Center for Cyber
& Homeland Security
THE GEORGE WASHINGTON UNIVERSITY

Mutual Legal Assistance:
Understanding the Challenges for Law Enforcement in Global Cybercrime Cases

Issue Brief - By Adam Palmer - January 2018

Because of the global connectivity of the internet, cybercrime has a transnational dimension that poses numerous challenges for law enforcement agencies. Some of these challenges, such as issues of sovereignty, international cooperation/mutual legal assistance, and evidence collection, are common to many types of transnational crime. However, some of the challenges of investigating transnational cybercrime are unique. As widespread use of the Internet increases, more potential victims are available to cybercriminals. The availability of devices that connect to the Internet is growing rapidly, and activity is no longer confined to traditional desktop computers. When a data transfers occurs it may also involve several countries, and because criminals do not need to be present at the scene of the crime, many cybercrimes are perpetrated across international borders.

International Cooperation in Cybercrime Cases

International law enforcement cooperation can be either formal or informal. Generally, the formal mechanisms for international cooperation are developed through bilateral or multilateral treaties, whereas informal measures are those developed through unofficial lines of communication for information sharing type purposes.[1]

The general principle for mutual legal assistance is derived from the general principle for international cooperation. Therefore, like international cooperation generally, the Council of Europe's Convention on Cybercrime states that each State should,

> "***afford one another mutual assistance to the widest extent possible*** for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence . . . ***adopt such legislative and other measures*** as may be necessary to carry out the obligations . . . [and] in urgent circumstances, make requests for mutual assistance or communications related thereto by expedited means of communication."

[1] Kimberly Prost, *Breaking down barriers: International cooperation in combatting transnational crime* (Nov. 29, 2015 12:08 P.M.), www.oas.org/juridico/mla/en/can/en_can_prost.en.html.

The most formal and traditional mechanism for obtaining evidence from other countries are through ***letters rogatory***, which are requests issued by courts of one State to the courts of another State asking the requested State to assist, through its judiciary, in the collection of evidence for an ongoing investigation in the requested State. Practitioners should be aware, however, that there exists no international legal obligation to comply with a request in a letter rogatory.

The second formal mechanism for requesting international legal assistance from a foreign State is through a ***mutual legal assistance treaty***. MLATs are agreed-upon frameworks and procedures by which States can request legal assistance from each other, such as evidence collection or the apprehension of criminal suspects, and can be either bilateral or multilateral depending on the particular treaty.[2] Developed as an alternative to letters rogatory, MLATs have established new forms of cooperative relationships between the law enforcement authorities of different States that streamline and standardize procedures for seeking foreign legal assistance. Although MLATs are generally much quicker than letters rogatory, "[i]nvestigations that require mutual legal assistance do in general take even longer due to the time consuming formal requirements in the communication of the law enforcement agencies."[3]

In addition to the formal mechanisms, there are informal ways of cooperation such as exchange of intelligence among law enforcement agencies in different countries. Informal methods of cooperation are particularly useful where the requested assistance involves information sharing or where the two States involved do not have an applicable bilateral or multilateral agreement through which to request assistance. Informal (direct) communication assistance involves direct contact between law enforcement organizations, agencies, and officials. Requests for assistance, usually in the form of information, are handled at the police or investigative level by operating through longstanding relationships between the two States. Despite the speed in which assistance can be requested and fulfilled with informal measures of international cooperation, these voluntary measures are often limited to information sharing because requests such as those for evidence or information not in police possession must be authorized through the proper legal channels. It is quite common for States to place liaisons from various law enforcement agencies within embassies or consulates located in foreign nations so that requests for legal assistance may be facilitated when either country needs such assistance. Examples of such cooperative contact points are the G8 and Council of

---

[2] United Nations Off. on Drugs and Crime, *Manual on Mutual Legal Assistance and Extradition* , %20https:/www.unodc.org/documents/organized-crime/Publications/Mutual_Legal_Assistance_Ebook_E.pdf; see generally pg. 19-22 (2012).

[3] United Nations Off. on Drugs and Crime, *supra* note 2, at 19.

Europe "24/7" networks, which facilitate a broad range of international cooperative efforts facilitating requests for both formal and informal cooperation.[4]

Grounds for refusal of mutual legal assistance, whichever form it may come in, usually include issues with: dual criminality[5], sufficiency of evidence[6], the non-extradition of nationals[7], concerns regarding the severity of punishment (usually the death penalty)[8], and human rights concerns.

Types of Mutual Legal Assistance Specific to Cybercrime

1. Expedited Preservation and Disclosure of Stored Computer Data

Recognizing that computer data is "highly volatile" and can be deleted in a single key-stroke, many international treaties combating cybercrime include procedural provisions that provide for the expedited preservation and disclosure of stored

[4] United Nations Off. on Drugs and Crime, *supra* note 2, at 209-210, 212.

[5] "Dual or double criminality is a legal principle that requires that the conduct of the person who, in this case, is the subject of a mutual legal assistance request be conduct that can be viewed as a criminal offence in both the requesting and the requested State. It is a concept that tends to play a larger role in the law pertaining to extradition; however, it can be found from time to time in the law pertaining to mutual legal assistance. . . . It should be emphasized that the test for dual criminality is whether the conduct that is the subject of the mutual legal assistance request is criminal in both States, not whether the conduct is punishable as the same offence in each State." United Nations Off. on Drugs and Crime, *supra* note 2, at 67.

[6] "The amount of evidence required is dictated partly by the legislation of the requested State and partly by the nature of the assistance sought. Generally, the more coercive the means of obtaining the evidence, the more involved and complex the evidentiary requirements become. . . . The evidentiary requirements to obtain the same type of assistance in different States will vary greatly, depending on treaty requirements, domestic legislation and the legal systems of the States involved. Reviewing the laws of the requested State and holding prior discussions with the requested State's central authority will enable a requesting State to provide a mutual legal assistance request that satisfies these basic requirements." United Nations Off. on Drugs and Crime, *supra* note 2, at 69.

[7] "The doctrine of non-extradition of nationals is found in many States, particularly those with a civil law tradition. Depending on the country, the refusal may be mandatory or discretionary; as always, it is worthwhile to look at the domestic legislation of the requested State to see if there is a possibility that the suspect who is a national of that State can be extradited under its legal system. It should be noted, however, that non-extradition does not necessarily mean non-prosecution." United Nations Off. on Drugs and Crime, *supra* note 2, at 49-50.

[8] Severity of punishment has been used in both the mutual legal assistance and extradition contexts, and is usually encountered with crimes "that may result in the imposition of the death penalty or cruel, inhuman, degrading punishment or torture." United Nations Off. on Drugs and Crime, *supra* note 2, at 71. Therefore, "[a] central authority that is well versed in international criminal law and has experience in dealing with certain regions or countries where this outcome is likely can assist in anticipating that this issue may arise and be proactive in addressing it with the requesting State by obtaining necessary information regarding sentencing in the event of a conviction prior to the assistance being provided." *Id*.

computer data.[9] This procedural mechanism ensures the availability of "data pending a lengthier and more involved process of executing a formal mutual assistance request, which can take weeks or months."[10]

For an example of one such provision contained in an international agreement see Article 29 of the Council of Europe's Convention on Cybercrime:

> ***Article 29 – Expedited preservation of stored computer data***
>
> 1. A Party may request another Party to order or otherwise obtain the expeditious preservation of data stored by means of a computer system, located within the territory of that other Party and in respect of which the requesting Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the data.[11]

It should be noted that while this procedure is designed to be much quicker that traditional mutual assistance, it is also less intrusive as the requested party does not have to actually acquire possession of the data from its custodian.[12] Often referred to as a "quick freeze," this investigative tool has the "advantage of being rapid and protective of [privacy]" because information is disclosed only to an authorized government official until procedural criteria for full disclosure have been met for a mutual assistance request.[13] Ultimately, the quick freeze procedure ensures that data essential to investigative efforts of law enforcement is not irretrievably lost.[14]

2. Expedited Preservation and Partial Disclosure of Traffic Data[15]

It is not uncommon for a State to be asked if it will preserve and/or disclose the traffic data of a transmission that has travelled through a computer located in its territory to trace the transmission to its source and identify the perpetrator of the crime, or locate evidence.[16]

---

[9] Council of Europe Convention on Cybercrime ETS Treaty No. 185 para 282 (2004).

[10] Id. para 282.

[11] Id. Art. 9.

[12] Id. para 283.

[13] Id. para 282-83; UCC 177.

[14] Id. para 283.

[15] Id. para 290; UCC 180-181.

[16] Id. para 290.

Article 30 – Expedited disclosure of preserved traffic data

1. Where, in the course of the execution of a request [for preservation and disclosure of computer data] to preserve traffic data concerning a specific communication, the requested Party discovers that a service provider in another State was involved in the transmission of the communication, the requested Party shall expeditiously disclose to the requesting Party a sufficient amount of traffic data to identify that service provider and the path through which the communication was transmitted.
2. Disclosure of traffic data under paragraph 1 may only be withheld if:

   (a) the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence; or

   (b) the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, public order or other essential interests.

Disclosure of preserved traffic data gives investigative authorities the ability to provide States that have requested the "quick freeze" procedure detailed above additional information regarding the identity of a service provider of a perpetrator and the path of the communication used to commit his crime.[17]

3. Production Orders

A production order allows law enforcement authorities to compel a person or service provider in its territory to provide stored computer data or subscriber information.[18] It also provides authorities with a more flexible mechanism to apply in cases where the disclosure of computer data is needed, while making service providers more comfortable with such disclosures by providing them legal basis upon which to rely in providing that information.[19]

[17] Id. para 290.

[18] Id. para 170. "The data in question are stored or existing data, and do not include data that has not yet come into existence such as traffic data or content data related to future communications." para 170.

[19] Id. para 170.

Article 18 – Production order[20]

1. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order:

   (a) a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and

   (b) a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control.

Subscriber information, according to the provision above, is defined as "any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services" that can establish "the type of communication service used," "the subscriber's identity" or "geographic address," as well as "any other information . . . available on the basis of the service agreement or arrangement."[21] This information is often necessary to ascertain the technical services that were used to perpetrate a cybercrime and to assist law enforcement authorities in accurately identifying the person alleged to have committed these crimes.[22]

4. Mutual Assistance in the Real-Time Collection of Traffic Data

This investigative tool gives law enforcement authorities the ability to acquire "the real-time collection of traffic data and the real-time interception of content data associated with specified communications transmitted by a computer system" from both "competent authorities" and "by service providers."[23] The Convention on Cybercrime illustrates this procedural mechanism in an international instrument.

Article 33 – Mutual assistance in the real-time collection of traffic data[24]

1. The Parties shall provide mutual assistance to each other in the real-time collection of traffic data associated with specified communications in their territory transmitted by means of a

[20] Id. Art. 18.

[21] Id. Art. 18(3)(a)-(c).

[22] Id. para 178.

[23] Id. para 205.

[24] Id. Art. 33.

> computer system. Subject to the provisions of paragraph 2, this assistance shall be governed by the conditions and procedures provided for under domestic law.
>
> 2. Each Party shall provide such assistance at least with respect to criminal offences for which real-time collection of traffic data would be available in a similar domestic case.

A mechanism that can be employed by law enforcement to acquire real time collection of data is essential to bringing offenders to justice because some information such as traffic data is no longer available once the perpetrator of an intrusion ceases its activity or changes its access route.[25]

5. Mutual Assistance with the Interception of Content Data

Interception of content data involves the use of technical means to collect or record "content data, in real time, of specified communications . . . transmitted by means of a computer system."[26] Content data differs from other forms of computer information, such as traffic data, because instead of providing information about the sender and an intended recipient of a communication, authorities are privy to the actual information communication—the content of the transmission.[27] A provision regarding interception is illustrated by the Busapest Convention on Cybercrime, which states,

> ***Article 34 – Mutual assistance regarding the interception of content data***
>
> The Parties shall provide mutual assistance to each other in the real-time collection or recording of content data of specified communications transmitted by means of a computer system to the extent permitted under their applicable treaties and domestic laws.[28]

This investigative tool, which is currently an emerging area of mutual assistance, is most useful to determine whether a communication is of an illegal nature or to collect evidence of past or future crimes.[29] However, because this form of interception is intrusive, deference has been given to national laws and applicable

[25] Id. para 216, 295.

[26] Id. Art. 21.

[27] Id. para 229.

[28] Id. Art. 34.

[29] Id. para 228.

treaties regarding how such procedures should be carried out by law enforcement authorities.[30]

6. Data Retention

Data retention obligates service providers to save traffic data for specified periods of time and is an attempt to avoid the automatic deletion of certain types of data that may be crucial to a criminal investigation.[31] Data retention typically is not an obligation established at the international level, despite the fact that it can have serious consequences on the effectiveness of an international cybercrime investigation.

7. Orders to Disclose Encryption Keys

Encryption technology creates serious difficulties for law enforcement authorities. For example, even if investigators are fortunate enough to have acted swiftly and recovered content data that may assist in the apprehension of a cyber-criminal, law enforcement may be unable to view the data obtained if it was previously encrypted by the perpetrator. To prevent this serious impediment to investigative success, law enforcement authorities are apt to secure a production order, which can then be used to force whomever has the key to the encryption to release it to them.

8. 24/7 Contact Points

In order to better facilitate mutual legal assistance in cybercrime investigations, many instruments obligate States to set up "24/7 Points of Contact" that are available twenty-four (24) hours a day seven (7) days a week to handle requests for assistance should they arise. For example:

> ***Article 35 – 24/7 Network[32]***
>
> 1. Each Party shall designate a point of contact available on a twenty-four hour, seven-day-a-week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning

[30] Id. para 228 and 297.

[31] Patrick Breyer, *Telecommunications Data Retention and Human Rights: The Compatibility of Blanket Traffic Data Retention with the ECHR*, European L. J. 365 (2005) (providing an introduction to data retention).

[32] Council of Europe Convention on Cybercrime ETS Treaty 185, Art. 35 (2004).

criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. Such assistance shall include facilitating, or, if permitted by its domestic law and practice, directly carrying out the following measures:

(a) the provision of technical advice;

(b) the preservation of data pursuant to Articles 29 and 30;

(c) the collection of evidence, the provision of legal information, and locating of suspects.

2. (a) A Party's point of contact shall have the capacity to carry out communications with the point of contact of another Party on an expedited basis.

   (b) If the point of contact designated by a Party is not part of that Party's authority or authorities responsible for international mutual assistance or extradition, the point of contact shall ensure that it is able to co-ordinate with such authority or authorities on an expedited basis.

3. Each Party shall ensure that trained and equipped personnel are available, in order to facilitate the operation of the network

The "critical task" to be carried out by the 24/7 Networks is the immediate facilitation of mutual assistance requests either themselves or via the competent authorities located within the law enforcement community. Concomitant with obligation is the requirement that each State ensure its 24/7 Networks have both the expertise and resources to fulfill their mandate.

Useful Resources for Determining Mutual Assistance and Extradition Requirements

Law enforcement authorities attempting to determine the extradition requirements of another State have many resources available to assist in ascertaining that information.[33]

1. UNODC Online Directory of Competent National Authorities[34]

"The online directory of competent national authorities provides access to the

[33] Inshik Sim, *Senior-level Workshop on Mutual Legal Assistance in East-Asia and the Pacific* (UNODC Regional Centre for East Asia and the Pacific 2012), http://www.unodc.org/documents/southeastasiaandpacific//2012/07/mla-workshop/UNODC_-_Regional_Cooperation_Networks.pdf.

[34] United Nations Off. on Drugs and Crime, *supra* note 2, at 43.

contact information of competent national authorities designated under the United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances of 1988 and the United Nations Convention against Transnational Organized Crime and the Protocols thereto. With a view to facilitating communication and problem-solving among competent authorities at the interregional level, the directory contains essential information on: State membership in existing international cooperation networks; Legal and procedural requirements for the granting of requests; Use of the Organized Crime Convention as the legal basis for requests; Links to national laws and websites; Indication of requests that can be made through INTERPOL."[35]

2. Commonwealth Network of Contact Persons (CNCP)[36]

"The purpose of the Commonwealth Network of Contact Persons is to facilitate international cooperation in criminal cases between Commonwealth member States, including on mutual legal assistance and extradition, and to provide relevant legal and practical information."[37]

3. European Judicial Network (EJN)[38]

"The European Judicial Network is a network of national contact points for the facilitation of judicial cooperation in criminal matters between the member States of the European Union. The Network's secretariat forms part of Eurojust but functions as a separate unit."[39]

4. Eurojust[40]

"Eurojust is a judicial cooperation body that was established with the goal of providing an area of freedom, security and justice within the European Union. It is also able, through the Council of the European Union, to conclude cooperation agreements with non-member States and international organizations or bodies such as UNODC for the exchange of information or the secondment of officers. At the request of a member State, Eurojust may assist investigations and prosecutions concerning that particular member State and a non-member State, if a cooperation agreement has been concluded or if there is an essential interest in providing such

[35] Id.

[36] Id. at 44.

[37] Id.

[38] Id.

[39] Id.

[40] Id.

assistance. In addition to cooperation agreements, Eurojust also maintains a network of contact points worldwide."[41]

5. Hemispheric Information Exchange Network for Mutual Assistance in Criminal Matters and Extradition of the Organization of American States[42]

"The Hemispheric Information Exchange Network for Mutual Assistance in Criminal Matters and Extradition has three components: a public website, a private website and a secure electronic communications system. The public component of the Network provides legal information related to mutual assistance and extradition for the 34 States members of the Organization of American States. The private component of the Network contains information for individuals who are directly involved in legal cooperation in criminal matters. The private site includes information on meetings, contact points in other countries, a glossary of terms and training on the secure electronic communication system."[43]

6. Ibero-American Legal Assistance Network (IberRed)[44]

"The Ibero-American Legal Assistance Network (IberRed) is a structure formed by contact points from the ministries of justice, central authorities, prosecutors and public prosecutors and judicial branches of the 23 countries and territories comprising the Latin American community of nations. It is aimed at optimizing instruments for civil and criminal judicial assistance and strengthening cooperation between countries."[45]

7. Judicial Regional Platform of Sahel and of Indian Ocean Commission Countries[46]

"Judicial Regional Platforms have been established by UNODC's Terrorism Prevention Branch and Organized Crime and Illicit Trafficking Branch to strengthen international cooperation in criminal matters in the regions of the Sahel and the Indian Ocean. Their main focus is to prevent and combat forms of serious crime, such as organized crime, corruption, drug trafficking or terrorism. The Platforms

---

[41] Id.

[42] Id. at 45.

[43] Id.

[44] Id.

[45] Id.

[46] Id. at 43.

are international cooperation networks of focal points, that facilitate extradition and mutual legal assistance in criminal matters. They also identify technical assistance needs for strengthening the judicial cooperation among them and sensitize the national stakeholders of the penal chain on the role and mechanisms of the Platforms. The national focal points meet, at least, once a year."[47]

A. Introduction to International Cooperative Instruments

There are three ways in which law enforcement authorities may invoke an instrument for international cooperation. First, relevant procedures can be part of multilateral international agreements, such as the United Nations Convention against Transnational Organized Crime (UNTOC)[48], or regional conventions, such as the Inter-American Convention on Mutual Assistance in Criminal Matters,[49] the European Convention on Mutual Assistance in Criminal Matters[50] or the Council of Europe Convention on Cybercrime.[51]

Second, international cooperative procedure may be established through bilateral agreements. Generally, such agreements refer to specific requests that can be submitted, define the relevant procedures and forms of contact, as well as the rights and obligations of the requesting and requested states.[52] For example, Australia has signed more than 30 bilateral agreements with other countries regulating aspects of extradition.[53] Although mentioned in some bilateral agreements, it is uncertain to what extent the existing bilateral agreements adequately govern cybercrime.[54]

---

[47] Id.

[48] United Nations Off. on Drugs and Crime, *Convention Against Transnational Organized Crime* (2000); J.M. Smith, *An International Hit Job: Prosecuting Organized Crime Acts as Crimes Against Humanity*, Georgetown L. J. 1118 (2009).

[49] Organization of American States, *Inter-American Convention on Mutual Assistance in Criminal Matters* (1992), http://www.oas.org/juridico/english/sigs/a-55.html.

[50] European (Council of Europe) Convention on Mutual Assistance in Criminal Matters ETS 30 (1959).

[51] Council of Europe Convention on Cybercrime (2001).

[52] UN Model Treaty on Mutual Legal Assistance (1999); United Nations Off. on Drugs and Crime, *Legislative Guides for the Implementation of the United Nations Convention against Transnational Organized Crime* 217 (2004), http://www.unodc.org/pdf/crime/legislative_guides/Legislative%20guides_Full%20version.pdf.

[53] A full list of these agreements is available at: http://www.ag.gov.au/www/agd/agd.nsf/page/Extradition_and_mutual_assistanceRelationship_with_other_countries.

[54] Organization of American Studies, *Second Meeting of Ministers of Justice or of Ministers or Attorneys General of the Americas on Cybercrime, Background Documents on the Developments on Cyber Crime in the Framework of the REMJAS and the OAS* (1999), http://www.oas.org/juridico/english/cybGE_IIIrep3.pdf.

If neither a multilateral nor a bilateral agreement is applicable, international cooperation generally needs to be founded on international courtesy, what is often referred to as *comity*, based on reciprocity.[55] Cooperation based on bilateral agreements and comity very much depends on the circumstances of the actual case, the nature of the bilateral treaty, if present, and the countries involved. Therefore, the following overview focuses on international and regional conventions.

Overview of Relevant Instruments

Many of the instruments relevant to international cooperation in combating cybercrime cover similar substantive areas, such as criminalization, cybersecurity, and e-commerce. However, the provisions most relevant for international cooperative purposes are those that address jurisdiction, international cooperation in the forms of mutual legal assistance and extradition, and other specific forms of international cooperation directly relevant to cybercrime, such as expedited preservation of computer information or production orders. These pertinent provisions in several major instruments will be discussed below.

1. The Council of Europe (COE) – Convention on Cybercrime (2001)

The Budapest Convention is an instrument related to cybercrime that was drafted in 2001 by the Council of Europe. The scope of the Convention's international cooperation provisions includes all crimes that can be classified as "cybercrimes."[56] Drafted to "achieve a greater unity" between the Council of Europe and other State signatories, the Convention hopes to create "a common criminal policy aimed at the protection of society against cybercrime, *inter alia*, by adopting appropriate legislation and fostering international cooperation."[57]

Article 23 of the Budapest Convention contains three general principles regarding international cooperation in the investigation of cybercrime. First, members are supposed to provide cooperation in international investigations to the widest extent possible, which reflects the importance of cooperation in international cybercrime investigations.[58] Second, Article 23 establishes that cooperation "to the widest extent possible" applies not only to the "offenses related to computer systems and

---

[55] Oana Mihaela Pop, *The Principle and General Rules of the International Judicial Cooperation in Criminal Matters, AGORA International Journal of Juridical Science* 160 (2008); Ellery C. Stowell, *International Law: A Restatement of Principles in Conformity with Actual Practice* 262 (1931); *Recueil Des Cours*, Collected Courses, Hague Acad. of Int'l L. 119 (Brill 1976).

[56] United Nations Off. on Drugs and Crime, *supra* note 2, at 199.

[57] Council of Europe Convention on Cybercrime at Preamble.

[58] Id. 242.

data," but also "for the collection of evidence in electronic form" for any other criminal offence.[59] Therefore, cooperation to the widest extent possible, under the Convention, should be given in cybercrime investigations as well as traditional criminal investigations where electronic evidence may be present.[60] The third principle established in Article 23 is that the Convention's provisions dealing with international cooperation do not substitute, but rather complement, other provisions of international agreements pertaining to mutual legal assistance and extradition or relevant provisions of domestic law pertaining to international cooperation.[61] The intent of the drafters of the Budapest Convention was not to create a separate regime on mutual legal assistance but to establish a legal basis to carry out international cooperation in the event that none existed between parties affected by cybercrimes.[62]

With regard to mutual assistance, paragraph 1 of Article 25 complements the principles set out in Article 23 in that it provides for parties to assist one another "to the widest extent possible."[63] Additionally, paragraph 3 contains one of the most important provisions in Article 25, namely, creating a basis for urgent communication between parties in cybercrime investigations, provided such communication is accomplished with the "appropriate levels of security and authentication."[64] A number of cybercrime investigations at the national level fail because they take too long and important data is deleted before procedural measures to preserve it are undertaken; therefore the Convention provides for an expedited means of communication in hopes that more of the evidence/data necessary for trans-border investigations will be available to those authorities.[65]

In addition to the Budapest Convention, other global instruments for mutual assistance include:

---

[59] Id. 243.

[60] Id. 243; "However, it should be noted that Articles 24 (Extradition), 33 (Mutual assistance regarding the real time collection of traffic data) and 34 (Mutual assistance regarding the interception of content data) permit the Parties to provide for a different scope of application of these measures."

[61] Id. 244.

[62] Id. 244.

[63] Id. at 253.

[64] Id. Art. 25, para 3.

[65] Id. 256. "Computer data is highly volatile. By a few keystrokes or by operation of automatic programs, it may be deleted, rendering it impossible to trace a crime to its perpetrator or destroying critical proof of guilt. Some forms of computer data are stored for only short periods of time before being deleted. In other cases, significant harm to persons or property may take place if evidence is not gathered rapidly." Id.

Economic Community of West African States (ECOWAS) – Directive on Fighting Cybercrime Within ECOWAS (2009)

The Directive on Fighting Cybercrime was created in 2009 by the ECOWAS based on a desire of its participating African States to adopt a framework of penal legislation designed to effectively fight cybercrime.[66] The Directive is binding on all ECOWAS Member States and applies to all "cybercrime-related offences within the ECOWAS sub-region."[67]

Shanghai Cooperation Organization (SCO) – Agreement on Cooperation in the Field of International Information Security (2010)

The SCO Agreement on Cooperation in the Field of International Information Security was created in 2009 by the members of the Shanghai Cooperation Organization. The members of the SCO, expressing concern over threats from the use of information technology and media in manners incompatible with maintaining security and stability, created the SCO Agreement to limit these threats to international security and protect its members' security interests in the informational environment.[68] The scope of the SCO is broad when compared with other international instruments. The SCO Agreement contains several provisions that established general principles for international cooperation in combating offences related to informational security.[69] Although not as detailed in its establishment of specific mechanisms of cooperation as other international agreements, the SCO Agreement lists several key areas in which cooperation is required.

African Union (AU) – Draft Convention on the Establishment of a Legal Framework Conducive to Cybersecurity in Africa (2012)

The AU Draft Convention was created in 2012 in an effort by the AU's member States to establish "a credible framework for cyber[-]security in Africa through organization of electronic transactions, protection of personal data , promotion of cyber security , e-governance and combating cybercrime."[70] The AU Draft

---

[66] Econ. Community of West African States (ECOWAS), *Directive on Fighting Cybercrime within ECOWAS* (2009).

[67] Id.

[68] Shanghai Cooperation Organization (SCO), *Agreement on Cooperation in the Field of Int'l Info. Security* (2010).

[69] Id.

[70] African Union (AU), *Draft Convention on the Establishment of a Legal Framework Conductive to Cybersecurity in Africa* (2012).

Convention is a binding instrument whose scope encompasses "cybersecurity," which is broader than matters related directly to cybercrime.[71] For example, the Draft Convention "sets forth the security rules essential for establishing a credible digital space for electronic transactions, personal data protection, and ***combating cybercrime***."[72]

The AU Draft Convention requires member States to adopt measures that harmonize legislation related to cybercrime and specifically to ensure that they are consistent with the principle of dual criminality.[73] In addition, member States must adopt mutual legal assistance treaties between themselves that provide for information sharing and exchange on both a bilateral and multilateral basis.[74] Paragraph 3 of Article III-14 requires member States to set up "institutions that exchange information on cyber threats and evaluate vulnerabilities[,] such as Computer Emergency Response Teams (CERTs) or Computer Security Incident Response Teams (CSIRTs)."[75] Thus, although it provides only general obligations to undertake certain mutual assistance procedures, the AU Draft Convention makes obligatory several mechanisms that are crucial to effective international cooperation in combating cybercrime.

League of Arab States (LAS) – Arab Convention on Combating Information Technology Offences (2012)

The LAS Convention was adopted by the League of Arab States on December 21, 2012 in Cairo in an effort to "enhance cooperation between [member States and] combat information technology offences threatening the security, interests, and safety of their communities" by developing a "common criminal policy aimed at protecting Arab society against information technology offences."[76] The LAS Convention is a binding instrument whose scope encompasses all "information technology offences," which are defined as criminal offences that use,

> "any material or virtual means or group of interconnected means used to store, sort, arrange, retrieve, process, develop and exchange information according to commands and instructions stored

[71] Id.

[72] Id.

[73] Id.

[74] Id.

[75] Id.

[76] League of Arab States (LAS), *Arab Convention on Combating Information Technology Offences* (2012).

> therein. This includes all associated inputs and outputs, by means of wires or wirelessly, in a system or network."[77]

In addition, many of the LAS Convention's provisions are similar or identical to those in the Council of Europe's Convention on Cybercrime above.[78]

About the Author

Adam Palmer (JD, MBA, CISSP) is a former U.S. Navy JAG cybercrime attorney and also led the UN Global Program Against Cybercrime. He is based in Madrid, Spain.
This is a personal work of Adam Palmer and not associated with any organization.

About the Center for Cyber and Homeland Security

The Center for Cyber and Homeland Security (CCHS) at the George Washington University is a nonpartisan "think and do" tank whose mission is to carry out policy-relevant research and analysis on homeland security, counterterrorism, and cybersecurity issues.

The opinions expressed in this Issue Brief are those of the author alone.

[77] Id.

[78] See Council of Europe Convention on Cybercrime.