The Seybold Report

ISSN 1533-9211

DOI 10.17605/OSF.IO/N4XA5

SOVEREIGNTY OF STATES IN THE DIGITAL SPACE AND ITS RELATIONSHIP TO TRANSBOUNDARY DAMAGE

RAED HAMEED SALIH

Assistant Lecturer, Al - Nahrain University, College of Law, Iraq. Email: raed.hamid@turath.edu.iq

Dr. MAHA MOHAMMED AYOUB

Professor, Al - Nahrain University, College of Law, Iraq. Email: Maha.m@nahrainuniv.edu.iq

Abstract

With the entry of states into the era of digital space, the concept of sovereignty of traditional states has changed; It is no longer able to control the movements of the actors in this digital space; The concept of state sovereignty is no longer as stable as it was before modern technological developments, especially the Internet, which does not recognize international borders and which has exceeded all expectations set for it. Countries have become fearful of their sovereignty, which has become clearly and explicitly infiltrated. As a result of the activities and processes that occur in the digital space, which may inflict citizens, companies, institutions, and sensitive vital facilities of the countries themselves, with severe harm that transcends the borders of countries due to the nature of this virtual space, the countries demanded recognition of a new concept of sovereignty in light of these new technological transformations; namely the digital sovereignty of states, which is exposed to various violations in light of this virtual space.

Keywords: Digital Sovereignty, Transboundary Damage, Digital Space, Digital Activities.

INTRODUCTION

The entry of the Internet into the international arena of action and its dominance over state institutions and its use by the peoples of the world and the territories of sovereign states; In a digital world that does not recognize the traditional borders of states, the idea of the digital sovereignty of states has begun to emerge on the international scene. Before the revolution of communication and information technology, in particular; the development of the Internet as an international means of communication between peoples, states were able to control their territories: through their enactment of a set of legislation through which they control all the movements that may take place within their territory, whether issued by individuals or institutions; As a result, it is capable of accepting international responsibility for all actions taken from its territory; however, with the emergence of the digital space, the traditional concept of sovereignty has changed due to rapid technological developments; countries are no longer able to control and dominate their sovereignty in the digital space, as is the case in the physical space. This is because there are actors in this virtual space who are able to carry out dangerous activities that cause serious harm to other countries: that is, these damages occur in a territory other than the region in which the activity took place; these activities cross the borders of states. All this is due to the lack of recognition by the digital space of the geographical borders of countries and the networking of communications between different

The Seybold Report
ISSN 1533-9211
DOI 10.17605/OSF.IO/N4XA5

countries of the world, which has become a miniature village due to the presence of this virtual space.

1. The concept of state sovereignty in the digital space

As far back as 1648, the Treaty of Westphalia established the principle of state sovereignty over its territory and internal affairs, without interference from other states; ([1]) Sovereignty is one of the fundamental elements on which contemporary international law is constructed, Its concept is one of the important concepts that legal scholars are interested in. It was and is still the subject of controversy and jurisprudential discussion among thinkers due to the many transformations that took place in its concept, beginning with its absolute concept and progressing to the relative concept in response to subsequent advancements and new evidence,([2]),Its concept was confirmed by many international treaties, including the Charter of the United Nations in Article (2/ paragraph 1) of it, which states: (The Commission is based on the principle of sovereign equality among all its members) [(3)]; The international judiciary also emphasized the concept of sovereignty within the rulings of the International Court of Justice in the Corfu case, as it was stated in the court's ruling that "respect for territorial sovereignty among independent states is considered a fundamental basis of international relations[(4)]) However, practical and technological developments in recent decades have resulted in a significant change in the concept of sovereignty around the world, affecting the lives of governments, institutions, and individuals; like the so-called (virtual) digital space emerged on the international scene as a new world parallel to the real world, leading to the need to reconsider and evaluate international law principles, the most important of which is the concept of sovereignty ([5]).

As a result, at the international level, the concept of "digital sovereignty" has evolved, which defines the principles of sovereignty in the information era. It discovered new sovereign arenas, prompting international governments to assert security authority over them; the concept of sovereignty is no longer limited to the three pillars of the geographical environment (land, sea, and air).

Rather, communication networks have created a new space in which vast amounts of information about the world's countries are mixed in various fields. In light of the world's accelerating digital transformation, the concept of national digital sovereignty has become critical for any country. As digital space has become the new homeland of the individual and the modern state in its digital age, which is characterized by the lack of borders and adopted by the Internet networks spread around the world ([6]).

Digital sovereignty is a modern and distinct concept related to the protection of digital infrastructure and Internet-related processes; Digital sovereignty is concerned with the information and content that the digital space provides; Hence, digital sovereignty means the subordination of the digital space to the interests and values of the state; It is the state's ability to control and domination of its own digital space, that is, within its territory, which ensures that the digital space of a country follows the same rules, standards, and cultural and social considerations; In general, it is used to express the power and independence of the state in the

The Seybold Report
ISSN 1533-9211
DOI 10.17605/OSF.IO/N4XA5

digital space in order to describe different forms of control and domination, over digital infrastructures, various digital tools and technologies, and all forms that can be linked to the digital space ([7])It is summarized in the state's ability to regain control over its official data and the data of its citizens. In the military aspect, it is represented by the state's ability to possess and develop offensive and defensive digital capabilities against any attack on its military digital systems. As for the economic aspect, it includes the state's ability to control and domination, banks and all financial transfers, and its ability to impose taxes on locally emerging companies in the field of information technology([8]). However, the nature of the digital space causes its borders to be penetrated by its actors, creating new challenges to the state's sovereignty over its data and raising the question of whether international law concepts can be applied in the digital space. Due to technological progress, regional sovereignty in its traditional sense has become open, and the most powerful technology has become a superior ability to discover what is going on with others and know the most accurate secrets without their permission this subjected the traditional concept of sovereignty to a review and redefinition from the absolute concept to

The limited or relative concept ([9]), which led to the emergence of two contradictory trends. The first one sees the erosion or fading of sovereignty in the digital space; the second trend sees its continuation in it.

1.1 First direction: evanescence Sovereignty in the digital space ([10])

Proponents of this trend believe that the digital space has affected the subjective nature of the state on the one hand and motivated non-state actors on the other hand; In light of the state of change in the global context, this has affected the role and function of state sovereignty. The process of escalating the role of non-state actors was characterized by the state's "bargaining professionalism"; weakening its authority over its territory and the functions entrusted to it, which led to non-state actors with the participation in the state in carrying out its traditional functions; The emergence of digital space has created difficulties for states to impose restrictions on the entry of goods into them, as well as the ability to impose taxes, which are the most important resource of the state budget and which reflect the sovereignty of the state through its ability to use its legitimate right to collect taxes; In particular, if local capital is leaked abroad, which constitutes serious economic damage to domestic investment, large technological companies can use commercial advertisements for products without paying any fees to the state, which affects the local market and enhances their monopoly on services and technology, affecting the national economy. ([11])Digital space has also affected the transformation of the traditional state into an information state characterized by constructive entanglement and participation with citizens; in the traditional perspective, the state retains the central role, while in the information state, the citizen has become involved in achieving the state-related goals and is the center in achieving the goals associated with it, The traditional state acts in accordance with the vision of its ruling political elites, while in the information state, new actors have emerged who have the capacity to influence public policies; According to the traditional perspective, the state controls information and the process of its circulation, while in the era of information and communications, it works on a balance between security

The Seybold Report
ISSN 1533-9211
DOI 10.17605/OSF.IO/N4XA5

and freedom of information circulation with the possibility of losing this balance due to its weak control over the information circulation process. This is what forced the state in the information age to interact faster with the event, and this is what many countries lose ([12]) The digital space has contributed to the existence of new forms of aggression against state institutions and its citizens, in contrast to the traditional invasion of the state's territory through communication and information networks that depend on it.

Vital installations, which weaken the State if we do not reduce the inability to provide security at the internal level by preserving its data and by preserving the safety, data, and funds of individuals; in addition to challenging the task of defending such data because of the inability to identify the source of attacks or threats; and thus taking a quick reaction, especially under the difficult legal frameworks adopted by the State, whether in the form of international law or criminal law to regulate the use of digital space;

The intensity of information flows through the digital space has challenged state control and created alternative media that will take citizens out of the control of their governing systems and thus the digital space has brought about changes in the international system in a way that has affected degrees of independence and national sovereignty, which has affected the ability to adopt national policies, dependency relations and the changing shape of relations between the State and non-State actors. ([13])Hence, the digital space and the resulting technological developments and effects have naturally led to a decline in the sovereignty of the state in the virtual space; however, the reasons behind the disintegration of sovereignty were and are still under discussion among writers and theorists of this trend, and these reasons can be summarized as follows:

1.1.1 Reasons related to the mechanism of organizing the Internet and its implications for sovereignty: The disintegration of the traditional sovereignty of the state in the digital space comes as a result of technological development and the spread of the Internet, as sovereignty includes (in addition to other dimensions such as political and legal) another technical dimension, as states seek to obtain names for private domains on the Internet, and each country has its own domain name that distinguishes it from other countries, and this is done through the "ICANN" organization, and the United States imposes its control over the administration of the Internet as it is the one who issues orders to the "ICANN" organization ([14])It supervises the original distributor of the Internet, which controls the group of the naming system to which all computers connected to the Internet belong. The flow of information and the flow of investments, in this situation, it is impossible to talk about the sovereignty of the state, which no longer controls

On the flow of information, ideas, and domain names, ([15]) and therefore the tremendous development of the means of communication and information technology contributed to the penetration of the sovereignty of states; no country can monopolize the media because of the huge amount of news, information, ideas, and images flowing unconditionally or restrictions from outside its borders. ([16])

The Seybold Report
ISSN 1533-9211
DOI 10.17605/OSF.IO/N4XA5

1.1.2 Reasons for the nature of digital space: some believe that digital space has special features that distinguish it from other international spaces; they have adopted this trend as a result of the metaphysical nature of the Internet; ([17])The transactions are seen as taking place in a city of digital units; Some countries, such as the United States of America and the European Union, see the digital space from the perspective of the free market; These countries recognize that the digital space transcends national borders and thus deserves a concept that transcends these borders; This trend considers that it is necessary to talk about sovereignty in its legal sense to have a physical existence in reality ([18]).Thus, talking about state sovereignty in digital space means legal sovereignty without a tangible physical presence; this has strengthened the role of non-State actors in the digital space, as well as the role of unidentified actors, who, of course, are engaged in their activities outside the authority of the State in most cases ([19]).

1.2 The second direction: the continuation of sovereignty in the digital space ([20])

The use of digital processes by States to harm, disrupt, influence or even disturb citizens and institutions in other States is a phenomenon commensurate with existing models of international law;

But not without controversy; while there had previously been some disagreement over whether current rules of international law were applicable to digital space at all; States agreed at the 2013 and 2015 meeting of the United Nations Group of Government Experts that international law, including the principles of State sovereignty and non-interference, applied to activities in the digital space, As in the physical realm of space; As stated in the two reports, the sovereignty of the state and the international standards and principles that flow from sovereignty apply to the state's conduct of Information and Communication Technology-related activities, and to its jurisdiction over the information and communication technology infrastructure within its territory. The experts also agreed that the principles of the Charter of the United Nations apply: (b) States must, when using information and communications technology; observe other principles of international law; sovereignty of States; compromise sovereignty; settle disputes by peaceful means; not interfere in the internal affairs of other States; and obligations under international law apply to State uses of Information and Communication Technology ([21]).

In addition to states, many international bodies and organizations have recognized the applicability of the principles of international law, including those related to the principle of sovereignty over digital space;

As the North Atlantic Treaty Organization announced and declared at the 2014 Wales Summit, alliance policy recognizes that international law, including international humanitarian law and the Charter of the United Nations, applies in the digital space) ([22]).As stated in the 2016 European Security and Aid Organization resolution on confidence-building measures to reduce the risk of conflict arising from the use of information technology, (calling on the international community to develop a peaceful, secure, just and open information space based on the principles of cooperation, respect for sovereignty, and non-interference in the internal affairs of other countries), ([23])

The Seybold Report
ISSN 1533-9211
DOI 10.17605/OSF.IO/N4XA5

In short, the principle of state sovereignty summarizes the supreme authority of the state in the unity of the territory, equality in sovereignty and political independence within its territory, with the exclusion of all other states' interference in this authority.

There are two jurisprudential direction on how international law can be applied to state-sponsored digital activities that occur below the threshold for the use of force, the first is that the principle of non-interference applies to some state-sponsored digital penetrations; that occur below the threshold of this principle; the activity may be unfriendly but will not violate international law, but in the event of serious damage in other states, it leads to a rise in state responsibility. According to this view; Sovereignty is one of the principles of international law that states' interactions may be directed towards; but they do not live up to the basic rules of their own; at least not in the context of digital space; the United Kingdom prefers this view, and the second is that digital processes below the non-intervention threshold may be illegal as violations of the sovereignty of the target state; this is the approach adopted in the 2017 Second Tallinn Guide; which derives and applies rules from sovereignty and non-interference. On operations in the digital space ([24]). There was discussion and debate about "Sovereignty as a rule" since the publication of the second Tallinn Guide, among many thinkers in the context of digital space; Until recently, however, there had been little public state practice to help enrich this debate, Some states have chosen to adopt a "policy of ambiguity and silence" on how international law can be applied in the digital space; some States have generally commented on the application of international law in the digital space but have not explained how they consider the application of the principles of sovereignty and non-interference([25]) For example, Estonia's statement on electronic and international law addressed a number of aspects of the application of international law to digital space; but did not explicitly address sovereignty and non-interference; Iran also stated that "the harmful use of information and communications technology represents a serious and imminent threat to violate state sovereignty and internal affairs," but without specifying how these principles are applied in practice([26]) . The United Kingdom had recorded its view that the principle of non-interference in the internal affairs of states applied to the digital processes of states and provided specific examples of cases where it considered that such a principle might apply, and the United Kingdom also stated that, in its view, there was no additional ban on digital activity that could be extrapolated from the principle of sovereignty other than prohibited interference([27]) And took a note issued in the year2017 The General Counsel of the US Department of Defense takes a similar position on sovereignty, although it; This contradicts other statements by US government officials, which expect a role for sovereignty in the application of international law to the digital space([28]) . Other countries have stated that the non-interference principle also applies in the digital space. The Australian strategy made it clear that the obligations enshrined in the Charter of the United Nations and in customary international law apply in the digital space as well as in the physical realm; harmful behavior in the digital space that does not constitute the use of force may constitute a violation of the duty of non-interference in internal or external affairs, and this obligation is stipulated in Article (2/Pq7) of the Charter of the United Nations([29]), and other countries have not indicated whether the general principle of sovereignty applies. In the digital domain; you may prefer to adopt a "wait andanticipation "at titude; or strategic ambiguity ([30])

The Seybold Report
ISSN 1533-9211
DOI 10.17605/OSF.IO/N4XA5

China's International Strategy for Cooperation in Digital Space 2017 states that the principle of sovereignty applies in the digital space; that (no state should seek digital domination; interfere in the internal affairs of other states, or engage in, condone or support digital activities that undermine the "national security" of other States) ([31])However, since violations of sovereignty can cover a range of activities; including in the context of specific rules on the use of force and non-interference derived from the principle of sovereignty; it is unclear to what extent China or other States consider an activity below the non-interference threshold to be a violation of sovereignty, and government data on sovereignty, in general, must therefore be carefully read since sovereignty is a word that can be used in different meanings in digital and non-digital contexts([32]). Due to the presence of digital infrastructures within the territory of the state, it has sovereignty over these infrastructures, and then it can cut off Internet networks from them, such as China's Great Firewall; On the basis that sovereignty includes the right of the state to control entry to its territory; And then it has the right to limit Internet access on its territory, and China has also developed a program that gives it the ability to cut off the Internet from it in the event of an attack; Meanwhile, the network remains local. This Chinese firewall allows China to network with the world; It is, of course, equipped with filtering programs to block websites, data and content that the Chinese government considers to be a threat to the system; Hence, states can impose their sovereignty and have sovereign power; In implementing the internal laws in which it sees the protection of the Internet within its borders, some countries even adopt laws to implement them outside their borders as well ([33])

2. The relationship of digital sovereignty of states to cross-border damage

The traditional concept of state sovereignty, based on the fact that states are defined by a well-defined physical territory with known and recognized boundaries over which different state bodies exercise control, has changed in the light of modern technological developments; and the emergence of a new concept of sovereignty that keeps pace with these developments with the emergence of

What is known as the concept of digital sovereignty has emerged, represented by the state's extension of its control and jurisdiction over the transnational digital space, which creates a virtual group of people within the Internet that transcends any national affiliation ([34])

The real challenge has therefore emerged about the existence of such sovereignty in the digital space between those who advocate the disappearance or disintegration of this sovereignty and those who assert its continuity in the digital space, Considering that the digital space is cross-border and does not recognize the traditional boundaries established by the Treaty of Westalvia in 1648, which One of its most important components is non-interference in the internal affairs of other countries. As the sovereignty of states according to the traditional concept cannot be in line with the digital space in which various digital operations and activities take place, whether that is done by states or by non-state actors, this is when these operations take place in one country against the digital assets and infrastructures of another country, causing harmful effects on it; It transcends its geographical borders in a virtual world that does not recognize these borders; For example, if digital operations and attacks do not take place in war conditions, it is a violation of the concept of Westphalian sovereignty, as are the military operations that

The Seybold Report
ISSN 1533-9211
DOI 10.17605/OSF.IO/N4XA5

take place on the ground against another state. ([35])For example, the digital attacks on Estonia in 2007 and Georgia in 2008 constitute an attack on their respective sovereignty by Russia, considering that the source of the attacks was from Russian territory; causing adverse and serious effects on both states, which is in line with the concept and logic of article (2/paragraph G) of the Draft International Responsibility for harmful consequences of acts not prohibited by international law; ([36])Considering that the damage occurred in the territory of a country other than the countries exporting these activities and caused serious harm to both Estonia and Georgia, in this example, the exporting country of the activities is Russia; This will enable it to activate its responsibility for these operations, whether these digital activities were carried out with its knowledge or not. It is therefore held internationally responsible for these activities if they are carried out or if they are denied for such operations; Considering that it should have known or should have known of the existence of harmful activities that seriously harm another state and therefore have a duty to commit to preventing such harmful activities and to take all necessary measures to prevent them, which took place in their territory or in Places under their jurisdiction, control or reduction of the risk of such activities (as evidenced by Article 3of the Cross-Border Damage Prevention Project) ([37])Therefore, if there are digital operations and activities taking place in the territory of a country, the source country had to conduct an assessment of these activities for the possibility of causing serious cross-border harm to other countries. This converges with the concept of Article seven of the project to prevent cross-border harm; Hence, it (the country of origin) has to notify the countries that are likely to be affected by these activities taking place in the digital space; The activities in this case include those that the source state and private entities operating in its territory, jurisdiction or control intend to undertake; The notification clause constitutes an indispensable part of any system aimed at preventing cross-border damage or, in any case, minimizing its risks, in accordance with the concept of Article(8/ paragraph 1) of the Draft to Prevent Cross-Border Damage([38]).

In light of this, it is necessary for states to enact national legislation to address the problems of sovereignty in digital space, in order to avoid the risks to their sovereignty in the present or in the future as a result of the use of digital space by its actors;

Both at the national and international levels and developed to accommodate harmful digital activities and processes occurring within their territory, while coordinating with other States in the context of accommodation and assistance to prevent cross-border damage in the digital space([39])By concluding agreements on digital processes, resolving the problem of digital sovereignty and dangerous activities that cause serious harm to other States, and agreeing on mechanisms to trace and combat the sources of such activities; such as the Council of Europe's 2001 Information Crime Convention and its additional protocol on racist behavior and acts committed through a network

the computer([40]) Recommendation of the Committee of Ministers of the Council of Europe on Problems of the Criminal Procedure Code relating to Information Technology 1995([41]), and the Arab Convention against Information Technology Crimes of 2010 dealing with crimes committed on information technology; This agreement aims to support and enhance cooperation between Arab countries in the field of combating information technology crimes

The Seybold Report
ISSN 1533-9211
DOI 10.17605/OSF.IO/N4XA5

to ward off the dangers resulting from these crimes and to preserve the security and interests of Arab countries and their sovereignty over their websites and the safety of their societies and individuals ([42])The question of sovereignty and its relation to transboundary harm has been raised in a number of issues; In the "The Trail Smelter case" between Canada and the United States of America, the arbitration court ruled in favor of the United States of America placing liability on Canada([43])

A large number of international law jurists went on to consider it a judicial precedent that can be relied on in similar cases that fall in the digital field, especially the law of international responsibility ([44])The ruling has gained wide fame, which made many researchers consider it a judicial precedent in this context. In the case of cross-border harm, if the results are to a "serious degree,"

It has been proven by clear and convincing evidence; Examples include activities that take place in the digital space. In this case, the principle of state responsibility for private entities operating within the state was established. The violation or violation committed in this case was committed by a private company.

Nevertheless, the Canadian government assumed international responsibility towards the United States for the activity of this company; Hence, the principle of the state bearing international responsibility for the actions of private actors such as private sector companies is a precedent Judicial and applied in the event of cases similar to those ruled in the digital space ([45])That is, if private actors in the territory of the state or in places under its jurisdiction or control commit dangerous activities against other states in the digital space and cause serious harm to them; The state in which these actors are located bears international responsibility towards the state affected by these activities against which this activity occurred; Judicial judgment pursuant to that precedent; Although it occurred in the real field, this liability includes compensation for damages caused to the complaining state.([46])The decisions of the International Court of Justice deal with important issues in the absence of the authority of the Security Council, although these decisions were not without criticism; However, they give an important reference for the analysis of international rules related to the peaceful settlement of disputes in the virtual field. These decisions are also useful in assessing the capabilities of international law and international courts to maintain order in the hypothetical realm.

Giving due consideration to the legitimate needs of states to protect their essential security interests; It was the first dispute to be brought to court. That's about the strait of Corfu channel, which included disputes over a state's duty not to allow its territory to be used to the detriment of another state; The Corfu Strait issue establishes the responsibility of the state as a result of its failure to take action; Although Albania denied placing and installing mines in the strait, the Court decided and issued a ruling placing the responsibility on Albania to notify other countries of the coalfields and to warn British ships of the danger posed by their exposure to the coal fields

Hence, the judgment in the Corfu Strait case is a judicial precedent according to which it is determined that if a state knows or should have known about a particular activity that takes

The Seybold Report
ISSN 1533-9211
DOI 10.17605/OSF.IO/N4XA5

place within its territory but which causes serious harm to other states, it has an obligation either to mitigate the damages and effects of this activity or (if that is possible) to notify other countries before the activity takes place. ([47]) As a judicial precedent in real space, this trend is also seen as a precedent in the digital space that can be measured in similar cases and disputes that can occur in the digital space, and in the light of the above, the State can be held responsible for the actions of individuals and private entities in the digital space; and that cause harm to other States through programmes, activities, and processes in the digital space ([48])

On the approach taken with respect to the International Court of Justice; there are those who believe that Article (8) of the Rome Statute of the International Criminal Court (ICC) can cover and apply to space operations. digital by measuring the kinetic processes; Although this opinion is correct, some of them questioned whether such a broad approach to interpretation could be consistent with Article 22 of the court system; which prohibits scaling expansion; But the general juristic trend believes that the Rome Statute of the Court does not exclude the trial of hackers who seize and control the country's missile operations systems and use them to launch aggression against another country. Hence, the equal impact of crimes of aggression increases the scope of application of the Rome Statute on information crimes that fall under the name of "crimes of aggression." ([49])

Also, other crimes provided for in this Rome Statute can be committed through hypothetical mechanisms and methods; this extends the scope of the court to include these crimes and its jurisdiction to adjudicate the aforementioned crimes that occur in the digital space. ([50])

CONCLUSION

The above shows us that the first trend adopts a concept that includes the decline of the concept of traditional sovereignty in the digital space as a result of the monopoly of its organization by the Organization of ICANN and the metaphysical natural consequence of this new field, while the second trend adopts a concept in favor of the continuation of state sovereignty in the digital space through some international practices with regard to the Internet, which prove its continuation in this new virtual world. According to the researcher, the dialectic of the disappearance or continuation of sovereignty in the digital space will continue between the thinkers and theorists of both directions, noting that the sovereignty of states in the digital space is constantly declining due to rapid technological and scientific development, which would enable actors in the digital space to penetrate and violate the sovereignty of digital states; For countries that do not have the modern tools and technologies to maintain their sovereignty in this space,

While other technologically advanced countries that have these tools and technologies or states that are trying to catch up with and own scientific development continue to control and seigniory their sovereignty in the digital space, we can therefore know digital sovereignty over "the extension of the state's control and jurisdiction in the digital space of the Internet."

Hence, it becomes clear to us that there is a strong relationship between the sovereignty of states in the digital space and the transboundary harm resulting from dangerous activities that

The Seybold Report
ISSN 1533-9211
DOI 10.17605/OSF.IO/N4XA5

cause serious damage located outside the territory of the country issuing this activity; Hence, the sovereignty of digital countries is being violated, which requires concerted efforts to prevent these dangerous activities or, in any case, reduce their grave effects. Through cooperation between countries and providing assistance among them, with the obligation of the source country to take all appropriate measures to prevent the occurrence of this damage, with notification and warning to the countries that are likely to be affected by these dangerous activities, and with the need to enact national and international legislation to help prevent or minimize these dangerous activities.

References

❖ **Arabic references**

1) Ali Sadiq Abu Heif, Public International Law, Mansha'at al-Maaref, Alexandria, 1995.
2) Ahmed Abu Al-Wafa, Mediator in Public International Law, Sixth Edition, Dar Al-Nahda Al-Arabiya, Cairo, 2016.
3) Hamdan Mohamed El-Tayeb, Khenish Magda, Electronic Warfare and its Impact on the Sovereignty of States, Journal of Legal and Political Studies, Algeria, Issue 7, January, 2018.
4) Mohamed Saadi, bookThe Impact of New Technology on International Law, New University House, Egypt, Alexandria, 2014.
5) Elias Abu Jaoude, Human Security and State Sovereignty, University Foundation for Studies, Publishing and Distribution, Beirut, 2008.
6) Mualem Youssef, International Responsibility without Harm: The Case of Environmental Damage, PhD thesis, Faculty of Law, Mentouri University, Constantine, Algeria, 2008.

❖ **International Agreements**

1) Yearbook of the International Law Commission, Draft International Responsibility of States for Their Internationally Wrongful Acts 2001, Volume Two Part Two, Document, A/CN.4/SER.A/2001/Add.1 (Part2).
2) United Nations General Assembly, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications and Wireless in the Context of International Security, June 24, 2013, UN Doc A/68/98.
3) United Nations General Assembly, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunicationsand Wireless in the Context of International Security, July 22, 2015, UN Doc A/70/174.
4) The Rome Statute of the International Criminal Court of 1998.
5) The Arab Convention to Combat Information Technology Crimes, 2010, the League of Arab States (General Secretariat), the Arab Legal Network, conventions and treaties, Chapter Five, Arab conventions in the legal and judicial field.

❖ **Foreign References**

1) 2019 International Law Supplement , Australia's Position on the Application of International Law to State Conduct in Cyberspace, Australia's International Cyber Engagement Strategy, 2019.
2) Brian J. Egan, International Law and Stability in Cyberspace, Berkeley Journal of International Law, Volume 35, Issue, 1, 2017.

The Seybold Report
ISSN 1533-9211
DOI 10.17605/OSF.IO/N4XA5

3) Catherine Lotrionte, "state sovereignty and self-Defense in cyberspace: A Normative Framework for Balancing legal rights", Emory international law Review, vol. 26 (2012).

4) Cindy Chen,United States and European Union Approaches to Internet Jurisdiction and Their Impact on E-Commerce, Published by Penn Law: Legal Scholarship Repository, University of Rennsylvania Law School, Vol. 25:1,2014.

5) Colonel Gary P. Corn ,Cyber National Security: Navigating Gray Zone Challenges In and Through Cyberspace, US Cyber Command, Lieber Institute for Law, December 2017.

6) D. Brown, "A Proposal for an International Convention to Regulate the use of Information systems in Armed Conflict", Harvard International Law Journal, Vol.47.(2006).

7) David G. Post & Danielle Kehl, Controlling Internet Infrastructure: The IANA Transition and Why It Matters for the Future of the Internet, Part 1, New America's Open Technology Institute, April 2015.

8) Eric Talbot Jensen. Cyber Sovereignty: The Way Ahead, Texas International Law Journal, Vol. 50 (2). December 2014.

9) Forrest HARE, Borders in Cyberspace: Can Sovereignty Adapt to the Challenges of Cyber Security? School of Public Policy, George Mason University,January 2009.

10) Harold Hongju Koh, International Law in Cyberspace , Harvard International Law Journal Online , Volume. 54.(2012).

11) Harriet Moynihan, The Application of International Law to State Cyberattacks: Sovereignty and Non-intervention, Research Paper ,International Law Programme, December 2019.

12) Jackson Adams, Mohamad Albakaja , Cyberspace : A New Threat to the Sovereignty of the State, University of Essex, Colchester, UK, Management Studies, Vol.4, No. 6, November – December. 2016.

13) Jason Healey and Hannah Pitts, "Applying International Environment Legal Norms to Cyber State Craft", Journal of Law and Policy for the information society, Volume:8, Issue: 2, (2012).

14) Jeffrey Roy,E-governance and International Relations. Journal of Electronic Commerce Research. Volume. 6, NO.1, 2005.

15) Johnson David and Post David, "Law and Borders: The Rise of Law in Cyberspace", Stanford law Review, Vol. 48, 1996.

16) Julia Knight, Jeanette Steemers and Alexis Weedon," Cyberspace as Place and the Limits of Metaphor", Convergence, Volume 11 Issue 1, (March 2005).

17) Lieutenant Colonel Patrick W Franzese, Sovereignty In Cyberspace: Can It Exist?Air Force Law Review, Volume 64, Jun 20 .2014.

18) Michael Schmitt &Brian T.ODonnell, U.S. Department of Defense Office of General Counsel ,An Assessment of International Legal Issues in Information Operations, Computer Network Attack and International Law, International Law Studies, Volume. 76. Second Edition, November 1999.

19) Michael Schmitt and Liis Vihul, Sovereignty in Cyberspace: Lex Lata Vel None? American Journal of International Law, Symposium on Sovereignty, Cyberspace, and Tallinn Manual 2.0. 2017.

20) Milton L. Mueller, Networks and States: The Global Politics of Internet Governance. Information Revolution and Global Politics. October 2010.

21) Organization for Security and Co-Operation in Europe ,Decision No. 1202 Osce Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the use of Information and Communication Technologies, 10 March 2016.

The Seybold Report
ISSN 1533-9211
DOI 10.17605/OSF.IO/N4XA5

22) Pierre de la Coste: La gouvernance internationale de l'internet : Institut français des relations internationales (IFRI) , Revue Politique étrangère : 2006 /3 Automne.

23) Recommendation No. R (95) 13 of the Committee of Ministers to member states concerning problems of criminal procedural law connected with information technology adopted on 11 September 1995.

24) The Corfu Channel Case (United Kingdom V. Albania), international court of justice, reports of judgments, advisory opinions and orders, (Merits). Judgement of April 9th, 1949.

25) the corfu channel case (United Kingdom V. Albania) ،international court of justice, reports of judgments, advisory opinions and orders, (Merits) ،Judgement of April 9th, 1949.

26) Treaty of Westphalia; October 24, 1648, International Relations and Security Network, Primary Resources in International Affair (PRIA).

27) United Nations, Report of international Arbitral Awards, Trail smelter case (United States, Canada) ،Vol III.

28) Wolff Heintschel von Heinegg, Territorial sovereignty and neutrality in cyberspace, international law studies ،U.S. Naval War College, Volume 89, Issue, 1, (2013).

❖ **Foreign Websites**

1) Niels Nagelhus Schia and Lars Gjesvik. The Chinese Cyber Sovereignty Concept (Part 1). Available at: https://theasiadialogue.com/2018/09/07/the-chinese-cyber-sovereignty-concept-part-1

2) Clothilde Goujard, France is ditching Google to reclaim its online independence, 20.11.2018. Available at: https://www.wired.co.uk/article/google-france-silicon-valley

3) NATO, Wales Summit Declaration, Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales, 5. September. 2014, para. 72. Available at: https://www.nato.int/cps/en/natohq/official_texts_112964.htm

4) Jeremy Wright, Cyber and International Law in the 21st Century, speech at Chatham House Royal Institute for International affairs. 23 May 2018. Available at: https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century

5) International Strategy of Cooperation on Cyberspace, Ministry of Foreign Affairs of the People's Republic of China, 2017. Available at: https://www.fmprc.gov.cn/mfa_eng/wjb_663304/zzjg_663340/jks_665232/kjlc_665236/qtwt_665250/t1442390.shtml