السيادة الرقمية للدول في مواجهة التهديدات السيبرانية غير الحكومية نحو بناء إطار قانوني دولي مرن ومتكامل

د. نانسي عبد اللّه حامد الديب

مدرس القانون الدولي العام

بالمعهد العالي للتجارة والعلوم الإدارية بالمنصورة

البريد الالكتروني

nancyeldeeb1982@gmail.com

(ISSN: 2537 - 0758)

السيادة الرقمية للدول في مواجهة التهديدات السيبرانية غير الحكومية نحو بناء إطار قانوني دولي مرن ومتكامل

د. نانسي عبد الله حامد الديب

الملخص:

يشهد العالم تحولًا نوعيًا في طبيعة التهديدات الأمنية نتيجة الانتقال إلى الفضاء السيبراني، حيث باتت الهجمات الرقمية تشكّل تحديًا مباشرًا لسيادة الدول، خاصة في ظل تصاعد دور الفاعلين غير الحكوميين المدعومين أو المستقلين. ويطرح هذا الواقع إشكاليات قانونية معقدة تتعلق بكيفية تكييف الهجمات السيبرانية ضمن قواعد القانون الدولي العام، ومدى كفاية المبادئ التقليدية مثل مبدأ عدم التدخل، وحق الدفاع عن النفس، وإسناد الأفعال، لتوفير الحماية اللازمة للدول في المجال الرقمي.

يهدف هذا البحث إلى دراسة مفهوم **السيادة الرقمية** وتطوراته في ظل غياب معاهدة دولية ملزمة تنظم الأمن السيبراني، مع تحليل التحديات التي تعيق تطبيق قواعد المسؤولية الدولية على الفاعلين غير الحكوميين. كما يتناول البحث الحاجة إلى إطار قانوني جديد، ويستعرض البدائل الواقعية المتاحة، مثل التعاون الإقليمي، والمبادئ الطوعية، والممارسات الفضلى.

اعتمدت الدراسة على المنهج التحليلي المقارن، بالرجوع إلى الأدبيات القانونية، والتقارير الدولية، والتشريعات النموذجية، بهدف تقديم تصور متوازن يجمع بين ضرورة **تعزيز الأمن الرقمي** وحماية **مبدأ السيادة** في الفضاء السيبراني، مع الحفاظ على التوازن بين الحرية والرقابة، والسيادة والتعاون الدولي.

الكلمات المفتاحية: السيادة الرقمية– الفضاء السيبراني– الهجمات الإلكترونية– القانون الدولي– الأمن السيبراني– الفاعلون غير الحكوميين– مبدأ عدم التدخل– الدفاع عن النفس– المسؤولية الدولية.

Abstract:

The world is witnessing a qualitative transformation in the nature of security threats due to the expansion of cyberspace, where digital attacks have become a direct challenge to state sovereignty. This shift is particularly critical in light of the growing influence of non-state actors—whether state-sponsored or independent—who possess advanced cyber capabilities. These developments raise complex legal questions concerning the applicability of international law, especially the adequacy of traditional principles such as non-intervention, the right of self-defense, and attribution of acts in the cyber domain.

This research explores the concept of **digital sovereignty** and its evolution in the absence of a binding international treaty governing cybersecurity. It analyzes the limitations of the current international legal framework in addressing threats posed by non-state cyber actors and highlights the pressing need for a new international legal instrument. The study also reviews alternative mechanisms, including regional cooperation, voluntary norms, and best practices.

Using an analytical and comparative methodology, this paper draws upon legal literature, international reports, and model legislations to provide a balanced perspective that reconciles the need to **strengthen digital security** while **preserving state sovereignty** in cyberspace, all within a framework that respects the delicate balance between freedom and control, and sovereignty and international cooperation.

Keywords: Digital Sovereignty– Cyberspace– Cyberattacks– International Law– Cybersecurity– Non-State Actors– Non-Intervention Principle– Self-Defense– State Responsibility.

(ISSN: 2537 - 0758)

مقدمة البحث:

أحدثت الثورة الرقمية تحولات جذرية في مفاهيم السيادة والأمن القومي، إذ لم تعد حدود الدولة تقف عند المجال الجغرافي التقليدي، بل امتدت إلى الفضاء السيبراني، الذي أضحى ميدانًا جديدًا للصراع والتفاعل الدولي. ومع تنامي التهديدات السيبرانية، خاصة تلك التي تقوم بها جهات غير حكومية مدعومة أو مستقلة عن الدول، برزت الحاجة الملحّة لإعادة النظر في الأطر القانونية الناظمة لهذا المجال. ففي ظل غياب معاهدة دولية شاملة تحكم الفضاء السيبراني، تواجه الدول تحديات حقيقية تتعلق بحماية سيادتها الرقمية، وتحديد المسؤولية الدولية، والتعامل مع الفاعلين غير الحكوميين الذين يتحركون بحرية في بيئة تتجاوز الحدود. من هنا تنبع أهمية تناول هذا الموضوع بالتحليل القانوني والواقعي، بغية بلورة رؤية واضحة لآليات المواجهة القانونية والتعاون الدولي في هذا السياق المعقد والمتغير.

مشكلة البحث:

تكمن إشكالية هذا البحث في التساؤل المحوري التالي: **إلى أي مدى تستطيع الدول حماية سيادتها الرقمية في مواجهة التهديدات السيبرانية الصادرة عن فاعلين غير حكوميين، في ظل غياب إطار قانوني دولي ملزم، وما هي البدائل القانونية والعملية الممكنة؟**

ويتفرع من هذا التساؤل عدة تساؤلات فرعية، منها:

- كيف يمكن تكييف الهجمات السيبرانية قانونيًا في ظل القواعد التقليدية للقانون الدولي؟
- هل يندرج حق الدفاع السيبراني عن النفس ضمن ميثاق الأمم المتحدة؟
- ما مدى فعالية المبادئ الطوعية وأشكال التعاون الإقليمي والدولي في الحد من التهديدات الرقمية؟
- هل هناك حاجة فعلية لمعاهدة دولية شاملة، أم أن البدائل الواقعية كافية في الوقت الراهن؟

أهمية البحث:

تتجلى أهمية هذا البحث في النقاط التالية:

١. **أهمية عملية وتشريعية:** حيث يُسلط الضوء على إحدى أخطر القضايا التي تهدد الدول المعاصرة، وهي حماية سيادتها في الفضاء الرقمي، في ظل تصاعد التهديدات السيبرانية المتقدمة.

٢. **أهمية قانونية:** لأنه يُعالج فراغًا قانونيًا كبيرًا في القانون الدولي العام، يتمثل في غياب إطار قانوني مُلزم يُنظم الأمن السيبراني، مما يفرض ضرورة البحث عن بدائل أو حلول مرحلية.

٣. **أهمية بحثية نظرية:** إذ يُسهم البحث في إثراء الأدبيات القانونية المتعلقة بالسيادة الرقمية والمسؤولية الدولية، من خلال دراسة مقارنة وتحليلية دقيقة.

٤. **أهمية إقليمية:** حيث يُعد هذا الموضوع ذا صلة مباشرة بتحديات تواجه الدول النامية والعربية، التي تسعى إلى تعزيز أمنها الرقمي دون أن تكون طرفًا مؤثرًا في صياغة القواعد الدولية.

أهداف البحث:

يهدف هذا البحث إلى تحقيق ما يلي:

١. تحليل مفهوم السيادة الرقمية في ضوء التغيرات التكنولوجية والتحديات السيبرانية الحديثة.

٢. دراسة مدى انطباق قواعد القانون الدولي التقليدي على الهجمات السيبرانية، لاسيما تلك الصادرة عن فاعلين غير حكوميين.

٣. تقييم مدى فعالية المبادئ الطوعية والمبادرات الحالية للأمم المتحدة في تنظيم السلوك السيبراني.

٤. استكشاف البدائل الواقعية لمواجهة غياب المعاهدة الدولية، مثل التعاون الإقليمي، التكييف القانوني، وبناء الثقة الرقمية.

٥. تقديم توصيات قانونية عملية من شأنها تعزيز الإطار الدولي لحماية السيادة الرقمية للدول.

(ISSN: 2537 - 0758)

منهج البحث:

يعتمد هذا البحث على المنهج التحليلي– الوصفي– المقارن، وذلك على النحو التالي:

- **المنهج التحليلي:** لتحليل النصوص القانونية الدولية ذات الصلة، مثل ميثاق الأمم المتحدة، ودليل تالين، وتقارير مجموعات خبراء الأمم المتحدة (UN GGE).
- **المنهج الوصفي:** لوصف وتحليل الظواهر والممارسات السيبرانية الواقعية، سواء من خلال دراسات حالة أو تقارير أمنية.
- **المنهج المقارن:** للمقارنة بين المواقف القانونية المختلفة للدول والمنظمات، وكذلك بين النماذج الدولية في التعامل مع الهجمات السيبرانية، مثل النموذج الأوروبي والأمريكي.

كما سيتم الاعتماد على الأدبيات الفقهية الحديثة، والوثائق الدولية، والمقالات المحكمة، والتقارير التقنية الصادرة عن المنظمات الدولية والإقليمية.

خطة البحث:

المقدمة

المبحث الأول: السيادة في الفضاء الرقمي– المفهوم والتحول

- المطلب الأول: مفهوم السيادة التقليدية وحدودها في البيئة السيبرانية
- المطلب الثاني: نشأة وتطور مفهوم "السيادة الرقمية"

المبحث الثاني: الفاعلون غير الحكوميين في الفضاء السيبراني

- المطلب الأول: التصنيف القانوني والواقعي للفاعلين السيبرانيين غير الحكوميين
- المطلب الثاني: خصائص الهجمات السيبرانية غير الحكومية وتحديات مواجهتها

المبحث الثالث: قصور القانون الدولي التقليدي أمام التهديدات السيبرانية

- المطلب الأول: حدود تطبيق قواعد المسؤولية الدولية والسيادة
- المطلب الثاني: مبدأ عدم التدخل وحق الدفاع السيبراني عن النفس

المبحث الرابع: نحو إطار قانوني دولي أكثر فاعلية

- المطلب الأول: الحاجة إلى معاهدة دولية جديدة للأمن السيبراني
- المطلب الثاني: البدائل الواقعية– التكييف القانوني وتعزيز التعاون الدولي

الخاتمة

النتائج والتوصيات

قائمة المراجع

المبحث الأول
السيادة في الفضاء الرقمي- المفهوم والتحول

تمهيد:

شكّلت السيادة منذ معاهدة وستفاليا (١٦٤٨) أحد أبرز المفاهيم المؤسسة للنظام الدولي، حيث رسخت مبدأ استقلال الدولة داخل حدودها الجغرافية، وعدم التدخل في شؤونها الداخلية، واعتبار الدولة الكيان الوحيد المخول بممارسة السلطة السياسية والقانونية على إقليمها. وقد تكرّس هذا المفهوم في مختلف فروع القانون الدولي، وخصوصًا في علاقات السلم والحرب، وتحديد المسؤوليات الدولية.

غير أن تطور تكنولوجيا المعلومات، وتوسع الفضاء السيبراني، أدى إلى إعادة النظر في حدود السيادة التقليدية. فقد أصبح من الممكن التأثير على نظم الدول الحيوية عن بُعد، دون اختراق مادي للإقليم، ما أفرز تحديات جوهرية تمس قدرة الدولة على ممارسة سيطرتها الكاملة على الفضاء الرقمي المرتبط بمواطنيها أو بنيتها التحتية.

من هنا تبرز الحاجة إلى إعادة تفكيك مفهوم السيادة التقليدية، وبحث مدى قدرته على التكيّف مع متغيرات الواقع الرقمي، وصولًا إلى بلورة مفهوم "السيادة الرقمية" كامتداد طبيعي للسيادة في عصر المعلومات، وهو ما يتطلب معالجة مفهومية وتأصيلية دقيقة، وهو ما يسعى هذا المبحث لتناوله من خلال مطلبين رئيسيين:

(ISSN: 2537 - 0758)

التقسيم:

- **المطلب الأول: مفهوم السيادة التقليدية وحدودها في البيئة السيبرانية** يتناول هذا المطلب الجذور التاريخية لمفهوم السيادة في إطار القانون الدولي، وأهم مبادئه، مع تسليط الضوء على الإشكاليات التي يفرضها الفضاء السيبراني على التطبيق العملي للسيادة، مثل إسناد الفعل السيبراني، وتجاوز الحدود المادية.
- **المطلب الثاني: نشأة وتطور مفهوم "السيادة الرقمية"** يعالج هذا المطلب بروز مفهوم السيادة الرقمية نتيجة الفجوة بين مبادئ القانون التقليدي ومتطلبات البيئة الرقمية، ويستعرض تطور المفهوم من الناحية القانونية والسياسية، مع الإشارة إلى نماذج دول تبنّت مفاهيم سيبرانية للسيادة، مثل الصين وروسيا.

المطلب الأول

مفهوم السيادة التقليدية وحدودها في البيئة السيبرانية

أولًا: السيادة وفق معاهدة وستفاليا

تُعدّ السيادة من المبادئ الأساسية التي يقوم عليها النظام الدولي المعاصر، وقد ظهر هذا المفهوم بشكل واضح مع **معاهدة وستفاليا** عام ١٦٤٨، والتي أرست مبدأ السيادة الكاملة للدولة على إقليمها، وحقها المطلق في تنظيم شؤونها الداخلية دون تدخل خارجي. وقد تميزت السيادة، وفق هذا التصور التقليدي، بكونها سلطة عليا تحتكر التشريع والتنفيذ داخل حدود الدولة، وتُمارس استقلالًا كاملًا في علاقاتها الخارجية (زيتون، ٢٠٢٥، ص ١٥٧).

ويتكون هذا المفهوم من شقين رئيسيين: السيادة الداخلية، والتي تعني أن للدولة السلطة المطلقة في سن القوانين وممارسة السلطة داخل أراضيها، والسيادة الخارجية، التي تفرض على الدول الأخرى احترام استقلال الدولة وعدم التدخل في شؤونها. وتقوم هذه السيادة على أساس إقليمي بحت، أي أن الدولة تمارس سيادتها داخل حدودها الجغرافية المعلومة والمعترف بها دوليًا (بريم، ٢٠٢٠، ص ١٩).

غير أن هذا المفهوم التاريخي تطور في سياق دولي كان يتسم بوضوح الحدود الجغرافية وانفصال الكيانات السياسية بعضها عن بعض، ما يجعل هذا النموذج غير قابل للتطبيق الكامل في البيئة الرقمية.

ثانياً: قيود الجغرافيا مقابل انسيابية الفضاء السيبراني

في مقابل وضوح الحدود المادية التي قامت عليها السيادة التقليدية، يتميز **الفضاء السيبراني** بطبيعته اللاتمركزية واللامادية، إذ لا يمكن تحديد موقعه جغرافيًا أو حصره داخل حدود دولة بعينها. فالبيانات والبرمجيات والبنى التحتية الرقمية غالبًا ما تكون موزعة عبر عدة دول، وتُدار أحيانًا من قبل شركات خاصة وليس حكومات، ما يجعل من فرض السيادة التقليدية أمرًا بالغ التعقيد (مليح ومليح، ٢٠٢١، ص ٢٢٥).

لقد أصبحت الدولة عاجزة عن فرض الرقابة المطلقة على أنظمتها الرقمية، لا سيما أن البنى التحتية للإنترنت تخضع لمنظمات دولية غير حكومية مثل "إيكانICANN"، التي تتولى إدارة أسماء النطاقات على مستوى العالم. وهذا الوضع يحد من قدرة الدولة على ممارسة سيادتها الرقمية كما تمارسها في المجالين البري والجوي (بريم، ٢٠٢٠، ص ٢٣).

ويشير زيتون (٢٠٢٥، ص ١٥٨) إلى أن السيادة في البيئة السيبرانية "تحوّلت من سيطرة جغرافية تقليدية إلى صراع على التحكم بالمعلومة والبنية التحتية الرقمية"، مما يفرض على الدول إعادة تعريف مفهوم السيادة بما يتماشى مع طبيعة الفضاء الرقمي.

ثالثاً: إشكالية الإسناد والحدود القضائية

تُعدّ مسألة **الإسناد (Attribution)** من أخطر التحديات التي تواجه تطبيق السيادة في البيئة السيبرانية. فبخلاف الهجمات المادية التي يمكن تتبع مصدرها بسهولة، فإن الهجمات السيبرانية غالبًا ما تُنفّذ من خلال تقنيات تشفير وتزييف تجعل من الصعب تحديد الجهة المسؤولة عنها بدقة. وقد يكون الهجوم صادرًا من دولة

(ISSN: 2537 - 0758)

معينة، لكنه يُنفّذ عبر خوادم تقع في دول أخرى، ما يثير تعقيدات قانونية وسياسية بشأن تحديد المسؤولية (زيتون، ٢٠٢٥، ص ١٥٩).

ونتيجة لذلك، تواجه الدول صعوبات في ممارسة اختصاصها القضائي على الجرائم الإلكترونية التي تستهدف بنيتها التحتية أو مؤسساتها السيادية. إذ أن القوانين الجنائية الوطنية، وحتى الاتفاقيات الدولية الحالية، مثل اتفاقية بودابست، لا تواكب تعقيد البيئة الرقمية وطبيعتها العابر للحدود (مليح ومليح، ٢٠٢١، ص ٢٢٩).

ويُجمع الباحثون على أن غياب أطر قانونية واضحة للإسناد والمسؤولية الدولية في الفضاء السيبراني يمثل "ثغرة سيادية" تُضعف قدرة الدول على الردع والحماية، وتفتح المجال أمام فاعلين غير حكوميين أو مدعومين من دول أخرى لتنفيذ هجمات دون محاسبة (بريم، ٢٠٢٠، ص ٢٧).

المطلب الثاني

نشأة وتطور مفهوم "السيادة الرقمية"

شهد مفهوم السيادة في العقود الأخيرة تحولات عميقة بفعل التطور التكنولوجي الهائل، وظهور الفضاء السيبراني بوصفه مجالًا جديدًا للتفاعلات السياسية والاقتصادية والعسكرية. فقد أدّى تزايد الاعتماد على التقنيات الرقمية وتكاملها في البنية التحتية للدول إلى بروز مصطلح "السيادة الرقمية"، وهو مفهوم جديد يسعى إلى توسيع نطاق السيادة التقليدية لتشمل الفضاء الإلكتروني وبيانات الأفراد والمؤسسات.

أولًا: نشأة المفهوم

ظهر مفهوم السيادة الرقمية كردّ فعل على **فقدان الدول السيطرة الحصرية على البيانات والمعلومات والبنية التحتية الرقمية داخل إقليمها. فمع** تحول الاقتصاد العالمي إلى اقتصاد معرفي رقمي، باتت البيانات تمثّل موردًا استراتيجيًا لا يقل أهمية عن النفط أو المياه. وقد أثار هذا الوضع تساؤلات حول من يملك البيانات؟ ومن يحق له تنظيمها وحمايتها؟ (زيتون، ٢٠٢٥، ص ١٥٨).

لقد جاءت السيادة الرقمية لتجيب عن هذه التساؤلات، بحيث تُفهم بأنها" **:حق الدولة في التحكم الكامل في فضائها الرقمي، بما يشمل البنية التحتية للمعلومات،**

وتدفق البيانات، وسياسات الأمن السيبراني، والرقابة على المعلومات ذات الأهمية الاستراتيجية "(مليح ومليح، ٢٠٢١، ص ٢٢٤)

ويرى البعض أن ظهور هذا المفهوم جاء نتيجة لاختلال توازن القوى في الفضاء الرقمي، حيث تهيمن شركات التكنولوجيا الكبرى مثل Google و Facebook وAmazon، على حركة البيانات والبنى التحتية للإنترنت، في الوقت الذي تتراجع فيه قدرة الدول على تنظيم تلك الفضاءات داخل حدودها الوطنية (بريم، ٢٠٢٠، ص٢٤).

ثانياً: تطور المفهوم وتحولاته

مع تعمّق استخدام الفضاء السيبراني في المجالات الحيوية– من الاتصالات إلى التعليم والدفاع– بدأت الدول تدرك أن **السيادة في القرن الحادي والعشرين لم تعد تقتصر على الأرض والجو والبحر، بل تشمل المجال الرقمي بكل أبعاده** .ومن ثم، بدأ تطور مفهوم "السيادة الرقمية" يأخذ منحى مؤسسيًا وقانونيًا في عدد من الدول.

فعلى سبيل المثال، **أعلنت الصين في وثيقة "استراتيجية الفضاء السيبراني" لعام ٢٠١٧ أن السيادة الرقمية هي امتداد للسيادة الوطنية، وتشمل السيطرة الكاملة على البنية الرقمية والبيانات المتداولة داخل الدولة** (بريم، ٢٠٢٠، ص ٢٦). كما تبنّى الاتحاد الأوروبي نهجًا مشابهًا، عبر مفهوم "الاستقلال الرقمي الاستراتيجي"، الذي يهدف إلى تعزيز قدرة أوروبا على حماية بنيتها الرقمية دون الاعتماد على أطراف خارجية.

وفي السياق العربي، لا تزال السيادة الرقمية في طور التشكل، غير أن بعض الدول بدأت بتطوير تشريعات تخص حماية البيانات، وإنشاء هيئات للرقابة على الأمن السيبراني، في محاولة لإرساء دعائم هذه السيادة الجديدة.

ويُلاحظ أن مفهوم السيادة الرقمية يتداخل مع مفاهيم أخرى مثل "الأمن السيبراني" و"الخصوصية الرقمية"، إلا أنه يتميز بكونه **يمنح الدولة حقًا قانونيًا وسياسيًا شاملاً في إدارة فضائها الرقمي بكل مكوناته، بما يشمل التدخل في**

(ISSN: 2537 - 0758)

تدفقات البيانات، وحجب المواقع، وتنظيم المحتوى الرقمي، ومراقبة الأنشطة السيبرانية (زيتون، ٢٠٢٥، ص ١٥٩)

ثالثاً: جدل السيادة الرقمية عالمياً

أثار هذا المفهوم خلافات عميقة في المجتمع الدولي، إذ ترى بعض الدول الغربية أن السيادة الرقمية قد تُستخدم كذريعة لتقييد حرية التعبير وتجزئة الإنترنت (Internet Fragmentation)، في حين ترى دول أخرى، مثل روسيا والصين، أن السيادة الرقمية هي أداة لحماية الأمن الوطني والتنوع الثقافي من هيمنة النمط الرقمي الغربي (مليح ومليح، ٢٠٢١، ص ٢٢٦).

وبالتالي، لا يزال مفهوم السيادة الرقمية في طور التطور القانوني والفقهي، ويعاني من غياب إجماع دولي بشأن تعريفه وحدوده، وهو ما يستدعي بلورة إطار قانوني دولي ينظم هذه السيادة ويحميها دون المساس بالحقوق الرقمية الأساسية للمستخدمين.

المبحث الثاني
الفاعلون غير الحكوميين في الفضاء السيبراني

تمهيد:

يمثل الفضاء السيبراني بيئة فريدة من نوعها من حيث طبيعة الفاعلين المؤثرين فيها؛ إذ لم يعد التهديد السيبراني مقتصرًا على الدول أو الجيوش النظامية، بل برزت فئة جديدة من الفاعلين غير الحكوميين الذين يمتلكون أدوات تقنية متقدمة وقدرات عالية على تنفيذ هجمات سيبرانية عابرة للحدود، قد تفوق في تأثيرها ما تقوم به الجهات الرسمية.

وتتنوّع هذه الكيانات ما بين مجموعات قرصنة مستقلة، وشبكات إرهابية رقمية، وفاعلين مدعومين من دول لكنهم لا يخضعون لها رسميًا، مما يخلق إشكالية قانونية تتعلّق بكيفية تصنيفهم، وإسناد أفعالهم، وترتيب المسؤولية الدولية المترتبة عن هجماتهم، خاصةً عندما تُوجّه ضد بنى تحتية سيادية أو مصالح وطنية لدول أخرى.

كما أن خصائص الهجمات السيبرانية التي ينفذها هؤلاء الفاعلون تتسم بالتعقيد، والغموض، وصعوبة التتبع، ما يجعل من مواجهتها تحديًا مضاعفًا أمام الدول، سواء من حيث الرد القانوني، أو من زاوية الدفاع التقني أو حتى السياسي.

وللوقوف على هذه الإشكالات، يقسّم هذا المبحث إلى مطلبين أساسيين على النحو الآتي:

التقسيم:

- **المطلب الأول: التصنيف القانوني والواقعي للفاعلين السيبرانيين غير الحكوميين** يُعالج هذا المطلب أنواع الفاعلين غير الحكوميين في الفضاء السيبراني، مثل القراصنة، الجماعات الإرهابية الرقمية، ومجموعات الجريمة المنظمة، إضافة إلى الفاعلين شبه الرسميين المدعومين من الدول، مع مناقشة إشكالية تصنيفهم القانوني وفق القانون الدولي.
- **المطلب الثاني: خصائص الهجمات السيبرانية غير الحكومية وتحديات مواجهتها** يركز هذا المطلب على السمات التي تميز الهجمات غير الحكومية (مثل السرية، صعوبة الإسناد، تنوع الأهداف، استخدام أدوات مفتوحة المصدر)، والتحديات التي تفرضها على أنظمة الأمن الوطني، وأدوات الرد التقني والقانوني المتاحة للدول.

المطلب الأول

التصنيف القانوني والواقعي للفاعلين السيبرانيين غير الحكوميين

يشهد الفضاء السيبراني تناميًا واضحًا في عدد وتنوع الجهات الفاعلة غير الحكومية، والتي تمارس أنشطة رقمية قد تكون ضارة أو مؤثرة على سيادة الدول، سواء عبر الهجمات أو التدخل في البنى التحتية أو نشر الدعاية. ويمكن تصنيف هؤلاء الفاعلين من منظور قانوني وواقعي إلى أصناف متعددة بحسب أهدافهم، وأساليبهم، ومدى صلتهم بالدول.

(ISSN: 2537 - 0758)

أولًا: الفاعلون السيبرانيون غير الحكوميون- تعريف عام

يقصد بالفاعلين السيبرانيين غير الحكوميين أولئك الأفراد أو الجماعات أو الكيانات التي تعمل خارج الإطار الرسمي للدولة، وتمتلك القدرة على تنفيذ أنشطة رقمية هجومية أو دفاعية في الفضاء السيبراني. وقد يكون هؤلاء الفاعلون مدفوعين بدوافع سياسية أو أيديولوجية أو مالية، أو حتى بدوافع ترفيهية أو استكشافية بحتة.

وتزداد أهمية هؤلاء الفاعلين لأنهم غالبًا ما يعملون في بيئة قانونية ضبابية تفتقر إلى التنظيم الدولي الواضح، مما يعيق محاسبتهم أو تتبعهم قانونيًا. وقد أشار باحثون إلى أن بعض الفاعلين غير الحكوميين قد يمتلكون من المهارات والتقنيات ما يضاهي الدول أحيانًا، بل وقد يخترقون أنظمة سيادية حساسة ويؤثرون على العلاقات الدولية (زيتون، ٢٠٢٥، ص. ٢٠٣).

ثانيًا: التصنيف الواقعي لهؤلاء الفاعلين

يمكن تصنيف الفاعلين السيبرانيين غير الحكوميين إلى الفئات التالية:

١. الهاكرز الأفراد:(Hacktivists)

وهم أفراد أو مجموعات يستخدمون أدوات سيبرانية للتعبير عن مواقف أيديولوجية أو سياسية، مثل مجموعة "أنونيموس". لا يسعون غالبًا إلى تحقيق مكاسب مالية، بل إلى توجيه رسائل احتجاجية رقمية.

٢. الجماعات الإجرامية السيبرانية:

وهم شبكات منظمة تسعى لتحقيق أرباح مادية من خلال سرقة البيانات، طلب الفدية (Ransomware)، الاحتيال المالي، وغيرها من الأشكال غير القانونية. غالبًا ما تكون هذه الجماعات منتشرة دوليًا ويصعب تحديد موقعها.

٣. الفاعلون المدعومون من الدول:(State-sponsored actors)

رغم أنهم لا ينتمون رسميًا لأجهزة الدولة، إلا أنهم يعملون ضمن أجندات وطنية، وبتغطية أو تمويل أو سكوت من السلطات. هؤلاء يشكلون تحديًا كبيرًا للسيادة الرقمية، لأنهم يضعفون مبدأ عدم التدخل التقليدي، ويصعب تحميل الدول المسؤولية

المباشرة عن أعمالهم. وقد أشار بعض الباحثين إلى أن هذا الشكل من الفاعلين قد يكون هو الأخطر على الأمن السيبراني الدولي (عبدالواحد، ٢٠٢٢، ص. ٣).

٤. المرتزقة السيبرانيون:(Cyber Mercenaries)

وهم أفراد أو شركات خاصة يقدمون خدمات هجومية أو دفاعية لمن يدفع أكثر، سواء كانت دولًا أو شركات أو حتى جماعات مسلحة. هذا النوع يطرح إشكالات قانونية وأخلاقية كبيرة لأنه يخلق سوقًا للسلاح الرقمي.

ثالثاً: التكييف القانوني للفاعلين غير الحكوميين

من الناحية القانونية، فإن النظام الدولي الحالي يعاني من فراغ تشريعي تجاه هؤلاء الفاعلين. فلا توجد معاهدات دولية ملزمة تنظم مسؤولية الأفراد أو الجماعات غير الحكومية في الفضاء السيبراني، وهو ما يجعل تحميل المسؤولية الجنائية أو المدنية مسألة معقدة. وقد أشار تقرير من إعداد زيتون (٢٠٢٥) إلى أن تصنيف هذه الكيانات بين "مجرمين رقميين" أو "أعداء رقميين" يخضع أحيانًا للمنظور السياسي للدول، مما يزيد الغموض القانوني (زيتون، ٢٠٢٥، ص. ٢٠٤).

وبحسب دراسة صادرة عن جامعة الشرق الأوسط، فإن أبرز تحدٍ قانوني يتمثل في غياب الإرادة الدولية الموحدة لتنظيم سلوك هؤلاء الفاعلين في ظل غلبة المصالح السيادية للدول الكبرى التي قد تبرر دعمها لبعض هذه الكيانات (عبدالواحد، ٢٠٢٢، ص. ٤).

رابعاً: تداخل التصنيفين وأثره على السيادة

في الواقع العملي، يصعب أحيانًا التمييز بين الفاعلين المدعومين من الدول والفاعلين المستقلين، لا سيما مع استخدامهم لهويات وهمية وتقنيات تمويه متقدمة. وهذا التداخل يُضعف من قدرة الدول على الدفاع السيادي، ويزيد من الضبابية القانونية بشأن مسؤولية الهجوم، الأمر الذي يهدد الأمن الجماعي ويفرض الحاجة إلى تبني إطار قانوني دولي واضح لتصنيفهم ومساءلتهم.

(ISSN: 2537 - 0758)

المطلب الثاني

خصائص الهجمات السيبرانية غير الحكومية وتحديات مواجهتها

تُعدّ الهجمات السيبرانية غير الحكومية من أخطر التهديدات الأمنية التي تواجه الدول في العصر الرقمي، نظرًا لطبيعتها المعقدة وفاعليتها العالية مقارنة بتكلفتها المنخفضة، بالإضافة إلى ما تتميز به من خصائص تجعل التصدي لها أمرًا بالغ الصعوبة، خاصة في ظل غياب إطار قانوني دولي ملزم.

أولًا: الطابع غير المادي للهجوم السيبراني

تتميّز الهجمات السيبرانية بكونها لا تُحدث أضرارًا مادية بالمعنى التقليدي، بل تستهدف الأنظمة المعلوماتية، والبنية التحتية الرقمية، والبيانات، وشبكات الاتصال. هذا "الطابع غير المادي" يجعل اكتشاف الهجوم، أو قياس أثره، أو حتى إثبات وقوعه مسألة معقدة، بخلاف الهجمات العسكرية أو الإرهابية التقليدية (زيتون، ٢٠٢٥، ص ٢٠٦).

فعلى سبيل المثال، قد يستغرق الأمر أيامًا أو أسابيع قبل أن تكتشف الدولة أنها تعرضت لهجوم سيبراني، كما أن الأضرار قد تظهر لاحقًا في صورة فقدان بيانات أو إيقاف خدمات حيوية. وبذلك، يتعذر أحيانًا تطبيق قواعد القانون الدولي التقليدي التي تستلزم وجود "عدوان مسلح" واضح لكي تتفعّل مسؤولية الدولة أو يُشرع الرد عليها.

ثانياً: تعقيد الإسناد وتحديات إثبات المسؤولية

من أبرز خصائص الهجمات السيبرانية غير الحكومية أنها **غالبًا ما تُنفّذ بأساليب تجعل من الصعب إسنادها إلى جهة معينة** .فالمهاجمون يستخدمون تقنيات تشويش متقدمة، مثل البروكسي، والـVPN، والانتحال الرقمي، لتضليل الأجهزة الأمنية، وقد يمر الهجوم عبر عدة خوادم موزعة عالميًا.

وقد لاحظ الباحثون أن حتى الدول الكبرى مثل الولايات المتحدة عانت في مناسبات عدة من صعوبات في إثبات مسؤولية جهات محددة عن هجمات كبيرة مثل اختراقات SolarWinds أوColonial Pipeline، مما يؤكد أن الإسناد في المجال

الرقمي ليس مجرد مسألة تقنية، بل هو **تحدٍّ سياسي وقانوني** (عبدالواحد، ٢٠٢٢، ص ٥)

إن هذه الإشكالية تقوّض مبدأ "**المسؤولية الدولية**"، حيث لا يمكن تحميل دولة أو جهة مسؤولية انتهاك السيادة الرقمية إذا لم يمكن إثبات تورطها بشكل قانوني واضح، وهو ما يجعل الهجمات السيبرانية أداة مثالية للحرب غير المباشرة والحروب الرمادية.

ثالثاً: الانتشار العابر للحدود وصعوبة الاحتواء

بعكس الأعمال العدائية التقليدية التي تحدث في مناطق محددة، فإن الهجمات السيبرانية تمتاز بـ"العابرة للحدود"، حيث يمكن أن تبدأ من دولة ما، وتمر عبر خوادم في دول أخرى، وتستهدف ضحية في مكان ثالث، مما يؤدي إلى **تشابك الاختصاصات القضائية وتضارب القوانين** بين الأنظمة القانونية الوطنية.

كما أن الأنظمة المستهدفة قد تكون مملوكة من جهات خاصة أو مؤسسات حيوية (مستشفيات، بنوك، مطارات)، ما يجعل آثار الهجوم أكثر شمولية وخطورة من الناحية الاقتصادية والاجتماعية، ويخلق تحديًا أمام القانون الدولي التقليدي الذي اعتاد التعامل مع الدول بوصفها وحدات قانونية واضحة (زيتون، ٢٠٢٥، ص٢٠٧).

رابعاً: التباين في القدرات السيبرانية بين الدول

تواجه العديد من الدول النامية أو الأقل تطورًا تحديًا آخر يتمثل في **ضعف بنيتها التحتية الرقمية، وهشاشة أنظمتها الأمنية، وقلة كوادرها التقنية المتخصصة**، ما يجعلها أكثر عرضة للهجمات السيبرانية غير الحكومية، وأكثر تأخرًا في اكتشافها أو الرد عليها.

ويؤدي هذا التفاوت في القدرات إلى **خلل في التوازن السيادي الرقمي بين الدول**، ويعزز من تفوق الجهات غير الحكومية المدعومة أو المنظمة جيدًا، والتي قد تستخدم أدوات رقمية متقدمة تم تطويرها في السوق السوداء، أو حتى في مؤسسات بحثية متطورة.

(ISSN: 2537 - 0758)

تشكل الخصائص السابقة للهجمات السيبرانية غير الحكومية معضلة أمام المنظومة القانونية الدولية الحالية، التي لم تُصمم أصلًا للتعامل مع هجمات غير مادية، مجهولة المصدر، عابرة للحدود، وذات آثار ممتدة ومتعددة. الأمر الذي يعزز من أهمية التفكير في **إطار قانوني دولي جديد** يأخذ بعين الاعتبار هذه الخصوصيات ويضمن حماية سيادة الدول الرقمية وحقوق المستخدمين.

المبحث الثالث

قصور القانون الدولي التقليدي أمام التهديدات السيبرانية

تمهيد:

رغم التطور التاريخي الطويل للقانون الدولي، وتراكم المبادئ القاعدية المنظمة للعلاقات بين الدول، فإن هذا النظام القانوني نشأ وتبلور في بيئة مادية تقليدية، تستند إلى مفاهيم ملموسة مثل الإقليم، القوة المسلحة، الحدود، والمسؤولية المباشرة. ومع ذلك، فإن الفضاء السيبراني كواقع افتراضي يتجاوز هذه الحدود، قد كشف عن قصور هيكلي في قدرة القانون الدولي التقليدي على مواجهة التحديات التي تطرحها الهجمات الإلكترونية والاختراقات السيبرانية المتزايدة.

إذ يجد مبدأ المسؤولية الدولية نفسه أمام صعوبات جمّة تتعلق بإسناد الأفعال السيبرانية لجهات فاعلة، لا سيما في ظل استخدام تقنيات الإخفاء والتضليل (مثل تقنيات "proxy" أو الشبكات المظللة)، كما أن مبدأ السيادة ذاته يتعرض لاختبارات جديدة في ظل اعتداءات إلكترونية لا تنتهك الحدود المادية، لكنها تصيب مباشرة البنى التحتية الحيوية للدولة.

كما يواجه **مبدأ عدم التدخل** و**حق الدفاع عن النفس** إشكاليات حادة عند تكييفها في السياق الرقمي، حيث لا تتوافر في معظم الهجمات السيبرانية شروط "القوة المسلحة التقليدية"، رغم أنها قد تسبب أضرارًا استراتيجية مماثلة أو حتى أشد، مما يجعل تطبيق هذه المبادئ محل جدل قانوني متجدد.

بناء على ما تقدم، يتفرع هذا المبحث إلى مطلبين رئيسيين، كما يلي:

التقسيم:

- **المطلب الأول: حدود تطبيق قواعد المسؤولية الدولية والسيادة** يتناول هذا المطلب المعايير القانونية المعتمدة في تحميل الدول المسؤولية عن الأفعال الدولية غير المشروعة، والتحديات التي تطرحها الهجمات السيبرانية على هذه القواعد، خصوصًا فيما يخص الإسناد، إثبات النية، وطبيعة الأضرار السيبرانية، إضافة إلى تأثير هذه الصعوبات على مبدأ السيادة الرقمية.
- **المطلب الثاني: مبدأ عدم التدخل وحق الدفاع السيبراني عن النفس** يناقش هذا المطلب حدود تطبيق مبدأ عدم التدخل في البيئة السيبرانية، ومتى تُعتبر الهجمات الإلكترونية تدخلًا في الشؤون الداخلية للدول، كما يُعالج مسألة الحق في الرد والدفاع عن النفس وفقًا للمادة ٥١ من ميثاق الأمم المتحدة، وتطبيق ذلك في الحالات السيبرانية، في ظل غياب تعريف دقيق لـ "القوة المسلحة" في الفضاء الرقمي.

المطلب الأول

حدود تطبيق قواعد المسؤولية الدولية والسيادة في الفضاء السيبراني

أصبحت السيادة الرقمية اليوم محل نزاع قانوني دولي، خاصة في ظل تزايد الهجمات السيبرانية العابرة للحدود، والتي غالبًا ما تُنفذ من قبل فاعلين غير حكوميين أو جهات مدعومة ضمنيًا من دول دون إعلان رسمي. ويُطرح تساؤل محوري في هذا السياق: هل تملك القواعد التقليدية للمسؤولية الدولية، كما أرستها الأعراف والاتفاقيات الدولية، القدرة على احتواء هذه الممارسات الجديدة؟ وما هي حدود تطبيقها في بيئة لا تعترف بالحدود المادية التقليدية للدول؟

أولًا: قصور معيار الإسناد في المجال السيبراني

ينص القانون الدولي العرفي، كما كرسته **لجنة القانون الدولي** في "مشروع مواد مسؤولية الدول عن الأفعال غير المشروعة دوليًا" (٢٠٠١)، على أن الدولة تُسأل دوليًا عن كل فعل:

(ISSN: 2537 - 0758)

- يكون منسوبًا لها؛
- ويشكّل انتهاكًا لالتزام دولي قائم تجاه دولة أخرى.

إلا أن الفضاء السيبراني يطرح إشكالية حقيقية في **إثبات الإسناد Attribution**، إذ قد تُشنّ هجمات إلكترونية من قبل أفراد داخل أراضي دولة ما، دون أن يكون هناك دليل قاطع على أنهم تصرّفوا بناءً على توجيه أو علم تلك الدولة.

وقد أكّد **دليل تالين ٢.٠** أن إثبات الإسناد يتطلب توافر أدلة تقنية وقانونية وسياسية معقدة، وأن **الدول لا تلتزم دوليًا بمشاركة أدلة الإسناد، مما يعيق عملية المحاسبة** .(Tallinn Manual 2.0, Rule 7)

ويذهب بعض الباحثين إلى أن معيار الإسناد المستخدم في القانون الدولي التقليدي قد يصبح غير ذي صلة إذا لم يُعدَّل بما يتناسب مع طبيعة المجال الرقمي، خاصة في ظل إمكانية انتحال الهويات الرقمية، واستخدام أدوات تمويه متقدمة (زيتون، ٢٠٢٥، ص ٢١٠).

ثانياً: ضعف إلزامية "واجب العناية الواجبة" في المجال الرقمي

يُعتبر مبدأ "عدم السماح باستخدام الإقليم للإضرار بالغير" أحد المبادئ الأساسية في القانون الدولي، كما ظهر في قضايا مثل قضية Trail Smelter (١٩٤١) وقضية نيكاراغوا ضد الولايات المتحدة (١٩٨٦)، التي رسّخت ما يُعرف بواجب العناية الواجبة (Due Diligence).

ويفترض هذا الواجب أن على الدولة التزامًا قانونيًا باتخاذ إجراءات معقولة لمنع الأضرار التي قد تلحق بدول أخرى نتيجة أفعال تنطلق من داخل إقليمها. لكن في المجال السيبراني، فإن:

- حجم البيانات الضخم،
- سرعة تنفيذ الهجمات،
- تشابك الشبكات العامة والخاصة،

كلها تجعل من الصعب تطبيق هذا الواجب عمليًا، حتى لو توفر حسن النية.

وقد جاء في تقرير **مجموعة الخبراء** الحكوميين GGE للأمم المتحدة (٢٠٢١) أن العناية الواجبة تظل "إطارًا توجيهيًا غير ملزم"، وأن الخلافات السياسية حالت دون تطويره إلى قاعدة إلزامية في المجال السيبراني.

كما أشار تقرير مركز الدراسات الاستراتيجية والدولية الأمريكي (CSIS, 2019) إلى أن عدم تحديد الحد الأدنى من الالتزامات الفنية والأمنية التي يجب على الدولة اتخاذها لحماية فضائها السيبراني يؤدي إلى تقويض فعالية هذا المبدأ.

ثالثاً: فجوة تشريعية دولية واضحة

رغم اعتراف المجتمع الدولي بخطورة الهجمات السيبرانية، إلا أنه **لا توجد حتى الآن معاهدة دولية شاملة وملزمة** تنظم قواعد السلوك السيبراني بين الدول أو تُحدّد كيفية مساءلتها في حال انتهاك السيادة الرقمية.

فالجهود الدولية تظل موزعة بين:

- اتفاقية بودابست لمكافحة الجرائم الإلكترونية (٢٠٠١): وتركز على التعاون الجنائي وليس على مسؤولية الدول؛
- تقارير GGE وOEWG: وهي جهود سياسية غير ملزمة؛
- مبادرات مثل Paris Call و Global Commission on Stability in Cyberspace: وهي بيانات نوايا أكثر منها قواعد قانونية.

وهذا الوضع يخلق "فراغًا قانونيًا" يسمح للدول الكبرى بالتنصّل من المسؤولية أو استخدام الفاعلين غير الحكوميين كأدوات هجومية دون مساءلة، مما يقوّض ثقة الدول الصغرى في النظام الدولي (UN GGE Report, 2021؛ زيتون، ٢٠٢٥، ص ٢١٢).

رابعاً: إشكالية السيادة الرقمية كمفهوم ناشئ

تعترف بعض الدول، كروسيا والصين، بمفهوم "السيادة الرقمية"، وتُطالب بحق الدولة في السيطرة الكاملة على محتوى الإنترنت داخل حدودها، بما في ذلك البنية التحتية الرقمية، والبيانات، والسياسات الأمنية.

(ISSN: 2537 - 0758)

إلا أن دولًا أخرى، كألمانيا وكندا، ترفض الاعتراف بسيادة مطلقة على الفضاء الرقمي، وتُطالب بترك هذا الفضاء مفتوحًا حرًا، مما يُنتج **ازدواجًا قانونيًا ومعياريًا في تفسير السيادة نفسها.**

ويؤكد **دليل تالين** أن السيادة تظل مبدأً قائمًا في الفضاء السيبراني، لكن "تطبيقه العملي محل جدل"، حيث أن السيطرة الرقمية قد تتعارض مع حقوق الإنسان وحرية التعبير.(Tallinn Manual 2.0, Rule 1)

خامساً: الواقع العملي وصمت الدول

في كثير من الحالات الواقعية، تُشنّ هجمات سيبرانية ذات طابع عدائي واضح، دون أن يُقابل ذلك برد قانوني دولي حاسم. بل تفضل معظم الدول عدم التصعيد القانوني، أو حتى عدم الإعلان عن الجهات المهاجمة، **وذلك لأسباب تتعلق:**

- بعدم رغبتها في فضح ضعفها السيبراني؛
- أو خوفًا من التصعيد العسكري أو الدبلوماسي؛
- أو لأنها لا تملك الدليل الفني المؤكد.

وهذا "الصمت السيبراني" يضعف من فكرة المسؤولية الدولية ذاتها، ويُرسل رسائل خاطئة مفادها أن الفضاء الرقمي ساحة مباحة وغير خاضعة للمساءلة القانونية (CSIS, 2019)؛ عبدالواحد، ٢٠٢٢، ص ٦.

إن حدود تطبيق قواعد المسؤولية الدولية في الفضاء السيبراني لا تنبع من رفض الدول لمبادئ القانون الدولي، بل من **عدم كفاية تلك المبادئ في صيغتها الحالية للتعامل مع خصوصية البيئة الرقمية** .فضعف الإسناد، وغموض العناية الواجبة، وغياب الاتفاقيات الملزمة، والتباين في تفسير السيادة الرقمية، كلها عوامل تُقيد فعالية المساءلة الدولية، وتستدعي تدخلًا قانونيًا دوليًا لتجديد قواعد القانون الدولي بما يتلاءم مع العصر الرقمي.

المطلب الثاني
مبدأ عدم التدخل وحق الدفاع السيبراني عن النفس

يمثل مبدأ عدم التدخل أحد المبادئ الجوهرية في القانون الدولي العام، ويعني التزام الدولة بالامتناع عن التدخل في الشؤون الداخلية أو الخارجية لدولة أخرى، سواء كان ذلك التدخل سياسيًا، عسكريًا، أو حتى رقميًا. ومع اتساع نطاق الهجمات السيبرانية، أصبح من الضروري مراجعة هذا المبدأ في ضوء التطورات الرقمية، خاصة عندما تمتد الاعتداءات إلى البنية السيادية لدولة ما دون استخدام أدوات القوة التقليدية.

أولًا: مبدأ عدم التدخل في البيئة السيبرانية

ينص إعلان مبادئ القانون الدولي الصادر عن الجمعية العامة للأمم المتحدة عام ١٩٧٠ على أن "ليس لأية دولة أو مجموعة من الدول أن تتدخل، مباشرة أو غير مباشرة، لأي سبب كان، في الشؤون الداخلية أو الخارجية لدولة أخرى" (United Nations, 1970).

ومع توسع الفضاء السيبراني، أدرجت مجموعة الخبراء الحكوميين للأمم المتحدة GGE هذا المبدأ ضمن البيئة الرقمية، موضحة أن الهجمات التي تستهدف التأثير في الوظائف السيادية مثل الانتخابات، والسلطة القضائية، والتشريعية، أو الأنظمة الأمنية يمكن أن تشكّل انتهاكًا لمبدأ عدم التدخل (UN GGE, 2021).

وقد دعم هذا التوجه دليل تالين ٢.٠، حيث نص في القاعدة ٦٦ على أن "الهجوم السيبراني يعتبر تدخلًا غير مشروع إذا استهدف صلاحيات جوهرية للدولة" (Schmitt, 2017).

لكن الفقه القانوني يواجه إشكالية في تحديد العتبة التي يتحول عندها الفعل السيبراني من مجرد تأثير غير مشروع إلى تدخلٍ يُعدّ خرقًا للقانون الدولي (زيدان، ٢٠٢٣، ص. ٢١٨).

(ISSN: 2537 - 0758)

ثانياً: الدفاع السيبراني عن النفس في ضوء المادة ٥١ من ميثاق الأمم المتحدة

تجيز المادة (٥١) من ميثاق الأمم المتحدة للدول الدفاع عن نفسها في حال وقوع "هجوم مسلح"، وهو ما يُفسَّر تقليديًا على أنه استخدام للقوة المادية. ومع ذلك، فإن البيئة الرقمية فرضت تساؤلات جديدة حول ما إذا كان الهجوم السيبراني يمكن أن يُعد "هجومًا مسلحًا" بالمعنى القانوني.

يرى بعض الفقه أن الهجمات السيبرانية التي تُحدث دمارًا ماديًا واسعًا، مثل قطع الكهرباء عن مدن كاملة، أو تعطيل المستشفيات، ترقى إلى مستوى الهجوم المسلح (Schmitt, 2017) (Tallinn Manual 2.0, Rule 71).

وقد أشار **تقرير مركز الدراسات الاستراتيجية والدولية CSIS** إلى أن المعايير الحالية غامضة، ولا بد من تحديد "العتبة السيبرانية" التي تجيز ردًا دفاعيًا متكافئًا.(CSIS, 2019)

أما الدفاع عن النفس في الفضاء الرقمي، فيجب أن يلتزم بمبادئ:

- **الضرورة:** أي وجود تهديد حقيقي ووشيك؛
- **التناسب:** بحيث يكون الرد مساوٍ للضرر؛
- **التمييز:** بين العسكري والمدني؛
- **الإسناد:** وهو إثبات الجهة المنفذة للهجوم، وهي من أعقد الإشكاليات التقنية والسياسية (حسن، ٢٠٢٢، ص. ١٤٤).

ثالثاً: قيود الدفاع السيبراني والرد المشروع

رغم الإقرار المبدئي بحق الدولة في الدفاع عن نفسها سيبرانيًا، فإن القانون الدولي يفرض ضوابط صارمة على هذا الرد، خشية أن يستخدم غطاء "الدفاع عن النفس" في تنفيذ أعمال هجومية.

وقد حدد **دليل تالين ٢.٠** هذه الضوابط، مؤكدًا أنه لا يجوز شن دفاع سيبراني ما لم يكن الهجوم واضحًا، جسيمًا، ومثبتًا، ولا يُقبل الدفاع الاستباقي أو الوقائي في الحالات الغامضة.(Schmitt, 2017)

وأشار تقرير معهد الدراسات الأمنية الدولية IISS إلى أن غالبية الدول لا تزال مترددة في تبني سياسة "ردع سيبراني هجومي"، لأنها تدرك حجم المخاطر الأخلاقية والقانونية التي قد تترتب على ردود غير متناسبة أو موجهة ضد أطراف مدنية (IISS, 2020).

إن تطبيق مبدأ عدم التدخل وحق الدفاع عن النفس في البيئة السيبرانية لا يزال موضوعًا محلّ جدل فقهي وقانوني. فلا توجد معايير دولية حاسمة تضبط متى يصبح الفعل السيبراني تدخلًا غير مشروع، أو متى يسمح برد عسكري رقمي مشروع. ويُعدّ غياب إطار قانوني دولي خاص بالهجمات الرقمية أحد أهم مظاهر قصور النظام القانوني الدولي في مواكبة التحولات التكنولوجية.

المبحث الرابع
نحو إطار قانوني دولي أكثر فاعلية

تمهيد:

لقد بيّنت المباحث السابقة أن القانون الدولي التقليدي، بما في ذلك قواعد المسؤولية الدولية، ومبادئ السيادة وعدم التدخل وحق الدفاع عن النفس، يعاني من قصور واضح في الاستجابة للتهديدات السيبرانية المعاصرة. ويعود ذلك إلى الطبيعة الخاصة لهذا الفضاء، الذي يتجاوز الحدود الجغرافية، ويتسم بالغموض التقني، وتعدد الفاعلين، وسرعة التحولات.

في ضوء هذا القصور، تبرز الحاجة الماسّة إلى **إطار قانوني دولي جديد** يواكب التطورات التكنولوجية، ويُرسي قواعد واضحة تحكم سلوك الدول والجهات غير الحكومية في الفضاء السيبراني. ومع أن بعض المبادرات الدولية قد أحرزت تقدمًا نسبيًا، مثل "دليل تالين" و"تقارير الأمم المتحدة GGE و"OEWG، فإن غياب **معاهدة دولية ملزمة** يترك فراغًا قانونيًا يعوق التوافق الدولي بشأن معايير السلوك، ويضعف آليات الردع والمساءلة.

(ISSN: 2537 - 0758)

ورغم الصعوبات السياسية والجيواستراتيجية التي تعترض صياغة مثل هذه المعاهدة، فإن المجتمع الدولي أمام خيارين: إما الدفع نحو اتفاقية ملزمة، أو تعزيز البدائل الواقعية المؤقتة كالمعايير الطوعية، الاتفاقيات الإقليمية، وآليات التعاون التقني والتدريبي.

وانطلاقًا من هذا الواقع، يقسَّم هذا المبحث إلى مطلبين أساسيين:

التقسيم:

- **المطلب الأول: الحاجة إلى معاهدة دولية جديدة للأمن السيبراني** يتناول هذا المطلب أسباب عجز القانون الدولي الحالي عن تنظيم الفضاء السيبراني بفعالية، ويُبرز الحاجة الملحة لإبرام اتفاقية دولية متخصصة، تحدد تعريفات واضحة للهجمات السيبرانية، وتُرسّخ قواعد إسناد، ومساءلة، وضمانات حماية، مع استعراض العقبات التي تعوق تحقيق هذا الهدف.
- **المطلب الثاني: البدائل الواقعية– التكييف القانوني وتعزيز التعاون الدولي** يركز هذا المطلب على البدائل المتاحة في غياب معاهدة ملزمة، مثل التفسير الموسّع للقواعد الحالية، واعتماد آليات التعاون الإقليمي، والمبادئ الطوعية، وتبادل المعلومات، مع تحليل أوجه القوة والضعف في هذه البدائل، ومدى إمكانية تطويرها لتشكل "قانونًا عرفيًا سيبرانيًا" متدرجًا.

المطلب الأول

الحاجة إلى معاهدة دولية جديدة للأمن السيبراني

أولًا: قصور النظام القانوني الدولي التقليدي

رغم تطور قواعد القانون الدولي العام، فإنها لا تزال غير كافية للتعامل مع التهديدات السيبرانية المتزايدة. فالنظام الحالي يستند إلى مبادئ عامة مثل احترام السيادة، عدم التدخل، واستخدام القوة، إلا أن هذه المبادئ صيغت في بيئة ما قبل الرقمية، ولا تراعي خصائص الفضاء السيبراني، مثل اللامادية، والسرعة، وغموض المصدر.

وقد أظهرت الأزمات السيبرانية الأخيرة– مثل الهجمات على المنشآت النووية الإيرانية (Stuxnet)، والتدخلات المزعومة في الانتخابات الأمريكية عام ٢٠١٦– أن النظام القائم يعاني من فراغ تشريعي خطير يمنع مساءلة الفاعلين، ويقيّد الدول من الدفاع المنظم (Zittrain, 2018).

كما أن قواعد **القانون الإنساني الدولي** لم تُصمم أصلاً لتطبيقها في بيئة افتراضية، مما يخلق تباينات في تفسير مفاهيم مثل "الهجوم المسلح" أو "الضرر الجسيم" في السياق الرقمي.(Schmitt, 2017)

ثانياً: المبادرات الدولية غير الكافية

شهدت الأمم المتحدة خلال العقدين الماضيين عدة محاولات لمعالجة الفجوة السيبرانية من خلال تشكيل مجموعات خبراء (GGE، OEWG)، إلا أن نتائجها ظلت غير ملزمة قانونيًا، واقتصرت على مبادئ طوعية مثل "العناية الواجبة"، و"الامتناع عن مهاجمة البنى التحتية الحيوية" (UN GGE, 2021).

ومع غياب توافق دولي، لا تزال المحاولات الرامية إلى تبني معاهدة شاملة تراوح مكانها. فعلى سبيل المثال:

- **الولايات المتحدة وحلفاؤها** يدفعون باتجاه احترام القانون الدولي الحالي وتطوير مدونات سلوك غير ملزمة؛
- بينما تسعى **روسيا والصين** إلى وضع معاهدة دولية جديدة تُنظّم "محتوى المعلومات" و"سيادة الدولة الرقمية"، بما يعكس فلسفة أكثر تقييدًا للفضاء السيبراني.

وقد فشلت الجهود الأخيرة لصياغة معاهدة ملزمة في لجنة الأمم المتحدة الخاصة بالجريمة السيبرانية، بسبب الخلافات الجذرية حول تعريف "التهديد"، وحقوق الإنسان الرقمية، ودور الشركات التكنولوجية.(IISS, 2023)

ثالثاً: مبررات الحاجة إلى معاهدة دولية جديدة

تتزايد الأصوات القانونية والأكاديمية المطالِبة بوضع **إطار تعاقدي ملزم** في مجال الأمن السيبراني، استنادًا إلى عدة اعتبارات:

(ISSN: 2537 - 0758)

١. **الطبيعة العابرة للحدود للهجمات:** إذ إن الأضرار لا تقف عند حدود دولة واحدة، بل تنتقل إلى الأنظمة العالمية المتصلة.(Zhou, 2022)
٢. **غياب المحاسبة الدولية:** لا توجد آليات فعالة لمساءلة الفاعلين غير الحكوميين أو الجهات المدعومة من دول، مما يعزز الإفلات من العقاب.
٣. **تزايد التهديدات السيبرانية الموجهة للبنى التحتية الحيوية:** مثل الطاقة، الاتصالات، والمياه، والتي باتت أهدافًا شائعة للحروب الرقمية.
٤. **عدم كفاية المعاهدات القائمة:** مثل اتفاقية بودابست ٢٠٠١، التي تُعنى فقط بالجرائم السيبرانية، ولا تتناول الأمن السيبراني من منظور السيادة والدفاع.
٥. **الحاجة إلى توازن بين الأمن وحقوق الإنسان الرقمية:** لا بد من حماية الخصوصية وحرية التعبير بالتوازي مع حماية الأمن القومي، وهو ما لا تضمنه المبادرات الحالية.

رابعاً: ملامح المعاهدة المقترحة

يرى الخبراء أن المعاهدة المطلوبة يجب أن تتضمن العناصر التالية:

- تعريف دقيق للهجمات السيبرانية التي ترقى إلى مستوى التهديد الدولي؛
- قواعد واضحة للإسناد السيبراني والمعايير الفنية المقبولة دوليًا؛
- تنظيم الردود المشروعة بما يضمن التناسب وعدم التوسع؛
- فرض التزامات قانونية على الشركات المزودة للبنية الرقمية؛
- إنشاء هيئة رقابية دولية لمتابعة الامتثال.

وقد اقترح **الاتحاد الأوروبي** إنشاء "وكالة للأمن السيبراني الأممي" تكون بمثابة منصة تقنية– قانونية لرصد ومتابعة التهديدات الرقمية.(ENISA, 2022)

لم يعد النقاش حول الحاجة إلى معاهدة دولية جديدة للأمن السيبراني مسألة نظرية أو فقهية، بل أصبح **ضرورة عملية** تستدعي توافقًا عالميًا حقيقيًا يوازن بين متطلبات السيادة، والأمن، والحريات الرقمية. فغياب هذا الإطار القانوني يُعرّض النظام الدولي للفوضى السيبرانية، ويهدد أسس الأمن الجماعي.

المطلب الثاني

البدائل الواقعية- التكييف القانوني وتعزيز التعاون الدولي

في ظل غياب معاهدة دولية شاملة تُنظّم الأمن السيبراني، يواجه المجتمع الدولي إشكاليات عميقة في التعامل مع التهديدات الرقمية، سواء من حيث التكييف القانوني للهجمات، أو من حيث الاستجابة الجماعية لها. وبينما لا تزال الخلافات قائمة حول إمكانية التوافق على معاهدة ملزمة، تبرز عدة بدائل واقعية يمكن للدول اعتمادها للحد من المخاطر السيبرانية، وضمان استقرار الفضاء الرقمي العالمي.

أولًا: التكييف القانوني للهجمات السيبرانية

يُمثل التكييف القانوني حجر الزاوية في معالجة التهديدات السيبرانية، خاصة في غياب إطار قانوني خاص بهذه الأفعال. ويعتمد التكييف القانوني بشكل أساسي على إدراج الهجمات السيبرانية في إطار قواعد القانون الدولي العام، مثل ميثاق الأمم المتحدة، ومبادئ المسؤولية الدولية، وسيادة الدولة.

وتقضي المادة (٤/٢) من ميثاق الأمم المتحدة بعدم جواز استخدام القوة أو التهديد باستخدامها في العلاقات الدولية، بينما تسمح المادة (٥١) بحق الدفاع عن النفس في حال التعرض لهجوم مسلح. وقد أثار هذا النص جدلًا واسعًا حول مدى إمكانية اعتبار الهجمات السيبرانية ضربًا من "استخدام القوة" أو "الهجوم المسلح" يبرر الرد.

وقد طُوّر هذا التوجه من خلال "دليل تالين ٢.٠" الذي أعده عدد من خبراء القانون الدولي، وخلص إلى أن الهجمات السيبرانية التي تُحدث دمارًا ماديًا كبيرًا أو إصابات بشرية جسيمة، أو تشل البنى التحتية الحيوية، يمكن أن تُرقى إلى مستوى "الهجوم المسلح" (Schmitt, 2017). أما الأفعال الأخرى، مثل التجسس الرقمي أو سرقة البيانات، فهي دون هذا العتبة القانونية، لكنها قد تُصنّف ضمن انتهاكات السيادة أو أعمال تدخل غير مشروع (Zhou, 2022).

لكن التحدي الأكبر يكمن في مسألة الإسناد attribution، أي تحميل جهة معينة المسؤولية عن الهجوم. فالأدوات السيبرانية تتيح للمهاجمين إخفاء هويتهم أو

(ISSN: 2537 - 0758)

تقمص هوية دول أخرى، مما يصعّب إثبات العلاقة بين الفعل ودولة معينة أمام المحاكم الدولية، خاصة في ظل غياب معايير موحدة أو آليات تحقيق دولية مستقلة (UN GGE, 2021).

ومع ذلك، اعتمدت بعض الدول، مثل الولايات المتحدة والمملكة المتحدة، على أدلة تقنية وسياسية لتوجيه اتهامات صريحة ضد جهات أجنبية، معتبرة ذلك كافيًا لممارسة الحق في الرد، حتى وإن لم يكن ذلك الاعتراف محل إجماع دولي.

ثانياً: أدوات التعاون الدولي خارج إطار المعاهدات

في غياب اتفاق شامل، لجأت الدول إلى وسائل بديلة لتعزيز الأمن السيبراني، تقوم على التعاون العملي وبناء الثقة والتنسيق في الاستجابة.

١. الاتفاقيات الثنائية والإقليمية

تُعد الاتفاقيات الثنائية أو متعددة الأطراف ذات الطابع الإقليمي أحد أهم البدائل. ومن أبرزها:

- **اتفاقية بودابست لعام ٢٠٠١** التي تُنظم التعاون القضائي في الجرائم الإلكترونية، وقد انضمت إليها أكثر من ٦٥ دولة، منها دول غير أوروبية مثل اليابان وأستراليا، رغم أنها لا تُنظم الهجمات السيبرانية العسكرية.
- **مبادئ الأمن السيبراني في الاتحاد الأوروبي** التي تُلزم الدول الأعضاء بتطوير خطط وطنية واستراتيجيات حماية البنى التحتية الرقمية، وتبادل المعلومات الحساسة.

كما أعلن حلف شمال الأطلسي (الناتو) منذ عام ٢٠١٦ أن الفضاء السيبراني يُعد ساحة عمليات قتالية، يمكن تفعيل الدفاع المشترك بموجبه إذا ثبت أن الهجوم السيبراني يرقى إلى مستوى الهجوم المسلح.(IISS, 2023)

٢. مجموعات الخبراء التابعة للأمم المتحدة

منذ عام ٢٠٠٤، شكّلت الجمعية العامة للأمم المتحدة مجموعة من الخبراء الحكوميين (GGE) لدراسة تهديدات الفضاء السيبراني. وقد توصلت هذه

المجموعات إلى سلسلة من التوصيات غير الملزمة قانونيًا، لكنها تؤسس لتقاليد قانونية دولية متنامية، منها:

- ضرورة احترام سيادة الدول في الفضاء السيبراني؛
- عدم استخدام البنية التحتية المدنية في الهجمات؛
- الامتناع عن تقديم الدعم للفاعلين غير الحكوميين؛
- التعاون في التحقيقات الجنائية السيبرانية.(UN GGE, 2021)

٣. مراكز تنسيق الاستجابة السيبرانية

شهدت السنوات الأخيرة توسعًا في إنشاء مراكز استجابة وطنية وإقليمية للحوادث السيبرانية (CSIRT)، مثل:

- المركز الأوروبي لمكافحة الجريمة الإلكترونية؛
- المركز العربي للأمن السيبراني التابع للجامعة العربية؛
- مراكز الإبلاغ والتحليل في دول الخليج (مثل CERT السعودية والإماراتية).

تعمل هذه المراكز على تبادل المعلومات حول الهجمات، وتحليل الثغرات، وتنسيق جهود الرد التقني، بما يُسهم في تعزيز المرونة السيبرانية المشتركة.

٤. القانون النموذجي والإرشادات غير الملزمة

تساهم منظمات مثل الاتحاد الدولي للاتصالات (ITU) والمنتدى الاقتصادي العالمي (WEF) في صياغة قوانين نموذجية وأدلة إرشادية، تهدف إلى تقوية الحوكمة الرقمية على المستوى العالمي، خاصة في ما يتعلق بحماية البنية التحتية، وتنظيم سلوك الشركات التكنولوجية الكبرى، وتحقيق التوازن بين الأمن وحقوق الإنسان الرقمية.

وقد اقترحت هذه المنظمات عدة مبادرات لإنشاء شبكات تعاون دولي مرن لا يرتكز بالضرورة على معاهدات، بل على مذكرات تفاهم، وإفصاحات طوعية، وبروتوكولات ثقة.(ENISA, 2022)

(ISSN: 2537 - 0758)

ثالثاً: بناء الثقة الرقمية وتعزيز الشفافية

من بين أهم الأدوات الفعالة في غياب إطار قانوني ملزم، تبرز **آليات بناء الثقة (CBMs)**، التي تهدف إلى خفض التوتر ومنع التصعيد، وتشمل:

- الإعلان عن العقيدة الدفاعية الرقمية للدولة؛
- إنشاء خطوط اتصال مباشر بين الجهات المعنية؛
- الإبلاغ الطوعي عن الحوادث؛
- دعم التحقيقات المشتركة في الحوادث العابرة للحدود.(Zittrain, 2018)

تُسهم هذه التدابير في تقليص فرص سوء الفهم، وتعزيز بيئة من الشفافية الرقمية المتبادلة، تمهيدًا لتطوير إطار قانوني ملزم مستقبلاً.

تُشكّل البدائل الواقعية، كالتكييف القانوني، والتعاون الفني، والمبادئ الطوعية، أدوات فعالة لحوكمة الفضاء السيبراني في ظل غياب معاهدة دولية شاملة. ورغم محدودية إلزامها، فإنها تُمثل مسارًا تراكميًا يمكن من خلاله بناء نظام قانوني دولي عرفي، يُمهّد لتوافق مستقبلي على إطار قانوني عالمي للأمن السيبراني. غير أن نجاح هذا المسار مرهون بقدرة الدول على تجاوز الخلافات السياسية، وتوحيد المفاهيم القانونية، وتعزيز الشفافية والثقة المتبادلة.

الخاتمة

مع اتساع الفضاء السيبراني وازدياد اعتماده في كافة مناحي الحياة، لم تعد السيادة مقتصرة على المجال الجغرافي التقليدي، بل أصبحت تمتد إلى النطاق الرقمي حيث تتعدد مصادر التهديد، لا سيما من قبل فاعلين غير حكوميين باتوا يمتلكون قدرات تقنية قد تفوق بعض الدول. وقد كشف هذا الواقع عن فراغ قانوني دولي خطير، إذ لا تزال قواعد القانون الدولي التقليدي عاجزة عن الإحاطة الكاملة بالتحديات الناشئة في هذا المجال، سواء من حيث التكييف القانوني للأفعال السيبرانية، أو من حيث ضمان مساءلة مرتكبيها، أو حماية الدول من التدخل في شؤونها الرقمية.

لقد أظهر البحث أن السيادة الرقمية باتت جزءًا لا يتجزأ من سيادة الدولة الحديثة، غير أن التعامل القانوني مع التهديدات السيبرانية غير الحكومية لا يزال يفتقر إلى أدوات واضحة، وهو ما يستدعي إما تطوير قواعد القانون الدولي القائم أو الدفع نحو صياغة اتفاقية دولية جديدة خاصة بالأمن السيبراني. كما تبين أن المبادرات الإقليمية والمبادئ الطوعية تمثل أدوات جزئية ومرحلية، لا ترقى إلى مستوى الحل الشامل، وإن كانت تمهّد له.

النتائج:

خلص البحث إلى النتائج التالية:

١. **أن مفهوم السيادة الرقمية** هو امتداد طبيعي للسيادة التقليدية، ويستلزم اعترافًا قانونيًا صريحًا بوجوب حماية الفضاء السيبراني لكل دولة كجزء من مجالها السيادي.

٢. **أن قواعد القانون الدولي العام**، بما فيها ميثاق الأمم المتحدة، تفتقر إلى التفصيل في معالجة الهجمات السيبرانية، لا سيما تلك الصادرة عن فاعلين غير حكوميين، مما يصعّب مسألة التكييف القانوني والمساءلة.

٣. **أن مبدأ عدم التدخل وحق الدفاع عن النفس** يواجهان تحديات كبيرة في المجال السيبراني بسبب صعوبة إسناد الأفعال، وغموض المعايير التي تُميز الهجوم المسلح الرقمي عن غيره.

٤. **أن المبادئ الطوعية الدولية، كالمعتمدة من مجموعة الخبراء الحكوميين (UN GGE)**، تُعد خطوة مهمة، لكنها تفتقر إلى الإلزامية وتُواجه غياب الإجماع الدولي.

٥. **أن هناك حاجة فعلية وملحّة لمعاهدة دولية شاملة للأمن السيبراني**، تُحدد الأفعال المحظورة، وتُرسخ مبدأ احترام السيادة الرقمية، وتُنشئ آليات للمساءلة القانونية الدولية.

(ISSN: 2537 - 0758)

٦. **أن البدائل الواقعية المؤقتة**، مثل الاتفاقيات الإقليمية، ومراكز الاستجابة المشتركة، والقواعد العرفية الناشئة، تلعب دورًا مهمًا، لكنها غير كافية لضمان الأمن السيبراني العالمي على المدى الطويل.

التوصيات

بناءً على النتائج أعلاه، يُوصي الباحث بما يلي:

١. **العمل على إطلاق مفاوضات دولية برعاية الأمم المتحدة** لصياغة اتفاقية شاملة تنظم الأمن السيبراني وتُحدد مسؤوليات الدول، وتُميز بين الأفعال العدائية والتجسسية والإعلامية.

٢. **تعزيز أدوات الإسناد الفني المشترك(Joint Attribution)**، وتطوير آليات دولية مستقلة للتحقيق في الهجمات السيبرانية.

٣. **توسيع التعاون الإقليمي والدولي** من خلال إنشاء تحالفات مرنة تضم الدول المتقاربة في التوجهات، بهدف مشاركة الخبرات والاستجابة الموحدة.

٤. **العمل على تطوير "عقيدة سيبرانية وطنية" واضحة**، تشمل تحديد المواقف القانونية من الهجمات الرقمية، ومتى يمكن اعتبارها تهديدًا للسيادة يستوجب الرد.

٥. **تشجيع التعليم والتدريب القانوني والفني في مجال الأمن السيبراني**، لضمان وجود كفاءات قانونية قادرة على التعامل مع التحديات المعقدة لهذا المجال.

٦. **دفع الشركات التكنولوجية الكبرى نحو الالتزام بالمعايير القانونية الدولية**، خاصة فيما يتعلق بالبيانات، والتشفير، وأمن الشبكات، من خلال أنظمة مساءلة عابرة للحدود.

قائمة المراجع

المراجع العربية:

- بريم، ف. (٢٠٢٠). السيادة الوطنية السيبرانية في ظل الفضاء السيبراني والتحولات الرقمية: الصين نموذجًا. مجلة الدراسات القانونية والسياسية، جامعة قسنطينة ٣.
- اللجنة الدولية للقانون الدولي. (٢٠٠١). مشروع مواد مسؤولية الدول عن الأفعال غير المشروعة دوليًا. الأمم المتحدة.
- زيتون، م.م. (٢٠٢٥). القوة السيبرانية أداة للتأثير والسيطرة في الفضاء السيبراني والعلاقات الدولية. المجلة العربية للنشر العلمي، ٧٠(٣)، ٢٠٢–٢٠٤.
- زيتون، م. م. (٢٠٢٥). العمليات السيبرانية وتحولات السيادة الرقمية. المجلة العربية للنشر العلمي، العدد ٧٨، ١٥٧–١٥٩.
- زيدان، م. (٢٠٢٣). مبدأ عدم التدخل في الفضاء السيبراني. المجلة القانونية الدولية الإلكترونية، ٨(٢)، ٢١٠–٢٣٠.
- عبد الواحد، ص. ح. (٢٠٢٢). حروب الفضاء الإلكتروني: دراسة في مفهومها وخصائصها وسبل مواجهتها (رسالة ماجستير، جامعة الشرق الأوسط)
- المركز العربي للأبحاث والدراسات. (٢٠٢٣). العمليات السيبرانية وتحولات السيادة في الفضاء الرقمي، ص. ٢٠٥–٢٢٥.
- المجلة الجزائرية للدراسات الأمنية. (٢٠٢٢). القوة السيبرانية في العلاقات الدولية، ١٠(٣)، ١٥٥–١٨٠.
- مليح، ي.، & مليح، ي. (٢٠٢١). السيادة الرقمية وتجلياتها وممكنات تحقيقها بالمغرب. مجلة القانون والأعمال الدولية، ٣٦، ٢٢٣–٢٢٩.

(ISSN: 2537 - 0758)

المراجع الأجنبية:

- CSIS. (2019). Thresholds for Cyber Warfare and the Law of Armed Conflict. Center for Strategic and International Studies.
- ENISA. (2022). Proposal for an International Cybersecurity Governance Framework. European Union Agency for Cybersecurity.
- Hassan, S. (2022). Cyber Sovereignty and the International Legal Challenges. Cyber Journal of International Security Studies, 4(1), 135–152.
- IISS. (2020). Cyber Capabilities and National Power: A Net Assessment. The International Institute for Strategic Studies.
- IISS. (2023). Cyber Capabilities and Global Governance: Progress and Pitfalls. The International Institute for Strategic Studies.
- Schmitt, M. N. (Ed.). (2017). Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge University Press.
- United Nations. (1970). Declaration on Principles of International Law Concerning Friendly Relations and Co-operation among States. General Assembly Resolution 2625.
- UN GGE. (2021). Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security. United Nations.
- Zhou, L. (2022). Transnational Cyber Threats and the Fragmentation of International Law. Oxford Journal of Cybersecurity Law, 5(1), 113–129.
- Zittrain, J. (2018). The Ethics of Cybersecurity Regulation. Harvard Law Review.