Challenges of the Definition of the Cybercrime Jurisdiction in the European Union

by Valeriia Lymishchenko

ITSS Verona Magazine, Vol. 1, n. 2

Fall/Winter 2022

Challenges of the Definition of the Cybercrime Jurisdiction in the European Union

Valeriia Lymishchenko

To cite this article: Valeriia Lymishchenko, *Challenges of the Definition of the Cybercrime Jurisdiction in the European Union,* ITSS Verona Magazine, Vol. 1, no. 2, Fall/Winter 2022.

Keywords: Cybercrime, Conflict of Jurisdiction, Criminal Jurisdiction in the EU, Mutual Recognition, Investigation of Cybercrime

ITSS Verona website: https://www.itssverona.it/itss-magazine

LinkedIn: https://www.linkedin.com/company/itss-verona/

Instagram: https://instagram.com/itss_verona?igshid=YmMyMTA2M2Y=

Twitter: https://twitter.com/itssverona

Published online: December 30th, 2022

Abstract: Despite the extensive research on cybercrime phenomena, there is a lack of comprehensive analysis of the challenges associated with an investigation of cybercrime. Due to the peculiarities of cybercrime, one of the main challenges in cybercrime investigation is the establishment of its jurisdiction. The overall image of cybercrime makes conflicts of jurisdiction possible. These are understood as situations where different states have legitimate authority over the same criminal case. Because of the unique character of relationships between the Member States of the European Union (EU), conflict of jurisdiction became a problem for cybercrime investigators when two or more Member States have a strong interest in prosecuting the same cybercrime. Accordingly, the emergence of conflicts of jurisdiction in the cybercrime domain could delay the investigation, cause impunity, and even increase the number of cybercrimes. Based on examining conflicts of jurisdiction in EU law, this study discusses how to avoid the possible challenges to establishing coherent cybercrime jurisdictions and the future perspectives for cybercrime investigation.

The development of informational technologies has led to new challenges. Among these, the increasing threat of cybercrime, or computer crimes, namely crimes committed in information technology.

The most common types of cybercrime include malware, ransomware, and phishing attacks.[1] Malware (or “malicious software”) is a type of software that, like viruses, is used to gain unauthorised access to the computer or network.[2] Ransomware attacks, originally a form of malware, are allocated to a separate type of cybercrime. Ransomware are softwares designed to gain unauthorised access to victims' computers and encrypt the necessary files or data on the systems, followed by a demand for a ransom to decrypt these files.[3] Still, phishing attacks include social engineering techniques aimed at stealing the victim’s data or opening access to the victim’s computer. Similar attacks are usually conducted through the phishing links spread via emails or just through the fake websites.[4]

According to Federal Bureau of Investigation data, in 2021, the United States registered 847,376 cybercrimes. In comparison, in 2019, the number of committed cybercrimes in the United States was approximately 460,000.[5] Two years later, the global cost of cybercrime had reached USD $6 trillion.[6] This damage includes the paid ransom from the ransomware viruses, stolen bank account information and the losses incurred to the restore of the data and infrastructure.[7] According to the data from cybersecurity companies, more than 71.1 million people in the United States are

---

[1] CrowdStrike, “Top 14 Most Common Cyber Attacks Today: CrowdStrike,” crowdstrike.com, October 20, 2022, https://www.crowdstrike.com/cybersecurity-101/cyberattacks/most-common-cyberattacks/.
[2] Cisco, “What Is Malware? - Definition and Examples,” Cisco (Cisco, June 6, 2022), https://www.cisco.com/c/en/us/products/security/advanced-malware-protection/what-is-malware.html.
[3] Cisco, “What Is Ransomware?,” Cisco (Cisco Systems, Inc., January 20, 2022), https://www.cisco.com/c/en/us/solutions/security/ransomware-defense/what-is-ransomware.html.
[4] “Spam vs. Phishing: What Is the Difference?,” Cisco (Cisco, September 6, 2022), https://www.cisco.com/c/en/us/products/security/spam-vs-phishing.html.
[5] “IC3 Releases 2020 Internet Crime Report.” FBI, March 17, 2021. https://www.fbi.gov/news/press-releases/press-releases/fbi-releases-the-internet-crime-complaint-center-2020-internet-crime-report-including-covid-19-scam-statistics.
[6] Di, Freeze, “Global Cybercrime Damages Predicted to Reach $6 Trillion Annually by 2021,” Cybercrime Magazine, November 9, 2020, https://cybersecurityventures.com/annual-cybercrime-report-2020/.
[7] Cybercrime Mag, “Cybercrime to Cost the World $10.5 Trillion Annually by 2025,” Cybercrime Magazine, April 27, 2021, https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/.

victims of cybercrime every year,[8] with only 10 to 12% of the victims reaching out for help among the 307 million Internet users in the United States.[9] All this makes cybercrime one of the most dangerous challenges for the information society.

While investigating cybercrimes, law enforcement agencies declare many challenges that they face in the fight against cybercrime, among which there is the issue of defining the cybercrime jurisdiction. First, one should understand the concept of “place of crime", or, in other words, the place where the crime was conducted. Defining the cybercrime jurisdiction is particularly relevant in those situations where the “place of crime” is situated in the European Union (EU). The special relationship tying EU Member States together makes the crime’s territoriality dimension tricky. According to this principle, the exercise of criminal jurisdiction is limited to a state's territory.[10] However, several difficulties arise when determining the location of cybercrimes committed through the Internet. One of the main features of computer crimes is their cross-border nature, and what takes place on the territory of one state may affect other territories and jurisdictions. This can lead to cases of “conflict of criminal jurisdiction”.[11]

Overall, cybercrime is a type of crime, and thus cybercrime matters are regulated by criminal legislation. Consequently, to answer the question of how to define the cybercrime jurisdiction in the EU, it is necessary to analyse the current situation regarding the definition of the general criminal jurisdiction in the EU and then examine the state of the art concerning attempts to solve problems related to such a contested definition. To do this, the next section will provide an analysis of the attempts at defining a criminal jurisdiction in cybercrime matters in the European Union. Then, in the section dedicated to the application of the mutual recognition principle, an investigation on how the implementation of this principle could help in solving possible problems regarding the

---

[8] “2022 Cyber Security Statistics Trends & Data,” PurpleSec, October 17, 2022, https://purplesec.us/resources/cyber-security-statistics/.
[9] Published by Statista Research Department and Aug 31, “Number of Internet Users in the U.S. 2022,” Statista, August 31, 2022, https://www.statista.com/statistics/325645/usa-number-of-internet-users/.
[10] Kenneth S. Gallant, “International Criminal Jurisdiction: Whose Law Must We Obey?” New York, NY: Oxford University Press, 2022, 181-345.
[11] European Law Institute (ELI), “Draft Legislative Proposals for the prevention and resolution of conflicts of jurisdiction in criminal matters in the European Union,” ELI, 2017, 6. https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/Conflict_of_Jurisdiction_in_Criminal_Law_FINAL.pdf.

definition of cybercrime criminal jurisdiction is provided. The last section discusses how the peculiarities of cybercrimes affect the choice of the correct criminal jurisdiction for the conduct of a proper cybercrime investigation.

Attempting to Define a Criminal Jurisdiction for Cybercrimes in the EU

The Budapest Convention on Cybercrime is the main legal document regulating cybercrime internationally.[12] The Budapest Convention on Cybercrime was adopted by the Council of Europe in 2001, and to this day it is signed by 67 countries. Most relevantly, Art. 22 contains the provision for establishing cybercrime jurisdiction. According to it, the jurisdiction is determined based on the territoriality principle. Thus, the Parties of the Convention may guarantee the jurisdiction

"[...] when the offence was committed:

- in its territory;
- on board a ship flying the flag of that Party;
- on board an aircraft registered under the laws of that Party;
- by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any state".[13]

Moreover, para. 5 of Art. 22 of the Budapest Convention established that "when more than one Party claims jurisdiction over an alleged offence, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution".[14] However, there seem to be two problems here. First, the list of cyber offences regulated by the Budapest Convention includes only 10 cybercrimes (Art 2 through Art. 11 of the Budapest Convention), and, therefore, the Party cannot establish its territorial jurisdiction over the cybercrimes that are not mentioned in this list, like cyberextortion (a type of attack in which the performer demands money to stop the attack) or cryptojacking (an unauthorised use of the victims' devices to mine

[12] David Wicki-Birchler, "The Budapest Convention and the General Data Protection Regulation: acting in concert to curb cybercrime?", International Cybersecurity Law Review, 1, 2020, 63, https://link.springer.com/article/10.1365/s43439-020-00012-5#citeas.
[13] Council of Europe, Convention on Cybercrime, art. 22(1), https://rm.coe.int/1680081561.
[14] Council of Europe, Convention on Cybercrime, art. 22(5), https://rm.coe.int/1680081561.

cryptocurrencies). Second, the mechanism mentioned in para. 5 of Art. 22 is not described in detail, so it is unclear how the parties to the Budapest Convention should "consult with a view to determining the most appropriate jurisdiction for prosecution"[15] in the event of a conflict of jurisdiction.

According to Art. 83(1) of the Treaty on the Functioning of the European Union (TFEU), computer crimes apply to the area of crimes under EU jurisdiction. This means that the EU must take steps to harmonise member states' legislation by developing directives that establish minimum standards for the definition of cybercrime and sanctions in this area. Within the meaning of Art. 83(1) of the TFEU, computer crime is a grave crime with the specific characteristic of a cross-border dimension.[16] However, the main problem is the lack of an official definition of computer crime at the EU level.

In addition, one should note that cybercrime lies within the Area of Freedom, Security, and Justice (AFSJ) of the EU, regulated by Title V of the TFEU, which highlights the specific importance of cybercrime regulation. However, even within the AFSJ, there is no prohibition on national authorities initiating parallel proceedings on the same case.[17] The only limitation in this regard is the principle of *ne bis in idem*, which forbids double punishment for the same crime. Procedural criminal law patterns, particularly the practice of the European Union's Court of Justice (CJEU), developed this principle, pursuing it in the legal institution that now exists independently of substantive criminal law. The function of ne bis in idem evolved over time into "the principle of priority," which means that if a Member State first takes over the prosecution of a criminal case, it is illegal for another state to begin a second prosecution against the accused person. [18]

Most cybercrimes can be considered multi-territorial offences since they affect the territory of two or more Member States due to the specificity of the cybercrimes, which, unlike most

---

[15] Council of Europe, Convention on Cybercrime, art. 22(5), https://rm.coe.int/1680081561.
[16] Treaty on the Functioning of the European Union (TFEU), art. 83(1), https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:12012E/TXT:en:PDF.
[17] ELI, "Draft Legislative Proposals," 10.
[18] P. P. Paulesu, "Ne bis in idem and Conflicts of Jurisdiction," Handbook of European Criminal Procedure, 2018, 394.

"traditional" crimes, could be performed from a distance.[19] This can trigger a positive jurisdictional conflict, which occurs when two or more Member States want to exercise their jurisdiction over the cybercrime case.[20] In this regard, the concerned Member States can either start parallel or multiple proceedings. Parallel proceedings involve the proceedings of two or more Member States over the same suspect (or accused person) in relation to the same facts, thus leading to the *ne bis in idem* principle and triggering "the principle of priority." On the other hand, "multiple proceedings" are held in the jurisdiction of two or more Member States against the same suspect (or accused) in relation to *different facts* or against *different suspects* (or accused persons) in relation to the same set of facts.[21]

Hence, a decision to concentrate criminal proceedings in a single Member State may be more convenient for all the participants in the criminal process due to the simplification of the process itself and the concentration of all the efforts in one jurisdiction. Nevertheless, as of the current date, there are no strictly binding instruments that can establish a mechanism to resolve conflicts of jurisdiction between Member States in criminal matters.[22] However, among the existing non-binding mechanisms, one could name the principle of mutual recognition as an attempt to solve conflicts of jurisdiction.

The Principle of Mutual Recognition and the Definition of Cybercrime's Jurisdiction: a Way Forward?

One of the main mechanisms for dealing with jurisdictional conflicts is the principle of mutual recognition, according to which the Member States' national legislation and national judicial decisions in several areas are recognized by other member States as their own.[23] It is considered that the most critical area for the development of mutual recognition is the criminal justice area, strictly

[19] J. Kleijssen & Perri, P. "Cybercrime, Evidence and Territoriality: Issues and Options," Netherlands Yearbook of International Law 2016, https://rm.coe.int/cybercrime-evidence-and-territoriality-issues-and-options/168077fa98, 150.
[20] Pedro Caeiro, "Jurisdiction in Criminal Matters in the EU: Negative and Positive Conflicts, and Beyond," Kritische Vierteljahresschrift Für Gesetzgebung Und Rechtswissenschaft (KritV) 93, no. 4, 2010, pp. 366-379, http://www.jstor.org/stable/43203168.
[21] ELI, "Draft Legislative Proposals",7.
[22] ELI, "Draft Legislative Proposals", 9.
[23] Gisèle Vernimmen-Van Tiggelen, , Laura Surano, and Anne Weyembergh, "The Future of Mutual Recognition in Criminal Matters in the European Union," Bruxelles: Éditions de l'Université de Bruxelles, 2009, 18.

linked with cooperation in criminal matters based on the provisions of the Treaty of Lisbon. Several provisions of the EU treaties deal with the principle of mutual recognition, spreading its activities to various criminal proceedings, including the one regarding cybercrimes. This includes the rules of mutual recognition in the investigation and prosecution of cybercrimes and the collection of evidence.

The principle of mutual recognition is based on three main elements: mutual trust in each Member States' commitment to fundamental rights; equivalence, in which other Member States' judgments are recognized as equivalent to domestic ones; and extraterritoriality, which gives legal effect to other Member States' decisions in domestic systems.[24]

Applying the principle of mutual recognition is mandatory in some cases, including an adjudication of the European Arrest Warrant (EAW) and European Investigation Order (EIO). The first one has been introduced by the Framework Decision 2002/584/JHA on the European arrest warrant and the surrender procedures between the Member States (the FD on EAW), while the second by the Directive 2014/41/EU on the European Investigation Order in criminal matters. The FD on EAW listed the 32 crimes subject to the European arrest warrant, among which is also mentioned computer-related crime.[25] The Directive 2014/41 states that if the conduct for which the European investigation order has been issued does not constitute an offence under the law of the State executing the European investigation order, such an order may be refused by the executing State.[26] However, an exception from this rule is the same list of crimes (including computer-related crimes), as in FD on EAW.[27]

---

[24] Communication from the Commission to the Council and the European Parliament, "Mutual recognition of Final Decisions in criminal matters," Accessed October 23, 2022. https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A52000DC0495.

[25] Council of European Union, Council Framework Decision, 13 June 2002, on the European arrest warrant and the surrender procedures between Member States, art. 2(2), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32002F0584.

[26] European Parliament and the Council, Directive 2014/41/EU, 3 April 2014, regarding the European Investigation Order in criminal matters, art. 11(1).

[27] See note above, art. 11(1)(g).

Nonetheless, both the FD on EAW and Directive 2014/41 are considered outdated when dealing with cybercrime.[28] For example, Directive 2014/41 does not contain any rules on how to work with electronic evidence, which constitutes the cybercrime investigation, which has led to the development of the Proposal for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters.[29] Besides, the statements under Article 11 of Directive 2014/41 essentially negate the value of the national cybercrime definition. This approach can lead to difficult issues of non-recognition of cybercrime in countries with more "relaxed" national legislation on cybercrime or, conversely, over-recognition in countries with a stricter legal order.

This concern can also spread over the FD on EAW issues since these two sources (the FD on EAW and the Directive 2014/4) are strictly linked. Failure of Directive 2014/4 regarding the lack of rules on how to work with electronic evidence will lead to the very likely violation of the fundamental rights and trigger of *ne bis in idem* principle, both listed as grounds for non-execution of the European arrest warrant in the art. 3 FD on EAW and the relevant case law.[30] Therefore, the investigation of cybercrime requires a particular approach, starting with the initial steps of the investigation, namely the definition of the cybercrime jurisdiction and of the cybercrime itself.

Curiously enough, the European Commission attempted to develop such an approach on the legislative level. According to the Green Paper "On Conflicts of Jurisdiction and the Principle of the *ne bis in idem* in Criminal Proceedings", the creation of the additional mechanism for assigning cases to a single jurisdiction will also help to avoid positive jurisdictional conflicts through the use of the *ne bis in idem* principle. This mechanism would complement the principle of mutual recognition and consists of three main steps. First, it would start with the identification and information of "interested parties" (significantly linked to procedures) on the initiation of the

---

[28] Jorge A. Espina Ramos, "The European Investigation Order and Its Relationship with Other Judicial Cooperation Instruments : Establishing Rules on the Scope and Possibilities of Application," Eucrim - The European Criminal Law Associations' Forum, 2019, https://doi.org/10.30709/eucrim-2019-004.

[29] European Commission, "Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters," EC, 2018. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A225%3AFIN.

[30] *See* Stefano Melloni v. Ministerio Fiscal, case C-399/11, 26 February 2013; Joined cases Pál Aranyosi (C-404/15) and Robert Căldărăru (C-659/15 PPU), 5 April 2016; Minister for Justice and Equality v LM, case C-216/18 PPU, 25 July 2018.

criminal proceedings by an "initiating Member State". Second, consultation and discussion of the criminal proceeding with all "interested parties" would be provided. Finally, if necessary, dispute resolution or mediation with "interested parties" would be implemented.[31]

So far, the mechanism of mutual recognition has still not been widely accepted and has been criticised at the EU level as "too voluntary" and contradicting the nature of the *ne bis in idem* principle.[32] Some legal organisations, like the Meijers Commission, have also considered that the European Commission has overestimated the size of the problem regarding a conflict of jurisdictions in criminal matters.[33] However, as was highlighted in the previous section, since cybercrime is still one of the most severe boundless crimes, the transfer of the criminal proceedings to one Member State instead of the dispersal to the numerous "interested parties" would speed up the investigation. On this basis, the elaboration of the cybercrime definition could lead to the resolution of the jurisdictional conflict even before this problem could even arise.

Conclusion

An analysis of the definition of cybercrime jurisdiction starts by examining the issues of general criminal jurisdiction at the EU level. The main challenge regarding the definition of criminal jurisdiction at the EU level is the rising problem of "conflicts of jurisdiction," which is understood as the situation where two or more Member States are willing to investigate and prosecute the crime. Currently, there are no binding legal mechanisms that could help resolve these types of jurisdictional conflicts. The principle of mutual recognition is one of the most prominent among these non-binding mechanisms. The future development of such a principle, also regarding

---

[31] European Commission, "Green Paper on Conflicts of Jurisdiction and the Principle of ne bis in idem in Criminal Proceedings," EC, 2005, 4-6. https://op.europa.eu/en/publication-detail/-/publication/8c2f5cc9-3bcf-4f88-9ed5-e0f882647ff4.

[32] European Criminal Bar Association, "Response to the Green Paper and the Working Paper on *Conflicts of Jurisdiction and the Principle of ne bis in idem in Criminal Proceedings* Presented by the European Commission," ECBA, 28 March 2006, 4. https://www.ecba.org/extdocserv/jurisdictionnebisinidemresponsefinal.PDF.

[33] Standing Committee of experts on international immigration, refugees, and criminal law, "The Response on the Green Paper *on Conflicts of Jurisdiction and the Principle of ne bis in idem in Criminal Proceedings,"* Meijers Commission, 2006, https://www.statewatch.org/media/documents/news/2006/apr/meijers-committee-reaction-ne-bis-in-idem-Greenpaper.pdf.

the cybercrime jurisdiction, could help to direct the approaches definition of cybercrime jurisdiction matter in the right direction.

In order to analyse the definition of criminal jurisdiction in cybercrime matters, the Budapest Convention on Cybercrime, and an attempt to apply the mutual recognition mechanism to the solving of conflict of jurisdiction problem have been discussed. According to its provisions, the criminal jurisdiction for cybercrimes is defined based on the principle of territoriality. However, the analysis demonstrates that the Budapest Convention is not inclusive in regard to cybercrime jurisdiction, as it regulates the limited scope of cybercrimes and does not provide a functional mechanism helping to solve the problem of conflict of jurisdiction.

However, the mechanism of mutual recognition could address the problem of finding the right place of jurisdiction only if the legislation is developed and implemented rapidly. The constant development of Information and Communication Technologies, the cross-border nature of cybercrimes, and the use of techniques providing anonymity all contribute to the quick expansion of cybercrime matters. This finding is confirmed by the increasing number of cybercrimes and the amount of damage they inflict. An elaboration of the cybercrime jurisdiction is already a complex task due to the nature of cybercrime; hence, the lack of legislative and soft-law instruments leads to situations where the conflict of jurisdiction cannot be solved legally.

Jurisdictional conflicts can be exploited by cybercriminals for their own benefit and must be prevented at their earliest stages. Existing legal instruments, including the Budapest Convention, which was established to eliminate difficulties in the international fight against cybercrime, do not contain sufficient mechanisms to prevent jurisdictional conflicts and foster international collaboration in the fight against cybercrime. Hence, a boost in international cooperation on the elaboration of instruments for this purpose would help to avoid legal vacuums and be the main way to control the spread of cybercrime while holding cybercriminals accountable for their illegal actions. After an analysis of the peculiarities of cybercrime, it became apparent that the solution to the problem of conflict of jurisdiction cannot be found by using “traditional” crime mechanisms.

In conclusion, additional attempts to define the cybercrime jurisdiction in the EU through non-legal instruments should be undertaken. The author believes that using these instruments could provide for more effective solutions than the implementation of strictly legal instruments. Therefore, they should be considered to fully implement cybercrime protection mechanisms.

Bibliography

Caeiro, Pedro. "Jurisdiction in Criminal Matters in the EU: Negative and Positive Conflicts, and Beyond." *Kritische Vierteljahresschrift Für Gesetzgebung Und Rechtswissenschaft (KritV)* 93, no. 4 (2010): 366–79. http://www.jstor.org/stable/43203168.

Cisco. "What Is Ransomware?" Cisco. Cisco Systems, Inc., January 20, 2022. https://www.cisco.com/c/en/us/solutions/security/ransomware-defense/what-is-ransomware.html.

Communication from the Commission to the Council and the European Parliament, "Mutual recognition of Final Decisions in criminal matters." Accessed October 23, 2022. https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A52000DC0495.

Council Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32002F0584.

Council of Europe, Convention on Cybercrime, 01 July 2004. https://rm.coe.int/1680081561.

Cybercrimemag. "Cybercrime to Cost the World $10.5 Trillion Annually by 2025." Cybercrime Magazine, April 27, 2021. https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/.

Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32014L0041.

Espina Ramos, Jorge A. "The European Investigation Order and Its Relationship with Other Judicial Cooperation Instruments : Establishing Rules on the Scope and Possibilities of Application." *eucrim - The European Criminal Law Associations' Forum*, 2019. https://doi.org/10.30709/eucrim-2019-004.

European Commission, "Green Paper on Conflicts of Jurisdiction and the Principle of ne bis in idem in Criminal Proceedings." EC, 2005. https://op.europa.eu/en/publication-detail/-/publication/8c2f5cc9-3bcf-4f88-9ed5-e0f882647ff4.

European Criminal Bar Association, "Response to the Green Paper and the Working Paper on Conflicts of Jurisdiction and the Principle of ne bis in idem in Criminal Proceedings Presented by the European Commission." ECBA, 28 March 2006. https://www.ecba.org/extdocserv/jurisdictionnebisinidemresponsefinal.PDF.

European Law Institute. "Draft Legislative Proposals for the prevention and resolution of conflicts of jurisdiction in criminal matters in the European Union." ELI, 2017.

FBI. (2020). The Internet Crime Report. https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf.

Freeze, Di. "Global Cybercrime Damages Predicted to Reach $6 Trillion Annually by 2021." Cybercrime Magazine, November 9, 2020. https://cybersecurityventures.com/annual-cybercrime-report-2020/.

Gallant, Kenneth S. International Criminal Jurisdiction: Whose Law Must We Obey? New York, NY: Oxford University Press, 2022. https://doi.org/10.1093/oso/9780199941476.001.0001.

Kleijssen, J., & Perri, P. Cybercrime. “Evidence and Territoriality: Issues and Options.” Netherlands Yearbook of International Law 2016, 147-173. https://rm.coe.int/cybercrime-evidence-and-territoriality-issues-and-options/168077fa98.

Standing Committee of experts on international immigration, refugees, and criminal law, “The Response on the Green Paper on Conflicts of Jurisdiction and the Principle of ne bis in idem in Criminal Proceedings.” Meijers Commission, 2006. https://www.statewatch.org/media/documents/news/2006/apr/meijers-committee-reaction-ne-bis-in-idem-Greenpaper.pdf.

Tiggelen, Gisèle Vernimmen-Van, Laura Surano, and Anne Weyembergh. The Future of Mutual Recognition in Criminal Matters in the European Union. Bruxelles: Éditions de l'Université de Bruxelles, 2009. https://library.oapen.org/viewer/web/viewer.html?file=/bitstream/handle/20.500.12657/24543/1005568.pdf?sequence=1&isAllowed=y.

Treaty on the Functioning of the European Union. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12012E%2FTXT.

Wicki-Birchler, David. “The Budapest Convention and the General Data Protection Regulation: acting in concert to curb cybercrime?” International Cybersecurity Law Review, 1, 2020, 63-72, https://link.springer.com/article/10.1365/s43439-020-00012-5#citeas.

“IC3 Releases 2020 Internet Crime Report.” FBI. FBI, March 17, 2021. https://www.fbi.gov/news/press-releases/press-releases/fbi-releases-the-internet-crime-complaint-center-2020-internet-crime-report-including-covid-19-scam-statistics.

“Spam vs. Phishing: What Is the Difference?” Cisco. Cisco, September 6, 2022. https://www.cisco.com/c/en/us/products/security/spam-vs-phishing.html.

“Top 14 Most Common Cyber Attacks Today: CrowdStrike.” crowdstrike.com, October 20, 2022. https://www.crowdstrike.com/cybersecurity-101/cyberattacks/most-common-cyberattacks/.

“What Is Malware? - Definition and Examples.” Cisco. Cisco, June 6, 2022. https://www.cisco.com/c/en/us/products/security/advanced-malware-protection/what-is-malware.html.