International Journal of Development and Conflict
12(2022) 166–172

INTERNATIONAL COOPERATION AGAINST CYBERCRIME: THE NECESSITY TO EMBRACE MULTILATERALISM AND ADOPT A UNITED NATIONS CYBERCRIME CONVENTION

DR. RABAÏ BOUDERHEM
Assistant Professor, College of Law,
Prince Mohammad Bin Fahd University (Al Khobar, Saudi Arabia),
Research Associate CREDIMI (FRE 2003)
CNRS-University of Burgundy Franche-Comté (Dijon, France),
Legal Consultant

Cybercrime can be perpetrated by offenders anywhere in the world with an Internet connection. The transnational nature of cybercrime challenges traditional notions of jurisdiction and requires cooperation of law enforcement agents across the globe. International cooperation depends on harmonized national substantive cybercrime laws which criminalize certain behaviors, and national procedural cybercrime laws that set the rules of evidence and criminal procedure. International cooperation can also be facilitated by signing—and ratifying—bilateral, regional and multilateral instruments on cybercrime in order to harmonize states parties' legislations. Indeed, such legal instruments will only be legally binding after the ratification process. International cooperation is facilitated by bilateral, regional, and multilateral cybercrime treaties as long as dual criminality exists. Treaties have been signed at a regional level such as the Council of Europe or the Arab League, but today there is no legal tool signed under the supervision of the United Nations. An international cybercrime convention will facilitate interstate cooperation and increase the protection of individuals, corporations and states against crimes committed through information and communication technology (ICT). Indeed, legal tools and different informal and formal international cooperation mechanisms but they depend entirely on the consent and goodwill of states. We can cite here bilateral extradition treaties, mutual legal assistance treaties (MLATs) and informal mechanisms such as the exchange of information between national agencies. These existing mechanisms are limited; a UN Cybercrime Convention will necessarily increase interstate cooperation, criminalize certain behaviors and help to settle international disputes when states are involved or use proxy.

Keywords: Cybercrime; international cooperation; law enforcement; dispute; harmonization; multilateralism.

I. Introduction

Cybercrime such as denial of service (DoS) attacks or ransomwares can be perpetrated by offenders anywhere in the world with an Internet connection and includes a wide range

*Corresponding author Email: Please provide

of offences[1]. The adverse impacts of cybercrime can be experienced outside of the state in which the offenders live. The difficulty with cybercrime is that we deal with cross-border offences that challenges the traditional concepts of jurisdiction: which state has jurisdiction? Which law is applicable to a cybercrime dispute? Moreover, cybercrime requires a proactive cooperation of cybercrime investigators[2], prosecutors, judges who can be located in different countries. Therefore, interstate cooperation depends on the goodwill of states but also on the existence of harmonized national laws criminalizing cybercrime and clarifying rules of evidence and procedures. Traditionally, we distinguish between formal and informal international cooperation mechanisms. Interstate cooperation in the field of cybercrime can be facilitated by the adoption of bilateral, regional and multilateral instruments on cybercrime. States need to compromise, sign and ratify such cybercrime instruments if they want to effectively combat cybercrime and improve dispute resolution. International law is indeed gaining attention and prominence in the field of cybercrime[3]. Today, interstate cooperation is facilitated by different bilateral, regional, and multilateral cybercrime treaties as long as dual criminality[4] exists: it means that a given provision may refer to the existence of substantive national laws criminalizing a certain cybercrime in all cooperating states. Another challenge faced by states is the existence of safe havens due to a lack of harmonization and national cybercrime laws; in these countries, offenders of cybercrime cannot be prosecuted, extradited and convicted if found guilty. The international community can only combat safe havens if multilateralism becomes the rule and not the exception. For many cybercriminals, Africa is an illustration of a safe haven[5]. Regarding cybercrime and international cooperation, a multilateral treaty signed within the United Nations seems to be the right answer to this new trend and global threat. Indeed, existing legal tools such as bilateral extradition treaties, mutual legal assistance treaties (MLATs) and informal international cooperation mechanisms are limited (II). They depend on the goodwill of states and favor safe havens if national laws are not harmonized. In order to enhance the prevention of cybercrimes and help the settlement of disputes, the international community has to work on a multilateral cybercrime convention. Multilateralism seems to be the best option offered to states to tackle cybercrime as it encompasses many forms and aspects (III). UN members will face numerous challenges and vivid debates before signing and ratifying a UN Cybercrime Convention but this will benefit to the international community as a whole (IV).

---

1. Adam M. Bossler & Tamar Berenblum (2019) Introduction: new directions in cybercrime research, Journal of Crime and Justice, 42:5, 495-499, DOI: 10.1080/0735648X.2019.1692426.

2. Bajovic V. (2017) Criminal Proceedings in Cyberspace: The Challenge of Digital Era. In: Viano E. (eds) Cybercrime, Organized Crime, and Societal Responses. Springer, Cham. https://doi.org/10.1007/978-3-319-44501-4_5.

3. D. B. HOLLIS, A Brief Primer on International Law and Cyberspace, June 2021, Carnegie Endowment for International Peace. Available online: https://carnegieendowment.org/files/Hollis_Law_and_Cyberspace.pdf

4. Calderoni, F. (2010). The European legal framework on cybercrime: striving for an effective implementation. Crime, Law and Social Change, 54(5), 339-357. https://doi.org/10.1007/s10611-010-9261-6.

5. Nir Kshetri (2019) Cybercrime and Cybersecurity in Africa, Journal of Global Information Technology Management, 22:2, 77-81, DOI: 10.1080/1097198X.2019.1603527.

II. Limitations of the existing international cooperation mechanisms

With the emergence of information and communication technology (ICT), new risks emerge especially for data privacy[6] and security of online transactions[7]. States also face new challenges in terms of confidentiality and integrity of data and communication. E-services proposed by institutional websites or sensitive information can be targeted by cybercriminals. Traditionally, states use formal and informal international cooperation mechanisms to combat cybercrime, initiate investigations and prosecute offenders who may be located in foreign countries. Here, we will focus primarily on extradition treaties, mutual legal assistance treaties (MLATs), and informal exchange of information between national law enforcement authorities. We can cite for instance the League of Arab States' Arab Convention on Combating Information Technology Offences of 2010[8]. The latter includes provisions on mutual assistance, procedures for cooperation, and mutual assistance requests. Another example is the African Union Convention on Cyber Security and Personal Data Protection of 2014[9]. For instance, Article 28[10] of the African Union Convention includes provisions on harmonization, mutual legal assistance on cybercrime matters, and information exchange. This Article invites and requests from states parties to create national agencies dedicated to cybercrime and cybersecurity. Such national bodies will guarantee effective interstate cooperation and will facilitate the exchange of information for example. The African Union Convention on cybersecurity also calls for the creation of specific entities: Computer Emergency Response Teams (CERTs) or Computer Security Incident Response Teams (CSIRTs)[11]. These entities play a key role in interstate cooperation and can also involve the private sector throughout the signature of public-private partnerships in the field of international cooperation[12].

---

6. Sasha Romanosky, Examining the costs and causes of cyber incidents, *Journal of Cybersecurity*, Volume 2, Issue 2, December 2016, Pages 121–135, https://doi.org/10.1093/cybsec/tyw001.

7. Joseph Gualdoni, Andrew Kurtz, Ilva Myzyri, Megan Wheeler, Syed Rizvi, Secure Online Transaction Algorithm: Securing Online Transaction Using Two-Factor Authentication, Procedia Computer Science, Volume 114, 2017, pp. 93-99, ISSN 1877-0509, https://doi.org/10.1016/j.procs.2017.09.016.

8 Art. 32 related to Mutual Assistance and Art. 34 related to Procedures for Cooperation and Mutual Assistance Requests. For an English version of the Arab Convention on Combating Information Technology Offences of 2010, see: https://www.asianlaws.org/gcld/cyberlawdb/GCC/Arab%20Convention%20on%20Combating%20Information%20Technology%20Offences.pdf

8. Art. 32 related to Mutual Assistance and Art. 34 related to Procedures for Cooperation and Mutual Assistance Requests. For an English version of the Arab Convention on Combating Information Technology Offences of 2010, see: https://www.asianlaws.org/gcld/cyberlawdb/GCC/Arab%20Convention%20on%20Combating%20Information%20Technology%20Offences.pdf

9. See official website of the African Union: https://au.int/en/treaties/african-union-convention-cyber-security-and- personal-data-protection.

10. Under Article 28(4) states are instructed to "make use of existing means for international cooperation," which can include "international, intergovernmental, regional or… public private partnerships," to respond to cybercrime.

11. Van der Kleij, Rick et al. "Computer Security Incident Response Team Effectiveness: A Needs Assessment." *Frontiers in psychology* vol. 8 2179. 12 Dec. 2017, doi:10.3389/fpsyg.2017.02179.

12. Manley, Max. "Cyberspace's Dynamic Duo: Forging a Cybersecurity Public-Private Partnership." Journal of Strategic Security 8, no. 3 Suppl. (2015): 85-98.

States also cooperate throughout mutual legal assistance[13] (MLATs) and extradition treaties[14] especially in the investigation and prosecution of cybercriminals. Mutual legal assistance treaties (MLATs) are agreements between states on a bilateral basis and apply to a specific list of crimes. MLATs determine the scope and nature of states parties' obligations; these bilateral treaties essentially deal with cybercrime investigations and access to digital evidence[15]. Undoubtedly, MLATs are an asset in international law but they cover exhaustive list of cybercrimes. Practically, international cooperation will depend on the inclusion of a specific cybercrime in a given MLAT. If two states signed a MLAT without any reference to cyberbullying, their respective national law enforcement agencies will only be able to cooperate and implement such formal international cooperation mechanisms if cyberbullying has been included in the treaty. As we mentioned, cybercrime evolves as new technologies emerge. Some authors pointed out this shortcoming and argued that states should instead take in consideration the changing nature of cybercrime[16].

Extradition treaties are another illustration of formal international cooperation. These conventions are concluded on a bilateral or regional basis. We can cite here the European Convention on Extradition of 1957[17] and the Organization of American States (OAS) Inter-American Convention on Extradition of 1981[18] which are agreements to arrest and/or extradite individuals to the requesting country if punishment thresholds are met for extraditable offences. African countries also signed the ECOWAS Convention on Extradition of 1994[19] with a threshold at a '*minimum period of two (2) years*'[20].

It is very interesting to note that European Union members decided to adopt a new legal tool in order to facilitate intra-EU cooperation in the field of criminal proceedings. The European Arrest Warrant[21] (EAW) simplifies cross-border judicial surrender procedure, especially for the purpose of prosecuting or executing a custodial sentence or detention order. To this effect, a warrant issued by one EU member's judicial authority is valid in

---

13. For instance, ASEAN Member States concluded a MLAT on 29 November 2004 in Kuala Lumpur, Malaysia. See: https://asean.org/our-communities/asean-political-security-community/rules-based-people-oriented-people- centred/treaty-on-mutual-legal-assistance-in-criminal-matters/.

14. J T Soma; T F Muther Jr; H M L Brissette *Harvard Journal on Legislation* Volume: 34 Issue: 2 Dated: special issue (Summer 1997) Pages: 317-371. See: https://www.ojp.gov/ncjrs/virtual-library/abstracts/transnational-extradition- computer-crimes-are-new-treaties-and-laws.

15. Maras, 2016, p. 78.

16. Garcia and Doyle, 2010.

17. This convention has been signed under the auspices of the Council of Europe and entered into force in 1960. See https://rm.coe.int/1680064587.

18. For the full text of the OAS Inter-American on Extradition of 1981, see: https://www.oas.org/juridico/english/treaties/b-47.html

19. Economic Community of West African States (ECOWAS) Convention A/P.1/8/94 on Extradition 1994. See: https://documentation.ecowas.int/wpfb-file/convention-on-extradition2-pdf/

20. See Article 3 of the ECOWAS Convention on Extradition of 1994.

21. The European Arrest Warrant has been operational since 1 January 2004. It has replaced the lengthy extradition procedures that used to exist between EU member states. Council Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States - Statements made by certain Member States on the adoption of the Framework Decision, 2002/584/JHA, *OJ* L 190, 18.7.2002, p. 1–20. Available online: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32002F0584.

the entire territory of the European Union[22]. The EAW was designed to replace extradition procedures and solve the difficulties faced by EU members wishing to prosecute offenders located in another EU member state. Another issue encountered by states parties to extradition treaties is that extradition will not be automatically granted by the requesting authorities. Indeed, several regional extradition treaties include exceptions and situations where states may refuse to extradite individuals. In its Law Model, the United Nations Office on Drugs and Crime[23] expressly specifies that dual criminality is a substantive condition for extradition[24].

MLATs, extradition treaties, the European Arrest Warrant are efficient international cooperation mechanisms and have the merit to exist but, with increased globalization, the international community needs a multilateral cybercrime convention to tackle this real plague.

III. Multilateralism as a solution for combating cybercrime

We can refer first to the Budapest Convention on combating cybercrime discussed and signed under the supervision of the Council of Europe[25]. Today, the Budapest Convention on cybercrime is the only binding legal instrument in this field[26]. Our postulate is that the current international legal framework is not sufficient to regulate cybercrime at the international level. Some regulations do exist and can be useful in investigations and prosecutions of cybercrime—we can cite here the EU GDPR 2016[27]—but these rules are scattered and states need to adopt a multilateral legally binding treaty in order to facilitate international cooperation through compulsory procedures. Some authors also believe that multilateralism and the adoption of cybercrime conventions is essential as we deal with transnational offences and '*difficulties posed by the borderless, complex and rapidly evolving nature of modern economic and cyber crimes*'[28].

The United Nations has been working on possible international regulations since 2010. States are now moving towards a multilateral convention under the auspices of the

---

22. The European Arrest Warrant enables the arrest of offenders for computer-related crimes 'punishable in the issuing Member State by a custodial sentence or a detention order for a maximum period of at least three years (…) without verification of the double criminality [or dual criminality] of the act'. In this regard, see Art. 2(2) of the Council Framework Decision 2002/584/JHA of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States.

23. UNODC Law Model on Extradition, see: https://www.unodc.org/pdf/model_law_extradition.pdf.

24. See: III. PART 2: EXTRADITION FROM [COUNTRY ADOPTING THE LAW] (PASSIVE EXTRADITION), Chapter 1: Substantive conditions for extradition, Section 3: Extraditable offences—Double criminality requirement.

25. The Budapest Convention on cybercrime has been signed under the supervision of the Council of Europe. Available online: https://rm.coe.int/1680081561.

26. Wicki-Birchler, D. The Budapest Convention and the General Data Protection Regulation: acting in concert to curb cybercrime?. Int. Cybersecur. Law Rev. 1, 63–72 (2020). https://doi.org/10.1365/s43439-020-00012-5.

27. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance), OJ L 119, 4.5.2016, p. 1–88. Available online: https://eur-lex.europa.eu/eli/reg/2016/679/oj.

28. Menon S., Guan Siew T. (2012), "Key challenges in tackling economic and cyber-crimes: Creating a multilateral platform for international co-operation", *Journal of Money Laundering Control*, Vol. 15 No. 3, pp. 243-256. https://doi.org/10.1108/13685201211238016.

United Nations. To this effect, the UN Intergovernmental Expert Group on Cybercrime (IEG) was established in 2010 following the adoption of the UN General Assembly Resolution 65/230[29]. In December 2019, the UN General Assembly decided to take a new initiative and to start a new process. The UN General Assembly Resolution mandated the establishment of an Open-ended Ad Hoc Intergovernmental Committee of Experts, representative of all regions, to elaborate a comprehensive international convention on '*countering the use of information and communications technologies for criminal purposes*'[30]. Discussions have been postponed due to the COVID-19 pandemic but the UN General Assembly will resume the process to discuss and potentially sign a multilateral Cybercrime Convention. The task promises to be difficult as UN members apprehend cybercrime on a multifaceted basis. Topics such as cross-border access to data, exchange of digital evidence, regulation of Internet Service Providers have been subject to numerous controversy and vivid debates all around the globe. A consensus will be difficult to reach but the acceptance of UN members to initiate discussions on a multilateral cybercrime convention is already a major step forward. Indeed, states are now more than ever before confronted to critical situations and cybercrimes that affect their sovereignty. We witnessed for instance interferences with national presidential elections in the US in 2016[31]. According to the UN General Assembly Resolution 74/247, the Ad Hoc Intergovernmental Committee of Experts held a working session in May 2021, in New York. The Ad Hoc Committee agreed on its agenda and issues to be addressed by members. On 26 May 2021, the UN General Assembly adopted the Resolution 75/282[32] and decided that the Ad Hoc Committee shall convene at least six sessions, of 10 days each, to commence in January 2022, a concluding session in New York, and conclude its work in order to provide a draft convention to the General Assembly at its seventy-eighth session; it further decided that the Committee shall hold the first, third and sixth negotiating sessions in New York and the second, fourth and fifth sessions in Vienna. Efforts made by UN members are laudable but a multilateral Cybercrime Convention has to determine states parties' obligations regarding investigations, rules of evidence, procedures, prosecution and exchange of information. It has to contain a list of substantive rules to be applied by all states parties. We can also consider existing legal instruments such as the EU GDPR 2016 and MLATs, extradition treaties and customary

---

29. In 2010, the UN General Assembly adopted the Resolution 65/230 ('Twelfth United Nations Congress on Crime Prevention and Criminal Justice') based initially on the Art.42 of the Salvador Declaration. The Commission on Crime Prevention and Criminal Justice established '*an open-ended intergovernmental expert group to conduct a comprehensive study of the problem of cybercrime and responses to it by the Member States, the international community and the private sector, including the exchange of information on national legislation, best practices, technical assistance and international cooperation, with the view to examining options to strengthen existing and to propose new national and international legal or other responses to cybercrime*'.

30. In December 2019, the U.N. General Assembly adopted the Resolution A/RES/74/247 that set in motion a process to draft a global comprehensive cybercrime treaty. Negotiations will commence in January 2022 and are expected to conclude in 2023. Available online: https://undocs.org/A/Res/74/247.

31. Fidler, David P., "The U.S. Election Hacks, Cybersecurity, and International Law" (2017). Articles by Maurer Faculty. 2607. https://www.repository.law.indiana.edu/facpub/2607.

32. UN General Assembly Resolution on 'Countering the use of information and communications technologies for criminal purposes', A/RES/75/282. Available online: https://undocs.org/en/A/RES/75/282.

international rules regarding international cooperation as key references for any further multilateral treaty.

IV. Conclusion

As we explained, today's international cooperation mechanisms—both formal and informal—are not sufficient and are conditional to existing bilateral or regional treaties and the goodwill of states. A multilateral cybercrime convention signed under the supervision of the United Nations will help the prevention of cybercrime and facilitate the prosecution of offenders by providing a set of compelling rules applicable to all UN members. It will also give a great legitimacy to the international legal framework applicable to cybercrime. The current rules applicable to international cooperation are scattered and may differ from a region to another even though states and regional international organizations—the Arab League, the European Union, the OAS among others—tend to adopt the same definitions of cybercrime, data privacy or Internet Service Providers. Negotiations will be difficult as we deal with different legal systems and traditions but we believe that a consensus is possible as globalization created unified computer networks and increased online transactions with all the risks associated with the use of ICT.