WEP Warwick Evans Publishing

Transactions on Social Science, Education and Humanities Research
ISSN: 2960-1770, eISSN: 2960-2262 | Volume 12
LHPPR 2024

Exploring the Territorial Jurisdiction of Cybercrime in the ICC: An Application of the Doctrine of "Effects"

Zilan Huang

School of Law, Beijing Foreign Studies University, Beijing, China

202220115049@bfsu.edu.cn

Abstract. The doctrine of "effects", as an objective application of territorial jurisdiction, has been controversial since its establishment. The dispute becomes more intense when it comes to cybercrime. In the area of International Criminal Law, while some practices in the international criminal court and tribunals indicate a trend towards expanding territorial jurisdiction, which implies the application of the "effects" doctrine, whether the Court can adopt the doctrine or not remains uncertain. In the background that the integration of cybercrime and crimes stipulated by the Court is becoming a trend, considering the necessity and feasibility of applying the "effects" doctrine to the International Criminal Court, it is argued that the doctrine should be applied to the Court's territorial jurisdiction. However, some potential risks raised by the application require a more balanced solution for the problem, which means the "effects" doctrine can only be applied by the Court when there exists a substantial and reasonably foreseeable effect on the territory.

Keywords: Cybercrime; Territorial Jurisdiction; ICC; The Doctrine of "Effects".

1. Introduction

In 2023, there were 5.3 billion internet users, comprising two-thirds of the world's population [1]. However, the development of cyberspace has not triggered sufficient improvements in judicial regulations [2], leading to an increasing number of cybercrimes. Considering the cross-border nature of cybercrimes, jurisdiction issues emerge [3]. The issue becomes more pronounced when it comes to territorial jurisdiction, where the Defendant, regardless of nationality, falls under the legal authority of the territorial State. The doctrine of "effects", which allows jurisdiction over foreign citizens whose acts occur out of but have an effect in the territory of the State, belongs to an objective application of the territorial jurisdiction [4]. Given the wider effect cybercrimes may have compared to traditional crimes, the application of the "effects" doctrine on the territorial jurisdiction of cybercrimes is more likely to threaten state sovereignty.

This paper puts the above jurisdiction issue under the ICC framework. Article 4(2) of the Rome Statute (RS) grants the ICC the right to exercise its authority on the State Party [5]. Pursuant to Article 12 RS, which is deemed to be the main legal source of the territorial jurisdiction of the ICC [6], the Court may exercise its jurisdiction over the State where the crime conduct occurred [5]. When applying the "effects" doctrine to ICC's territorial jurisdiction, the question arises as to whether the balance between the State sovereignty and the requirements of international justice has been attained. This paper is structured as follows. Part II provides a more detailed statement of the problem at hand. Part III focuses on whether or not the doctrine of "effects" should be applied by the ICC, and attempts to identify a viable solution. In the final part, the paper presents its conclusion.

2. Problem Statement

As stated above, although the RS authorizes the ICC to exercise territorial jurisdiction, the scale of "the territory where the conduct occurred" in Article 12(2)(a) remains uncertain. The uncertainty becomes particularly problematic when a citizen from a non-State Party commits one of the crimes stipulated by the Court (as per Article 5 RS) via the Internet, and the conduct has an effect on a State Party. The question arises as to whether or not the Court could exercise its jurisdiction over the cybercrime, which depends on whether the place where the conduct occurs encompasses the place affected by the conduct.

It essentially pertains to whether the doctrine of “effects” can be adopted by the ICC as a basis for exercising territorial jurisdiction. In the 2009 ICC Assembly of States Parties, a proposal was made to apply the doctrine to the ICC, but it was ultimately not adopted by the Court due to the opposition of the majority of representatives [7]. However, the emergence of cybercrime forces a re-examination of this issue. In the context of cybercrime, if the ICC does not adopt the “effects” doctrine, it might result in a large number of most serious crimes that pose considerable hazards to the international community going unregulated, therefore blocking the realization of international justice. Conversely, if the ICC adopts the doctrine, it could potentially infringe upon State sovereignty.

Hence, in the context of cybercrime, it is necessary to determine whether or not the “effects” doctrine could be applied and, if so, to what extent it should be applied. The analysis should take into account the practices in international law and the ICC, and the future trends in the context of cybercrime concerning this issue.

3. Discussion

3.1. Introduction of the Doctrine of “Effect”

3.1.1. Origination in Competition Law Jurisdiction

The doctrine of “effect” has originally been set up in United States v. Aluminum Co. of America in 1945 (the Aluminum case), manifesting itself as part of the US antitrust law [8]. In this case, jurisdiction broke through the limitation of the traditional territorial principle and was applied outside of a state’s territory. After the case, US jurisprudence allows jurisdiction in the antitrust field beyond a state’s territory in the situation that it had a specific effect on the territory [8]. The doctrine was later innovated and adopted by EU competition law. Further, it gradually developed into a public international law principle in the establishment of the jurisdiction in competition laws [8].

3.1.2. Development in Criminal Law Jurisdiction

In addition to the competition law, the “effects” doctrine is also embodied in the domestic criminal codes of numerous nations. The most prevalent practice in criminal legislation worldwide is to consider the place where the conduct occurs as a combination of the place of action and the place where the effect occurs. Regions such as Switzerland, Germany, France, Italy and China all adopt this as a general principle for identifying the crime's location [9].

In the context of cybercrime, numerous countries such as Germany, France, Italy, Canada, Australia have imposed criminal penalties for transnational defamation, dissemination of pornographic information, and promotion of extreme violent speech [7]. In particular, in LICRA v. Yahoo, a court in France exercised its jurisdiction over an American Internet company called Yahoo, and mandated the removal of web pages showing Nazi memorabilia. This content is illegal in France but legal in most other jurisdictions [10]. A French judge determined that jurisdiction could be exercised based on the damage inflicted within France, rather than the location where the content was uploaded [11]. This case is particularly noteworthy, providing significant value for the paper. Further, NATO’s Tallinn Manual 2.0 on the International Law clearly establishes that states can exercise their jurisdiction over cyber actions that occur outside their borders but have a direct, material and foreseeable effect within their borders [7].

To conclude, the “effects” doctrine extends the territorial jurisdiction by considering the effects of the conduct as part of the conduct itself. It originates from the competition law system, and has gradually integrated into the international criminal law system. The principle has been generally recognized in the legislation and practice in the international community and has become a general legal principle for territorial jurisdiction, in the making.

3.2. Practices of the "Effects" Doctrine in the International Criminal Court and Tribunals

3.2.1. The Prosecutor v. Charles Chankay Taylor in the SCSL

The Sierra Leone Special Court (SCSL), as an international criminal tribunal, is best known for the trial of the president of Liberia named Taylor [12]. In this case, although Taylor had never set foot in Sierra Leonean territory, he was convicted by the SCSL for providing arms, ammunition, and food to AFRC and RUF rebels, thereby contributing to the escalation of the civil war [13].

Although the "effects" doctrine was not explicitly invoked in the Taylor case, it was apparent in two aspects. Firstly, from the literal interpretation of the Statute of the SCSL (SCSL Statute), according to Article 1, the Special Court is endowed with the authority to bring to trial those individuals who gravely violate both international humanitarian law and Sierra Leonean law that occurred within Sierra Leone [14]. This emphasizes the practical effects of crimes within the territory, which constitutes a formal manifestation of the "effects" doctrine. Secondly, in the Taylor case, although Taylor had never physically entered Sierra Leone during the commission of the crimes, he was convicted of crimes against humanity due to the deliberate, direct, and substantial impact of his actions on Sierra Leone. This corresponds with the substantive content of the "effects" doctrine.

It's worth noting that in 1999, the SCSL's prosecution of Charles Taylor was also widely recognized by the European legal community in Gencor Ltd v. European Commission [15]. This reflects the trend of the case is gradually gaining recognition from the international community.

3.2.2. Situation in the People's Republic of Bangladesh/Republic of the Union of Myanmar in the ICC

The Rohingya citizens in Myanmar have a long history of persecution by the Myanmar government. The government claims that they are illegal immigrants from Bangladesh and has refused to grant them citizenship [16]. Starting in 2017, the Myanmar military began committing atrocities against the Rohingya, which resulted in the forced expulsion of over 700,000 Rohingya between August 2017 to March 2018, with the majority of refugees fleeing to Bangladesh [16].

In this case, ethnic cleansing and genocide occurred in Myanmar, a non-State Party to the RS. The Pre-Trial Chamber (PTC) of the Court determined that according to Article 12(2)(a), the ICC's jurisdiction extends to cases where only one element of a crime to occur within the territory of a State Party [17]. Since the alleged conduct of expelling the civilian population from the Myanmar-Bangladesh border established a connection with the State Party, Bangladesh [18], the ICC exercised its jurisdiction over the case concerning deportation.

However, there is a dispute over whether the doctrine of "effects" applies to this case. On the one hand, Article 7(1)(d) RS lists "deportation or forcible transfer of population" among the crimes against humanity. The PTC held that the provision embodies two separate crimes, namely deportation and forcible transfer of population, with displacement across a border constituting an element of the crime of deportation [17]. Given that deportation inherently involves a trans-boundary nature, the connection established between territories is related to the nature of the charge itself. Thus, some may argue that the decision of the PTC is not based on the "effect" doctrine, but on the nature of the crime itself.

On the other hand, the Office of the Prosecutor also argued that the influx of refugees has resulted in a humanitarian crisis in Bangladesh [7], leading to significant economic and social repercussions within the territory of the State Party. Some scholars have pointed out that although the Court did not explicitly state it, it implied that even if the element of deportation does not occur within Bangladesh's territory, the effects of deportation still arise in Bangladesh [7]. Therefore, the ICC's decision is essentially in accordance with the "effects" doctrine.

3.3. Analysis of the Application of the Doctrine of "Effects" in the ICC's Territorial Jurisdiction in the Context of Cybercrime

3.3.1. Necessity Analysis of Application

The first question is whether it is necessary for applying the "effects" doctrine in the ICC. The conclusion is that there is a great necessity for the application. In the Internet Age, cyber technologies have become a new method for committing crimes. Moreover, the integration of cybercrime and the four types of crimes stipulated by the ICC is becoming a trend. According to Article 5 RS, the Court has jurisdiction over the crime of genocide, crimes against humanity, war crimes, and the crime of aggression. Most of the above crimes can be linked to the Internet.

When war crimes are committed during an armed conflict, they fall under the jurisdiction of the Court under Article 8 RS [5]. In the cyber age, armed conflict is increasingly influenced by new technologies. For example, artificial intelligence, precision-guided munitions, autonomous weapon systems, and other digital technologies are more prevalently used to command attacks more precisely and effectively [19]. Those cyber operations could help to create devastating physical harm in a simulated environment by disrupting the operating system of the critical infrastructure, which would also lead to deaths or destruction of property. The above conduct may fall within the scope of Article 8 RS, part of which address acts aimed at causing civilian casualties or destroying protected objects [5]. The cyber attacks described above, which cause harmful physical consequences to a civilian population, may constitute a crime of genocide in Article 6(a) RS if the specific requirements are met. Additionally, if the requisite context elements of such attacks are satisfied, they may constitute a crime against humanity in Article 7(1) RS [5], despite of the existence of an armed conflict. For instance, the promotion of discriminatory statements in the media may constitute the crime against humanity of persecution if certain conditions are met.

Further, cyber technology may potentially be employed to instigate the commission of offenses listed by the ICC [20]. For example, subsidiary liability can be established through acts like preparing for genocide, such as conducting a cyber hack on certain individuals of a certain race with the intention to participate in genocide. On blogs, tweets, and other social media sites, people can also encourage others to carry out acts of genocide by leaving comments. However, the above new trend has hardly been given serious attention. Even the Tallinn Manual 2.0, a book in the field of cyber operations, only includes two out of 154 regulations dealing with cyber-related international criminality [12]. Considering the increasing trend of cybercrimes in international criminal law, more and more cases are going untried in the ICC.

The urgent situation, along with the ICC's mission to prevent impunity, calls for the necessity of applying the "effects" doctrine. The goal of the RS is to hold those guilty for the most serious crimes that affect the global society and are clearly prohibited in both international and domestic legal frameworks, thereby contributing to their prevention [5]. Thus, Article 12(2)(a) RS shall be interpreted to allow criminal jurisdiction in situations where State Parties would exercise jurisdiction under their legal systems without violating international law or the RS [17]. Given the emerging trend of integration of cybercrime and crimes covered by the RS, if the ICC maintains a restrictive interpretation of "the place where the conduct occurs" in Article 12(2)(a) RS and refuses to apply the "effects" doctrine, more cases may go unprosecuted. This would go against the ICC's objective of ending impunity in the realm of cybercrime. Therefore, it is crucial to apply the "effects" doctrine to the ICC's territorial jurisdiction concerning cybercrime.

3.3.2. Feasibility Analysis of Application

Given the necessity for its application, the next question that arises is whether the "effects" doctrine could potentially be widely adopted in the ICC. The conclusion is that there is a possibility of achieving that.

Firstly, the fundamental principle established in the S.S. Lotus case provides the possibility. In that case, a French vessel "Lotus" collided with a Turkish vessel, resulting in the deaths of eight Turkish nationals. Consequently, the French national on board the "Lotus" became the target of criminal charges by the Turkish authorities, which sparked a series of jurisdictional disputes [7]. The Permanent Court of International Justice (PCIJ) ruled that Turkey's actions did not violate international law principles because the conduct committed on board the Lotus had an effect on Turkish territory, thereby allowing Turkey to exercise its jurisdiction [7]. Some scholars interpret the Lotus principle as sovereign states can freely establish a collective international jurisdiction that applies to the citizens of non-party countries unless there exists a breach of international law [21]. This interpretation aligns with the establishment of the ICC's jurisdiction, which deals with the question of jurisdiction over residents of non-State Parties when the ICC applies the "effects" doctrine to territorial jurisdiction.

Secondly, the similarities between the need for criminal jurisdiction and competition law (especially antitrust law) jurisdiction provide the possibility. Unlike civil and commercial disputes related to private law relationships, such as defamation, tort, contract disputes, and family law, both criminal law and antitrust law have a public law nature. Private law emphasizes the protection of individual rights, while public law emphasizes the protection of the public interest. In domestic antitrust cases, the conduct of monopolistic enterprises may have negative effects on the domestic market, harming the public interest. When a country's monopolistic enterprise adversely affects another country, it may endanger the public interest of a country or even the international community. At this point, the "effects" doctrine is used to exercise jurisdiction over such conduct for the protection of the public interest, reflecting the public law nature of antitrust law. Similarly, criminal law, as a public law, combats crimes that are extremely harmful to society and protects the public interest and justice. As mentioned above, the "effects" doctrine has become a public international law principle in the establishment of the jurisdiction in competition laws. Based on the similarities between criminal law and antitrust law in relation to their common public law nature and the purpose of protecting the public interest, it is possible to incorporate the "effects" doctrine into international criminal law as a basis for establishing territorial jurisdiction.

Thirdly, practices in criminal jurisdiction, especially the cases in the SCSL and the ICC, provide the possibility. Article 21 RS sets out the Court's applicable law, including general principles of law deprived by the Court from national legal systems worldwide, as well as principles and rules of law as interpreted in its previous decisions [5]. Particularly, these principles should also encompass those represented in case laws in the SCSL. As stated above, the "effects" doctrine has been widely used in the domestic criminal law of most countries, constituting general principles from national laws of the world. Also, in the practices of the International Criminal Court and Tribunals, the Taylor case in the SCSL and the Bangladesh/Myanmar Situation in the ICC provide precedents for this issue. Although there exists controversy over whether these practices have applied the "effects" doctrine, it cannot be denied that the substantive content of these cases is in accordance with the connotation of the doctrine. Thus, they at least provide some basis for the application of the doctrine.

3.3.3. Potential Risks of Application

Since there is a great necessity for the application and it is feasible for the ICC to apply the "effects" doctrine to its territorial jurisdiction, the application should be acknowledged in theory. However, to optimize the effectiveness of the application, potential risks must also be taken into consideration. The following part will present two possible risks.

The first potential risk is that the ICC's jurisdiction over citizens from the non-State Party might impose obligations on non-State Parties. Generally, the exercise of a state's jurisdiction over persons who commit crimes on its territory is based on state sovereignty. However, the ICC exercises jurisdiction on behalf of, and with the permission of States Parties [7]. According to Article 34 of the Vienna Convention on the Law of Treaties (VCLT), a treaty cannot impose obligations on non-contracting countries [22]. Extending the territorial jurisdiction as a form of the application of the doctrine of "effects" could potentially go beyond the established principles outlined in the VCLT.

Regarding this risk, America's long-standing objection to the RS [21] is a typical example. As one of the only seven countries voting against the RS for the ICC, the US is unwilling to be obligated to provide accused citizens in its territory for the ICC's investigation or prosecution in a situation where it has not accepted to be bound by the treaty [21]. This is considered a significant detriment to American foreign policy, a potential source of political risk, and a serious violation of the basic principle of treaty law [21]. The concern is believed to reflect the sentiments of many other non-State Parties like the US, constituting a significant risk to international law.

The second potential risk is that an overly broad interpretation of "effect" might damage national sovereignty. The dispute in this paper is not limited to whether or not the "effects" doctrine should be applied but also extends to the degree of the "effect". Since there is no definitive standard for it, an inappropriate interpretation is likely to create problems. In the context of cybercrime, considering the wide reach and speed of internet dissemination, an overly broad interpretation will harm the national sovereignty of more countries, posing a significant risk.

4. Proposal of Solutions

As stated above, given that there exists a great necessity and also the feasibility of the application of the "effects" doctrine to the ICC's territorial jurisdiction, the application should be implemented in theory in the context of cybercrime. But to prevent the expansion of its potential risks, the scope of "effect" should be limited. However, the standards for limitations are not entirely consistent in judicial precedents worldwide. Taking the United States as an example, the Aluminum case in 1945 clarified the "substantive" principle in the "effects" doctrine [7]. The Foreign Trade Antitrust Improvements Act of 1982 required the effect to be "direct, substantial, and reasonably foreseeable". The three elements determined thereby have become the starting point for many theoretical discussions on the effects doctrine [7]. However, Article 2(i) of the Commodity Exchange Act requires the effect to be "direct and significant". The General Court of the EU adopted the "immediate, substantial and foreseeable" effects doctrine in the Gencor case in 1999 [7].

Looking at the aforementioned practices, firstly, the application of the "effects" doctrine should at least meet the "substantial" requirement. Secondly, according to Article 30 RS, all crimes stipulated by the ICC require the intent and knowledge of the material elements [5]. The outcome is considered intended when it aligns with actor's purpose, or the actor realizes that it will occur in the normal course of events [5]. Thus, the condition is accordance with the "reasonably foreseeable" requirement. Thirdly, in the practice of the ICC, for example, an attack may take the shape of exerting pressure on the population to act in a specific manner [23], which constitutes an indirect conduct. Thus, the element of "direct" is indeed unnecessary.

In conclusion, only when the act has a substantial and reasonably foreseeable effect on the State Party, can jurisdiction be exercised over non-contracting country citizens according to the "effects" doctrine.

5. Conclusion

In conclusion, the application of the "effects" doctrine to the territorial jurisdiction of the ICC in the context of cybercrime presents both opportunities and challenges. The doctrine, which allows jurisdiction over foreign citizens whose acts occur outside but have an effect within the territory of the State, offers a potential solution to the jurisdictional issues raised by the cross-border nature of cybercrimes. However, its application also raises potential risks, particularly in terms of threatening state sovereignty. This paper has argued that the "effects" doctrine should be applied to the ICC's territorial jurisdiction, given the increasing integration of cybercrime and crimes stipulated by the Court and the ICC's purpose of prohibiting impunity. However, it has also highlighted the need for a balanced solution that takes into account the potential risks associated with the doctrine's application. Specifically, it is argued that the "effects" doctrine should only be applied by the Court when there exists a substantial and reasonably foreseeable effect on the territory.

The exploration of the territorial jurisdiction of cybercrime in the ICC, particularly the application of the “effects” doctrine, is a complex and evolving issue. It is hoped that this paper has contributed to the ongoing dialogue and will serve as a foundation for future research and policy development. As we continue to navigate the digital age, it is crucial that our legal frameworks adapt to ensure justice is served, while also respecting the sovereignty of states. This balance is not easily achieved, but it is a challenge that must be met head-on. The “effects” doctrine, with its potential to extend the ICC’s territorial jurisdiction concerning cybercrime, represents one possible path toward this goal. However, as this paper has argued, its application must be carefully considered and managed to mitigate potential risks. As such, this paper concludes with a call for continued research and dialogue in this area, to ensure the most effective and equitable application of international criminal law in the digital age.

References

[1] Ani Petrosyan. Internet usage worldwide-statistics & facts. 13 Feb. 2024. Retrieved from https://www.statista.com/topics/1145/internet-usage-worldwide/

[2] Maillart J.B. The limits of subjective territorial jurisdiction in the context of cybercrime. Era Forum, 2019, 19(3): 375-390.

[3] C. Viano E. Section II-Criminal law. Special part-information society and penal law: General report. Revue Internationale De Droit Pénal, 2013, (3): 335-355.

[4] Samie, Najeeb. The doctrine of effects and the extraterritorial application of antitrust laws. Lawyer of the Americas, 1982, 14(1): 23-59.

[5] Rome Statute of the International Criminal Court, 2002, Preamble, Article 4(2), Article 7(1), Article 8(1), Article 8(2)(b)(i), Article 8(2)(b)(ii), Article 8(2)(b)(iv), Article 8(2)(e)(i), Article 12, Article 21, Article 30.

[6] Klamberg, M. Commentary on the law of the international criminal court. Torkel Opsahl Academic EPublisher, 2017.

[7] Han Jingying, Ma He. The principle of effect rectification and the cause of our criminal law. Foreign Legal History Research, 2022, 24(00): 205-225.

[8] Zelger, B. EU Competition law and extraterritorial jurisdiction-a critical analysis of the ECJ’s judgement in Intel. European Competition Journal, 2020, 16(2-3): 613-617.

[9] Yan Han, Conflicts of international criminal jurisdiction and its settlement. Beijing Foreign Studies University, 2021.

[10] Brenner, S. W., Koops, Bert-Jaap. Approaches to cybercrime jurisdiction. Journal of High Technology Law, 2004, 4(1): 10.

[11] Greenberg, M. H. A Return to Lilliput: The “LICRA v. Yahoo!” case and the regulation of online content in the world market. Berkeley Technology Law Journal, 2003, 18(4): 1208.

[12] Schmitt, Michael N., ed. Tallinn manual 2.0 on the international law applicable to cyber operations. Cambridge University Press, 2017.

[13] The Prosecutor v. Charles Chankay Taylor, SCSL-03-01-T, Judgement, 18 May 2012.

[14] Statute of the Special Court for Sierra Leone, 2000, Article 1.

[15] Gencor Ltd v. European Commission, 1999 E.C.R.753.

[16] Associated Press. U.N. genocide advisor: Myanmar waged ‘scorched-earth campaign’ against the Rohingya. 13 Mar. 2018. Retrieved from https://www.latimes.com/world/la-fg-myanmar-rohingyas-20180313-story.html

[17] Decision on the “prosecutor’s request for a ruling on jurisdiction under article 19(3) of the statute”. ICC-RoC46(3)-01/18, 6 Sep. 2018.

[18] Situation in the people’s republic of bangladesh/republic of the union of myanmar. ICC-01-09, 14 Nov. 2019.

[19] Gabrielli G. Individual criminal responsibility of non-state actors operating in cyberspace for war crimes under the ICC statute. EU and Comparative Law Issues and Challenges Series, 2023, 7: 287.

[20] Roscini, M. Gravity in the statute of the International Criminal Court and cyber conduct that constitutes, instigates or facilitates international crimes. Criminal Law Forum, 2019, 30(3): 251.

[21] Scharf, M. P. The ICC's jurisdiction over the nationals of non-party states: a critique of the U.S. position. Law and Contemporary Problems, 2001, 64(1): 64-73.

[22] Vienna Convention on the Law of Treaties, 1969, Article 34.

[23] Prosecutor v. Akayesu, Judgement, ICTR-96-4, 2 Sep. 1998.