercrime
3-4 May 2018	Kyiv, Ukraine	Regional meeting on international cooperation on cybercrime and electronic evidence
8-12 May 2018	Dublin, Ireland	Long-distance master programme at UCD
14-18 May 2018	Vienna, Austria	The 27th session of the UN Commission for Crime Prevention and Criminal Justice "Criminal justice responses to prevent and counter cybercrime in all its forms, including through the strengthening of cooperation at the national and international levels"
14-15 May 2018	Bucharest, Romania	Regional workshop on criminal justice statistics on cybercrime and electronic evidence
5-6 June 2018	Tbilisi, Georgia	EuroDIG 2018 – focus on criminal justice action in cyberspace
12–15 June	Belgrade, Serbia	Second National Delivery of the Introductory training module on cybercrime, electronic evidence and online crime proceeds
9-10 July 2018	Strasbourg, France	The 19th T-CY plenary
11-13 July 2018	Strasbourg, France	Octopus Cybercrime Conference

4-7 Sep 2018	Strasbourg, France	Underground Economy Conference 2018 (co-organised with Team Cymru) (combined with the 5th meeting of the Project Steering Committee)
4-5 Oct 2018	Zagreb, Croatia	Regional Forum on Online Fraud in South-eastern Europe in cooperation with the Judicial Academy of Croatia
5-7 Nov 2018	Budapest, Hungary	Training on virtual currencies in cooperation with the International Training Centre, International College of Financial Investigations
12-15 Nov 2018	Bucharest, Romania	Regional case simulation exercise on cybercrime and financial investigations
27-29 Nov 2018	Strasbourg, France	The 20th Plenary of the T-CY and Protocol Drafting Plenary
10-14 Dec 2018	Dublin, Ireland	Long-distance master programme
11–12 March 2019	Belgrade, Serbia	Advice to public authorities and law reform working group to bring legal framework in line with EU and Council of Europe standards
25–26 March 2019	Vienna, Austria	6th meeting of the T-CY Protocol Drafting Group
27 – 29 March 2019	Vienna, Austria	UN intergovernmental expert group meeting on cybercrime
29 March 2019	Bucharest, Romania	6th Meeting of the Project Steering Committee
8-11 April 2019	Belgrade, Serbia	Case simulation exercise on cybercrime and financial investigations (for Bosnia and Herzegovina, Montenegro and Serbia)
22 April 2019	Belgrade, Serbia	Advice on lessons learnt from case simulation exercises
30 April 2019	Zagreb, Croatia	International conference on digital forensics and digital evidence: DataFocus 2019
8-9 May 2019	Bucharest, Romania	Table-top exercise on international cooperation on cybercrime
15-17 May 2019	Bucharest, Romnaia	Meeting on Free Forensic Tools for the Law Enforcement Community (FREETOOL) in cooperation with UCD
25-27 June 2019	Singapore	Workshop on channels and avenues for international cooperation in cybercrime in cooperation with INTERPOL
26-27 June 2019	Bucharest, Romania	Fourth annual Symposium on Cybersecurity Awareness organised by the Anti-Phishing Working Group
8-11 July 2019	Strasbourg, France	21st T-CY plenary and 4th PDP plenary
10-12 July 2019	Strasbourg, France	First International Meeting of the national trainers on cybercrime and electronic evidence
3-6 Sep 2019	Strasbourg, France	Underground Economy Conference 2019
17-20 Sep 2019	Bucharest, Romania	Regional training on Undercover Online Investigations
30 Sep-1 Oct 2019	The Hague, Netherlands	International Joint Conference on Internet Investigations in cooperation with EUROJUST
8 Oct 2019	The Hague, Netherlands	Meeting of the 24/7 Contact Points under Budapest Convention
9-11 Oct 2019	The Hague, Netherlands	INTERPOL-Europol Annual Cybercrime Conference
14 Oct 2019	Belgrade, Serbia	Workshop to review progress in all project areas
21-25 Oct 2019	Bucharest, Romania	Regional training on Open Source Intelligence

18-22 Nov 2019	Strasbourg, France	The 22nd Plenary of the T-CY and Octopus Conference
25–28 Nov 2019	Belgrade, Serbia	Introductory training course on cybercrime, electronic evidence and online crime proceeds for judges and prosecutors
2-6 Dec 2019	Bucharest, Romania	Pilot ECTEG Training on Crypto currency and Dark Web Investigation in cooperation with SELEC
3 Dec 2019	Dublin, Ireland	UCD Graduation Ceremony for students having acquired a master degree in cybercrime investigations and computer forensics from project areas and supported by iPROCEEDS
9-10 Dec 2019	Strasbourg, France	Closing Conference: evaluation of progress made and the way forward

4.2.4 Latin America: Dominican Republic

The Dominican Republic adopted Law 53-07 on High Technology Crimes and Offences, published on 23 April 2007, which is based on the Budapest Convention. In 2013, it became the first country of Latin America to join this treaty as a Party. In 2016, the Dominican Republic not only became a priority country of the project on Global Action on Cybercrime Extended (GLACY+) but also a hub for Latin America and the Caribbean region. Activities have included so far:

Date	Place	Title
13-15 May 2008	Port of Spain, Trinidad and Tobago	Workshop on cybercrime legislation in the Caribbean
Multiple	Strasbourg, France	Octopus Conferences 2008, 2009, 2010, 2011, 2013, 2015, 2016, 2018, 2019
19-23 Sep 2016	Santo Domingo, Dominican Republic	Initial country assessment visit in view of the country's inclusion in the GLACY+ project
28-30 Sep 2016	Singapore	4th INTERPOL-Europol Cybercrime Conference
26-28 Oct 2016	Bucharest, Romania	GLACY Closing Conference to discuss the results of the project and adopt the Declaration on Strategic Priorities and Launching Event for the GLACY+ project
14-18 Nov 2016	Strasbourg, France	16th T-CY Plenary and Octopus Conference
27 Feb – 1 March 2017	Singapore	INTERPOL Joint training workshops for cybercrime units, prosecution, central authorities for mutual legal assistance and strengthening 24/7 POCs and International workshop on cooperation with Internet Service Providers
29-31 March 2017	Accra, Ghana	International workshop on criminal justice statistics on cybercrime and electronic evidence, with participation of all GLACY+ countries
24-28 April 2017	Santo Domingo, Dominican Republic	Introductory ToT on cybercrime and electronic evidence for Judges, Prosecutors and Lawyers and adaptation of materials to the local context
10-13 April 2017	Vienna, Austria	Participation in the 3rd meeting of the UN Intergovernmental Expert Group on Cybercrime (UNIEG)
24-28 April 2017	Manila, Philippines	Participation of one delegate from Ghana in the INTERPOL Malware Analysis Training
7-9 June 2017	Strasbourg, France	17th T-CY Plenary

14-16 June 2017	Brussels, Belgium	International workshop for cybercrime units and law enforcement training institutions on training strategies (technical level) and access to ECTEG training materials
10-13 Oct 2017	Santo Domingo, Dominican Republic	Support to the national delivery of Intro Course on cybercrime and electronic evidence for Judges and prosecutors
16-17 Oct 2017	Santo Domingo, Dominican Republic	Advisory mission on cybercrime reporting and workshop on collection and monitoring of criminal justice statistics on cybercrime and electronic evidence
4-7 Dec 2017	Santo Domingo, Dominican Republic	Forum on the policies on cybercrime capacity building by international/regional organisations in the LATAM and Caribbean regions
20-24 Nov 2017	Singapore	INTERPOL Instructor Development Course
27-29 Nov 2017	Strasbourg, France	18th T-CY Plenary
11-13 Dec 2017	Cebu, Philippines	International Workshop on Judicial Training Strategies on Cybercrime and Electronic Evidence
7-8 March 2018	The Hague, Netherlands	CoE/Eurojust joint International conference on Judicial Cooperation in Cybercrime Matters
3-5 April 2018	Vienna, Austria	Meeting of the UN Intergovernmental Expert Group on Cybercrime (UNIEG)
14-18 May 2018	Vienna, Austria	UN Commission for Crime Prevention and Criminal Justice
11-15 June	Santo Domingo, Dominican Republic	ECTEG Course: Live-Data Forensics for law enforcement officers
18-22 June 2018	Singapore	INTERPOL Instructor Development Course
26-28 June 2018	Santo Domingo, Dominican Republic	In Country workshops on data protection and INTERPOL Tools and Services combined with support on how to set-up and how to strength the 24/7 points of contact for cybercrime and electronic evidence
27-29 June 2018	London, United Kingdom	Participation in the 3rd INTERPOL Digital Forensics Experts Group
9-13 July 2018	Strasbourg, France	19th T-CY Plenary and Octopus Conference
27-31 Aug 2018	Singapore	Joint International Workshop for Cybercrime Investigation Units and MLA Central Authorities
4-7 Sep 2018	Strasbourg, France	Underground Economy Conference
18-20 Sep 2018	Singapore	6th INTERPOL-Europol Cybercrime Conference
25-26 Oct 2018	Santo Domingo, Dominican Republic	International Congress on Cybercrime organized by the Judicial School of Dominican Republic
27-30 Nov 2018	Strasbourg, France	20th T-CY Plenary and Protocol Drafting Plenary
11-15 March 2019	Santo Domingo, Dominican Republic	Advanced Judicial Training on cybercrime and electronic evidence for judges, magistrates and prosecutors
24-30 March 2019	Vienna, Austria	UN Intergovernmental Expert Group on Cybercrime

2-3 April 2019	Santo Domingo, Dominican Republic	Provide advice on the streamlining of procedures for mutual legal assistance related to cybercrime and electronic evidence
4-5 April 2019	Santo Domingo, Dominican Republic	In-country advisory mission on integration/ mainstreaming of training modules in curricula of training institutions
15-16 April 2019	Brussels, Belgium	EU Cyber Forum
15-17 May 2019	Bucharest, Romania	FREETOOL showcase workshop in co-operation with University College Dublin
28-30 May 2019	Santo Domingo, Dominican Republic	Development of Cybercrime investigations, digital forensics capabilities and operating procedures on digital evidence for law enforcement agencies, combined with in-country workshops and advice on interagency cooperation and private public partnerships to fight cybercrime
3-7 June 2019	Santo Domingo, Dominican Republic	Cryptocurrency investigations training to Police Cyber-units
12-14 June 2019	Santo Domingo, Dominican Republic	Regional conference on cybercrime and cyber security policies and strategies
25-27 June 2019	Singapore	Workshop on Channels and Avenues for International Cooperation in Cybercrime
1-3 July 2019	El Salvador	Advisory mission and workshop on legislation to FOPREL
8-11 July 2019	Strasbourg, France	21st T-CY Plenary and 4th Protocol Drafting Plenary
10-12 July 2019	Strasbourg, France	International Conference of Judicial Trainers on Cybercrime and Electronic Evidence
3-6 Sep 2019	Strasbourg, France	Underground Economy Conference
30 Sep - 1 Oct 2019	The Hague, Netherlands	Eurojust-CoE International conference on online investigations: Darknet and online sexual violence against children
8 Oct 2019	The Hague, Netherlands	Meeting of the 24/7 CPs of the Parties to the Budapest Convention
9-11 Oct 2019	The Hague, Netherlands	Europol-INTERPOL Cybercrime Conference
11-14 Nov 2019	Punta Cana, Dominican Republic	Meeting with cybercrime investigations heads of unit from the region to discuss operational activities and plan and organize a joint operation
18-20 Nov 2019	Strasbourg, France	22nd T-CY Plenary and 5th Protocol Drafting Plenary
16-18 Dec 2019	Santo Domingo, Dominican Republic	Advisory mission on Data Protection legislation

4.2.5 Pacific: Tonga

In 2003, Tonga adopted its Computer Crimes Act which covers broadly the provisions of the Budapest Convention. A major reform in view of a more comprehensive legal framework is underway. In December 2013, Tonga requested accession to the Budapest Convention and in 2017 it then became a Party.

Following its request for accession in December 2013, Tonga became immediately a priority country of the GLACY project. In 2016, Tonga then also became a regional hub for the South Pacific region under the GLACY+ project.

The Kingdom of Tonga has participated in the following activities:

Date	Place	Title
16-17 June 2010	Nuku'alofa, Tonga	Meeting of ICT ministers of the Pacific region
27-29 April 2011	Nuku'alofa, Tonga	Pacific regional workshop on cybercrime
Multiple	Strasbourg, France	Octopus Conferences 2011, 2015, 2016, 2018, 2019
24-27 March 2014	Dakar, Senegal	Launching conference of the GLACY project combined with workshops on international cooperation and statistics/ reporting systems
28 April – 2 May 2014	Nuku'alofa, Tonga	National situation report and country assessment
12-16 May 2014	The Hague, Netherlands	International workshop on Law Enforcement Training Strategies
2-3 June 2014	Bucharest, Romania	International workshop to reach agreement on concept for judicial training, held at the National Institute of Magistracy of Romania
17-18 June 2014	Strasbourg, France	11th T-CY Plenary
1-3 Oct 2014	Singapore	Participation in the INTERPOL-Europol Cybercrime Conference
2-3 Dec 2014	Strasbourg, France	12th T-CY Plenary
Jan-May 2015	Nuku'alofa, Tonga	Analysis of draft legislation of Tonga
26-27 March 2015	Colombo, Sri Lanka	International workshop on cybercrime strategies for all GLACY countries
24 April & 1 May 2015	Nuku'alofa, Tonga	Introductory Judicial ToT Course for judges and prosecutors
27-29 April 2015	Nuku'alofa, Tonga	First Responder training course for law enforcement
30 April 2015	Nuku'alofa, Tonga	Workshop on establishing national CERT
30 April 2015	Nuku'alofa, Tonga	Workshop on Interagency Cooperation
15-19 June 2015	Strasbourg, France	13th T-CY Plenary and Octopus Conference
Aug-Sep 2015	Nuku'alofa, Tonga	Support for legislative drafting for Tonga
30 Sep – 2 Oct 2015	The Hague, Netherlands	Participation in the INTERPOL-Europol Cybercrime Conference

30 Nov – 2 Dec 2015	Strasbourg, France	14th T-CY Plenary
24-26 Feb 2016	Nuku'alofa, Tonga	Support GPEN regional workshop for the prosecutors/attorneys of the Pacific
21-23 March 2016	Port Louis, Mauritius	Second international workshop on adaptation and update of the Electronic Evidence Guide through development of the Standard Operating Procedures for digital forensics (with participation of all GLACY countries)
24-25 March 2016	Port Louis, Mauritius	Study visit of Tonga to CERT-MU
11-13 April 2016	South Africa	International workshop on judicial training curricula integration (with participation of all GLACY countries)
25-27 April 2016	Colombo, Sri Lanka	International workshop and training for 24/7 points of contact of the GLACY countries (with participation of all GLACY countries)
23-26 May 2016	Strasbourg, France	15th T-CY Plenary
30-31 May 2016	Nuku'alofa, Tonga	Advisory mission to Tonga on cybercrime reporting systems and workshop on reporting systems, interagency cooperation and public-private cooperation
1-3 June 2016	Nuku'alofa, Tonga	Progress review meetings and updated situation reports for the country's participation the GLACY/GLACY+ projects
27-28 July 2016	Rabat, Morocco	International Workshop on Effectiveness of legislation on cybercrime and electronic evidence measured through statistics
28-30 Sep 2016	Singapore	4th INTERPOL-Europol Cybercrime Conference
26-28 Oct 2016	Bucharest, Romania	GLACY Closing Conference to discuss the results of the project and adopt the Declaration on Strategic Priorities and Launching Event for the GLACY+ project
14-18 Nov 2016	Strasbourg, France	16th T-CY Plenary and Octopus Conference
27 Feb – 1 March 2017	Singapore	INTERPOL Joint training workshops for cybercrime units, prosecution, central authorities for mutual legal assistance and strengthening 24/7 POCs and International workshop on cooperation with Internet Service Providers
29-31 March 2017	Accra, Ghana	International workshop on criminal justice statistics on cybercrime and electronic evidence, with participation of all GLACY+ countries
23-25 May 2017	Nuku'alofa, Tonga	Regional Workshop on Cybercrime and Electronic Evidence for Prosecutors of PILON Network
26-May 2017	Nuku'alofa, Tonga	Provide advice on the streamlining of procedures for mutual legal assistance related to cybercrime and electronic evidence
5-8 June 2017	Madrid, Spain	Participation in INTERPOL Eurasian Working Group on Cybercrime for Heads of Units and in the Operational side-meeting on Business Email Compromise
7-9 June 2017	Strasbourg, France	17th T-CY Plenary
3-5 July 2017	Nuku'alofa, Tonga	Advisory mission on CERT capacities, digital forensics lab and public-private cooperation
6 July 2017	Nuku'alofa, Tonga	Workshop on cybercrime reporting systems and collection and monitoring of criminal justice statistics on cybercrime and electronic evidence.

10-13 July 2017	Nuku'alofa, Tonga	Development of Cybercrime investigations, digital forensic capabilities combined with in-country workshops and advice on interagency cooperation and private public partnerships to fight cybercrime
25-29 Sep 2017	Nuku'alofa, Tonga	Introductory Judicial ToT Course on cybercrime and electronic evidence for Judges, Prosecutors and Lawyers and adaptation of materials to the local context, with the participation of selected countries from the Pacific Region
6-10 Nov 2017	Suva, Fiji	Participation in the INTERPOL Cybercrime Training for the Pacific Region
20-24 Nov 2017	Singapore	INTERPOL Instructor Development Course
27-29 Nov 2017	Strasbourg, France	18th T-CY Plenary
11-13 Dec 2017	Cebu, Philippines	International Workshop on Judicial Training Strategies on Cybercrime and Electronic Evidence
7-8 March 2018	The Hague, Netherlands	CoE/Eurojust joint International conference on Judicial Cooperation in Cybercrime Matters
12-16 March 2018	Hong Kong	Participation in the Cyber Command Course organized by the Hong Kong Police
27-30 March 2018	Chisinau, Moldova	Participation in the Regional Meeting: Cybercrime Cooperation Exercise organized under Cybercrime@EAP 2018
8-10 May 2018	Tehran, Iran	Participation in the INTERPOL Eurasian Working Group on Cybercrime for Heads of Units
14-18 May 2018	Vienna, Austria	UN Commission for Crime Prevention and Criminal Justice
12-15 June 2018	Nuku'alofa, Tonga	Regional Cybercrime Workshop (PILON)
18-22 June 2018	Singapore	INTERPOL Instructor Development Course
9-13 July 2018	Strasbourg, France	19th T-CY Plenary and Octopus Conference
20-24 Aug 2018	Nuku'alofa, Tonga	ECTEG Course, in parallel: 1. Open-Source forensics and 2. Mobile forensics
27-30 Aug 2018	Nuku'alofa, Tonga	Advanced Judicial Training on cybercrime and electronic evidence for Judges, Prosecutors and Lawyers with participation of countries from the Pacific Region
30 Aug	Nuku'alofa, Tonga	In-country advisory mission on integration/ mainstreaming of training modules in curricula of training institutions
4-7 Sep 2018	Strasbourg, France	Underground Economy Conference
27-30 Nov 2018	Strasbourg, France	20th T-CY Plenary and Protocol Drafting Plenary
18-22 March 2019	Hong Kong	Participation in the Cyber Command Course organized by the Hong Kong Police
24-30 March 2019	Vienna, Austria	UN Intergovernmental Expert Group on Cybercrime
15-16 April 2019	Brussels, Belgium	EU Cyber Forum
15-17 May 2019	Nuku'alofa, Tonga	In-country workshops on data protection and INTERPOL Tools and Services combined with support on how to set-up and how to strength the 24/7 points of contact for cybercrime and electronic evidence

15-17 May 2019	Bucharest, Romania	FREETOOL showcase workshop in co-operation with University College Dublin
27-31 May 2019	Vanuatu	PILON Regional Workshop on cybercrime and electronic evidence in the Pacific. International Cooperation
25-27 June 2019	Singapore	Workshop on Channels and Avenues for International Cooperation in Cybercrime
8-11 July 2019	Strasbourg, France	21st T-CY Plenary and 4th Protocol Drafting Plenary
10-12 July 2019	Strasbourg, France	International Conference of Judicial Trainers on Cybercrime and Electronic Evidence
2-6 Sep 2019	Manila, Philippines	INTERPOL Malware Analysis Training
3-6 Sep 2019	Strasbourg, France	Underground Economy Conference
25-27 Sep 2019	Nuku'alofa, Tonga	Integration of ECTEG training materials into the law enforcement training academies and other professional law enforcement training bodies
30 Sep - 1 Oct 2019	The Hague, Netherlands	Eurojust-CoE International conference on online investigations: Darknet and online sexual violence against children
8 Oct 2019	The Hague, Netherlands	Meeting of the 24/7 CPs of the Parties to the Budapest Convention
9-11 Oct 2019	The Hague, Netherlands	Europol-INTERPOL Cybercrime Conference
18-20 Nov 2019	Strasbourg, France	22nd T-CY Plenary and 5th Protocol Drafting Plenary
26-28 Feb 2020	Tbilisi, Georgia	International Meeting on Cooperation with Foreign Service Providers

4.3 Capacity building: lessons learnt

Programmes to strengthen criminal justice capacities on cybercrime and electronic evidence have been implemented for some fifteen years but significantly increased during the past seven years. The outcome of the 2013 meeting of the UN Intergovernmental Expert Group on Cybercrime seemed to have contributed to this expansion.

Experience shows that capacity building:

- works, responds to needs and makes an impact in terms of
  - legislation with safeguards,
  - investigations and criminal proceedings,
  - public/private, interagency and international cooperation,
  - sustainable training;
  -
- facilitates multi-stakeholder cooperation and synergies;
- has human development benefits and feeds into Sustainable Development Goals;
- helps reduce the digital divide;
- is based on broad international support and may help overcome political divisions.

5 Conclusion

Any country may make use of the Budapest Convention as a guideline, check list or model law, and a large number already makes use of this opportunity. However, becoming a Party to this treaty entails additional advantages in terms of formal and informal cooperation as well as capacity building:

- The Convention provides a **legal basis for international cooperation** on cybercrime and electronic evidence. Chapter III of the treaty comprises general and specific provisions for cooperation among Parties "to the widest extent possible" not only with respect to cybercrime (offences against and by means of computers) but also with respect to any crime involving electronic evidence. Parties make ample use of this in practice.

- Parties are **members of the Cybercrime Convention Committee (T-CY)** and share information and experience, assess implementation of the Convention, interpret the Convention through Guidance Notes, or prepare templates for mutual assistance requests and other tools to facilitate the application of the treaty to counter cybercrime more effectively. Experience shows that new Parties are able to share new knowledge with other members and soon take active roles in meetings or may be elected to leading positions in the T-CY.

- Through the T-CY, Parties contribute to the further evolution of the Budapest Convention, for example, in the form of Guidance Notes or additional protocols. Thus, even if a State did not participate in the negotiation of the original treaty, a new Party is able to participate in the **negotiation of future instruments**. The forthcoming 2nd Additional Protocol on enhanced international cooperation and access to evidence in the cloud will provide practitioners with additional tools and gains in efficiency for cooperation with other Parties as well as service providers.

- Membership in the Budapest Convention means membership in **networks of practitioners** – the 24/7 network of contact points among them – and thus the ability to engage in trusted cooperation.

- Parties to the Convention are able to improve their **cooperation with the private sector**. Indications are that private sector entities are more likely to cooperate with criminal justice authorities of Parties to the Convention given that Parties need to have a domestic legal framework on cybercrime and electronic evidence in place, including the safeguards of Article 15.

- States requesting accession or having acceded may become **priority countries or hubs for capacity building** programmes. Such technical assistance is to facilitate full implementation of the Convention and to enhance the ability to cooperate internationally. Donors are consistently providing resources to support countries in this undertaking, in particular through the Cybercrime Programme Office of the Council of Europe (C-PROC).

Experience after almost twenty years since its opening for signature shows that there are no disadvantages in joining this treaty.

Given the benefits of the Budapest Convention in practice, and its further evolution through the 2nd Additional Protocol, this treaty will remain highly relevant and membership will expand in the years to come.

6 Appendix: Parties, Signatories and States invited to accede to the Budapest Convention (status 30 June 2020)

Parties		**Signatories or invited to accede**
Andorra	Morocco	Benin
Argentina	Netherlands	Brazil
Armenia	North Macedonia	Burkina Faso
Australia	Norway	Guatemala
Austria	Panama	Ireland
Azerbaijan	Paraguay	Mexico
Belgium	Peru	Niger
Bosnia and Herzegovina	Philippines	Nigeria
Bulgaria	Poland	South Africa
Cabo Verde	Portugal	Sweden
Canada	Romania	Tunisia
Chile	San Marino	
Colombia	Senegal	
Costa Rica	Serbia	
Croatia	Slovak Republic	
Cyprus	Slovenia	
Czech Republic	Spain	
Denmark	Sri Lanka	
Dominican Republic	Switzerland	
Estonia	Tonga	
Finland	Turkey	
France	Ukraine	
Georgia	United Kingdom	
Germany	United States of America	
Ghana		
Greece		
Hungary		
Iceland		
Israel		
Italy		
Japan		
Latvia		
Liechtenstein		
Lithuania		
Luxembourg		
Malta		
Mauritius		
Republic of Moldova		
Monaco		
Montenegro		