Pakistan Journal of Criminology
Vol. 16, No. 01, January—March 2024 (549-560)

Cybercrimes in Light of The Rules of Public International Law

Ola Ghazi Abbasi[1], Amer Fakhoury[2]

Abstract

Despite what has been witnessed by the international community during the recent decade in connection with the widespread use of modern technology based on the World Wide Web in all aspects of life, as well as what this has achieved, including the easiness of having access to information and the reliance by the fundamental infrastructures and services provided to citizens on it, there have been adverse effects of this revolution with which we live in our life. However, legal experts have attempted to research how applicable its rules are to cybercrimes being considered cross-border crimes, and they can threaten the principles of sovereignty and non-interference. Therefore, this research has addressed the problem related to how applicable the rules of international law are to cross-border cybercrimes, which might violate the two principles above deemed to be some of the fundamental principles on which international law is based.

Keywords: Cyber, Cybercrimes, Rules Public International Law

Introduction

One of the most prominent criminal problems recently that is significantly paid attention on the regional and international levels is what is known as cyber criminality. This is because of its profound effects affecting states and individuals on equal footing. This is something natural resulting from the electronic development of societies and the resort by many countries to the expansion of applying what is known as E. Governments. This also administers state affairs as an alternative to traditional administrative governments.

Cybercrimes are committed by professional persons against electronic systems inside certain countries. The matter is characterized by being extremely serious due to the incapability of any country to impose its sole control and sovereignty on this Cyberspace in a way that results in the occurrence of cyber-attacks. These attacks have adversely affected the national security of the state.

In addition, the consequences of these attacks have increased the severity of the conflict among the states because states have committed crimes against other states that have been called cyber war. This is what was done by the occupying

1 Department of Comparative Law, Sheikh Nouh Al-Qudah College of law for Sharia and law. The World Islamic Sciences and Education University- Jordan
2 College of Law- American University in the Emirates – United Arab Emirates

state against Iran in 2009 and what was done by Russia against Georgia in 2008 and Estonia in 2007 (Rabbah, 2021).

I. Cybercrimes and The Principle of Sovereignty

Preamble and Division

Cybercrimes raise a problem concerning the principle of sovereignty. This issue has become complex and interfering in light of the international variables. It resulted in the expansion of protecting the principles of human rights and the tremendous technological advancement in the modern era in a way that has led to the easiness of penetrating the borders of the state and adversely affecting its sovereignty, especially for developing countries (Mabrouk, 2015).

In light of the above, the study attempts to show the situation of international instruments and agreements concerning the principle of sovereignty.

a. The situation of International Instruments and Agreements concerning The Principle of Sovereignty

Sovereignty can be defined as the " Supreme power of the state, nothing superior to it and not subject to anyone, but it has superiority over all imposes itself on the society" (Gassem, 2016). This definition shows that sovereignty is a political and legal concept connected with the state's existence and is one of its most prominent features.

The common concept of cybercrime connected with the transnational dimension must be analyzed concerning when and how we can say any cybercrime involves a transnational dimension. We find the answer in the UN Convention Against Transnational Organized Crime, where Paragraph Two of Article Three provides that " an offense is transnational if:

(i) It is committed in more than one state.

(ii) It is committed in one state, but a substantial part of its preparation, planning, direction, or control takes place in another state.

However, what is the situation of the international instruments and agreements in relation to the principle of sovereignty?

Article 4 of the Arab Convention on Combating Information Technology Offences of 2010 provides that "to the discharge of its obligations stemming from the application of this convention in a manner consistent with the two principles of equality of the regional sovereignty of States and the non-interference in the internal affairs of other States"

This violation of the sovereignty of the state takes place even though this unauthorized access has taken place by an investigation based on a cybercrime committed in a third state in an attempt of the latter one to specify the source of the cyber-attack or to prevent the continuity of these attacks (Al-Bouqairat, 2014).

This means that judicial jurisdiction is connected with sovereignty, where the state enjoys the authority to determine the rights and obligations within its territory as well as the application of the principle of legality through the enforcement of law and imposition of punishment on whoever violates it (Serag, 2011).

Regarding the extradition of the perpetrators of cybercrimes, extradition treaties have been drafted as one of the forms of international cooperation for carefully combating these offenses to guarantee respect by their mechanisms for the fundamental principles of sovereignty (Al-Saady, 2012). Article 4 of the UN Convention against Transnational Organized Crime states that" States Parties shall carry out their obligations under this convention in a manner consistent with the principles of sovereign equality and territorial integrity of States and that of non-intervention in the domestic affairs of other States.".

b. The situation of International Courts about the Principle of Sovereignty

i. The situation of Permanent Court of International Justice in Connection with the Principle of Sovereignty:

The Permanent Court of International Justice PCIJ contributed to the settlement of many international disputes submitted to it, particularly those connected with borders and regionality, despite its short duration of work where 29 dispute cases were submitted to it, and it showed 27 advisory opinions. As regards the borders and regionality cases, there were eight cases only[3].

As for the principle of sovereignty, PCIJ had a clear situation in the " Lotus Case" filed by France against Turkey in September 1927 when it stated that " the substantial restriction imposed by international law on the state lies in the exclusion of any exercise of its power in the territory of another state unless there is a contrary rule."[4].

Some of the most prominent disputes submitted to PCIJ concerning the principle of sovereignty are the cases of Wimbledon in 1923 and Lotus in 1927, When the dispute was submitted to PCIJ, it rendered its judgment on obliging Germany to pay indemnities for losses in favor of the French company (Al-Magzoub, 2013).

A French steamship and a Turkish steamship carrying coal collided in the Mediterranean Sea in 1926, resulting in the Lotus Case. The Turkish judiciary detained and prosecuted the French ship's master, resulting in his incarceration and

---

[3] To access border and regionality cases heard by the Permanent Court of International Justice, See this website: http://www.icj-cij.org/pcij/index.php. Retrieved on 16/2/2022.

[4] See Legal Training Program on Combating terrorism (2012), International Cooperation in Criminal Issues Connected with Terrorism, UN Office on Drugs and Crime, Vienna, P.80.

fine. Following France's objection, the Turkish government and the parties came to an arrangement. The PCIJ's decision in Turkey's favor sparked a jurisprudential discussion. According to a 1952 French view, criminal jurisdiction is associated with the state whose flag a ship is flying (Hamdy, 2012).

ii. Situation of the International Court of Justice concerning the Principle of Sovereignty:

The International Court of Justice ICJ is deemed an international judicial body composed of fifteen judges the United Nations General Assembly selects. It is vested with an advisory function in addition to its judicial function. It conducts an excellent activity for settling international conflicts peacefully, and its jurisdiction is voluntary. Furthermore, 38 states have agreed to the compulsory jurisdiction of the court out of 54 states as an exception to the principle of voluntary jurisdiction (Derbash, 2012).

ICJ has gone in the same direction as the international Judiciary in connection with the principle of supremacy of international law over national law. Moreover, any state is not entitled to argue its domestic laws before the other states to escape its obligations imposed by international law (Al-Fatalawi, nd).

This is in addition to its decision in the case of the nationals of the United States of America in Morocco rendered in 1952, where it has held that the Moroccan decrees issued in 1948 were contrary to the treaty previously concluded between the United States of America and Morocco. This confirms the principle of supremacy of international law over domestic law, whether the source of the former is an international custom or treaty (Rashid, 2014).

iii. The extent of Violation by Cybercrimes of the Principle of Sovereignty

Owing to the technological advancement of the modern era and the emergence of new types of cybercrimes have led to the development of the concept of sovereignty to include the imposition by the state of its powers on the virtual territory represented by databases and information systems subject to the state that is called "Digital Sovereignty" (Moussa, 2013).

The widespread use of the Internet has impacted various fields, including government and academic curricula, affecting states' physical territorial borders. States have adopted electronic storage of information and data, allowing other states to control it due to progress in informatics and domination of the software industry (Meliany, 2018).

The prominence of the term "Cyber Sovereignty" was due to the confrontation of the effects of internet globalization that exceeded the capability of states to maintain their sovereignty and borders, particularly after the

infiltration of information to the nationals of the state in a way that diminishes the limits of sovereignty and imposes a breeding ground of space globalization where there are no state and no homeland (Naous, 2015).

Therefore, any act done via the Internet targeting the authorities and institutions of the state is deemed to be a cybercrime against the state sovereignty (Soaady, 2017).

II. Cybercrimes and the Principle of Non-Interference

Preamble and Division

Any legal system aiming at achieving specific interests through its regulation according to logical methodology making available its targeted protection and Public International Law aims at the same goal, which is the regulation of relations among the persons of Public International Law (Tayeb, 2016).

It is noteworthy that most of the relevant international agreements in connection with the regulation of using combat methods and means have been concluded at a time when the use of the internet was not known. The means of modern telecommunications were not known as it is currently known in a way that it was logical that there were no legal provisions regulating clearly and directly the use of cyber-attacks (Rex, 2010).

a. The situation of International Instruments and Agreements concerning the Principle of Non-Interference

i. Principle of Non-Interference in the UN Charter:

The UN Charter's Article 2 states that it cannot intervene in domestic matters or require Member states to settle them. However, this principle is complicated due to rapid technological advancements and cybercrimes threatening national security. Chapter VII allows exceptions for temporary measures in cases of peace threats or aggression.

The UN Charter's Paragraph 7 of Article 2 is criticized for not specifying matters related to internal affairs, potentially putting the Security Council and International Organizations in a critical situation. The development of the international community is crucial for allowing room for future developments, especially in the age of advanced technology and cyber criminality. The UN General Assembly has adopted numerous resolutions No. (A/RES31/2131) / No. (A/RES 24/2625)/ No. (A/RES 9/103/39) urging non-interference in other states' internal affairs. (Altam, 2017).

ii. Principle of Non-Interference in the Charter of League of Arab States:

Article 2 of the Charter of the League of Arab provides that " The purpose of the league is to promote the relations among the states participating in it and to coordinate their political plans for achieving cooperation among them, maintaining their independence and sovereignty and deliberating the affairs and interests of Arab states.

As regards the cyber-attacks and the principle of non-interference, we note that the more significant challenge facing their regulation from the international legal aspect and the inexistence of an international will, whether on the legal level represented by the resolutions of the Security Council or diplomacy via international negotiations. In return, there is a rapid technological advancement that has become capable of infiltration and penetration as well as the violation of the principle of non-interference for any state and causing damage to it in a way that could be described as direct aggression of vital institutions of the state (Nemaa, 2018).

This challenge has raised a type of vagueness in connection with the capability of Public International Law and International Humanitarian Law to curb the effects of cyber-attacks concerning the violation of the principle of non-interference in the internal affairs of states where some jurists state that most of the cyber-attacks are based on operations that do not meet the standards intended by international law to regulate (Vida, 2005).

The great seriousness of resorting to cyber-attacks has pushed the United Nations General Assembly to be interested in beginning international negotiations among the states to urge them to regulate Cyberspace following the rules of international humanitarian law. There have been many resolutions adopted in this regard, but they are not attractive to the international bodies concerned with the beginning of international negotiations (Resolutions of the UN General Assembly).

b. The situation of International Courts concerning the Principle of Non-

Interference

i. Situation of the Permanent Court of International Justice (PCIJ) concerning the Principle of Non-Interference:

The PCIJ was the first international arbitration panel in the advisory function. This court was established to help The League of Nations and its council. However, it achieved a great benefit from this function in a way that led to helping the states in addition to these two bodies above.

Moreover, the PCIJ exercised a preventive function for settling international disputes. It contributed to avoiding getting involved in complex and lengthy judicial procedures for settling disputes. The advisory function exercised by this court resulted in achieving progress in the area of international law (Samson, 2013).

The PCIJ heard nine cases from 1922 to 1923, including three cases in the first session, Tunis-Marokko Nationality Questions, four cases in the second session, and the Jaworznia Question in its second extraordinary session.(Hudson, 1934).

ii. The situation of the International Court of Justice concerning the Principle of Non-Interference:

The ICJ's inability to hear domestic cases raises confusion about non-interference and state scope, while concerns like cyber criminality and human rights now fall under international community concerns. Regarding the research subject matter, we often find that a group of individuals declare their responsibility for cyber-attacks. How does international law intervene in regulating such legal positions?

To answer this question, we must rely on the international judicial precedents connected with this problem to understand international courts' orientations. The ICJ stated while characterizing the fact of intervention that it has been proved to the court that the United States of America had a role in training and arming the Contras in Nicaragua and equipping them with modern telecommunications means.[5] We note that The ICJ has established the responsibility of the United States of America for the intervention in the internal affairs of Nicaragua in addition to bearing the consequences of their behavior contrary to the rules of Public International Law.

In the Tadic Case, the state responsibility has been established for the commission of violations by armed groups supported by this state before The International Criminal Tribunal for Former Yugoslavia ICTY. The decision of the

[5] Case: Prosecutor V. Tadic, 1995, Para, 70.

court has focused on the standard of full control stating that "The state had a role in organization and coordination as well as supporting the armed group and this means that it has full control over it and what is done by the armed groups is deemed to be done by the state itself[6].

c. The Extent of Violation by Cybercrimes of the Principle of Non-interference

The principle of non-interference is deemed to be one of the fundamental principles under Paragraph 7 of Article 2, which provides that "Nothing contained in the present Charter shall authorize the United Nations to intervene in matters which are essentially within the domestic jurisdiction of any state or shall require the Members to submit such matters to settlement under the present Charter, but this principle shall not prejudice the application of enforcement measures under Chapter Vll" (Ali, 2017).

Besides, the United Nations has paid great attention to the principle of non-interference in many resolutions adopted by it, including resolution No 25/26 on The Declaration of Principles of International Law for The Friendly Relations among States involving "It is mandatory not to intervene directly or indirectly in one of the states for any reason also it is mandatory not to use economic or military measures for forcing the states to leave the exercise of their sovereign rights to get any advantages" (Ghadhban, Mabrouk, 2001).

Although the principle of non-interference is one of the fundamental principles in Public International Law, it raises many problems, particularly with the emergence of cyber criminality and its impact on the extent of compliance with this principle. The vast and fast development of contemporary techniques and technology has affected the concept of the principle that moved from the absolute concept to the relative one (Maziti, 2018).

Cyber Security is deemed to be one of the most prominent elements of untraditional national security where the offender out of the users of Cyberspace can cause significant losses and the paralysis of the information infrastructure of the state resulting in enormous economic and military losses represented by cutting off the communication among the military units with each other as well as capturing their secret information (Khalifa, 2019)

The United States of America had the initiative to agree with China during peacetime to avoid launching cyber-attacks against the US information infrastructure or private sector companies in a way that makes the commission of crimes between states each other a severe violation of the principle of non-

6 http://www.icj-cij.org/docket/files/90/13685.pdf visited on 10/2/2022.

interference in the internal affairs of the other states and it could be characterized as cyber terrorism (Mansour, 2019).

NATO had the initiative to invite a group of international law experts to prepare this manual in the presence of the International Committee of Red Cross (ICRC). This manual is deemed the only legal document that governs assaults between states. It consists of 95 rules, most of which have been taken from the various rules of international law, such as the UN Charter and the rules of International Humanitarian Law, among other things (Abdelsadik, 2018)

Tallinn Manual has attempted to address the defectiveness of the rules of international law in connection with cybercrimes. Rule 1 of the Tallinn Manual provides that "The state shall exercise its control over the cyber enterprises and the relevant activities within the scope of its territorial sovereignty" (Al-Zahwani, 2017). Moreover, Rule 2, about jurisdiction, also states, "The state shall exercise its jurisdiction over the persons exercising the cyber activities inside its national territory." Rule 4 states that "any intervention by a state in the cyber enterprises of another state shall be deemed to be a violation of its sovereignty"[7].

There is a criticism connected with this manual that it is non-binding and does not mount to the level of international agreements in addition to the opposition by Russia and China of its provisions in reliance on their non-participation in its preparation and that it does not observe the global representation of states as for the selection of qualified experts for it.

Results

- There is no international agreement on the concept of cyber in a way that requires concerted international efforts to encounter this defectiveness being considered the basis for any international agreement regulating it in the future.
- Despite the stable rules of contemporary international law about the illegitimacy of using force or threatening to use it in international relations, there are many explanatory frameworks connected with cybercrimes and cyber-attacks revolving around the interpretation of the term "Force." One of these frameworks relies on the standard of the movement-related element of armed forces, and the other broadens the interpretation to include all forms of use of force so long as it explicitly violates the state's national security.
- There are difficulties in applying the rules of public international law with cybercrimes, but it is impossible to give a broader interpretation of the principles of international law.

[7] Available at the following website visited on 1/2/2022 http://www.ohchr.org/ar/Issues/digitalage/pages/DigitalAgeIndex.aspx.

Conclusion

This study shows that the confrontation of the problems of cybercrimes is a necessary matter in light of what is witnessed by the contemporary world about the imposition of adverse uses of modern technology. Besides, there has been a mutual influence between technological advancement and its challenges as well as the capability of international law and the international community of being adapt to them where states can have the pretext connected with the oldness of international law agreements to justify the launch of cyber-attacks without the existence of legal provisions regulating them.

It has been shown that international efforts actively attempt to control cyber-attacks. Even though these efforts are slow, they indicate an increase in international awareness related to the seriousness of these cybercrimes. In all cases, it is taken for granted that cyber-attacks will never cease. Thus, the states have to prepare early for the confrontation of the probable risks to maintain the infrastructure that directly affects the daily life of citizens.

To complete the benefit and the objective of this study, the two scholars show the most important results and recommendations that have been reached and which we hope that they will contribute to raising awareness in connection with the seriousness of cybercrimes and the necessity of regulating them to achieve the effective protection of citizens under international law.

References

Abdelrahman, M. Y. (2014). *Humanitarian Intervention in International Relations*, Emirates Center for Strategic Studies and Research, Abu Dhabi, P.22.

Abdelsadik, A. (2018). *Weapons of Cyberspace in Light of International Humanitarian Law*, 1st ed., Egypt, Arab Center for Cyberspace Research, Cairo, P.19.

Al-Bouqairat, A. (2014). Lectures on Sovereignty and Globalization, delivered to Master students in University of Algiers, P.3.

Al-Fatalawi, S. H. (nd). Waseet on Public International Law, P.449.

Al-Fatalawy, S. H. (2012). *Waseet on Public International Law*, 3rd ed., Lebanon, Arab Thought House, Beirut, P.465.

Ali M. K. (2017). *Principle of Non-Interference and Its Exceptions in Contemporary International Law*, 2nd ed., Lebanon, Law Aleppan Publications, Beirut, P.8.

Al-Magzoub, M. (2013). *Public International Law*, 4th ed., Lebanon, Halaby's Legal Publications, Beirut, P.369.

Al-Qahwagy, A. A. (2009). *Criminal Protection of Electronically Processed Data*, 3rd ed., Lebanon, Law Aleppan Publications, Beirut, P.50.

Al-Saady, A. H. (2012). *Criminal Responsibility of Individual for International Crime*,3rd ed., Dar Matboaat Gamiaa, Alexandria, P.63.

Altam, S. et al. (2017). *Cyclopedia of Agreements of International Humanitarian Law, Official Texts of Agreements and States Ratifying them*, 9th ed., International Committee of Red Cross in Cairo, P.46.

Al-Zahwani, Y. M. (2017). Strategic and Legal Dimensions of Cyber Warfare, *Research and Studies Journal of Wady University*, 23 (248).

Beraam, G. (2015). *Impact of Development of Cyber War Technology on Power Building in Israel*, Research Translated into Arabic, Foundation for Palestinian Studies, P.125.

Derbash, M. O. (2012). *Jurisdiction of International Court of Justice as For Settlement of Disputes: A Legal Study on Lockerbie Case*, 3rd ed., Libya, Al-Dar Al-Gamaheria for Publication, Distribution and Advertising, P.91.

Gassem, F. D. (2016). Impact of the Internet on The Principle of Sovereignty, *Journal of College of Law*, 18(2), 86

Ghadhban, M. (2001). *International Regulation and International Organizations*, 3rd ed., Egypt, University Publications, Cairo, P.179.

Gist of Resolutions of the UN General Assembly as regards Cyber Attacks as Follows: A/RES /55/28 of 20/11/2000, A/RES /59/61 of 3/12/2004, A/Res/61/54 of 6/12/2006, A/RES/62/17 of 5/12/2007.

Hamdy, S. A. (2012). *Studies on Public International Law*, Algeria, 3rd ed., P.354.

Hudson, M. (1934). The Twelfth Year of the Permanent Court of International Justice. *American Journal of International Law*, *28*(1), 1-18. doi:10.2307/2190290

Khalifa, E. (2019). *Impact of Fourth Industrial Revolution on National Security: Post-Information Society*, 1st ed., Egypt, Alaraby House For Publication and Distribution, Cairo, P.136.

M.G. Samson and D. G. (2013). *The Permanent Court of International Justice and The Invention of International Advisory Jurisdiction, in Legacies of The Permanent Court of International Justice* (des, C.J. Tams M., Fitzmaurice and P. Marcours) Leiden, Neuhoff, P.45.

Mabrouk, G. (2015). *Collision Between Globalization and Sovereignty: Human Rights as A Model*, Lecture Delivered at Setif University, Algeria, P.17.

Mansour, S. A. (2019). *Generation 5 Wars- Methods of Explosion from Within on International Level*, 1st ed., Egypt, Alaraby House for Publication and Distribution, Cairo, P.142.

Maziti, M. (2018). *Shadow Wars- US New Secret Wars*, Translated by Anton Basil, 4th ed., Lebanon, Publications Company, Beirut, P.123.

Meliany, D. M. (2018). Electronic Communication Surveillance in Algerian Legislation, *Journals of Bechar University* –Faculty of Law and Political Science, 1(16), 210, Tahri Mohammed University.

Moussa, M. A. (2013). *Electronic Surveillance via The Internet- A Comparative Study*, 3rd ed., Egypt, Legal Books Publishing House, Cairo, P. 192.

Naous, M. E. (2015). State Sovereignty in Cyberspace, *Journal of Sharia and Law*, 52(36), 136, University of United Arab Emirates University.

Nemaa, A. A. (2018). Cyber Attacks: Their Concept and International Responsibility for Them in Light of Contemporary International Regulation, *Investigator Journal of Legal and Political Sciences*, 12(8),116, College of Law, Babylon University, Iraq.

Rabbah, M. (2021). Legal Nature of Cyber Attacks Occurring Among States, 1st ed., *Research in Voice of Law Journal*, Institute of Law and Political Science, University Centre of Tipasa, Faculty of Law, University of Algiers, 8(1),539.

Randa, H. (2018). *Cyber Weapon in Israel's Cyber Wars*, 1st ed., Lebanon, Foundation for Palestinian Studies, Beirut, P.118.

Rashid, S. (2014). *International Human Rights Law and Constitutions*, Ph.D. Thesis, College of Law – University of Mosul, Iraq, P.77.

Rex H. (2010). A Treaty for Cyberspace, the Royal Institute of International Affairs, *International Affairs Journal*, 86(1),533, Blackwell Publishing Ltd.

Serag, A. M. (2011). *Principle of Integration in International Criminal Judiciary- An Origin Finding Analytical Study*, 3rd ed., Egypt, Dar Nahda Masria, Cairo, P.36.

Soaady, M. (2017). Digital Sovereignty and Challenges of Internet as For the Principle of State Sovereignty in Public International Law, *Journal of Jurisprudence and Law*, 6(1), 64.

Tayeb, M. (2016). *Legitimacy of Encountering Security Council Resolutions- The Right of State and Judicial Jurisdiction*, 3rd ed., Advisory Centre For Studies and Documentation, P.52.

Vida M. A. J. (2005). Defining the Parameters of Cyber War Operations: Looking for Law in All the Wrong Places, *Naval Law Review*, 51, 134.