*Quest Journals*
*Journal of Education, Arts, Law and Multidisplinary*
*Volume 13 ~ Issue 1 (Jan. – Feb. 2023) pp: 52-57*
*ISSN(Online): 2347-2895*
www.questjournals.org

**Research Paper**

# The International Legal Regime and Cybercrime

Kelvin Bribena Ph.D
*Faculty of law, Niger Delta University,*
*Wilberforce island, Bayelsa State, Nigeria.*

***Abstract***
*Bearing in mind the magnitude of cybercrime and the potential to impact negatively on the global community, the need for concerted action by all States cannot be overemphasized. This is more so as national effort and legislation cannot adequately deal with the transnational nature of cybercrime. Although, most States have legal frameworks designed to deal with the problem, nevertheless, the diversity in legal systems and attendant substantive and procedural laws of various jurisdictions have hindered the effective enforcement of cybercrime laws at the international level. The doctrinal research method was used for proper evaluation of primary and secondary sources of legal data and declassified informational materials for the purpose of inferences. The work found that international cooperation is crucial to the successful detection, apprehension and punishment of cybercrimes around the world. The paper examined the increasingly debilitating effect of cybercrime, the efforts being made by the international community to combat the scourge through conventions, legislation and recommended practices. The work emphasized on the international cooperation mechanisms that have been developed to combat cybercrimes around the world. To ensure uniformity in the responses of States, the paper recommended the need for an international regime, backed up by an international tribunal to try offenders or perpetrators of cybercrime. Existing national and regional laws and enforcement mechanisms should be galvanized to provide the much-needed impetus for international cooperation.*

***Keywords:*** *Cybercrimes, cyberspace, regional, international convention and legal regime.*

## I. Introduction

The advancement of information and communication technology has aided the fast and free flow of information across the globe. Cyberspace, also referred to as the world's "information superhighway," transcends national boundaries and physical frontiers. Despite its benefits, this advancement has inadvertently promoted a variety of illegal activities collectively referred to as cybercrime. Geographical location, time, or the legal jurisdiction of their intended victims do not constrain those who participate in these actions.

Coordination between countries is crucial because to the prevalence of cybercrime and the potential to seriously affect the global society. Crimes that are easily transboundary cannot be adequately addressed by national laws alone. Despite the fact that many nations have developed legal frameworks to combat cybercrime, it has proven challenging to implement cybercrime policies globally due to variations in legal traditions, practices, and substantive laws. Therefore, global collaboration is essential for locating, pursuing, and punishing cybercriminals.

This research examines the increasing seriousness of cybercrime and examines the measures the international community is attempting to combat it through laws, treaties, and suggested best practices. It emphasizes the significance of the structures for international collaboration that have been put in place to fight cybercrime worldwide.

### The Character and Scope of Cybercrime as a Global Concern

Any illegal activity that uses a computer to carry out the crime or store relevant evidence is considered cybercrime.[1] Computer-related crime is defined as "any illegal, unethical, or unauthorized conduct involving

[1] Computer-related criminality; Analysis of Legal Politics in the OECD Area (1986).

automated data processing or data transmission"[2] in the 1986 OECD Recommendations. Cybercriminals might be private citizens or members of the government.[3]

For instance, a person going by the handle "MafiaBoy" launched a string of denial-of-service (DoS) operations against well-known websites like CNN, Yahoo, Amazon, and eBay in February 2000. States have also been linked to cybercrime activities: in 2005, the Chinese cyber-espionage group "Titan Rain" gained access to aerospace companies, defence contractors, and U.S. military networks.[4] Similar to this, Estonia had extensive cyberattacks in 2007 that disrupted credit card and ATM networks, disabled parliamentary email services, and targeted political parties, large banks, and government agencies.[5] The majority of these attacks were linked to Russian IP addresses. Cyberattacks from Russia targeted Georgia's government and civilian digital networks during the 2008 conflict between Georgia and Russia. These operations, which frequently used Distributed Denial-of-Service (DDoS) techniques, were designed to interfere with communication networks and get military and political intelligence.[6]

Because the internet is worldwide and borderless, cybercrime is by its very essence international. Since victims and perpetrators are frequently located in several nations and attacks might occur concurrently in several jurisdictions, national laws by themselves are insufficient. The jurisdictional issues that can come up during cybercrime investigations are demonstrated by the case United States v. Gorshkov. Many nations lack the legal frameworks required to pursue crimes committed outside of their boundaries, even if some permit their courts to have extraterritorial jurisdiction.

Significant economic repercussions of cybercrime further solidify its standing as a global issue. Cybercrime damages the world economy more than USD $445 billion a year, according to a June 2014 report by McAfee and the Centre for Strategic and International Studies.[7] This amount accounts for both direct and indirect losses, including money theft, intellectual property theft, compromised sensitive data, opportunity costs, higher cybersecurity costs, recovery efforts, and reputational harm to impacted organizations. Strong international collaboration is essential because law enforcement authorities are under tremendous pressure to detect perpetrators.

**A Regime of Regional/International Cooperation**

Because cybercrime is intrinsically transnational, only international cooperation can result in effective regulation. It is crucial to harmonize these disparate frameworks because every nation has its own legal system. When states strive to harmonize and integrate their disparate approaches to cybercrime, international legal cooperation takes place.[8] International model laws, especially those created under the United Nations, can help eliminate jurisdictions where offenders might otherwise find protection because the same legal standards would apply across participating countries. This is one way to achieve this harmonization. Inconsistencies between country legal systems are frequently used by criminals. US v. Gary McKinnon, in which a system administrator from the UK gained access to 97 U.S. military and NASA systems from his home, is a prominent example. McKinnon's legal team fought extradition, claiming that the crime was committed exclusively in the United Kingdom, despite the fact that U.S. officials filed charges against him in 2004 and issued arrest warrants.[9] Their plan was based on the fact that the maximum penalty under the UK Computer Misuse Act was only five years, as opposed to the 70-year term he might receive in the US for violating military networks.

The development of regional and international tools to combat cybercrime also strengthens international cooperation.[10] Harmonizing national laws can be facilitated by both legally binding treaties and non-binding arrangements. The fact that these agreements exist shows that member states are committed to fighting cybercrime

[2] Maskun, Alma Manuputty, SM Noor, Juajir Sumardi, "Legal Standing of Cyber Crime in International Law Contemporary" Journal of Law, Policy and Globalization Vol 22, (2014) p 128

[3] Wavefront Consulting Group,"Brief History of Cybercrime" available at www.wavefrontcg.com/A_Brief_History_of_Cybercrime-4, html accessed 22 February 2023.

[4] Andrzej Kozlowski, "Comparative Analysis of Cyber-attacks on Estonia, Georgia and Kyrgyzstan" European Scientific Journal /Special/ edition Vol 3 (February 2014) P 239.

[5] Andrzej Kozlowski, "Comparative Analysis of Cyber-attacks on Estonia, Georgia and Kyrgyzstan "ibid 240.

[6] Maskun, Alma Manuputty, SM Noor, Juajir Sumardi, "Legal's Standing of Cyber Crime in International Law Contemporary" op cit, p 128.

[7] 2001 W1 1024026

[8] Section 1029 of the USA Patriot Act of 2001 and sections 4 and 5 of the UK Computer Misuse Act of 1990 provide for exterritorial jurisdiction

[9] Center for Strategic and International Studies, "Net Losses: Estimating the Global Cost of Cybercrime Economic impact of cybercrime II" June 2014 p3.

[10] 18 U.S.C.1030

and upholding common norms. These treaties usually contain clauses that promote collaboration, like extradition and mutual legal aid guidelines, which help states collaborate more successfully.[11]

To combat cybercrime, a number of regional and international tools have been created. While some are just meant to serve as guidelines for creating national laws, others have legal power for the governments that ratify them.[12] At least 82 nations had ratified or signed a legally binding cybercrime pact by 2013, and several of them were parties to multiple agreements. However, there isn't yet a single, global treaty on cybercrime, and all of the current instruments are still regional in nature. Many binding instruments have common aspects, such as jurisdiction, investigative powers, criminalization criteria, and international cooperation mechanisms, despite variations in their focus or scope.[13] The cooperation-related clauses in a few of these important treaties are reviewed in the sections that follow.[14]

**The Convention on Cybercrime of the Council of Europe 2001**

The first international agreement devoted only to addressing cybercrime is the Convention on Cybercrime, also referred to as the Budapest Convention.[15] Adopted by Council of Europe member states in Budapest in 2001, it was also made available for membership by other willing nations and for signature by non-member governments that helped write it. Legally, it went into force on July 1, 2004. The Council of Europe introduced this Convention to strengthen international cooperation against cyber-related offences as part of its larger role in influencing criminal policy among its members.[16] The Convention serves as a framework for cross-border cooperation among participating states as well as guidance for nations creating their own national cybercrime legislation.[17]

Despite being started by the Council of Europe, nations like the United States, Canada, Japan, and South Africa actively participated in the treaty's draughting and signed it. In 2006, the United States became a full party to the Convention after ratifying it. States pledge to make the types of behaviour outlined in the Convention's substantive criminal law provisions illegal by ratifying or acceding to it.[18]

The Convention covers international cooperation mechanisms and procedural standards in addition to substantive criminal law. Its main goals are to create a quick and effective system of international cooperation, develop sufficient procedural authorities to investigate and prosecute acts involving computer systems or electronic evidence, and harmonize national criminal laws pertaining to cybercrime.

The Convention lists a number of offences and associated legal provisions in order to accomplish these goals. Nine crimes are identified and divided into four categories. The first category includes offences such as unauthorized access, unlawful interception, data interference, system interference, and device misuse that target the confidentiality, integrity, and availability of computer systems and data. Computer-related offences including computer-related fraud and forgery fall under the second category. Crimes pertaining to content, such as those connected to child pornography, fall under the third category. The fourth category focusses on violations of copyright and related rights. The Convention also contains clauses pertaining to corporate culpability, attempt, aiding or abetting, and punishment. Additionally, it outlines procedural authorities including production

[11] UNODC, Comprehensive Study on Cybercrime (United Nations, New York 2013) p 63

[12] UNODC, Comprehensive Study on Cybercrime (United Nations, New York 2013) p 65.

[13] Judge Stein Schjolberg, (Ret.), "Crossing Jurisdictional Boundaries" A presentation at the Europol-INTERPOL Cybercrime Conference September 24-25, 2013 Europol Headquarter the Hague, The Netherlands p 3

[14] A universal international legal instrument in this regard will be a Convention having a very broad scope such as a United Nations Convention.

[15]

[16] Murdoch Watney, "Regulation of State Surveillance of the Internet" in Sachar Paulus, Nobert Pohlmann, Helmut Reimer (Eds) ISSE 2006 Securing Electronic Business Processes: Highlights of the Information Security Solutions Europe 2006 Conference (Springer Science & Business Media) p.418.

[17] States such as Argentina, Botswana, Egypt, Nigeria, Pakistan and the Philippines have modelled parts of the legislation on the Convention without formally acceding to it. See UN Secretariat, "Recent developments in the use of science and technology by offenders and by competent authorities in fighting crime, including the case of cybercrime" 12th United Nations Congress on Crime Prevention and Criminal Justice Salvador, Brazil, 12-19 April 2010 A/CONF.213/9 para, 33.

[18] Maskun, Alma Manuputty, SM Noor, Juajir Sumardi, "Legal's Standing of Cyber Crime in International Law Contemporary" op, cit. p. 131. Chapter II of the Convention provides for Measures to be taken at the national level. This includes the adoption of substantive law to incriminate certain acts in relation to computer system and data (section 1 Art. 2 - 13). It also includes the adoption of procedural laws to establish the powers and procedures provided for the purpose of specific criminal investigations or proceedings. (section 2 Article 14-21).

orders, real-time traffic data collection, content data interception, search and seizure of computer data, partial disclosure of traffic data, and expedited data preservation.

The Convention places a great deal of emphasis on international collaboration. States parties agree to work together "to the widest extent possible" in order to gather electronic evidence for any criminal offence and to investigate and prosecute cybercrime. The treaty contains provisions pertaining to mutual legal assistance and extradition. The Convention's procedural principles apply where there is no existing agreement governing mutual assistance between nations; but, if a separate treaty is already in force, its terms take precedence unless the parties agree differently.

In order to hasten the preservation of electronic data located within the requested state, mutual cooperation may be sought. Each state must make sure it has the legal authority to keep computer data for as long as necessary to formulate and execute a formal request for mutual aid, as information can be swiftly destroyed or altered. States can also ask for the quick release of traffic data that has been retained. A state shall immediately reveal enough traffic data to identify the provider and the communication route if, during the course of executing a preservation request, it learns that the communication was transmitted by a service provider in another nation.

States may also ask to view computer data that has been stored. Each state must be entitled to seek, access, seize, secure, or disclose data kept through computer systems within its borders on behalf of another state in accordance with this clause.

Regardless of where the data is physically located, the Convention allows member states to access publicly available stored computer data without requiring permission from another Party. Additionally, if a Party has secured the lawful and voluntary approval of the person authorized to release the data, it permits the Party to access or obtain stored data situated in another State using a computer system inside its own territory. This implies that access is allowed if consent is obtained or if the information is already accessible to the general public.[19]

Parties must also cooperate with each other in the real-time gathering of traffic data associated with particular communications that take place on their territory and are sent via computer systems. Parties must also provide mutual assistance in the real-time capture or recording of content data, but only to the extent allowed by their respective national laws and any applicable treaties. Therefore, each State's legislative structure limits the requirement to collaborate in intercepting content data.

However, it has been observed that the Convention is out of date when it comes to dealing with the more sophisticated cyberthreats of today because it reflects illicit cyber actions characteristic of the late 1990s.

Professor Marco Gercke also opined concerning the Convention on Cybercrime as follows:[20]

The list of reasons why the Convention did not succeed at global level is complex. It starts with a missing involvement of developing countries in the drafting process, a more demanding accession procedure compared to UN Conventions, a lack of updates in response to trends, the absence of regulations for electronic evidence and liability of Internet Service Provider (ISP), missing field offices outside Europe and maybe most importantly, a lack of supporting capacity building that is especially relevant for developing countries.

This view clearly sums up the inadequacy of the Convention on Cybercrime and the need to elaborate a new Convention that will take cognizant of identified lapses for a more comprehensive and up to date international regime.

**The African Union Convention on Cyber Security and Personal Data Protection 2014**

Adopted in July 2014, the African Union Convention is an early attempt to establish a common legislative framework for data protection and cybersecurity throughout Africa. Promoting uniform cybersecurity laws among AU member states is its main goal. The AU took into account the obligations that nations already have at the sub-regional, regional, and international levels while also recognising the significance of creating broad strategic guidelines for fighting cybercrime.[21]

By promoting the development of ICT-specific offences and coordinating punishments, offences, and criminal liability systems among member states to reflect the digital environment, the Convention essentially seeks to modernize the battle against cybercrime. It also specifies the requirements for starting proceedings especially connected to cybercrime and describes how conventional criminal procedures should be modified for ICT environments.

[19] Aldo Shkëmbi, Darjel Sina, "Cybercrime in the Perspective of the European Legal Framework" Mediterranean Journal of Social Sciences MCSER Publishing Rome-Italy Vol 4 No 9 (October 2013) p 328.

[19] See Council of Europe Treaty Series, "Explanatory Report to the Convention on Cybercrime Budapest, 23.XI.2001" European Treaty Series-No. 185 Para.16 4.

[20] In Marco Gercke "10 years Convention on Cybercrime" Computer Law Review International, Issue 5 15, October 2011, 129-160, see cr-international.com. See also his website www.cybercrime.de,

The Convention mandates that State Parties' laws and regulations uphold the dual criminality concept and promote regional harmonization in order to foster international cooperation.[22] By encouraging states without mutual legal aid agreements to seek such accords—again based on dual criminality—it further strengthens cooperation. Additionally, the Convention encourages the creation of institutions devoted to exchanging intelligence on cyberthreats and facilitates efficient data sharing and information exchange at the bilateral and international levels. [23]To strengthen cybersecurity, address cyberthreats, and foster stakeholder communication, states are urged to make use of the public-private, intergovernmental, regional, and international cooperation structures that are currently in place.[24]

The Convention has not yet come into effect since there have not been enough ratifications, despite its progressive provisions.[25] A lack of proper cybercrime laws, faster internet usage growth,[26] and more reasonably priced internet connection have all contributed to the perception of Africa as a cybercrime hotspot, according to recent studies.[27] African governments must take proactive measures to address this issue, such as making cybercrimes illegal,[28] harmonising their legal systems, and strengthening international cooperation.[29]

**In the direction of a United Nations Convention on Cybercrime**

As said before, there is no internationally standardized legal framework that addresses cybercrime at the moment.[30] Participants demanded the establishment of a worldwide cybercrime treaty during the four regional preparatory sessions for the Twelfth United Nations Congress on Crime Prevention and Criminal Justice.[31] Meetings of the Heads of National Law Enforcement Agencies from Africa, the Near and Middle East, and Europe[32] also showed that judicial systems and law enforcement agencies were unable to handle electronic evidence necessary for prosecutions or effectively combat evolving forms of cybercrime. It was generally accepted that in order to facilitate investigation, prosecution, and conviction based on digital evidence, national laws needed to be amended because they were out of date.[33]

The difficulties presented by current regional mechanisms were brought to light at the Twelfth UN Crime Congress. These include the slow rate of signatures and ratifications in comparison to international expectations and their restricted scope, as they only apply to member states of particular organizations. As a result, the Secretariat suggested that the creation of an international convention against cybercrime be given careful thought. In order to offer a global platform that focusses on developing nations, the United Nations Office on Drugs and Crime (UNODC) was tasked with combining its legal, technical, and law enforcement experience with that of other partners involved in the fight against cybercrime. It was also charged with educating law enforcement organizations on how to use instruments for international cooperation.[34]

After that, the Commission on Crime Prevention and Criminal Justice was directed by UN General Assembly Resolution 65/230 to form an open-ended intergovernmental expert group in order to carry out a thorough investigation of cybercrime and international responses to it.[35]

The necessity to safeguard the entire world community is driving the push for the ratification of a United Nations treaty on cybercrime. Global security is at risk, as analysts point out, and cyber threats are no longer limited to certain countries. States recognized their obligation to adequately address new cyberthreats at the Thirteenth UN Crime Congress, which took place in Doha in April 2015. The UN was given the responsibility of

[22] Chapter II Section 1.
[23] Article 2 of the Convention on Cybercrime of the Council of Europe 2001.
[24] Article 3 ibid.
[25] Article 4 ibid.
[26] Article 5 ibid.
[27] Article 6 ibid
[28] Article 7 ibid.
[29] Article 8 ibid.
[30] Article 28(4) ibid
[31] 15 States out of the 54 States that make up the African Union will need to ratify the text of the Convention for it to come into force. (Art.36). However, the Convention has received no ratification till date
[32] Eric Tamarkin, "The AU's cybercrime response: A positive start, but substantial challenges ahead" Institute for Security Studies Policy Brief 73 January 2015
[33] UN Secretariat, "Recent developments in the use of science and technology by offenders and by competent authorities in fighting crime, including the case of cybercrime" 12th United Nations Congress on Crime Prevention and Criminal Justice Salvador, Brazil, 12-19 April 2010A/CONF.213/9 Para.36.
[34] UN Secretariat, "Recent developments in the use of science and technology by offenders and by competent authorities in fighting crime, including the case of cybercrime" 12th United Nations Congress on Crime Prevention and Criminal Justice Salvador, Brazil, 12-19 April 2010 A/CONF.213/9 Para.37
[35] 12th United Nations Congress on Crime Prevention and Criminal Justice Salvador, Brazil, 12-19 April 2010.

investigating strategies for preventing online criminal activity and building a safe and secure cyberspace. In order to improve existing responses and create new national or international measures to combat cybercrime, states also committed to exchange information on laws, best practices, technical support, and opportunities for international collaboration.

**International Cooperation on Judicial Enforcement of Cybercrime Laws**

Strong judicial action and efficient enforcement of cybercrime legislation are essential for dealing with cyber offences. A common international legislative framework and cross-border cooperation amongst law enforcement organizations are both necessary to combat cybercrime. Many serious attacks might go unpunished if there isn't an international court devoted to dealing with serious cybercrimes that impact several nations. Discussions about how to accomplish global judicial enforcement have been sparked by this divide. The International Criminal Court (ICC) has been proposed by the UN as a potential venue for prosecuting cybercrimes that have a substantial influence on many countries.

Since large-scale, coordinated cyberattacks on vital information systems may qualify as serious crimes under Article 93, Paragraph 10(a), the ICC is thought to be equipped to handle such offences under its existing mandate. According to Stein Schjolberg:

If massive and coordinated global attacks in cyberspace are included in the jurisdiction of the International Criminal Court, the Rome Statute has Articles on investigation, prosecution and three divisions of Courts for normal and formal proceedings.[36]

Since the ICC now only has 123 member states,[37] it is unclear how effective its worldwide reach will be. This implies that nations outside of its membership may turn become safe havens for global cybercriminals. Given that cybercrime has grown to be a global problem, it has been suggested that more countries could be inclined to join the Rome Statute if the ICC's jurisdiction were extended to include worldwide cyberattacks.

Some experts have also suggested establishing a distinct organization known as the International Criminal Tribunal for Cyberspace (ICTC) or a specialized International Criminal Court for Cyberspace as a division of the ICC in The Hague.[38] According to a draft UN treaty, such a court or tribunal should be given the power to bring charges against those behind the most serious cyberattacks and cybercrimes of international importance. Because the tribunal would have authority over natural persons, people might be held directly responsible for these crimes. Only the most serious cybercrimes that endanger the global society would fall under its purview.[39] Information from a variety of sources, including states, UN agencies, intergovernmental organizations, and non-governmental organizations, would serve as the basis for investigations under this tribunal. The Office of the Prosecutor would have the authority to collect evidence, conduct a variety of cyber investigations, and ask for assistance from foreign law enforcement organizations that are partnered with INTERPOL.[40]

## II. Conclusion

This study acknowledges that disparities in legal systems, substantive legislation, and procedural regulations among jurisdictions might impede successful international collaboration after evaluating the scope and character of cybercrime and the pressing need for coordinated worldwide response. The report suggests creating an international framework backed by a worldwide court tasked with punishing cybercrime offenders in order to encourage uniformity in how states address cyberthreats. In order to better facilitate international cooperation, it also recommends that existing national and regional regulations, as well as their enforcement mechanisms, be reinforced and unified.

[36] Judge Stein Schjolberg, "An International Criminal Tribunal for Cyberspace (ICTC)" op. cit. p 13
[37] Judge Stein Schjolberg, "An International Criminal Tribunal for Cyberspace (ICTC)" op. cit. p 17
[38] Thomas J Holt and Adam M Bossler, Cybercrime in Progress op. cit. 191
[39] 6th Edition, November 2013 drafted by Judge Stein Schjolberg.
[40] Article 1 of the draft Treaty.