جامعة ستاردوم

مجلة ستاردوم العلمية للدراسات القانونية و السياسية

- مجلة ستاردوم العلمية للدراسات القانونية و السياسية -
تصدر بشكل ربع سنوي عن جامعة ستاردوم

العدد الأول - المجلد الرابع 2026م

رقم الإيداع الدولي: ISSN 2980-3764


بِسْمِ اللَّهِ الرَّحْمَٰنِ الرَّحِيمِ

هيئة تحرير مجلة ستاردوم العلمية للدراسات" القانونية والسياسية"

رئيس التحرير

أ.د عمار طارق عبد العزيز العاني

مدير التحرير

د. داليا عباس أحمد

أعضاء هيئة تحرير

د. سمر الخمليشي

د. بابكر بكري حسن

د. محمد بوبوش

د. عمر موفق

د. أنس حسين

د. حيدر بشير

د. فراس أحمد سلامة

د. رانيا الجميعابي

د. غالب عبد الله القعيطي

د. رويدة موسى عبد العزيز

د. طارق السر محمد

الهيئة الاستشارية

أ.د. أبكر عبد البنات أدم

أ.د. محمد علي هارب

أ.م.د. محسن الندوي

أ.م.د. يس حسن محمد عثمان

أ.م.د. إبراهيم قسم السيد محمد طه

أ.م.د. مصطفى نجاح مصطفى

أ.م.د. علي مير غني أحمد علي

د. أزهار محمد عيلان حسين الغرباوي

د. ملك أبو السعود رسلان عبد التواب

جميع حقوق الملكية الأدبية والفنية محفوظة

لمجلة ستاردوم العلمية للدراسات القانونية والسياسية

المسؤولية الدولية عن الهجمات السيبرانية :دراسة في إشكالية الإسناد والعناية الواجبة

إعداد

د.اميرة محمد ابراهيم ساتي

استاذ القانون الجنائي المساعد

أ.عبد الملك بن حمد العباد

مستخلص البحث

يتناول هذا البحث موضوع المسؤولية الدولية عن الهجمات السيبرانية في ضوء التطور المتسارع الذي يشهده الفضاء السيبراني، وما يترتب عليه من تحديات قانونية معقدة تمس أسس تطبيق قواعد القانون الدولي العام. ويأتي هذا الموضوع في ظل ازدياد الاعتماد على الوسائل الرقمية في مختلف مجالات الحياة، الأمر الذي جعل الفضاء السيبراني بيئة خصبة لوقوع أفعال غير مشروعة ذات طابع عابر للحدود، يصعب معها تحديد الفاعل وإثبات المسؤولية القانونية بدقة.

وتكمن إشكالية البحث في مدى كفاية وملاءمة قواعد المسؤولية الدولية التقليدية لمواجهة الطبيعة الخاصة للهجمات السيبرانية، خاصة فيما يتعلق بإسناد هذه الأفعال إلى الدول، وإثبات العلاقة بين الفعل غير المشروع والنتائج المترتبة عليه، في ظل غياب المعايير التقنية والقانونية الواضحة في هذا المجال. كما يثير البحث تساؤلًا حول مدى فعالية مبدأ "العناية الواجبة" في إلزام الدول بمنع استخدام بنيتها التحتية في تنفيذ أو دعم هجمات سيبرانية ضد دول أخرى.

ويهدف هذا البحث إلى تحليل الإطار القانوني للمسؤولية الدولية عن الهجمات السيبرانية، وبيان مدى قدرة القواعد التقليدية على استيعاب خصوصية هذا النوع من الأفعال، مع التركيز على إشكالية الإسناد والآثار القانونية المترتبة على قيام المسؤولية الدولية. كما يسعى إلى تقديم قراءة نقدية تكشف أوجه القصور في النظام القانوني الدولي الحالي عند تطبيقه على البيئة السيبرانية.

وقد اعتمدت الدراسة على المنهج التحليلي النقدي، من خلال تحليل النصوص القانونية الدولية ذات الصلة، ودراسة الاتجاهات الفقهية والتطبيقات العملية، بهدف الوصول إلى تقييم موضوعي لمدى فعالية القواعد الدولية القائمة في ضبط المسؤولية عن الهجمات السيبرانية.

ويخلص البحث إلى أن قواعد المسؤولية الدولية، رغم أهميتها، لا تزال تواجه تحديات جوهرية عند تطبيقها على الفضاء السيبراني، الأمر الذي يستدعي تطويرًا قانونيًا ومؤسسيًا يواكب طبيعة هذا المجال المتغير، ويعزز من فعالية النظام القانوني الدولي في مواجهة هذه التهديدات الحديثة.

الكلمات المفتاحية:

المسؤولية الدولية – الجرائم السيبرانية – القانون الدولي العام – الأمن السيبراني – السيادة الرقمية – الفضاء السيبراني.

Abstract

This research examines the issue of international responsibility for cyberattacks considering the rapid developments taking place within cyberspace and the resulting complex legal challenges affecting the application of rules of public international law. The importance of this topic has increased with the growing reliance on digital technologies in various aspects of modern life, making cyberspace a fertile environment for unlawful cross-border acts, where identifying the perpetrator and establishing legal responsibility has become increasingly difficult.

The research problem lies in determining the adequacy and suitability of traditional rules of international responsibility in addressing the unique nature of cyberattacks, particularly about attributing such acts to states and establishing the relationship between the wrongful act and its consequences, amid the absence of clear technical and legal standards in this field. The study also raises questions regarding the effectiveness of the principle of due diligence in obligating states to prevent the use of their infrastructure in carrying out or supporting cyberattacks against other states.

This study aims to analyze the legal framework governing international responsibility for cyberattacks and to assess the extent to which traditional legal rules can accommodate the unique characteristics of such acts, with particular focus on the issue of attribution and the legal consequences arising from international responsibility. It further seeks to provide a critical analytical perspective highlighting the shortcomings of the current international legal system when applied to cyberspace.

The study adopts a critical analytical approach through the examination of relevant international legal texts, jurisprudential opinions, and practical applications, with the aim of reaching an objective assessment of the effectiveness of existing international rules in regulating responsibility for cyberattacks.

The study concludes that, despite the importance of international responsibility rules, significant challenges still arise when applying them to cyberspace. This necessitates legal and institutional developments capable of keeping pace with the evolving nature of cyberspace and enhancing the effectiveness of the international legal system in confronting modern cyber threats.

Keywords:

International Responsibility – Cybercrimes – Public International Law – Cybersecurity – Digital Sovereignty – Cyberspace.

مقدمة

تشهد البيئة الدولية المعاصرة تحوّلًا عميقًا بفعل التطور المتسارع في تقنيات المعلومات والاتصال، الأمر الذي أدى إلى بروز الفضاء السيبراني بوصفه مجالًا جديدًا للتفاعل بين الدول والأفراد، لكنه في الوقت نفسه أصبح ساحة محتملة لارتكاب أفعال غير مشروعة تتجاوز الحدود التقليدية للدول، وعلى رأسها الهجمات السيبرانية. هذه الهجمات لم تعد مجرد تهديد تقني أو جنائي داخلي، بل تطورت لتُشكّل خطرًا يمس الأمن الدولي والاستقرار السياسي والاقتصادي للدول، نظرًا لصعوبة تتبع مصادرها وتحديد مرتكبيها بدقة.

وفي ظل هذا التطور، برزت إشكالية قانونية جوهرية تتمثل في مدى قدرة قواعد القانون الدولي التقليدي، وخاصة قواعد المسؤولية الدولية عن الأفعال غير المشروعة، على استيعاب الخصوصية الفنية والقانونية للهجمات السيبرانية. فهذه القواعد التي نشأت في سياق مادي تقليدي تواجه تحديات كبيرة عند تطبيقها على أفعال تتم في بيئة رقمية غير ملموسة، تتسم بالغموض وسرعة التطور وإمكانية إخفاء الهوية الفاعلة.

وتكمن أهمية هذه الدراسة في أنها تحاول الانتقال من مجرد الوصف النظري للمسؤولية الدولية في المجال السيبراني إلى تحليل نقدي لمدى فعالية هذه القواعد، مع التركيز على أبرز الإشكالات العملية التي تواجه تطبيقها، وعلى رأسها إشكالية إسناد الفعل غير المشروع إلى الدولة، وصعوبة إثبات العلاقة السببية في الفضاء السيبراني، بالإضافة إلى تقييم مدى كفاية مبدأ "العناية الواجبة" في الحد من هذه الهجمات.

وانطلاقًا من ذلك، يهدف هذا البحث إلى بيان أوجه القصور في القواعد التقليدية للمسؤولية الدولية عند تطبيقها على الهجمات السيبرانية، وتحليل الإطار القانوني الحاكم لهذه المسؤولية، مع محاولة إبراز الحاجة إلى تطوير أدوات قانونية أكثر ملاءمة لطبيعة الفضاء السيبراني.

وقد اعتمدت الدراسة على المنهج التحليلي النقدي، من خلال تحليل النصوص القانونية الدولية ذات الصلة، ودراسة التطبيقات القضائية والمواقف الفقهية، بما يسمح بتقييم مدى فاعلية النظام القانوني الدولي الحالي في مواجهة هذه الظاهرة المستجدة.

وفي ضوء ما سبق، يسعى هذا البحث إلى الإسهام في توضيح الجوانب الغامضة في موضوع المسؤولية الدولية عن الهجمات السيبرانية، وبيان حدود القواعد القائمة، واقتراح رؤية أكثر واقعية لتطويرها بما يتناسب مع طبيعة التهديدات السيبرانية الحديثة.

إشكالية البحث

في ظل التطور المتسارع الذي يشهده الفضاء السيبراني، وما نتج عنه من ازدياد في حجم وتعقيد الهجمات السيبرانية العابرة للحدود، تبرز إشكالية قانونية مركزية تتمثل في مدى قدرة قواعد المسؤولية الدولية التقليدية في القانون الدولي العام على استيعاب خصوصية هذه الهجمات والتعامل معها بفعالية.

وتتجسد هذه الإشكالية في أن الهجمات السيبرانية تتميز بطبيعة فنية وقانونية خاصة، أهمها الطابع غير المادي، وصعوبة التتبع التقني، وإمكانية إخفاء هوية الفاعل الحقيقي، وهو ما يثير تحديات جوهرية عند تطبيق القواعد التقليدية المتعلقة بإسناد الفعل غير المشروع إلى الدولة، وإثبات العلاقة السببية بين الفعل والنتيجة.

كما يثور تساؤل جوهري حول مدى كفاية مبدأ "العناية الواجبة" كأحد أدوات القانون الدولي في ضبط سلوك الدول داخل الفضاء السيبراني، ومنع استخدامها أو التساهل في استخدام بنيتها التحتية في تنفيذ هجمات سيبرانية ضد دول أخرى.

وانطلاقًا من ذلك، تتمحور إشكالية هذا البحث حول التساؤل الآتي:

إلى أي مدى تُعد قواعد المسؤولية الدولية في القانون الدولي العام كافية وملائمة لمواجهة الهجمات السيبرانية، خاصة فيما يتعلق بإسناد هذه الهجمات إلى الدول، وتحديد مسؤوليتها القانونية في ضوء الطبيعة الخاصة للفضاء السيبراني؟

وتتفرع عن هذه الإشكالية مجموعة من التساؤلات الفرعية، من أبرزها:

- ما مدى قابلية قواعد الإسناد التقليدية للتطبيق على الهجمات السيبرانية؟
- هل يوفر القانون الدولي الحالي أدوات فعالة لإثبات مسؤولية الدولة في هذا المجال؟
- وما مدى فعالية التزام الدولة بالعناية الواجبة في الحد من هذه الهجمات أو منعها؟

أهداف البحث وأهمية اختيار الموضوع:

أهداف البحث :

أولاً: تحديد وتحليل قواعد القانون الدولي العام ذات الصلة بالمسؤولية الدولية (السيادة، عدم التدخل، حظر استخدام القوة، الأفعال غير المشروعة دولياً ومدى انطباقها على الهجمات السيبرانية.)

ثانياً:بناءً على الإطار القانوني المحدد، دراسة إشكالية إسناد الهجمات السيبرانية للدول من خلال تحليل معايير الإسناد وشروط تحمل الدولة للمسؤولية الدولية عن الأفعال غير المشروعة دوليًا.

ثالثاً: استكشاف التزام "العناية الواجبة" (Due Diligence) الذي يقع على عاتق الدول بموجب القانون الدولي، وتحديد نطاقه وآليات تطبيقه في السياق السيبراني، وكيفية ترتب المسؤولية على إخلال الدول به.

رابعاً: تقييم شامل لمدى كفاية المنظومة القانونية الدولية الحالية في مواجهة تحديات الجرائم السيبرانية، وتقديم توصيات عملية لتطويرها بما يضمن تحقيق الأمن والاستقرار والعدالة في الفضاء السيبراني.

خامسا:بيان الآثار القانونية المترتبة على ثبوت المسؤولية الدولية عن الهجمات السيبرانية (التعويض، رد الحال إلى ما كانت عليه، الترضية، التدابير المضاد، وحدود حق الدولة المتضررة في الرد.)

منهجية البحث:

لتحقيق أهداف البحث والإجابة عن تساؤلاته، سيتم الاعتماد على المنهج الوصفي والتحليلي، وذلك على النحو التالي:

- **الجانب الوصفي** : يتمثل في استعراض وتوصيف الإطار القانوني الدولي القائم ذي الصلة، وذلك من خلال تحليل قواعد مسؤولية الدول ومبادئ القانون الدولي العام والاتفاقيات الدولية، بالاستناد إلى مصادر رسمية محددة تشمل قرارات محكمة العدل الدولية، وقرارات مجلس الأمن، وتقارير الأمم المتحدة، إضافة إلى الممارسات والمواقف المعلنة للدول والمنظمات الدولية في الفضاء السيبراني.
- **الجانب التحليلي** : يتجلى في تحليل النصوص القانونية والممارسات الدولية الموصوفة، بهدف استنباط القواعد المطبقة، وتحديد مواطن القصور والغموض فيها، وتقييم مدى كفايتها في التعامل مع إشكاليات البحث، وصولًا إلى تقديم استنتاجات وتوصيات محددة.
- **الجانب المقارن:** كما اعتمد البحث على المنهج المقارن من خلال تحليل مواقف بعض الدول والاتجاهات الدولية المختلفة تجاه تطبيق قواعد المسؤولية الدولية على الهجمات السيبرانية.

الدراسات السابقة :

- **دراسة: المسؤولية الدولية عن الهجمات السيبرانية في ضوء قواعد القانون الدولي العام**
- الباحث :د. محمد بن علي القحطاني

الجهة :مجلة الدراسات القانونية – كلية الحقوق – جامعة الملك سعود , سنة النشر 2019

مضمون الدراسة:

تناولت هذه الدراسة الإطار القانوني لمسؤولية الدولة عن الهجمات السيبرانية، من خلال تحليل مدى انطباق قواعد القانون الدولي العام التقليدية، ولا سيما قواعد السيادة، وعدم التدخل، وحظر استخدام القوة، على الأفعال السيبرانية. كما ركزت على إشكالية إسناد الهجمات السيبرانية إلى الدول في ظل صعوبة الإثبات، وتعدد الفاعلين، واستخدام وسطاء غير حكوميين.

أوجه الاستفادة:

- تحليل قانوني دقيق لمفهوم الهجوم السيبراني من منظور القانون الدولي العام.
- بيان العلاقة بين الهجمات السيبرانية ومبدأ عدم التدخل.
- إبراز الصعوبات العملية في إسناد الفعل السيبراني للدولة.

أوجه الاختلاف عن البحث الحالي:

- لم تتناول الدراسة مبدأ **العناية الواجبة** كأداة مستقلة للمسؤولية الدولية.
- لم تبحث الآثار القانونية المترتبة على المسؤولية الدولية مثل جبر الضرر أو التدابير المضادة.
- ركزت على الجانب النظري دون التوسع في الجانب التطبيقي.
- الآثار القانونية للمسؤولية

ومن هنا، تتميز هذه الدراسة الحالية بكونها تتناول المسؤولية الدولية عن الجرائم السيبرانية بصورة متكاملة، وبمنهج تحليلي يجمع بين البعد القانوني والبعد الإنساني، مع التركيز على تطوير القواعد الدولية بما يتلاءم مع طبيعة الفضاء السيبراني وتحدياته المعاصرة.

المبحث التمهيدي

التطور التاريخي للهجمات السيبرانية وخصائص الفضاء السيبراني

أدى التطور التقني المتسارع منذ أواخر القرن العشرين إلى نشوء فضاء جديد للتفاعل الإنساني والدولي يُعرف بالفضاء السيبراني، والذي أصبح يشكّل ركيزة أساسية لإدارة شؤون الدولة الحديثة، سواء في المجال الاقتصادي أو الإداري أو الأمني أو العسكري. ومع اتساع الاعتماد على البنية الرقمية، ظهرت أنماط جديدة من التهديدات تمثلت في الهجمات السيبرانية، التي تجاوزت نطاق الجرائم التقنية الفردية لتتحول إلى أدوات ذات آثار استراتيجية تمس الأمن الدولي والاستقرار المجتمعي وحقوق الإنسان.

وقد أفرز هذا التحول واقعًا قانونيًا جديدًا فرض على القانون الدولي العام تحديًا يتمثل في ضرورة التعامل مع أفعال تقع في بيئة غير مادية، عابرة للحدود، يصعب فيها تحديد الفاعل أو ضبط نطاق الاختصاص القانوني.

ومن ثم، فإن دراسة التطور التاريخي للهجمات السيبرانية وتحليل خصائص الفضاء السيبراني يمثلان مدخلًا أساسيًا لفهم الإشكاليات المرتبطة بالمسؤولية الدولية الناشئة عنها.

وعليه، يتناول هذا المبحث مطلبين رئيسيين:

المطلب الأول

التطور التاريخي للهجمات السيبرانية

لم تظهر الهجمات السيبرانية بصورتها الحالية بشكل مفاجئ، بل مرت بمراحل تطور متعاقبة ارتبطت ارتباطًا وثيقًا بتطور التكنولوجيا الرقمية وانتشار شبكات الاتصال العالمية. [1]

مرحلة النشأة التقنية (1970–1990)

في هذه المرحلة، ارتبطت الهجمات السيبرانية بظهور الحواسيب المركزية والشبكات الأولية، حيث اقتصرت الأفعال الرقمية الضارة على تجارب فردية قام بها مبرمجون أو هواة بهدف اختبار القدرات التقنية أو استكشاف الثغرات البرمجية. وتمثلت هذه الهجمات في فيروسات بدائية وبرمجيات ذاتية الانتشار لم يكن هدفها تحقيق مكاسب سياسية أو اقتصادية، بل كانت في الغالب ذات طابع استعراضي أو تجريبي.

ورغم محدودية آثارها آنذاك، فقد كشفت هذه المرحلة عن قابلية الأنظمة الرقمية للاختراق، الأمر الذي مهّد لظهور مفهوم الأمن السيبراني لاحقًا.

مرحلة الانتشار العالمي للإنترنت (1990 –2005)

مع الانتشار الواسع لشبكة الإنترنت، شهدت الهجمات السيبرانية تحولًا نوعيًا، حيث بدأت تتخذ طابعًا إجراميًا منظمًا، تمثل في سرقة البيانات المالية، واختراق المؤسسات التجارية، ونشر البرمجيات الخبيثة على نطاق واسع.

وخلال هذه المرحلة، أدركت الدول أن الفضاء السيبراني لم يعد مجرد بيئة تقنية، بل أصبح مجالًا جديدًا قد يُستغل لتهديد الأمن الاقتصادي والاجتماعي، مما أدى إلى ظهور أولى التشريعات الوطنية المتعلقة بالجرائم المعلوماتية.

([1]) عبد الفتاح بيومي حجازي، *الجرائم المعلوماتية بين النظرية والتطبيق*، دار الفكر الجامعي، الإسكندرية، 2010، ص 21–30.

مرحلة التسييس والأمن القومي (2005–2015)

شهدت هذه المرحلة انتقال الهجمات السيبرانية من نطاق الجريمة الفردية إلى مستوى الصراع بين الدول، حيث ظهرت هجمات استهدفت بنى تحتية حيوية وأنظمة حكومية، مما أبرز قدرة الوسائل الرقمية على إحداث آثار واقعية قد تماثل في خطورتها بعض صور استخدام القوة التقليدية.

وأدى ذلك إلى بدء النقاش الدولي حول مدى خضوع العمليات السيبرانية لقواعد القانون الدولي العام، خاصة مبادئ السيادة وعدم التدخل واستخدام القوة.

المرحلة المعاصرة – الحروب السيبرانية والهجمات الذكية (2015– حتى الآن)

في المرحلة الراهنة، أصبحت الهجمات السيبرانية أكثر تعقيدًا وتنظيمًا، حيث تستخدم تقنيات الذكاء الاصطناعي، والهجمات الموجهة، والتضليل المعلوماتي، واستهداف البنية التحتية الحيوية مثل الطاقة والاتصالات والقطاع الصحي.

كما برز دور الفاعلين غير الحكوميين، مما أدى إلى تعقيد مسألة إسناد الفعل إلى الدولة، وهو ما يمثل أحد أبرز التحديات أمام قواعد المسؤولية الدولية التقليدية.

ومن الناحية الإنسانية، لم تعد آثار الهجمات السيبرانية تقتصر على الأضرار التقنية، بل امتدت لتشمل تعطيل الخدمات الأساسية، وانتهاك الخصوصية الرقمية، والتأثير في الاستقرار المجتمعي، الأمر الذي عزز الحاجة إلى تطوير قواعد قانونية دولية أكثر ملاءمة لهذا الواقع الجديد.

المطلب الثاني

خصائص الفضاء السيبراني

يتميّز الفضاء السيبراني بخصائص فريدة تجعله مختلفًا جوهريًا عن المجالات التقليدية التي نشأت في إطارها قواعد القانون الدولي، وهو ما يفسر الصعوبات القانونية المرتبطة بتنظيم الأفعال التي تقع داخله. [2]

(2) محمد أمين الشوابكة، *الجرائم المعلوماتية*، دار الثقافة للنشر والتوزيع، عمّان، 2014، ص 55–65.

الطبيعة العابرة للحدود

لا يخضع الفضاء السيبراني لحدود جغرافية واضحة، إذ يمكن تنفيذ الهجوم من دولة، ومروره عبر عدة دول، واستهداف دولة أخرى خلال ثوانٍ معدودة. ويؤدي ذلك إلى تعقيد مسألة الاختصاص القضائي وتحديد القانون الواجب التطبيق، فضلًا عن إشكالية احترام السيادة الإقليمية.

إشكالية الإسناد وصعوبة تحديد الفاعل

تتيح البيئة الرقمية استخدام تقنيات متقدمة لإخفاء الهوية، مثل الشبكات الافتراضية والخوادم الوسيطة، مما يجعل تحديد المسؤول الحقيقي عن الهجوم أمرًا بالغ التعقيد، ويضع عبئًا كبيرًا على قواعد الإثبات في القانون الدولي.

عدم التماثل في القوة

يمكّن الفضاء السيبراني جهات صغيرة أو حتى أفرادًا من إحداث تأثيرات واسعة النطاق بتكاليف منخفضة نسبيًا، وهو ما يغيّر المفهوم التقليدي لتوازن القوة بين الدول، ويمنح الفاعلين غير الحكوميين دورًا غير مسبوق في العلاقات الدولية.

الترابط العالمي للبنية الرقمية

تعتمد الأنظمة الحديثة على شبكات مترابطة عالميًا، بحيث قد يؤدي هجوم واحد إلى آثار متسلسلة تمتد إلى عدة دول وقطاعات، وهو ما يمنح الجرائم السيبرانية طابعًا دوليًا مباشرًا حتى وإن كان مصدرها محليًا.

الطبيعة غير المادية للأفعال السيبرانية

تتم العمليات السيبرانية دون استخدام القوة المادية التقليدية، مما يثير إشكالية قانونية حول توصيفها: هل تعد استخدامًا للقوة؟ أم مجرد عمل غير مشروع دوليًا؟ وهو تساؤل يشكّل أحد محاور النقاش المعاصر في القانون الدولي العام.

البعد الإنساني للفضاء السيبراني

لم يعد الفضاء السيبراني مجرد بيئة تقنية، بل أصبح مجالًا لممارسة الحقوق الأساسية للأفراد، كحرية التعبير والخصوصية والوصول إلى المعلومات. وبالتالي فإن الاعتداءات السيبرانية قد تمس حقوق الإنسان بصورة مباشرة، مما يضفي على تنظيمه بعدًا إنسانيًا إلى جانب البعد الأمني والقانوني.

المبحث الأول

الإطار المفاهيمي والقانوني للمسؤولية الدولية عن الجرائم السيبرانية

المطلب الأول

ماهية الجرائم السيبرانية وتكييفها في منظور القانون الدولي

إن تحديد ماهية الجريمة السيبرانية يعد الخطوة الأولى والأساسية في بناء أي نظام للمسؤولية الدولية. فبدون تعريف جامع ومانع، يظل التكييف القانوني للفعل محل نزاع، مما قد يؤدي إلى إفلات الجناة من العقاب أو تهرب الدول من مسؤولياتها القانونية. إن الطبيعة المعقدة والمتطورة لهذه الجرائم تفرض تحديات على الفقه والقانون الدوليين، مما يستدعي تحليلاً معمقاً لمفهومها وخصائصها وتكييفها القانوني.

الفرع الأول: التعريف الفقهي والقانوني للجريمة السيبرانية وخصائصها

أولاً: التعريف الفقهي والقانوني

تعددت التعريفات الفقهية والقانونية للجريمة السيبرانية، ويعود هذا التعدد إلى حداثة الظاهرة، وسرعة تطورها، واختلاف الزوايا التي ينظر منها إليها (جنائية، دولية، تقنية). ومع ذلك، يمكن استخلاص تعريف أكاديمي شامل يركز على الأبعاد القانونية والدولية للجريمة السيبرانية، بوصفها :

كل فعل أو امتناع عن فعل غير مشروع يتم ارتكابه باستخدام تكنولوجيا المعلومات والاتصالات، سواء كان النظام المعلوماتي هو الهدف المباشر للاعتداء (جرائم صلبة)، أو كان مجرد وسيلة لارتكاب جريمة تقليدية (جرائم لينة)، وتترتب عليه آثار تمس المصالح المحمية قانوناً، وتتجاوز في الغالب الحدود الإقليمية للدولة الواحدة. [3]

([3]) د. سامر نمر سالم الجاروشة، الجرائم السيبرانية وحقوق الإنسان في القوانين الدولية والوطنية، دار النهضة العربية، القاهرة، 2023، ص 45

ويلاحظ أن هذا التعريف يركز على شمولية الجريمة السيبرانية، حيث لا تقتصر على الجرائم التقنية البحتة، بل تشمل أيضاً الجرائم التقليدية التي تتم في البيئة الرقمية. وقد تبنت اتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية (2024) هذا التوجه الشامل، حيث جرمت مجموعة واسعة من الأفعال التي تتراوح بين الدخول غير المشروع واستغلال الأطفال جنسياً عبر الإنترنت [4] . إن هذا التوسع في التجريم يعكس إدراكاً دولياً بأن الفضاء السيبراني لم يعد مجرد أداة، بل أصبح مسرحاً كاملاً للنشاط الإجرامي المنظم.

ثانياً: الخصائص المميزة للجريمة السيبرانية

تتميز الجرائم السيبرانية بمجموعة من الخصائص التي تمنحها طابعاً فريداً وتجعلها تحدياً حقيقياً للقواعد القانونية التقليدية، ومن أبرز هذه الخصائص:

1. اللاجغرافية :

تعد هذه الخاصية هي الأهم على الإطلاق في سياق المسؤولية الدولية. فالجريمة السيبرانية لا تعترف بالحدود الإقليمية للدول، حيث يمكن للمجرم أن يدير هجومه من قارة، ويستهدف ضحية في قارة أخرى، وتمر بيانات الهجوم عبر خوادم في دول ثالثة [5] . هذا التشتت الجغرافي يثير إشكالية تنازع الاختصاص القضائي بين الدول، ويضعف من فاعلية مبدأ السيادة الإقليمية التقليدي الذي يقوم عليه القانون الدولي العام [6]. إن غياب المركزية في الفضاء السيبراني يفرض على الدول إعادة النظر في مفهوم الاختصاص الجنائي، والانتقال من الاختصاص الإقليمي إلى الاختصاص العالمي أو على الأقل الاختصاص القائم على المصالح المحمية.

2. صعوبة الإسناد والإثبات :

تتيح البيئة الرقمية للمجرمين إمكانية كبيرة لإخفاء هويتهم الحقيقية، واستخدام تقنيات التخفي وتزوير العناوين الرقمية، مما يجعل عملية إسناد الفعل إلى شخص أو جهة معينة أمراً بالغ الصعوبة [7] . وفي سياق المسؤولية الدولية، تزداد الصعوبة عندما يتعلق الأمر بإسناد الهجوم إلى الدولة نفسها، خاصة إذا تم استخدام وكلاء غير حكوميين أو جماعات إجرامية منظمة [8] . إن هذه الصعوبة التقنية في الإسناد هي التي تدفع الدول إلى

([4]) اتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية، اعتمدتها الجمعية العامة في ديسمبر 2024، المادة.(2)

([5]) د. محمد محمود شوقي و د. محمد سعيد عبد العاطي، الوسيط في مكافحة الجرائم السيبرانية، منشورات الحلبي الحقوقية، بيروت، 2024، ص 112.

([6]) د. أثير هلال فليح الدليمي، القواعد الدولية لمكافحة الجرائم الإلكترونية والسيبرانية، دار النشر والتوزيع، عمان، 2024، ص 67.

([7]) المستشار د. عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والإنترنت في القانون العربي النموذجي، دار الفكر الجامعي، الإسكندرية، 2006، ص 89.

([8]) د. نورية الساعدي المقريف، الحرب السيبرانية في ضوء أحكام القانون الدولي العام، مجلة كلية الحقوق، جامعة ليبيا، 2022، ص 156.

استخدام الفضاء السيبراني كأداة للحرب الهجينة، حيث يمكنها تحقيق أهداف استراتيجية دون تحمل المسؤولية الدولية المباشرة. كما أن الأدلة الرقمية بطبيعتها هشة وقابلة للتعديل أو المحو بسهولة، مما يضع تحديات كبيرة أمام قواعد الإثبات الجنائي والدولي . [9]

3. السرعة الفائقة والانتشار الواسع:

تتميز الهجمات السيبرانية بقدرتها على الانتشار بسرعة هائلة، حيث يمكن لبرمجية خبيثة أن تصيب ملايين الأجهزة حول العالم في غضون دقائق، مما يجعل من الصعب على الدول احتواء الأضرار أو تداركها قبل وقوعها . [10] هذه السرعة تتطلب استجابة فورية وتعاوناً دولياً على مدار الساعة، وهو ما لا يتوفر دائماً في الأطر القانونية التقليدية التي تتسم بالبطء والبيروقراطية. إن عنصر الزمن هنا يمثل تحدياً قانونياً، حيث قد لا تملك الدولة المتضررة الوقت الكافي لتحديد مصدر الهجوم قبل أن يتسبب في أضرار كارثية، مما يثير تساؤلات حول مشروعية الرد الفوري (الرد السريع) في الفضاء السيبراني.

4. الضرر غير المادي:

في كثير من الأحيان، لا تترتب على الجريمة السيبرانية أضرار مادية ملموسة (كالتدمير أو القتل)، بل قد تقتصر على أضرار اقتصادية أو معنوية أو سياسية، مثل سرقة البيانات، أو التجسس الصناعي، أو تعطيل الخدمات الحيوية دون تدمير مادي . [11] هذا يثير تساؤلاً حول معيار الضرر الكافي لتقرير المسؤولية الدولية، خاصة وأن القواعد التقليدية كانت تركز على الأضرار المادية الملموسة. إن قيمة البيانات والمعلومات في العصر الحديث تفرض على القانون الدولي الاعتراف بالضرر الاقتصادي والسياسي الناجم عن الهجمات السيبرانية كضرر يوجب المسؤولية، حتى لو لم يكن مصحوباً بتدمير مادي . [12]

([9]) د. عبد الفتاح بيومي حجازي، الإثبات الإلكتروني في المواد الجنائية، دار النهضة العربية، القاهرة، 2017، ص 210.

([10]) د. صديقي سامية، المسؤولية الدولية الناشئة عن الهجمات السيبرانية في ضوء القانون الدولي المعاصر، مجلة الزرقاء للبحوث والدراسات الإنسانية، المجلد 19، العدد 1، 2019، ص 203.

([11]) تقرير فريق الخبراء الحكوميين التابع للأمم المتحدة (GGE) المعني بالتطورات في ميدان المعلومات والاتصالات، 2021، الفقرة 71.

([12]) اللجنة الدولية للصليب الأحمر(ICRC) ، إسناد التصرف في الفضاء السيبراني لأغراض مسؤولية الدولة، ورقة موقف، 2019، ص 8.

الفرع الثاني: تصنيف الجرائم السيبرانية وتكييفها في القانون الدولي

أولاً: التصنيف وفقاً لطبيعة الفعل

يتم تصنيف الجرائم السيبرانية إلى فئتين رئيستين، وهو التصنيف الأكثر شيوعاً في الأدبيات الأكاديمية والمنظمات الدولية مثل:(UNODC)

إن هذا التصنيف له أهمية بالغة في تحديد الإطار القانوني المطبق، فالفئة الأولى تخضع بشكل أساسي لقوانين الجرائم المعلوماتية المتخصصة، بينما الفئة الثانية تخضع للقوانين الجنائية التقليدية مع تعديلات تتعلق بالإجراءات والإثبات.

ثانياً: التكييف القانوني في منظور القانون الدولي العام

إن التحدي الأكبر يكمن في تكييف هذه الأفعال في ضوء قواعد القانون الدولي العام، لتحديد متى يمكن أن ترقى الجريمة السيبرانية من مجرد فعل جنائي داخلي إلى "عمل غير مشروع دولياً" يوجب مسؤولية الدولة.

1. التكييف كخرق لمبدأ السيادة وعدم التدخل:

يمكن تكييف الهجوم السيبراني الذي يهدف إلى تعطيل البنية التحتية الحيوية لدولة أخرى (مثل شبكات الكهرباء أو الاتصالات) كخرق لمبدأ السيادة الإقليمية للدولة المستهدفة. [13] فمبدأ السيادة يمنح الدولة الحق الحصري في ممارسة سلطتها على إقليمها، وأي تدخل خارجي في هذا الإقليم، حتى لو كان افتراضياً، يعد انتهاكاً للسيادة. كما يمكن تكييف الهجمات التي تستهدف التدخل في العمليات الانتخابية أو الشؤون الداخلية للدولة كخرق لمبدأ عدم التدخل في الشؤون الداخلية للدول الأخرى، وهو مبدأ أساسي في القانون الدولي العرفي [14] . إن هذا التكييف يفتح الباب أمام مساءلة الدولة التي ينطلق منها الهجوم، حتى لو لم تكن هي الفاعل المباشر، وذلك بناءً على مبدأ العناية الواجبة الذي سيتم تفصيله لاحقاً.

2. التكييف كاستخدام للقوة أو عدوان سيبراني:

يثور الجدل حول متى يمكن اعتبار الهجوم السيبراني "استخداماً للقوة " بموجب المادة (4/2) من ميثاق الأمم المتحدة، أو "هجوماً مسلحاً "يبرر حق الدفاع عن النفس (المادة 51). وقد استقر الرأي الفقهي في "دليل

(13) د. السيدة حليمة الدرمكي و أ.د. وائل علام، المسؤولية الدولية عن الهجمات السيبرانية الواقعة من كيانات من غير الدول، مجلة جامعة الشارقة للعلوم القانونية، 2024، ص 88.

(14) بسمة صلال طه، المسؤولية الدولية الناجمة عن الهجمات السيبرانية، مجلة جامعة البيان للدراسات والبحوث، 2024، ص 42.

تالين" على أن الهجوم السيبراني يعد استخداماً للقوة إذا كانت آثاره (من حيث الموت أو الإصابة أو التدمير المادي) تماثل آثار الهجوم التقليدي [15] . هذا المعيار، المعروف باسم "معيار الآثار "، هو المعيار الأكثر قبولاً دولياً، حيث يركز على النتيجة بدلاً من الوسيلة. أما إذا لم تترتب عليه آثار مادية، فإنه يظل في إطار "العمل غير الودي "أو "الإكراه "الذي لا يبرر الرد العسكري، ولكنه يوجب المسؤولية الدولية [16] .

3. التكييف كخرق للقانون الدولي الإنساني:

في سياق النزاعات المسلحة، تخضع العمليات السيبرانية لقواعد القانون الدولي الإنساني . فالهجمات السيبرانية التي تستهدف الأعيان المدنية (مثل المستشفيات أو محطات الطاقة المدنية) أو التي تسبب أضراراً عرضية مفرطة للمدنيين، تعد جرائم حرب [17]. وقد أكدت اللجنة الدولية للصليب الأحمر أن القانون الدولي الإنساني ينطبق بالكامل على العمليات السيبرانية، ويحظر استخدامها بطريقة عشوائية أو غير متناسبة [18]. إن هذا التكييف يفرض على القادة العسكريين تطبيق مبادئ التمييز والتناسب والاحتياط في الهجمات السيبرانية، تماماً كما يطبقونها في الهجمات الحركية التقليدية.

المطلب الثاني

القواعد العامة لمسؤولية الدول ومدى انطباقها على الفضاء السيبراني

تعد المسؤولية الدولية حجر الزاوية في النظام القانوني الدولي، حيث تهدف إلى ضمان احترام الدول لالتزاماتها القانونية وجبر الأضرار الناجمة عن انتهاكها. ومع ظهور الفضاء السيبراني، ثار تساؤل جوهري حول مدى كفاية القواعد التقليدية للمسؤولية الدولية، والمتمثلة أساساً في "مشروع مواد مسؤولية الدول عن الأفعال غير المشروعة دولياً" لعام 2001، في استيعاب التحديات الفريدة التي يفرضها هذا الفضاء الافتراضي.

([15]) دليل تالين 2.0 بشأن القانون الدولي المنطبق على العمليات السيبرانية، إعداد مجموعة من الخبراء الدوليين، 2017، القاعدة 69.

([16]) اللجنة الدولية للصليب الأحمر(ICRC) ، إسناد التصرف في الفضاء السيبراني لأغراض مسؤولية الدولة، ورقة موقف، 2019، ص 8.

([17]) د. متولي رشاد متولي الصعيدي و د. عبد اللطيف، آثار الذكاء الاصطناعي والحرب السيبرانية على البيئة الإنسانية أثناء النزاعات المسلحة، مجلة البحوث الفقهية والقانونية، 2024، ص 134.

([18]) اللجنة الدولية للصليب الأحمر(ICRC) ، القانون الدولي الإنساني والعمليات السيبرانية خلال النزاعات المسلحة، ورقة موقف، 2019، ص 7.

الفرع الأول: أركان المسؤولية الدولية في المجال السيبراني وتحديات الإسناد

لكي تترتب المسؤولية الدولية على دولة ما نتيجة فعل سيبراني، يجب توافر ركنين أساسيين وفقاً للمادة (2) من مشروع مواد لجنة القانون الدولي:

أولاً: الركن الذاتي (إسناد الفعل للدولة)

يعد الإسناد أصعب التحديات في الفضاء السيبراني. فمن الناحية القانونية، يُسند الفعل للدولة إذا ارتكبه أحد أجهزتها الرسمية (القوات المسلحة، أجهزة الاستخبارات) وفقاً للمادة (4)، أو إذا ارتكبه أشخاص يعملون بتوجيه من الدولة أو تحت رقابتها (المادة 8) [19]. ومع ذلك، فإن الطبيعة التقنية للفضاء السيبراني تسمح للدول باستخدام "الوكلاء السيبرانيين" أو الجماعات غير الحكومية للقيام بهجمات بالنيابة عنها، مما يجعل إثبات "الرقابة الفعلية" أمراً في غاية الصعوبة من الناحية القانونية والتقنية . [20]

إن التحدي يكمن في تطبيق "معيار السيطرة الفعالة " الذي وضعته محكمة العدل الدولية في قضية نيكاراغوا، على الأفعال السيبرانية. فإثبات أن الدولة كانت تسيطر فعلياً على كل عملية سيبرانية يقوم بها فرد أو مجموعة من داخل إقليمها هو أمر شبه مستحيل تقنياً. لذلك، يرى بعض الفقهاء ضرورة تخفيف معيار الإسناد في الفضاء السيبراني، أو الاعتماد بشكل أكبر على القرائن التقنية التي تربط الهجوم بالدولة، مثل استخدام البنية التحتية الحكومية أو أدوات برمجية حصرية . [21]

ثانياً: الركن الموضوعي (وقوع فعل غير مشروع دولياً)

يتمثل هذا الركن في كون الفعل السيبراني يشكل خرقاً لالتزام دولي يقع على عاتق الدولة. وفي الفضاء السيبراني، قد يتمثل هذا الخرق في انتهاك مبدأ السيادة، أو مبدأ عدم التدخل في الشؤون الداخلية، أو الالتزام بحظر استخدام القوة [22]. كما يشمل ذلك خرق الالتزامات التعاقدية الواردة في الاتفاقيات الدولية المعنية

([19]) لجنة القانون الدولي، مشروع مواد مسؤولية الدول عن الأفعال غير المشروعة دولياً، 2001، المواد 4 و 8.

([20]) د. نورية الساعدي المقريف، الحرب السيبرانية في ضوء أحكام القانون الدولي العام، مجلة كلية الحقوق، جامعة ليبيا، 2022، ص 156.

([21]) د. السيدة حليمة الدرمكي و أ.د. وائل علام، المسؤولية الدولية عن الهجمات السيبرانية الواقعة من كيانات من غير الدول، مجلة جامعة الشارقة للعلوم القانونية، 2024، ص 88.

([22]) د. متولي رشاد متولي الصعيدي و د. عبد اللطيف، آثار الذكاء الاصطناعي والحرب السيبرانية على البيئة الإنسانية أثناء النزاعات المسلحة، مجلة البحوث الفقهية والقانونية، 2024، ص 134.

بالأمن السيبراني. إن أهمية هذا الركن تكمن في أنه لا يشترط أن يكون الفعل السيبراني مجرماً في القانون الداخلي للدولة، بل يكفي أن يكون مخالفاً لالتزام دولي، سواء كان هذا الالتزام عرفياً أو تعاقدياً.

الفرع الثاني: مبدأ "العناية الواجبة" كآلية بديلة لتقرير المسؤولية

نظراً لصعوبة إسناد الهجمات السيبرانية التي يقوم بها أفراد أو جماعات من داخل إقليم الدولة إلى الدولة نفسها بشكل مباشر، برز مبدأ "العناية الواجبة" كأداة قانونية بديلة لتقرير المسؤولية.

أولاً: مفهوم العناية الواجبة في القانون الدولي

يقضي هذا المبدأ بأنه "لا يجوز للدولة أن تسمح باستخدام إقليمها للقيام بأعمال تضر بحقوق الدول الأخرى" [23]. وقد رسخ هذا المبدأ في القانون الدولي العرفي من خلال قضايا تحكيمية ودولية شهيرة، مثل قضية مضيق كورفو. إن جوهر المبدأ هو التزام الدولة ببذل جهد معقول لمنع الأضرار التي قد تنشأ من إقليمها وتصيب دولاً أخرى، وهو التزام ببذل عناية وليس التزاماً بتحقيق نتيجة. [24]

ثانياً: تطبيق المبدأ في الفضاء السيبراني

في السياق السيبراني، يعني هذا أن الدولة ملزمة باتخاذ كافة التدابير المعقولة والممكنة لمنع استخدام بنيتها التحتية الرقمية لشن هجمات سيبرانية ضد دول أخرى، حتى لو لم تكن الدولة هي من باشر الهجوم بنفسها [25] . إن الإخفاق في ممارسة هذه العناية الواجبة يعد فعلاً غير مشروع دولياً يوجب المسؤولية، ليس عن الهجوم ذاته، بل عن التقصير في منعه أو قمع مرتكبيه. [26]

ويشمل التزام العناية الواجبة في الفضاء السيبراني ثلاثة أبعاد رئيسية:

1. البعد التشريعي: سن القوانين الداخلية التي تجرم الأفعال السيبرانية وتسمح بالتعاون الدولي.

2. البعد الوقائي: اتخاذ التدابير التقنية والأمنية لحماية البنية التحتية الحيوية ومنع استخدامها كمنصة للهجمات.

([23]) محكمة العدل الدولية، قضية مضيق كورفو (المملكة المتحدة ضد ألبانيا)، حكم عام 1949.

([24]) د. عبد العزيز سرحان، القانون الدولي العام، دار النهضة العربية، القاهرة، 2010، ص 450.

([25]) بسمة صلال طه، المسؤولية الدولية الناجمة عن الهجمات السيبرانية، مجلة جامعة البيان للدراسات والبحوث، 2024، ص 42.

([26]) تقرير فريق الخبراء الحكوميين التابع للأمم المتحدة (GGE) المعني بالتطورات في ميدان المعلومات والاتصالات، 2021، الفقرة 71.

3. البعد الإجرائي: الاستجابة الفورية لطلبات المساعدة من الدول المتضررة والتحقيق في الهجمات التي تنطلق من إقليمها. [27]

إن مبدأ العناية الواجبة يوفر حلاً عملياً لتجاوز عقبة الإسناد الصعبة، حيث يمكن مساءلة الدولة عن تقصيرها في السيطرة على إقليمها السيبراني، بدلاً من محاولة إثبات سيطرتها المباشرة على الفاعل غير الحكومي.

الفرع الثالث: التحديات القانونية والتقنية التي تواجه تطبيق قواعد المسؤولية

يواجه تطبيق القواعد العامة للمسؤولية الدولية في الفضاء السيبراني عدة عقبات جوهرية، تتطلب إيجاد حلول قانونية مبتكرة:

أولا: مشكلة الإثبات الرقمي وتحديد المصدر:

كما ذكرنا سابقاً، فإن الأدلة الرقمية بطبيعتها قابلة للتلاعب، كما أن تقنيات التخفي تجعل من الصعب تحديد المصدر الحقيقي للهجوم بيقين قانوني كافٍ لتقرير المسؤولية الدولية. [28] إن القانون الدولي بحاجة إلى تطوير معايير موحدة لجمع وحفظ وتحليل الأدلة الرقمية لضمان قبولها في المحاكم الدولية.

ثانيا: تعدد الفاعلين وتوزيع المسؤولية:

في كثير من الأحيان، يشترك في الهجوم السيبراني فاعلون من دول متعددة، مما يثير إشكالية توزيع المسؤولية الدولية بين هذه الدول، ومدى تضامنها في جبر الضرر [29]. فهل تتحمل الدولة التي انطلق منها الهجوم المسؤولية كاملة، أم تتحمل الدولة التي وفرت البنية التحتية جزءاً منها؟ إن مبدأ المسؤولية المشتركة قد يكون هو الحل، حيث تتحمل كل دولة مسؤولية الجزء الذي أسهمت به في الفعل غير المشروع.

ثالثا: تحديد معيار الضرر وجبره:

يثور الخلاف حول ما إذا كان الضرر المعنوي أو الاقتصادي الصرف (دون تدمير مادي) كافياً لترتيب المسؤولية الدولية، خاصة في ظل اعتماد المجتمعات الحديثة الكلي على البيانات الرقمية التي قد لا يكون لها

([27]) د. محمد محمود شوقي و د. محمد سعيد عبد العاطي، الوسيط في مكافحة الجرائم السيبرانية، منشورات الحلبي الحقوقية، بيروت، 2024، ص 112.

([28]) د. عبد الفتاح بيومي حجازي، الإثبات الإلكتروني في المواد الجنائية، دار النهضة العربية، القاهرة، 2017، ص 210.

([29]) د. متولي رشاد متولي الصعيدي و د. عبد اللطيف، آثار الذكاء الاصطناعي والحرب السيبرانية على البيئة الإنسانية أثناء النزاعات المسلحة، مجلة البحوث الفقهية والقانونية، 2024، ص 134.

كيان مادي ملموس [30]. إن جبر الضرر في المجال السيبراني قد لا يقتصر على التعويض المالي، بل قد يشمل أيضاً الضمانات بعدم التكرار والاعتذار الرسمي ، خاصة في حالة الهجمات التي تستهدف السيادة أو التدخل في الشؤون الداخلية.

الفرع الرابع: المقارنة بين مواقف الدول (الولايات المتحدة – فرنسا – الصين)

يُلاحظ أن التعامل الدولي مع مسألة الهجمات السيبرانية يختلف بشكل واضح بين الدول الكبرى، الأمر الذي يعكس غياب موقف دولي موحد تجاه تطبيق قواعد المسؤولية الدولية في الفضاء السيبراني.

ففي الولايات المتحدة الأمريكية، يتجه الفقه والممارسة العملية إلى اعتبار الهجمات السيبرانية التي ترقى إلى مستوى "استخدام القوة" أو "الهجوم المسلح" خاضعة لقواعد القانون الدولي التقليدي، مع تركيز واضح على مبدأ الردع والدفاع السيبراني، بما في ذلك إمكانية الرد السيبراني أو العسكري وفقًا لمبدأ الدفاع الشرعي.

أما فرنسا، فقد تبنت موقفًا أكثر تحفظًا، حيث أكدت على ضرورة تطوير إطار قانوني دولي جديد خاص بالفضاء السيبراني، مع التشديد على مبدأ سيادة الدولة الرقمية، وضرورة احترام الحدود السيبرانية للدول.

في حين تتبنى الصين رؤية أكثر سيادية، إذ تؤكد على مبدأ "السيادة المطلقة في الفضاء السيبراني"، وترفض بشكل واسع فكرة التدخل الخارجي أو التوسع في تطبيق قواعد المسؤولية الدولية التقليدية بشكل يسمح بتدخلات عبر الحدود في الفضاء الرقمي.

هذا التباين يعكس أن قواعد المسؤولية الدولية لا تُطبق بشكل موحد، بل تخضع لاختلافات سياسية وقانونية تؤثر على فعاليتها.

المبحث الثاني

أركان وآثار قيام المسؤولية الدولية عن الجرائم السيبرانية

تُعدّ المسؤولية الدولية عن الأفعال غير المشروعة دولياً الركن الأساسي في بناء النظام القانوني الدولي، فهي الضمانة الحقيقية لالتزام الدول بقواعد القانون الدولي. وفي سياق الفضاء السيبراني، تبرز تحديات جمة أمام تطبيق هذه القواعد التقليدية، لا سيما فيما يتعلق بإسناد الفعل غير المشروع إلى الدولة، والتحقق من التزامها

[30] اللجنة الدولية للصليب الأحمر(ICRC) ، إسناد التصرف في الفضاء السيبراني لأغراض مسؤولية الدولة، ورقة موقف، 2019، ص 8.

بمعيار العناية الواجبة. ويهدف هذا المبحث إلى تحليل هذين الركنين المحوريين، ومن ثم بيان الآثار القانونية المترتبة على قيام هذه المسؤولية.

المطلب الأول

إشكالية إسناد الجرائم السيبرانية إلى الدولة

تُعدّ إشكالية إسناد الأفعال غير المشروعة دولياً إلى الدولة هي العقدة القانونية والتقنية الأكثر تعقيداً في مجال المسؤولية الدولية عن الجرائم والهجمات السيبرانية. ففي حين أن قواعد القانون الدولي التقليدية، ممثلة في مواد لجنة القانون الدولي بشأن مسؤولية الدول، توفر إطاراً نظرياً للإسناد، فإن الطبيعة الفريدة للفضاء السيبراني تجعل تطبيق هذه القواعد أمراً بالغ الصعوبة، مما يهدد بتقويض فعالية القانون الدولي في هذا المجال الحيوي.

الفرع الاول: تحليل المعايير التقليدية للإسناد في سياق العمليات السيبرانية

تستند عملية الإسناد القانوني إلى مجموعة من القواعد التي تهدف إلى ربط السلوك المادي (الهجوم السيبراني) بالدولة، بحيث يُعتبر هذا السلوك تصرفاً صادراً عنها. وتتمحور هذه القواعد حول تصرفات أجهزة الدولة، وتصرفات الأفراد أو الكيانات التي تعمل تحت سيطرتها أو توجيهها.

أولا: الإسناد المباشر:

تنص المادة الرابعة من مواد مسؤولية الدول على أن تصرف أي جهاز من أجهزة الدولة يُعدّ فعلاً من أفعال الدولة بموجب القانون الدولي، بغض النظر عن طبيعة هذا الجهاز (تشريعي، تنفيذي، قضائي) أو مركزه في هيكل الدولة. [31]

وفي سياق العمليات السيبرانية، ينطبق هذا المعيار على الهجمات التي تشنها بشكل مباشر وحدات رسمية تابعة للدولة، مثل وحدات الحرب الإلكترونية أو الاستخبارات العسكرية أو وكالات الأمن القومي.

التطبيق في الفضاء السيبراني: يُعدّ الإسناد المباشر هو الأسهل من الناحية القانونية، لكنه الأصعب من الناحية التقنية. فالدول التي تشن هجمات سيبرانية رسمية نادراً ما تترك بصمات رقمية واضحة تربطها مباشرة بأجهزتها

([31]) لجنة القانون الدولي، مواد بشأن مسؤولية الدول عن الأفعال غير المشروعة دولياً، 2001، المادة 4.

الحكومية. وغالباً ما يتم استخدام تقنيات التمويه أو التوجيه عبر خوادم وسيطة لإخفاء المصدر الحقيقي للهجوم، مما يحول دون تطبيق المادة 4 بشكل قاطع إلا في حالات نادرة جداً.

ثانيا: الإسناد غير المباشر:

تُشكل المادة الثامنة، التي تتناول تصرفات الأشخاص أو المجموعات التي تعمل "بناءً على تعليمات الدولة أو بتوجيهها أو تحت رقابتها"، محور الجدل القانوني الأكبر في الفضاء السيبراني. [32]

فمعظم الهجمات السيبرانية الكبرى تُنفذ من قبل كيانات من غير الدول، مثل مجموعات الهاكرز المأجورة أو المنظمات الإجرامية السيبرانية، والتي قد تكون مدعومة أو مُوجهة من قبل دولة ما.

1. معيار "الرقابة الفعالة":

لإثبات الإسناد بموجب المادة 8، اعتمدت محكمة العدل الدولية في قضية الأنشطة العسكرية وشبه العسكرية في نيكاراغوا (1986) معيار "الرقابة الفعالة". ويقضي هذا المعيار بضرورة إثبات أن الدولة مارست رقابة فعلية على كل عملية محددة من العمليات التي أدت إلى الفعل غير المشروع، وليس مجرد تقديم الدعم العام أو التمويل . [33]

فشل المعيار في الفضاء السيبراني: يُعتبر معيار الرقابة الفعالة غير مناسب إلى حد كبير في البيئة السيبرانية. فالهجمات السيبرانية تتميز بالسرعة واللامركزية، وقد يتم إطلاقها ببرمجيات ذاتية التشغيل أو بتوجيهات عامة من الدولة، دون الحاجة إلى رقابة لحظية على كل خطوة. إن المطالبة بإثبات "الرقابة الفعالة" على كل نقرة أو حزمة بيانات يجعل من المستحيل تقريباً إسناد الهجمات التي تشنها مجموعات الهاكرز المدعومة من الدولة، مما يمنح الدول حصانة فعلية من المسؤولية.

2. معيار "الرقابة الشاملة":

([32]) المرجع السابق، المادة 8.

([33]) محكمة العدل الدولية، قضية الأنشطة العسكرية وشبه العسكرية في نيكاراغوا ضد الولايات المتحدة الأمريكية، حكم 27 يونيو 1986، الفقرة 115.

في المقابل، تبنت المحكمة الجنائية الدولية ليوغوسلافيا السابقة في قضية تاديتش (1999) معيار "الرقابة الشاملة"، وهو معيار أكثر مرونة يتطلب إثبات أن الدولة مارست رقابة عامة على المجموعة ككل وليس على كل عملية على حدة [34] .

ورغم أن هذا المعيار قد يكون أكثر ملاءمة للفضاء السيبراني، إلا أن الفقه القانوني الدولي يميل إلى تفضيل معيار "الرقابة الفعالة" في سياق مسؤولية الدول، مما يُبقي على التحدي قائماً.

الفرع الثاني: التحديات التقنية والقانونية للإثبات في الإسناد السيبراني

لا تقتصر إشكالية الإسناد على تطبيق القواعد القانونية فحسب، بل تتجذر في التحديات التقنية التي تحيط بعملية تحديد هوية المهاجمين.

أولا: التمييز بين الإسناد التقني والسياسي والقانوني

أصبح من الضروري التمييز بين مستويات الإسناد المختلفة التي تظهر في أعقاب الهجمات السيبرانية الكبرى:

نوع الإسناد	معيار الإثبات	الهدف الأساسي	الآثار المترتبة
الإسناد التقني	أدلة رقمية IPs، بصمات البرمجيات، الثغرات المستغلة.	تحديد المصدر التقني للهجوم (الخوادم، البرمجيات، البنية التحتية).	أساس للتحقيق، ولكنه غير كافٍ للمسؤولية القانونية.
الإسناد السياسي	أدلة استخباراتية، أدلة ظرفية, تقارير أمنية.	إعلان الدولة المتضررة عن مسؤولية دولة أخرى.	إجراءات دبلوماسية, عقوبات اقتصادية، تصعيد سياسي.
الإسناد القانوني	أدلة مقنعة تفي بمعيار الإثبات القانوني.	إثبات المسؤولية الدولية للدولة أمام هيئة قضائية أو دولية.	قيام المسؤولية الدولية, الالتزام بالجبر.

([34]) المحكمة الجنائية الدولية ليوغوسلافيا السابقة، قضية المدعي العام ضد تاديتش، حكم 15 يوليو 1999، الفقرة 137.

ثانيا: معيار الإثبات في القانون الدولي

لا يوجد معيار إثبات موحد في القانون الدولي، ولكن الفقه يميل إلى المطالبة بـ "أدلة مقنعة" أو "أدلة واضحة ومقنعة "لإثبات مسؤولية الدولة [35] .

وفي الفضاء السيبراني، يرى بعض الخبراء أن هذا المعيار يجب أن يكون مرناً ليأخذ في الاعتبار الطبيعة التخريبية للهجمات وصعوبة الحصول على أدلة مباشرة.

1. الأدلة الظرفية:

في غياب الأدلة المباشرة، يمكن الاعتماد على الأدلة الظرفية لإثبات الإسناد، مثل:

• نمط الهجوم: تكرار الهجمات بنفس الأسلوب أو الأدوات.

• توافق المصالح: وجود مصلحة واضحة للدولة المُسند إليها الهجوم في إلحاق الضرر بالدولة المتضررة.

• الفشل في منع الهجوم: إثبات أن الدولة كانت تعلم أو كان ينبغي أن تعلم بالهجوم وفشلت في اتخاذ الإجراءات اللازمة لمنعه (وهو ما يقودنا إلى مبدأ العناية الواجبة).

2. حالة هجمات إستونيا 2007 كنموذج:

تُعدّ الهجمات السيبرانية التي تعرضت لها إستونيا في عام 2007، والتي استهدفت البنية التحتية الحيوية، مثالاً واضحاً على تحدي الإسناد. فبالرغم من الإسناد السياسي للهجمات إلى روسيا، إلا أن إستونيا لم تتمكن من تقديم أدلة قانونية قاطعة تفي بمعيار "الرقابة الفعالة" لإثبات مسؤولية الدولة الروسية بموجب المادة 8، مما أدى إلى عدم تفعيل المسؤولية الدولية بشكل رسمي. [36]

([35]) William Banks, Cyber Attribution and State Responsibility, International Law Studies, Vol. 97, 2021, p. 18.

([36]) Eneken Tikk, Kadri Kaska, and Liis Vihul, International Law and Cyber Attacks: The Case of Estonia, Estonian Ministry of Defence, 2008, p. 45.

المطلب الثاني

التزام الدولة بالعناية الواجبة

يُعدّ مبدأ العناية الواجبة التزاماً قانونياً عرفياً، يفرض على الدولة اتخاذ التدابير المعقولة والمناسبة لمنع استخدام إقليمها للإضرار بالدول الأخرى.

الفرع الاول: الأساس القانوني لمبدأ العناية الواجبة

يستمد هذا المبدأ أساسه من مبدأ السيادة الإقليمية، الذي يفرض على الدولة التزاماً سلبياً بعدم التدخل في شؤون الدول الأخرى، والتزاماً إيجابياً بضمان عدم استخدام إقليمها بطريقة تضر بالدول الأخرى. وقد تم ترسيخ هذا المبدأ قضائياً في حكم محكمة العدل الدولية في قضية مضيق كورفو (1949)، حيث أكدت المحكمة على "التزام كل دولة بعدم السماح عن علم باستخدام إقليمها لأفعال تتعارض مع حقوق الدول الأخرى." [37]

الفرع الثاني: نطاق الالتزام في الفضاء السيبراني

يتطلب تطبيق مبدأ العناية الواجبة في الفضاء السيبراني من الدولة بذل جهد معقول ومناسب لحماية البنية التحتية الحيوية، ومنع الأنشطة السيبرانية الضارة التي تنطلق من أراضيها. ويُعدّ هذا الالتزام التزاماً ببذل عناية وليس التزاماً بتحقيق نتيجة، أي أن الدولة لا تُسأل عن وقوع الهجوم بحد ذاته، بل عن فشلها في اتخاذ الإجراءات الوقائية أو الردعية اللازمة.

أولا: معيار المعقولية والقدرة:

يجب أن يكون معيار العناية الواجبة مرناً ويأخذ في الاعتبار قدرات الدولة المعنية. فالتدابير المطلوبة من دولة ذات قدرات تقنية واقتصادية متقدمة تختلف عن تلك المطلوبة من دولة نامية. ويشمل الالتزام العناصر التالية:

1. الالتزام بالوقاية : اتخاذ تدابير تشريعية وإدارية وتقنية لتعزيز الأمن السيبراني للبنية التحتية الحيوية، ومراقبة الأنشطة المشبوهة.

2. الالتزام بالاستجابة: التحقيق الفوري في الهجمات السيبرانية التي تنطلق من الإقليم، واتخاذ الإجراءات اللازمة لوقفها ومعاقبة مرتكبيها.

([37]) محكمة العدل الدولية، قضية مضيق كورفو (المملكة المتحدة ضد ألبانيا)، حكم 9 أبريل 1949، ص 22.

3. **الالتزام بالتعاون:** الاستجابة لطلبات المساعدة من الدول المتضررة وتبادل المعلومات الاستخباراتية والتقنية ذات الصلة [38] .

ثانيا: حالة الإهمال الجسيم:

تُسأل الدولة عن الإخلال بالعناية الواجبة في حالتين رئيسيتين:

1. العلم المفترض: إذا كان ينبغي على الدولة أن تعلم بوجود نشاط سيبراني ضار ينطلق من إقليمها، وفشلت في اتخاذ الإجراءات اللازمة لوقفه.

2. التقاعس المتعمد : إذا علمت الدولة بوجود النشاط الضار وتقاعست عن اتخاذ الإجراءات اللازمة لوقفه، مما يرقى إلى مستوى التسامح أو التواطؤ. [39]

المطلب الثالث

الآثار المترتبة على قيام المسؤولية الدولية

متى ثبت قيام المسؤولية الدولية للدولة، سواء بالإسناد المباشر أو بالإخلال بالتزام العناية الواجبة، تترتب على الدولة المسؤولة مجموعة من الآثار القانونية الملزمة بموجب القانون الدولي العرفي وقواعد لجنة القانون الدولي.

الفرع الاول : الالتزام بوقف الفعل غير المشروع وضمان عدم التكرار

يُعدّ هذا الالتزام هو الأثر الفوري والأساسي لقيام المسؤولية. فالدولة المسؤولة ملزمة بـ:

اولا: وقف الفعل غير المشروع: إنهاء الهجوم السيبراني أو النشاط الضار فوراً.

ثانيا: تقديم ضمانات وتعهدات بعدم التكرار: اتخاذ الإجراءات اللازمة لضمان عدم تكرار الفعل غير المشروع مستقبلاً، وقد يشمل ذلك تعديلات تشريعية أو إدارية أو تقنية [40] .

([38]) حمزة محمود عبد الفتاح، الالتزام الدولي ببذل العناية الواجبة في الفضاء السيبراني بين التدابير الرادعة ومنع الأضرار السيبرانية العابرة، مجلة الدراسات القانونية والاقتصادية، 2025، ص 8.

([39]) Michael N. Schmitt, Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, Cambridge University Press, 2017, Rule 10.

([40]) لجنة القانون الدولي، مواد بشأن مسؤولية الدول عن الأفعال غير المشروعة دولياً، 2001، المادة 30.

الفرع الثاني: الإلتزام بجبر الضرر

يجب على الدولة المسؤولة أن تقوم بجبر كامل للضرر الذي لحق بالدولة المتضررة نتيجة الفعل غير المشروع. ويشمل الجبر كل الأضرار المادية والمعنوية، ويأخذ ثلاثة أشكال متكاملة:

أولا: الرد:

يهدف إلى إعادة الحال إلى ما كان عليه قبل وقوع الفعل غير المشروع. وفي سياق الهجمات السيبرانية، قد يشمل ذلك استعادة البيانات المحذوفة، أو إعادة تشغيل الأنظمة المعطلة، أو إلغاء المعاملات غير القانونية. ويُعدّ الرد هو الشكل الأفضل للجبر ما لم يكن مستحيلاً مادياً أو ينطوي على عبء غير متناسب.

ثانيا: التعويض:

يُستخدم التعويض لجبر الأضرار التي لا يمكن إصلاحها بالرد. ويشمل التعويض أي خسارة مالية قابلة للتقييم، مثل:

1. تكاليف التحقيق التقني والقانوني في الهجوم.
2. تكاليف إصلاح الأضرار المادية والبرمجية.
3. الخسائر الاقتصادية المباشرة الناتجة عن توقف الأنظمة أو تسرب البيانات [41] .

ثالثاً: الترضية:

تُستخدم الترضية لجبر الضرر المعنوي أو غير المادي، لا سيما في حالة انتهاك سيادة الدولة أو الإضرار بسمعتها. وقد تتخذ الترضية شكل:

1. الاعتراف بانتهاك القانون الدولي.
2. تقديم اعتذار رسمي.
3. معاقبة المسؤولين عن الفعل غير المشروع.

([41]) المرجع السابق، المادة 36.

الفرع الثالث: حق الدولة المتضررة في اتخاذ التدابير المضادة

في حال فشل الدولة المسؤولة في الوفاء بالتزاماتها بوقف الفعل وجبر الضرر، يحق للدولة المتضررة أن تتخذ تدابير مضادة ضد الدولة المسؤولة. وتُعرف التدابير المضادة بأنها أفعال غير مشروعة دولياً في الأصل، ولكنها تُصبح مشروعة لأنها تُتخذ رداً على فعل غير مشروع سابق من الدولة المسؤولة.

أولا: شروط مشروعية التدابير المضادة:

يجب أن تلتزم التدابير المضادة بشروط صارمة لضمان مشروعيتها:

1. الهدف: يجب أن يكون الهدف الوحيد للتدابير المضادة هو حمل الدولة المسؤولة على الوفاء بالتزاماتها.

2. التناسب: يجب أن تكون التدابير المضادة متناسبة مع الضرر الذي لحق بالدولة المتضررة، مع الأخذ في الاعتبار جسامة الفعل غير المشروع والحقوق المتضررة.

3. القيود الجوهرية: لا يجوز أن تنتهك التدابير المضادة الالتزامات الآمرة، أو الالتزامات المتعلقة بحقوق الإنسان الأساسية، أو الالتزامات المتعلقة بالقانون الدولي الإنساني. [42]

ثانيا: التدابير المضادة في الفضاء السيبراني:

يثير تطبيق التدابير المضادة في الفضاء السيبراني جدلاً حول مدى مشروعية الرد بهجوم سيبراني مقابل. ويُشترط في أي تدبير مضاد سيبراني أن يكون متناسباً، وأن يتم اتخاذه بعد إخطار الدولة المسؤولة، وأن يتم وقفه فور وفاء الدولة المسؤولة بالتزاماتها.

الخاتمة

لقد تناول هذا البحث إشكالية المسؤولية الدولية عن الجرائم السيبرانية، مؤكداً على التحديات الجوهرية التي تواجه تطبيق القواعد التقليدية للقانون الدولي العام في الفضاء السيبراني. وفي ضوء التحليل المعمق للمبحثين الأول والثاني، تم التوصل إلى النتائج والتوصيات التالية، مقدمة في شكل نقاط مترابطة:

([42]) المرجع السابق، المادة 51.

- **قصور معايير الإسناد التقليدية والحاجة إلى التطوير:**

أثبت التحليل أن معايير الإسناد التقليدية، لا سيما معيار "الرقابة الفعالة" المنصوص عليه في المادة الثامنة من مواد مسؤولية الدول، تُعدّ قاصرة وغير مناسبة لتطبيقها على الأفعال التي تقوم بها كيانات من غير الدول بتوجيه أو دعم من الدولة، مما يمنح الدول حصانة فعلية من المسؤولية [43]. وعليه، يوصى بضرورة تطوير معيار قانوني جديد للإسناد، يكون أكثر مرونة، وربما يتبنى معيار "الرقابة الشاملة" أو معيار "السيطرة أو التوجيه العام"، وذلك لتسهيل إسناد الأفعال التي تقوم بها الكيانات الوكيلة إلى الدولة الراعية.

- **فعالية مبدأ العناية الواجبة وضرورة تحديد نطاقه:**

يمثل مبدأ "العناية الواجبة" الآلية القانونية الأكثر واقعية وفعالية لتفعيل المسؤولية الدولية في هذا المجال، حيث يركز على فشل الدولة في اتخاذ التدابير المعقولة لمنع الأضرار السيبرانية التي تنطلق من إقليمها، بدلاً من التركيز على الإسناد المباشر الصعب الإثبات [44] . وبناءً على هذه النتيجة، يجب على الدول العمل على وضع إطار إلزامي يحدد بوضوح نطاق التزام الدولة بالعناية الواجبة في الفضاء السيبراني، مع الأخذ في الاعتبار التباين في القدرات التقنية بين الدول، وذلك لتعزيز الالتزام بالوقاية والاستجابة والتعاون.

- **التباين بين مستويات الإسناد والحاجة إلى آلية إثبات دولية:**

يوصي البحث بإنشاء آلية دولية متخصصة ومستقلة تُعنى بمتابعة الهجمات السيبرانية العابرة للحدود، على أن تعمل تحت مظلة منظمة الأمم المتحدة، وبالتنسيق مع الأجهزة الدولية المختصة بالأمن والسلم الدوليين، بما يضمن لها الشرعية الدولية والقدرة على التعاون مع الدول .

وتتمثل مهام هذه الآلية في :

- تقديم الدعم الفني والقانوني للدول في مجال التحقيق في الهجمات السيبرانية .
- المساهمة في تطوير قواعد دولية موحدة للإسناد الرقمي وإثبات المسؤولية .
- تعزيز تبادل المعلومات والأدلة الرقمية بين الدول .

([43]) لجنة القانون الدولي، مواد بشأن مسؤولية الدول عن الأفعال غير المشروعة دولياً، 2001، المادة 8.

([44]) محكمة العدل الدولية، قضية مضيق كورفو (المملكة المتحدة ضد ألبانيا)، حكم 9 أبريل 1949، ص 22.

- إعداد تقارير دولية دورية حول التهديدات السيبرانية العابرة للحدود.

ويستند إنشاء هذه الآلية إلى مقاصد ميثاق الأمم المتحدة المتعلقة بحفظ السلم والأمن الدوليين، إضافة إلى التطور المتزايد للتهديدات السيبرانية التي أصبحت تمثل خطرًا حقيقيًا على استقرار الدول والبنية التحتية الحيوية .

كما يمكن أن يستند الإطار القانوني لهذه الآلية إلى اتفاقية الأمم المتحدة لمكافحة الجرائم السيبرانية لعام 2024، باعتبارها خطوة دولية حديثة تدعم تعزيز التعاون الدولي في مواجهة الجرائم والتهديدات السيبرانية. (45)

- **تأكيد الآثار القانونية التقليدية وضرورة تقنين التدابير المضادة:**

على الرغم من التحديات في إثبات المسؤولية، فإن الآثار القانونية المترتبة على قيامها تظل تقليدية ومؤكدة، وتشمل الالتزام بوقف الفعل غير المشروع وجبر الضرر بكافة صوره (الرد، التعويض، الترضية)، وحق الدولة المتضررة في اتخاذ التدابير المضادة المشروعة. وفي هذا الصدد، يجب تقنين شروط وضوابط استخدام التدابير المضادة السيبرانية لضمان التناسب وعدم التصعيد، مع ضرورة الاعتراف القاطع بأن الأضرار الناجمة عن الهجمات السيبرانية التي تستهدف البنية التحتية الحيوية ترقى إلى مستوى الضرر الدولي الذي يستوجب جبر الضرر بكافة صوره. (46)

(45) Michael N. Schmitt, Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, Cambridge University Press, 2017, Rule 10.

(46) حمزة محمود عبد الفتاح، الالتزام الدولي ببذل العناية الواجبة في الفضاء السيبراني بين التدابير الرادعة ومنع الأضرار السيبرانية العابرة، مجلة الدراسات القانونية والاقتصادية، 2025، ص 8.

قائمة المراجع :

اولا: المراجع العربية :

- أثير هلال فليح الدليمي، القواعد الدولية لمكافحة الجرائم الإلكترونية والسيبرانية، دار النشر والتوزيع، عمّان، 2024 .
- عبد العزيز سرحان، القانون الدولي العام، دار النهضة العربية، القاهرة، 2010 .
- عبد الفتاح بيومي حجازي، الإثبات الإلكتروني في المواد الجنائية، دار النهضة العربية، القاهرة، 2017 .
- عبد الفتاح بيومي حجازي، الجرائم المعلوماتية بين النظرية والتطبيق، دار الفكر الجامعي، الإسكندرية، 2010 .
- عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والإنترنت في القانون العربي النموذجي، دار الفكر الجامعي، الإسكندرية، 2006 .
- محمد أمين الشوابكة، الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، عمّان، 2014 .
- محمد محمود شوقي ومحمد سعيد عبد العاطي، الوسيط في مكافحة الجرائم السيبرانية، منشورات الحلبي الحقوقية، بيروت، 2024.

ثانياً: الأبحاث والمقالات العلمية العربية

- بسمة صلال طه، "المسؤولية الدولية الناجمة عن الهجمات السيبرانية"، مجلة جامعة البيان للدراسات والبحوث، 2024 .
- حمزة محمود عبد الفتاح، "الالتزام الدولي ببذل العناية الواجبة في الفضاء السيبراني بين التدابير الرادعة ومنع الأضرار السيبرانية العابرة"، مجلة الدراسات القانونية والاقتصادية، 2025 .
- السيدة حليمة الدرمكي ووائل علام، "المسؤولية الدولية عن الهجمات السيبرانية الواقعة من كيانات من غير الدول"، مجلة جامعة الشارقة للعلوم القانونية، 2024 .
- سامر نمر سالم الجاروشة، الجرائم السيبرانية وحقوق الإنسان في القوانين الدولية والوطنية، دار النهضة العربية، القاهرة، 2023 .

- صديقي سامية، "المسؤولية الدولية الناشئة عن الهجمات السيبرانية في ضوء القانون الدولي المعاصر"، مجلة الزرقاء للبحوث والدراسات الإنسانية، المجلد 19، العدد 1، 2019 .
- متولي رشاد متولي الصعيدي وعبد اللطيف، "آثار الذكاء الاصطناعي والحرب السيبرانية على البيئة الإنسانية أثناء النزاعات المسلحة"، مجلة البحوث الفقهية والقانونية، 2024 .
- نورية الساعدي المقريف، "الحرب السيبرانية في ضوء أحكام القانون الدولي العام"، مجلة كلية الحقوق، جامعة ليبيا، 2022.

ثالثاً: الوثائق والاتفاقيات والتقارير الدولية

- اتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية، اعتمدتها الجمعية العامة، ديسمبر 2024 .
- اللجنة الدولية للصليب الأحمر (ICRC) ، إسناد التصرف في الفضاء السيبراني لأغراض مسؤولية الدولة، ورقة موقف، 2019 .
- اللجنة الدولية للصليب الأحمر (ICRC) ، القانون الدولي الإنساني والعمليات السيبرانية خلال النزاعات المسلحة، ورقة موقف، 2019 .
- دليل تالين 2.0 بشأن القانون الدولي المنطبق على العمليات السيبرانية، إعداد مجموعة من الخبراء الدوليين، 2017 .
- تقرير فريق الخبراء الحكوميين التابع للأمم المتحدة (GGE) المعني بالتطورات في ميدان المعلومات والاتصالات، 2021 .
- لجنة القانون الدولي، مشروع مواد مسؤولية الدول عن الأفعال غير المشروعة دولياً، 2001 .
- محكمة العدل الدولية، قضية الأنشطة العسكرية وشبه العسكرية في نيكاراغوا ضد الولايات المتحدة الأمريكية، حكم 27 يونيو 1986 .
- محكمة العدل الدولية، قضية مضيق كورفو (المملكة المتحدة ضد ألبانيا)، حكم 9 أبريل 1949 .
- المحكمة الجنائية الدولية ليوغوسلافيا السابقة، قضية المدعي العام ضد تاديتش، حكم 15 يوليو 1999.

رابعاً: المراجع الأجنبية

- Eneken Tikk, Kadri Kaska, and Liis Vihul, *International Law and Cyber Attacks: The Case of Estonia*, Estonian Ministry of Defence, 2008.
- Michael N. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge University Press, 2017.
- William Banks, "Cyber Attribution and State Responsibility", *International Law Studies*, Vol. 97, 2021.

STARDOM UNIVERSITY

Stardom University

Stardom Scientific Journal of Law and Political Studies

– Stardom Scientific Journal of Law and Political Studies –
Issued quarterly by Stardom University
1st issue- 4th Volume 2026
ISSN 2980-3764