العددِ 20 شباط 2026
المجلة العراقية للبحوث الانسانية والاجتماعية والعلمية
No.20 Feb.2026 Iraqi Journal of Humanitarian, Social and Scientific Research
Print ISSN 2710-0952 Electronic ISSN2790-1254

الحروب السيبرانية الصامتة وأثرها على مبدأ عدم استخدام القوة

م.د. مهند جاسم محمد
الجامعة العراقية / كلية العلوم الاسلامية

المستخلص

يتناول هذا البحث موضوع الحروب السيبرانية الصامتة وأثرها على مبدأ عدم استخدام القوة في القانون الدولي العام، في ظل التحولات المتسارعة التي يشهدها النظام الدولي نتيجة التطور الهائل في تكنولوجيا المعلومات والاتصال. ويهدف إلى بيان مفهوم هذا النمط المستحدث من الصراعات الدولية وخصائصه، وتحليل تكييفه القانوني في إطار القواعد التقليدية لاستخدام القوة، ولا سيما كما وردت في ميثاق الأمم المتحدة. ويعتمد البحث المنهج الوصفي التحليلي، من خلال استقراء آراء الفقه العربي والأجنبي، وتحليل النصوص الدولية ذات الصلة، والوقوف على بعض التطبيقات العملية البارزة. ويخلص البحث إلى أن الحروب السيبرانية الصامتة تمثل تحديًا جوهريًا لمبدأ عدم استخدام القوة، إذ تقع في كثير من صورها في منطقة رمادية بين السلم والنزاع المسلح، بما يفرض تفسيرًا ديناميكيًا لهذا المبدأ يراعي طبيعة الوسائل الرقمية وآثارها الواقعية. كما يؤكد البحث أن الإطار القانوني الدولي القائم يعاني من قصور في استيعاب هذه الظاهرة، مما يستدعي تطوير القواعد الحالية أو استكمالها، سواء عبر بلورة قواعد عرفية أو إبرام اتفاقية دولية خاصة بالأمن السيبراني. ويختتم البحث بالتأكيد على أهمية تعزيز التعاون الدولي والإقليمي، ولا سيما العربي، وبناء القدرات الوطنية لمواجهة مخاطر هذا النمط من الحروب، بما يسهم في حماية السلم والأمن الدوليين في العصر الرقمي.

الكلمات المفتاحية: الحروب السيبرانية الصامتة؛ استخدام القوة؛ ميثاق الأمم المتحدة؛ القانون الدولي العام؛ الأمن السيبراني؛ السيادة الرقمية.

Abstract

This study examines silent cyber warfare and its impact on the principle of the prohibition of the use of force in public international law, in light of the profound transformations brought about by rapid developments in information and communication technologies. It seeks to clarify the concept and main characteristics of this emerging form of international conflict and to analyze its legal qualification within the traditional framework governing the use of force, particularly as enshrined in the Charter of the United Nations. The study adopts a descriptive-analytical approach, drawing on Arab and foreign legal scholarship, relevant international legal texts, and selected practical cases. It concludes that silent cyber warfare poses a fundamental challenge to the principle of the non-use of force, as many cyber operations fall within a “grey zone” between peace and armed conflict, thus requiring a dynamic interpretation of this principle that takes into account the nature and effects of digital means. The study further finds that the existing international legal framework remains inadequate to fully address this phenomenon, calling for the development of current rules or their supplementation, either through the crystallization of customary norms or the adoption of a dedicated international treaty on cybersecurity. The paper finally emphasizes the need to strengthen international and regional cooperation, particularly within the Arab region, and to enhance national capacities in order to confront the risks of this new form of warfare and safeguard international peace and security in the digital age.

Keywords: Silent cyber warfare; use of force; United Nations Charter; public international law; cybersecurity; digital sovereignty.

المقدمة

أفرز التطور المتسارع في تكنولوجيا المعلومات والاتصال واقعًا دوليًا جديدًا أصبحت فيه الفضاءات الرقمية ميدانًا رئيسًا للتفاعل والتنافس بين الدول، بل وساحة محتملة للصراع والإكراه السياسي والاستراتيجي. ولم يعد الأمن القومي للدول مرتبطًا فقط بحماية حدودها الإقليمية أو قدراتها العسكرية التقليدية، بل بات مرهونًا كذلك بقدرتها على تأمين فضائها السيبراني الذي تقوم عليه اليوم معظم المرافق الحيوية للدولة، من طاقة واتصالات ونقل ومال وصحة وإدارة عامة. وفي ظل هذا التحول، برزت الحروب السيبرانية الصامتة بوصفها نمطًا مستحدثًا من النزاعات الدولية يُدار بأدوات رقمية خفية، قادرة على إحداث آثار عميقة دون اللجوء إلى القوة المسلحة التقليدية أو إعلان الحرب صراحة.

ويثير هذا النمط من الصراعات تساؤلات قانونية جوهرية حول مدى كفاية قواعد القانون الدولي العام القائمة، التي وُضعت في سياق تاريخي سابق للثورة الرقمية، لتنظيم السلوك الدولي في الفضاء السيبراني. ويأتي في مقدمة هذه القواعد مبدأ عدم استخدام القوة في العلاقات الدولية، المكرّس في المادة (4/2) من ميثاق الأمم المتحدة، بوصفه أحد أعمدة النظام القانوني الدولي الرامي إلى حفظ السلم والأمن الدوليين. ومن ثم، فإن بحث أثر الحروب السيبرانية الصامتة على هذا المبدأ يكتسي أهمية علمية وعملية بالغة في ضوء ما تطرحه من تحديات غير مسبوقة.

أهمية البحث:

تتجلى أهمية هذا البحث في عدة اعتبارات، أبرزها:

1. أهمية علمية :إذ يسهم في إثراء النقاش الفقهي حول مفهوم الحروب السيبرانية الصامتة وتكييفها القانوني، ولا سيما في ظل محدودية الدراسات العربية المتخصصة في هذا المجال مقارنة بنظيراتها الأجنبية.

2. أهمية عملية :نظرًا لتزايد وتيرة الهجمات السيبرانية ذات الطابع الدولي، وما تطرحه من مخاطر حقيقية على البنى التحتية الحيوية للدول وأمنها القومي.

3. أهمية قانونية :لكونه يتناول أحد المبادئ الأساسية في القانون الدولي العام، وهو مبدأ عدم استخدام القوة، ويختبر مدى قدرته على مواكبة التحولات الرقمية المعاصرة.

4. أهمية إقليمية عربية :في ظل تعرض الدول العربية، كسائر دول العالم، لمخاطر الفضاء السيبراني، وحاجتها إلى بلورة رؤى قانونية تنطلق من خصوصياتها وواقعها الإقليمي.

5. أهمية مستقبلية :إذ يفتح آفاقًا لتطوير القواعد القانونية الدولية أو اقتراح أطر تنظيمية جديدة للأمن السيبراني.

مشكلة البحث:

تتمحور إشكالية البحث حول التساؤل الرئيس الآتي:

إلى أي مدى تتعارض الحروب السيبرانية الصامتة مع مبدأ عدم استخدام القوة في القانون الدولي العام، وهل تكفي القواعد الدولية القائمة لتنظيم هذا النمط المستحدث من الصراعات؟

ويتفرع عن هذا التساؤل عدد من الأسئلة الفرعية، من بينها:

- ما المقصود بالحروب السيبرانية الصامتة وما أبرز خصائصها؟
- كيف يمكن تكييفها قانونيًا في ضوء ميثاق الأمم المتحدة وقواعد القانون الدولي العام؟
- متى يمكن اعتبار العمليات السيبرانية استخدامًا للقوة أو هجومًا مسلحًا؟
- ما أبرز التحديات القانونية التي تثيرها هذه الحروب؟

- وما الآفاق المستقبلية لتنظيمها على الصعيدين الدولي والإقليمي؟

منهج البحث:

يعتمد هذا البحث أساسًا على المنهج الوصفي التحليلي، من خلال وصف ظاهرة الحروب السيبرانية الصامتة وبيان خصائصها، ثم تحليل النصوص الدولية ذات الصلة، ولا سيما ميثاق الأمم المتحدة، في ضوء آراء الفقه العربي والأجنبي والاجتهادات الدولية. كما يستعين البحث بـ المنهج الاستقرائي في تتبع التطبيقات العملية البارزة للهجمات السيبرانية ذات الطابع الدولي، وبـ المنهج المقارن عند الاقتضاء، للمقارنة بين الاتجاهات الفقهية المختلفة في تكييف هذه الظاهرة وتقويمها قانونيًا.

هيكلية البحث:

استنادًا إلى الإشكالية المطروحة، قُسّم البحث إلى مقدمة ومبحثين وخاتمة، على النحو الآتي:

- المبحث الأول :الإطار المفاهيمي والتكييف القانوني للحروب السيبرانية الصامتة، ويتناول مفهوم هذه الحروب وخصائصها، ثم تكييفها القانوني في ضوء قواعد القانون الدولي العام.
- المبحث الثاني :أثر الحروب السيبرانية الصامتة على مبدأ عدم استخدام القوة، ويبحث مدى انسجام هذا النمط من الصراعات مع المبدأ، ثم يستعرض أبرز التحديات القانونية والآفاق المستقبلية لتنظيمه.
- الخاتمة :وتتضمن أهم النتائج التي توصل إليها البحث، وأبرز المقترحات التي يراها مناسبة لمواجهة الإشكالات المثارة.

المبحث الأول الإطار المفاهيمي للحروب السيبرانية الصامتة

يُعد الوقوف على الإطار المفاهيمي للحروب السيبرانية الصامتة مدخلًا أساسيًا لفهم طبيعتها وحدودها القانونية في نطاق القانون الدولي العام. فقبل بحث آثارها على مبدأ عدم استخدام القوة، يتعين تحديد مفهوم هذه الحروب وخصائصها، وتمييزها عن غيرها من صور الصراع الرقمي. كما يقتضي الأمر بيان التكييف القانوني الأولي لها في ضوء القواعد الدولية القائمة. ومن ثم، يهدف هذا المبحث إلى وضع الأساس النظري والقانوني الذي يُبنى عليه التحليل اللاحق. ولهذا الغرض، يتناول المبحث مفهوم الحروب السيبرانية الصامتة وتكييفها القانوني.

المطلب الأول: تعريف الحروب السيبرانية الصامتة وخصائصها

أفرز التطور المتسارع في تكنولوجيا المعلومات والاتصال واقعًا دوليًا جديدًا، أصبحت فيه الفضاءات الرقمية ميدانًا أساسيًا للتفاعل والتنافس بين الدول، سواء في أوقات السلم أو في حالات التوتر والنزاع. ولم يعد الأمن القومي للدول مرتبطًا فقط بحماية حدودها البرية أو البحرية أو الجوية، بل بات مرهونًا كذلك بقدرتها على تأمين فضائها السيبراني، الذي أضحى عصبًا رئيسًا لتسيير المرافق الحيوية وإدارة الشؤون الاقتصادية والسياسية والعسكرية. وفي هذا الإطار برز مفهوم «الحروب السيبرانية الصامتة» بوصفه تعبيرًا عن نمط جديد من الصراعات الدولية التي تُدار بأدوات رقمية خفية، وتُحقق آثارًا استراتيجية عميقة دون اللجوء إلى القوة المسلحة التقليدية.

ويقصد بالحروب السيبرانية الصامتة ذلك النوع من العمليات السيبرانية العدائية التي تُنفّذها دولة أو جهات تعمل بتوجيهها أو بدعم منها، ضد نظم المعلومات أو الشبكات أو البنى التحتية الرقمية لدولة أخرى، بقصد الإضرار بمصالحها الحيوية أو التأثير في قراراتها السيادية، دون إعلان صريح للحرب، وبأساليب تتسم بالخفاء وصعوبة الاكتشاف والإسناد[1]، ويُطلق عليها وصف «الصامتة» لأنها تجري بعيدًا عن أنظار الرأي العام، ولا تُحدث في الغالب دمارًا ماديًا فوريًا ظاهرًا، رغم ما قد تسببه من آثار خطيرة على المدى المتوسط والبعيد.

وقد حاول الفقه العربي الحديث استيعاب هذا المفهوم في إطار دراساته للأمن السيبراني. فيعرفها بعض الباحثين العرب بأنها «استخدام منظم ومقصود للوسائط الإلكترونية لاختراق أو تعطيل أو تدمير نظم

[1] محمد عبد الرحمن، الأمن السيبراني والقانون الدولي، دار النهضة العربية، القاهرة، 2021، ص 45.

المعلومات لدولة ما، بهدف تحقيق مكاسب سياسية أو عسكرية، مع تجنب المواجهة العسكرية المباشرة»[2]، ويذهب آخرون إلى أنها تمثل «أحد مظاهر الحروب الحديثة التي تعتمد على التكنولوجيا الرقمية لإضعاف الخصم دون الدخول في حرب تقليدية»[3]، وتُظهر هذه التعريفات التقاطع الواضح مع ما ذهب إليه الفقه الغربي في توصيف هذا النمط من الصراعات.

وعلى الصعيد الأجنبي، يعرّف ريتشارد كلارك الحرب السيبرانية بأنها «أعمال تقوم بها دولة لاختراق حواسيب أو شبكات دولة أخرى بقصد إحداث ضرر جسيم أو اضطراب في وظائفها الحيوية»[4]،بينما يرى توماس ريد أن المقصود بها هو «استخدام القدرات السيبرانية لإلحاق أذى مادي أو وظيفي بالخصم في إطار صراع سياسي أو عسكري»[5]، أما دليل تالين(Tallinn Manual 2.0) ، وهو المرجع الأبرز في هذا المجال، فيستخدم مصطلح «العمليات السيبرانية» ليشير إلى «أفعال تُنفّذ عبر الفضاء السيبراني لإحداث آثار في هذا الفضاء أو خارجه»[6].

وانطلاقًا من هذه التعريفات، يمكن القول إن الحروب السيبرانية الصامتة تمثل صورة خاصة من صور الحرب السيبرانية، تتميز بكونها لا تُعلن رسميًا، ولا تصل في الغالب إلى مستوى النزاع المسلح التقليدي، لكنها تُدار لتحقيق أهداف استراتيجية بعيدة المدى، في إطار ما يُعرف اليوم بـ«الحروب تحت العتبة(Sub-threshold Warfare)»[7]، وهي بذلك تندرج ضمن أنماط «الحرب الهجينة» التي تمزج بين الوسائل العسكرية وغير العسكرية، من سياسية واقتصادية وإعلامية وسيبرانية، لتحقيق غايات الدولة دون الانجرار إلى مواجهة عسكرية شاملة[8].

وتُظهر الوقائع العملية خطورة هذا النوع من الحروب. فالهجوم السيبراني المعروف بفيروس «ستاكسنت» الذي استهدف المنشآت النووية الإيرانية عام 2010 يُعد مثالًا بارزًا على عملية سيبرانية صامتة أدت إلى إتلاف مادي في أجهزة الطرد المركزي دون ضربة عسكرية مباشرة[9]، كما شهدت إستونيا عام 2007 موجة هجمات سيبرانية واسعة عطلت مواقع حكومية ومصرفية وإعلامية، في سياق توتر سياسي مع روسيا، مما كشف مبكرًا عن قابلية الفضاء السيبراني ليكون ساحة صراع بين الدول[10]، وتؤكد هذه الأمثلة أن الحروب السيبرانية الصامتة قادرة على إحداث آثار استراتيجية عميقة رغم طابعها غير المرئي.

وتتسم الحروب السيبرانية الصامتة بجملة من الخصائص التي تميزها عن غيرها من أنماط النزاع. أولى هذه الخصائص هي الخفاء وصعوبة الإسناد، إذ تُنفّذ الهجمات عبر شبكات معقدة من الخوادم

---

[2] أحمد فتحي سرور، "الحرب السيبرانية وتحديات الأمن القومي العربي"، مجلة السياسة الدولية، العدد 214 2018: ص 67.

[3] عبد الكريم علوان، القانون الدولي العام في عصر العولمة، دار الثقافة، عمّان، 2020، ص 312.

[4] Richard A. Clarke and Robert Knake, Cyber War: The Next Threat to National Security and What to Do About It New York: Ecco, 2010, p 6.

[5] Thomas Rid, Cyber War Will Not Take Place Oxford: Oxford University Press, 2013, p 14.

[6] Michael N. Schmitt, ed., Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations Cambridge: Cambridge University Press, 2017, p 258.

[7] Michael J. Mazarr, Mastering the Gray Zone Carlisle: U.S. Army War College Press, 2015, p 12.

[8] Frank G. Hoffman, "Hybrid Warfare and Challenges," Joint Force Quarterly 52 2009: p 34.

[9] David E. Sanger, Confront and Conceal New York: Crown, 2012, p 188.

[10] Rain Ottis, "Analysis of the 2007 Cyber Attacks against Estonia," NATO CCD COE Proceedings 2008: p 4.

والوسائط الرقمية، ما يجعل من الصعب تقنيًا وقانونيًا تحديد الجهة المسؤولة عنها على وجه اليقين[11]، وقد أشار الفقه العربي إلى أن هذه السمة تُعد من أخطر ما يميز الهجمات السيبرانية، لأنها تتيح للدول التملص من المسؤولية الدولية وإنكار علاقتها بالهجوم[12].

والخاصية الثانية تتمثل في انخفاض الكلفة مقارنة بالوسائل التقليدية، حيث لا تتطلب العمليات السيبرانية تجهيزات عسكرية باهظة، بل تعتمد أساسًا على خبرات بشرية وبرمجيات متطورة، ما يجعلها في متناول عدد كبير من الدول وحتى الفاعلين من غير الدول[13]، ويذهب بعض الباحثين العرب إلى أن هذه الميزة أسهمت في «ديمقراطية القوة» في العلاقات الدولية، إذ لم تعد القوة حكرًا على الدول الكبرى وحدها[14].

أما الخاصية الثالثة فهي الطابع العابر للحدود والسيادة، إذ يجري الفعل السيبراني في فضاء لا يعترف بالحدود الجغرافية التقليدية، مما يسمح بالوصول إلى أهداف في إقليم دولة أخرى خلال لحظات، دون الحاجة إلى اختراق مادي لحدودها[15]، ويثير ذلك إشكالات عميقة بشأن مفهوم السيادة في الفضاء السيبراني، وهو ما تناوله عدد من الفقهاء العرب مؤكدين أن السيادة الرقمية باتت امتدادًا طبيعيًا للسيادة الإقليمية للدولة[16].

وتتجلى الخاصية الرابعة في تعدد الأهداف وتنوعها، إذ لا تقتصر الحروب السيبرانية الصامتة على استهداف المنشآت العسكرية، بل تمتد لتشمل البنى التحتية المدنية الحيوية، كشبكات الكهرباء والمياه والمطارات والمصارف والاتصالات، فضلًا عن قواعد البيانات الحكومية والأنظمة الانتخابية[17]. ويؤكد هذا الاتساع في نطاق الأهداف أن آثار هذه الحروب قد تمس مباشرة حياة المدنيين وأمنهم، حتى في غياب نزاع مسلح معلن.

كما تتميز هذه الحروب بالاستمرارية والتراكم، حيث غالبًا ما تأتي في صورة حملات طويلة الأمد تهدف إلى جمع المعلومات الاستخباراتية، أو زرع برمجيات خبيثة نائمة، أو إنهاك الدولة المستهدفة تدريجيًا عبر تعطيل متكرر لنظمها الحيوية[18]. ويشير بعض الباحثين العرب إلى أن هذا الطابع التراكمي يجعل من الصعب على الدولة المستهدفة تحديد لحظة بدء «الهجوم» أو نهايته، بما يربك قدرتها على الرد القانوني والسياسي المناسب[19].

ومن خصائصها أيضًا المرونة وسرعة التطور التقني، إذ تتغير أدوات الهجوم وأساليبه بتغير البرمجيات والتقنيات الرقمية، ما يفرض على الدول سباقًا دائمًا في تطوير قدراتها الدفاعية والهجومية السيبرانية[20].ويؤدي هذا الواقع إلى نشوء سباق تسلح سيبراني غير معلن، يفتقر حتى الآن إلى أطر قانونية دولية ملزمة تنظم حدوده وضوابطه[21].

ويقتضي التحليل المفاهيمي كذلك التمييز بين الحروب السيبرانية الصامتة وغيرها من الظواهر القريبة. فهي تختلف عن الجريمة السيبرانية التي يكون دافعها في الغالب ماليًا أو فرديًا، وعن الإرهاب

---

11 Schmitt, Tallinn Manual, Previous reference, 2.0, p 80.
12 عبد الرحمن، الأمن السيبراني والقانون الدولي، المرجع السابق، ص 53.
13 Clarke and Knake, Cyber War, p 30.
14 سرور، "الحرب السيبرانية وتحديات الأمن القومي العربي"، المرجع السابق، ص 70.
15 Jack Goldsmith and Tim Wu, Who Controls the Internet? Oxford: Oxford University Press, 2006, p 2.
16 عبد الكريم علوان، القانون الدولي العام، المرجع السابق، ص 315.
17 Sanger, Confront and Conceal, Previous reference, p 190.
18 Rid, Cyber War Will Not Take Place, Previous reference, p 47.
19 عبد الرحمن، الأمن السيبراني والقانون الدولي، المرجع السابق، ص 60.
20 Mazarr, Mastering the Gray Zone, Previous reference, p 20.
21 Schmitt, Tallinn Manual, Previous reference, p 2.0, 9.

السيبراني الذي يسعى إلى بث الرعب لتحقيق أهداف أيديولوجية، وإن تشابهت الوسائل التقنية[22]. كما تختلف عن الدفاع السيبراني الذي يهدف إلى حماية الشبكات والنظم من الاختراق، إذ تقوم الحروب السيبرانية الصامتة على نية عدائية واستراتيجية واضحة تستهدف دولة أخرى أو مصالحها الحيوية[23].

ويُستفاد مما تقدم أن الحروب السيبرانية الصامتة تمثل تحولًا نوعيًا في طبيعة الصراع الدولي، حيث تتراجع أهمية المواجهة العسكرية المباشرة لصالح أدوات رقمية خفية قادرة على إحداث آثار سياسية واقتصادية وربما مادية بالغة الخطورة. فهي حروب بلا جبهات تقليدية، ولا إعلانات رسمية، ولا خطوط تماس واضحة، لكنها مع ذلك قد تُقوّض أمن الدول واستقرارها، وتُحدث اختلالًا في موازين القوى الإقليمية والدولية.

ومن ثم، فإن تحديد مفهوم هذه الحروب وخصائصها بدقة يُعد مدخلًا ضروريًا لفهم الإشكاليات القانونية التي تثيرها، ولا سيما فيما يتعلق بمبدأ عدم استخدام القوة في العلاقات الدولية، ومدى إمكانية إخضاعها لقواعد القانون الدولي العام القائمة. وهذا ما يمهد للانتقال في المطلب التالي إلى بحث التكييف القانوني للحروب السيبرانية الصامتة، في ضوء نصوص الميثاق الأممي والاجتهادات الفقهية المعاصرة.

المطلب الثاني: التكييف القانوني للحروب السيبرانية الصامتة في ضوء قواعد القانون الدولي العام

يثير بروز الحروب السيبرانية الصامتة في العلاقات الدولية المعاصرة إشكالًا قانونيًا بالغ التعقيد، يتمثل في كيفية تكييف هذا النمط الجديد من الصراعات في إطار قواعد القانون الدولي العام القائمة، التي وُضعت أساسًا لتنظيم علاقات الدول في سياق نزاعات تقليدية تقوم على استخدام القوة المسلحة المادية. فالقانون الدولي، كما استقر منذ ميثاق الأمم المتحدة سنة 1945، يقوم على حظر مبدئي لاستخدام القوة في العلاقات الدولية، مع استثناءين رئيسين هما الدفاع الشرعي عن النفس، والإجراءات التي يتخذها مجلس الأمن لحفظ السلم والأمن الدوليين[24]، غير أن العمليات السيبرانية الصامتة، بطبيعتها غير المادية والخفية، تضع هذا الإطار أمام تحديات غير مسبوقة.

وينطلق التكييف القانوني لهذه الحروب من التساؤل الجوهري الآتي: هل يمكن اعتبار العمليات السيبرانية الصامتة «استخدامًا للقوة» أو «هجومًا مسلحًا» بالمعنى المقصود في المادة (4/2) والمادة (51) من ميثاق الأمم المتحدة؟ أم أنها تندرج ضمن أفعال أقل خطورة، كالتدخل غير المشروع في الشؤون الداخلية للدول، أو مجرد أفعال غير ودية لا ترقى إلى مستوى القوة المحظورة؟[25]

لقد ذهب جانب من الفقه الدولي إلى أن معيار «القوة» في القانون الدولي لا ينبغي أن يُفهم حصرًا في إطار القوة العسكرية التقليدية، بل يجب أن يُفسَّر تفسيرًا وظيفيًا يأخذ في الاعتبار طبيعة وآثار الفعل محل البحث. وفي هذا السياق يرى مايكل شميت أن العمليات السيبرانية التي تُحدث آثارًا مماثلة لتلك التي تُحدثها الأسلحة التقليدية، كالتدمير المادي للبنى التحتية أو التسبب في خسائر بشرية، يمكن أن تُعد استخدامًا للقوة بالمعنى المقصود في المادة (4/2)[26]، وهو الاتجاه الذي تبناه دليل تالين 2.0 حين قرر أن معيار التكييف يقوم على «نطاق وآثار» العملية السيبرانية(Scale and Effects) [27].

وفي الاتجاه ذاته، يذهب عدد من الفقهاء العرب إلى أن العبرة ليست بوسيلة الفعل وإنما بنتيجته، فإذا أسفرت العملية السيبرانية عن تدمير منشآت حيوية أو تعطيل مرافق أساسية على نحو يماثل الهجوم

---

[22] Susan W. Brenner, Cybercrime and the Law Boston: Northeastern University Press, 2010, p 9.

[23] علوان، القانون الدولي العام، المرجع السابق، 318.

[24] عبد الكريم علوان، القانون الدولي العام في عالم متغير، دار الثقافة، عمّان، 2020، 287.

[25] محمد عبد الرحمن، الأمن السيبراني والقانون الدولي القاهرة، المرجع السابق، ص 92.

[26] Michael N. Schmitt, “Cyber Operations and the Jus ad Bellum Revisited,” Villanova Law Review 56, no. 3 2011: 569.

[27] Michael N. Schmitt, ed., Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations Cambridge: Cambridge University Press, 2017, 331.

العسكري، فإنها تُعد استخدامًا غير مشروع للقوة[28]، ويرى محمد عبد الرحمن أن «الهجوم السيبراني الذي يؤدي إلى شلّ شبكة الكهرباء أو السدود أو المستشفيات لا يقل خطرًا عن القصف العسكري، ويجب أن يخضع للقواعد ذاتها»[29].

غير أن هذا الاتجاه لا يحسم الإشكال في جميع الحالات، إذ إن أغلب الحروب السيبرانية الصامتة لا تُفضي إلى تدمير مادي مباشر، بل تقتصر آثارها على تعطيل مؤقت للأنظمة، أو سرقة بيانات، أو إرباك اقتصادي وإداري. وهنا يثور التساؤل حول ما إذا كانت هذه الأفعال، رغم خطورتها، ترقى إلى مستوى «استخدام القوة» أم تظل دون هذه العتبة.

وفي هذا الصدد، يرى فريق آخر من الفقه أن العمليات السيبرانية التي لا تُحدث أضرارًا مادية أو خسائر بشرية لا تُعد استخدامًا للقوة، وإنما تندرج ضمن أفعال التدخل غير المشروع أو الإخلال بمبدأ عدم التدخل في الشؤون الداخلية للدول[30]، ويؤكد هذا الاتجاه أن توسيع مفهوم القوة ليشمل كل ضرر اقتصادي أو تقني قد يؤدي إلى تفريغ مبدأ الحظر من مضمونه، ويفتح الباب أمام تبرير ردود عسكرية على أفعال لا ترقى في حقيقتها إلى مستوى القوة المسلحة[31].

وفي الفقه العربي، نجد من يذهب إلى هذا الرأي، معتبرًا أن «الهجمات السيبرانية التي تقتصر على سرقة معلومات أو تعطيل مؤقت للخدمات، رغم عدم مشروعيتها، لا يمكن مساواتها باستخدام القوة المسلحة الذي قصده واضعو الميثاق»[32]. غير أن هؤلاء لا ينكرون في الوقت ذاته أن هذه الأفعال قد تشكل خرقًا لمبدأ السيادة أو لمبدأ عدم التدخل، بما يرتب مسؤولية دولية على الدولة القائمة بها.

ويُضاف إلى ذلك إشكال آخر يتمثل في مدى إمكانية اعتبار بعض العمليات السيبرانية الصامتة «هجومًا مسلحًا» يبرر ممارسة حق الدفاع الشرعي عن النفس وفق المادة (51) من الميثاق. وهنا يميز الفقه عادة بين «استخدام القوة» من جهة، و«الهجوم المسلح» من جهة أخرى، باعتبار أن الثاني يمثل صورة أشد جسامة من الأول[33]. وقد استقر قضاء محكمة العدل الدولية، ولا سيما في قضية نيكاراغوا، على أن الهجوم المسلح يفترض درجة معينة من الخطورة والجسامة[34].

وبالقياس على ذلك، يذهب غالبية الفقه المعاصر إلى أن العملية السيبرانية لا تُعد هجومًا مسلحًا إلا إذا بلغت من الجسامة ما يُعادل الهجوم العسكري التقليدي، كأن تؤدي إلى تدمير واسع للبنى التحتية أو إزهاق الأرواح[35]، وقد تبنى دليل تالين هذا الاتجاه، معتبرًا أن العمليات السيبرانية التي تُسبب أضرارًا مادية جسيمة أو خسائر بشرية قد ترقى إلى مستوى الهجوم المسلح[36]، أما ما دون ذلك من عمليات، وإن كانت خطيرة، فلا يجيز للدولة المتضررة اللجوء إلى الدفاع الشرعي المسلح، وإنما يفتح لها مجال اتخاذ تدابير مضادة مشروعة في إطار القانون الدولي[37].

وفي الفقه العربي، يذهب عبد الكريم علوان إلى أن «التوسع في مفهوم الهجوم المسلح ليشمل كل عملية سيبرانية من شأنه أن يخل بتوازن نظام الأمن الجماعي، ويجعل من السهل تبرير استخدام القوة العسكرية

---

[28] أحمد فتحي سرور، "الحرب السيبرانية وتحديات الأمن القومي العربي"، مجلة السياسة الدولية، العدد 214 2018: 72.

[29] عبد الرحمن، الأمن السيبراني والقانون الدولي، المرجع السابق، ص 95.

[30] Gary P. Corn, "Cyber National Security: Navigating Gray Zone Challenges," Journal of National Security Law & Policy 9 2018: 66.

[31] Rid, Cyber War Will Not Take Place, 19.

[32] سرور، "الحرب السيبرانية وتحديات الأمن القومي العربي"، المرجع السابق، ص 74.

[33] علوان، القانون الدولي العام، المرجع السابق، ص 291.

[34] Military and Paramilitary Activities in and against Nicaragua Nicaragua v. United States, Merits, ICJ Reports 1986, p 101.

[35] Schmitt, "Cyber Operations and the Jus ad Bellum Revisited,"p 573.

[36] Schmitt, Tallinn Manual 2.0, p 334.

[37] Corn, "Cyber National Security,"p 70.

بدعوى الرد على هجمات رقمية قد لا تبلغ ذات الخطورة»[38]، وهو رأي يعكس الحذر من الانزلاق نحو عسكرة الفضاء السيبراني دون ضوابط واضحة.

ولا يقف التكييف القانوني عند حدود مبدأ عدم استخدام القوة والدفاع الشرعي، بل يمتد كذلك إلى مبدأ السيادة. فقد أصبح من المسلم به أن للدولة سيادة على بنيتها التحتية المعلوماتية الواقعة داخل إقليمها، وأن اختراق نظمها السيبرانية من قبل دولة أخرى دون رضاها يشكل مساسًا بهذه السيادة[39]، ويؤكد عدد من الفقهاء العرب أن السيادة الرقمية باتت امتدادًا طبيعيًا للسيادة الإقليمية، وأن أي عملية سيبرانية عدائية تمس نظم الدولة تمثل خرقًا لهذا المبدأ، ولو لم ترقَ إلى استخدام القوة[40].

كما تثير الحروب السيبرانية الصامتة مسألة المسؤولية الدولية للدول عن الأفعال غير المشروعة. فحتى مع صعوبة الإسناد التقني، فإن ثبوت نسبة العملية السيبرانية إلى دولة ما يرتب مسؤوليتها الدولية، سواء نُفذت العملية مباشرة من أجهزتها، أو من فاعلين غير دوليين بتوجيه أو دعم منها[41]، وقد أكد دليل تالين إمكانية إسناد الهجوم السيبراني إلى الدولة متى توافرت معايير السيطرة الفعلية أو التوجيه العام[42].

وفي هذا السياق، يشير بعض الباحثين العرب إلى أن إشكالية الإسناد لا ينبغي أن تكون ذريعة لإفلات الدول من المسؤولية، بل تستوجب تطوير آليات دولية للتعاون التقني والقضائي من أجل كشف مرتكبي الهجمات السيبرانية ومحاسبتهم[43].

ويُستخلص مما تقدم أن التكييف القانوني للحروب السيبرانية الصامتة يظل مسألة خلافية في الفقه الدولي، تتأرجح بين اتجاه موسّع لمفهوم استخدام القوة يربط التكييف بآثار العملية، واتجاه مضيق يحصر القوة في الأفعال ذات الطابع العسكري المادي. غير أن ثمة شبه إجماع على أن هذه الحروب، في حدها الأدنى، تمثل خرقًا لمبادئ أساسية في القانون الدولي، كاحترام السيادة وعدم التدخل، وتُرتب مسؤولية دولية متى ثبتت نسبتها إلى دولة معينة.

ويكشف هذا الجدل عن قصور الإطار القانوني الدولي الحالي عن استيعاب التحولات العميقة التي أحدثتها الثورة الرقمية في طبيعة الصراعات الدولية، ويبرز الحاجة الملحة إلى تطوير قواعد أكثر وضوحًا لتنظيم السلوك الدولي في الفضاء السيبراني. وهو ما يمهد للانتقال في المبحث التالي إلى دراسة أثر الحروب السيبرانية الصامتة على مبدأ عدم استخدام القوة، وتحليل مدى انسجام هذا النمط من الصراع مع أحد أهم أعمدة النظام القانوني الدولي المعاصر.

المبحث الثاني أثر الحروب السيبرانية الصامتة على مبدأ عدم استخدام القوة

بعد تحديد الإطار المفاهيمي والتكييف القانوني للحروب السيبرانية الصامتة، يقتضي البحث الانتقال إلى دراسة آثارها على أحد أهم مبادئ القانون الدولي العام، وهو مبدأ عدم استخدام القوة. فهذه الحروب تثير تساؤلات جوهرية حول مدى انسجامها مع هذا المبدأ وحدود انطباقه في الفضاء السيبراني. كما تفرض تحديات قانونية تستدعي البحث في سبل تنظيمها مستقبلًا. وعليه، يُخصص هذا المبحث لتحليل علاقة الحروب السيبرانية الصامتة بمبدأ عدم استخدام القوة، وبيان أبرز الإشكالات والآفاق المرتبطة بها.

المطلب الأول: مدى انسجام الحروب السيبرانية الصامتة مع مبدأ عدم استخدام القوة في القانون الدولي

يُعد مبدأ عدم استخدام القوة في العلاقات الدولية حجر الزاوية في النظام القانوني الدولي المعاصر، وقد كُرّس بصورة صريحة في المادة (4/2) من ميثاق الأمم المتحدة التي تحظر على الدول «التهديد

---

[38] علوان، القانون الدولي العام، المرجع السابق، ص 293.

[39] Schmitt, Tallinn Manual 2.0, p 13.

[40] عبد الرحمن، الأمن السيبراني والقانون الدولي، المرجع السابق، ص 101.

[41] James Crawford, State Responsibility: The General Part Cambridge: Cambridge University Press, 2013, p 149.

[42] Schmitt, Tallinn Manual 2.0, p 84.

[43] عبد الرحمن، الأمن السيبراني والقانون الدولي، المرجع السابق، ص 110.

باستعمال القوة أو استعمالها ضد سلامة الأراضي أو الاستقلال السياسي لأية دولة»[44]، وقد استهدف واضعو الميثاق من وراء هذا الحظر وضع حدٍّ لسياسات العدوان والحروب التقليدية التي شهدها النصف الأول من القرن العشرين. غير أن التحولات التكنولوجية المتسارعة، ولا سيما بروز الفضاء السيبراني كساحة جديدة للصراع، طرحت تساؤلات عميقة حول مدى قابلية هذا المبدأ للتطبيق على أنماط حديثة من النزاعات، من بينها الحروب السيبرانية الصامتة.

وينطلق البحث في مدى انسجام هذه الحروب مع مبدأ عدم استخدام القوة من التساؤل عما إذا كانت العمليات السيبرانية الصامتة تدخل أصلًا في نطاق «القوة» التي قصدها الميثاق، أم أنها تمثل صورة مختلفة من صور السلوك الدولي غير المشروع الذي لا يبلغ حدّ القوة المسلحة. وفي هذا السياق، يذهب جانب معتبر من الفقه العربي إلى أن مفهوم القوة في الميثاق لا ينبغي تفسيره تفسيرًا حرفيًا جامدًا يقتصر على الوسائل العسكرية التقليدية، بل يجب أن يُفهم في ضوء الغاية التي ابتغاها المشرّع الدولي، وهي منع كل فعل من شأنه أن يهدد السلم والأمن الدوليين أو يقوض سيادة الدول[45].

فقد ذهب عبد الكريم علوان إلى أن «القوة المحظورة في المادة (4/2) ليست مقصورة على السلاح الناري أو القصف الجوي، بل تشمل كل وسيلة تُستخدم لإكراه دولة أخرى على نحو يمس سلامة إقليمها أو استقلالها السياسي»[46]، وعلى النهج ذاته، يرى علي صادق أبو هيف أن التطور التاريخي لمفهوم القوة يقتضي توسيع نطاقه ليشمل الأشكال المستحدثة التي قد تكون في آثارها أشد خطرًا من القوة العسكرية التقليدية[47].

وانطلاقًا من هذا الفهم الموسّع، يذهب عدد من الباحثين العرب المعاصرين إلى أن الحروب السيبرانية الصامتة، متى أدت إلى تعطيل مرافق حيوية أو إحداث أضرار جسيمة في البنية التحتية الرقمية أو المادية لدولة ما، فإنها تُعد صورة من صور استخدام القوة المحظورة دوليًا[48]، ويؤكد محمد عبد الرحمن أن «الهجوم السيبراني الذي يشل شبكة الكهرباء أو أنظمة الطيران أو المستشفيات لا يقل في آثاره عن هجوم عسكري، ومن ثم لا يجوز إخراجه من نطاق الحظر الوارد في الميثاق»[49].

ويعزز هذا الاتجاه ما ذهب إليه عدد من الفقهاء العرب في دراساتهم حول الأمن السيبراني، حيث يرون أن التمسك بتفسير ضيق لمفهوم القوة من شأنه أن يفتح الباب أمام الدول للتحايل على أحكام الميثاق، من خلال استبدال الأسلحة التقليدية بأدوات رقمية تحقق الغاية ذاتها دون أن تُصنَّف قانونًا كقوة[50]، ويرى أحمد فتحي سرور أن ذلك «يفرغ مبدأ عدم استخدام القوة من مضمونه، ويجعله عاجزًا عن مواكبة تحديات العصر الرقمي»[51].

وفي مقابل هذا الاتجاه، يذهب فريق آخر من الفقه، ومنهم بعض الباحثين العرب، إلى أن الحروب السيبرانية الصامتة لا تُعد في جميع صورها استخدامًا للقوة بالمعنى المقصود في المادة (4/2)، ما لم تُفضِ إلى أضرار مادية جسيمة أو خسائر بشرية مباشرة[52]، ويؤكد أصحاب هذا الرأي أن توسيع مفهوم القوة ليشمل كل اختراق أو تعطيل سيبراني قد يؤدي إلى خلط بين القوة المحظورة وغيرها من صور السلوك غير المشروع، كالتدخل في الشؤون الداخلية أو الإضرار بالمصالح الاقتصادية[53].

---

44 عبد الكريم علوان، القانون الدولي العام في عالم متغير، دار الثقافة، عمّان، 2020، 279.

45 علي صادق أبو هيف، القانون الدولي العام الإسكندرية: منشأة المعارف، 2010، ص 512.

46 علوان، القانون الدولي العام في عالم متغير، المرجع السابق، ص 281.

47 أبو هيف، القانون الدولي العام، المرجع السابق، ص 514.

48 محمد عبد الرحمن، الأمن السيبراني والقانون الدولي، المرجع السابق، ص 133.

49 عبد الرحمن، الأمن السيبراني والقانون الدولي، المرجع السابق، ص 135.

50 عبد الله سليمان، "الأمن السيبراني وتطور مفهوم القوة في القانون الدولي"، مجلة الحقوق، جامعة الكويت، العدد 2 2020: ص 45.

51 أحمد فتحي سرور، "الحرب السيبرانية وتحديات الأمن القومي العربي"، المرجع السابق،2018، ص 75.

52 محمد مجدي عبد السلام، القانون الدولي واستخدام القوة، دار الفكر الجامعي، القاهرة، 2019، ص 201.

53 عبد السلام، القانون الدولي واستخدام القوة، المرجع السابق، ص 203.

ويرى محمد مجدي عبد السلام أن «الهجمات السيبرانية التي تقتصر على سرقة بيانات أو تعطيل مؤقت للخدمات، رغم خطورتها، لا ترقى إلى مستوى استخدام القوة المسلحة، وإنما تمثل إخلالًا بمبدأ السيادة أو عدم التدخل»[54]، ويذهب عبد الله عبد العزيز الهاجري إلى أن إدراج هذه الأفعال ضمن مفهوم القوة قد يبرر ردودًا عسكرية غير متناسبة، بما يهدد استقرار النظام الدولي[55].

غير أن هذا الاتجاه نفسه لا ينكر أن ثمة صورًا من الحروب السيبرانية الصامتة قد تبلغ من الخطورة ما يجعلها أقرب إلى القوة المحظورة، لاسيما إذا استهدفت منشآت نووية أو سدودًا أو شبكات كهرباء ومياه، بما قد يؤدي إلى خسائر بشرية جسيمة[56]، وفي هذه الحالات، يميل عدد من الباحثين العرب إلى القول بأن العبرة يجب أن تكون بآثار الهجوم لا بوسيلته، وهو ما ينسجم مع معيار «النطاق والآثار» الذي تبناه الفقه الدولي المعاصر[57].

ويُظهر هذا الجدل أن مدى انسجام الحروب السيبرانية الصامتة مع مبدأ عدم استخدام القوة يظل مرهونًا بطبيعة العملية السيبرانية وآثارها الملموسة. فإذا كانت هذه العمليات تُستخدم بوصفها أداة لإكراه دولة أخرى على نحو يمس استقلالها السياسي أو سلامة إقليمها، أو تُحدث دمارًا ماديًا واسعًا، فإنها تتعارض مع جوهر المبدأ وتندرج في نطاق الحظر الوارد في المادة (4/2). أما إذا اقتصر أثرها على أضرار محدودة أو مؤقتة لا ترقى إلى هذا المستوى، فإنها قد تظل دون عتبة استخدام القوة، مع بقائها أفعالًا غير مشروعة من زاوية مبادئ أخرى في القانون الدولي.

ويؤكد عدد من الفقهاء العرب أن هذا التمييز ضروري للحفاظ على التوازن بين حماية السلم الدولي ومنع التوسع غير المبرر في مفهوم القوة[58]، ففي هذا الإطار، يرى عبد الكريم علوان أن «التحدي الحقيقي يتمثل في رسم خط فاصل دقيق بين ما يُعد قوة سيبرانية محظورة، وما يظل في إطار الأفعال غير الودية أو التدخل غير المشروع»[59].

كما يثير هذا الموضوع مسألة العلاقة بين مبدأ عدم استخدام القوة وحق الدفاع الشرعي. فحتى لو اعتُبرت بعض الحروب السيبرانية الصامتة استخدامًا للقوة، فإن ذلك لا يعني بالضرورة أنها تُعد «هجومًا مسلحًا» يجيز الرد العسكري وفق المادة (51). وهنا يشدد عدد من الباحثين العرب على ضرورة التزام معيار الجسامة، حتى لا يتحول الدفاع الشرعي إلى ذريعة لتبرير استخدام القوة المسلحة ردًا على كل اختراق رقمي[60].

ويخلص كثير من الفقه العربي المعاصر إلى أن مبدأ عدم استخدام القوة، رغم نشأته في سياق تاريخي مختلف، يظل إطارًا صالحًا من حيث المبدأ لتنظيم السلوك الدولي في الفضاء السيبراني، شريطة إعادة تفسيره تفسيرًا ديناميكيًا يأخذ في الاعتبار طبيعة التهديدات الرقمية وآثارها الواقعية[61]،ويؤكد هؤلاء أن جوهر المبدأ يتمثل في حماية السلم والأمن الدوليين ومنع الإكراه بين الدول، وهو جوهر لا يتغير بتغير الوسائل[62].

وعليه، يمكن القول إن الحروب السيبرانية الصامتة، في صورها الخطيرة ذات الآثار الجسيمة، تتعارض مع مبدأ عدم استخدام القوة وتمثل تحديًا مباشرًا له، في حين أن صورها الأقل خطورة تظل في منطقة رمادية بين القوة المحظورة والتدخل غير المشروع. ويكشف هذا الواقع عن الحاجة إلى مزيد من

---

[54] عبد السلام، القانون الدولي واستخدام القوة، المرجع السابق، ص 205.
[55] عبد الله عبد العزيز الهاجري، "الهجمات السيبرانية ومبدأ عدم استخدام القوة"، مجلة الدراسات القانونية، جامعة الكويت، العدد 1 2021: ص 88.
[56] عبد الرحمن، الأمن السيبراني والقانون الدولي، المرجع السابق، ص140.
[57] Michael N. Schmitt, ed., Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations Cambridge: Cambridge University Press, 2017, p 331.
[58] سليمان، "الأمن السيبراني وتطور مفهوم القوة"، المرجع السابق، ص50.
[59] علوان، القانون الدولي العام في عالم متغير، المرجع السابق، ص 283.
[60] عبد السلام، القانون الدولي واستخدام القوة، المرجع السابق، ص 210.
[61] عبد الرحمن، الأمن السيبراني والقانون الدولي، المرجع السابق، ص 145.
[62] أبو هيف، القانون الدولي العام، المرجع السابق، ص520.

الجهد الفقهي والدولي لتحديد معايير أوضح تُمكّن من إخضاع هذا النمط من الصراعات لقواعد قانونية دقيقة، وهو ما يقود إلى بحث التحديات والآفاق المستقبلية لتنظيم الحروب السيبرانية الصامتة في المطلب التالي.

المطلب الثاني: التحديات القانونية والآفاق المستقبلية لتنظيم الحروب السيبرانية الصامتة

تكشف الحروب السيبرانية الصامتة، بما تنطوي عليه من خصائص تقنية وقانونية معقدة، عن فجوة متزايدة بين واقع الممارسات الدولية في الفضاء السيبراني وبين القواعد التقليدية للقانون الدولي العام التي صيغت في سياق تاريخي مغاير. فقد أضحى هذا النوع من الصراعات يمثل أحد أبرز التحديات التي تواجه النظام القانوني الدولي المعاصر، سواء من حيث تحديد طبيعته القانونية، أو من حيث ضبط آثاره على السلم والأمن الدوليين، أو من حيث إيجاد آليات فعالة للمساءلة والتنظيم. ومن ثم، فإن بحث التحديات القانونية التي تثيرها هذه الحروب، واستشراف الآفاق المستقبلية لتنظيمها، يُعد ضرورة علمية وعملية في آن واحد.

أولًا: التحديات القانونية لتنظيم الحروب السيبرانية الصامتة

يتمثل التحدي الأول في غياب تعريف دولي موحّد للحرب السيبرانية أو العمليات السيبرانية العدائية . فحتى الآن لا يوجد في إطار الأمم المتحدة أو غيرها من المنظمات الدولية تعريف ملزم يحدد على وجه الدقة ماهية الهجمات السيبرانية التي يمكن عدّها استخدامًا للقوة أو هجومًا مسلحًا[63]، ويشير عدد من الفقهاء العرب إلى أن هذا الغموض المفاهيمي ينعكس سلبًا على إمكانية تطبيق القواعد القائمة، ويؤدي إلى تباين واسع في مواقف الدول وتقديراتها[64]، ويرى محمد عبد الرحمن أن «افتقار القانون الدولي لتعريف واضح للهجوم السيبراني الخطير يجعل من الصعب بناء قواعد مسؤولية دولية مستقرة في هذا المجال»[65].

أما التحدي الثاني فيتمثل في إشكالية الإسناد(Attribution) ، أي صعوبة تحديد الجهة المسؤولة عن الهجوم السيبراني. فالطبيعة التقنية للفضاء السيبراني تسمح بإخفاء المصدر الحقيقي للهجوم عبر استخدام شبكات معقدة من الخوادم والوسطاء الرقميين، أو عبر الاستعانة بفاعلين من غير الدول[66]، ويؤكد عبد الله سليمان أن «إسناد الهجوم السيبراني إلى دولة معينة قد يستغرق وقتًا طويلًا، وربما يظل محل شك، وهو ما يعرقل إمكانية تفعيل قواعد المسؤولية الدولية أو ممارسة حق الدفاع الشرعي»[67].

ويُضاف إلى ذلك تحدي دور الفاعلين من غير الدول، إذ كثيرًا ما تُنفّذ الهجمات السيبرانية من قبل جماعات أو أفراد لا يتمتعون بصفة الدولة، سواء بدافع أيديولوجي أو إجرامي أو حتى بدعم غير مباشر من دول[68]، ويثير هذا الواقع تساؤلات حول مدى مسؤولية الدولة عن أفعال هؤلاء، خاصة في ظل صعوبة إثبات التوجيه أو السيطرة الفعلية. ويذهب بعض الباحثين العرب إلى أن توسع دور الفاعلين من غير الدول في الفضاء السيبراني يفرض إعادة النظر في المفهوم التقليدي لمسؤولية الدولة في القانون الدولي[69].

ويتمثل التحدي الرابع في عدم وضوح حدود السيادة في الفضاء السيبراني .فبينما استقر الفقه على أن للدولة سيادة على إقليمها وبناها التحتية الواقعة داخله، فإن تطبيق هذا المفهوم على الفضاء السيبراني يثير إشكالات عملية، نظرًا للطابع العابر للحدود للشبكات الرقمية[70]، ويؤكد عبد الكريم علوان أن «السيادة

---

63 عبد الكريم علوان، القانون الدولي العام في عالم متغير المرجع السابق، ص 301.
64 عبد الله سليمان، "الأمن السيبراني وإشكالية التنظيم الدولي"، المرجع السابق، ص22.
65 محمد عبد الرحمن، الأمن السيبراني والقانون الدولي القاهرة، المرجع السابق، ص162.
66 Schmitt, Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations Cambridge, p 80.
67 سليمان، "الأمن السيبراني وإشكالية التنظيم الدولي"، المرجع السابق، ص25.
68 عبد السلام، القانون الدولي واستخدام القوة، المرجع السابق، ص 215.
69 عبد الله عبد العزيز الهاجري، "الفاعلون من غير الدول في الفضاء السيبراني"، المرجع السابق، ص60.
70 عبد الرحمن، الأمن السيبراني والقانون الدولي، المرجع السابق، ص170.

الرقمية باتت ضرورة لحماية مصالح الدول في العصر الحديث، غير أن تحديد نطاقها وحدودها القانونية لا يزال يكتنفه كثير من الغموض»[71].

أما التحدي الخامس فيتمثل في قصور آليات الإنفاذ الدولي .فحتى في حال الاتفاق على عدم مشروعية هجوم سيبراني معين، فإن غياب أجهزة دولية متخصصة قادرة على التحقيق الفني المستقل، وفرض الجزاءات المناسبة، يجعل من الصعب ضمان احترام القواعد القانونية في هذا المجال[72]، ويشير محمد مجدي عبد السلام إلى أن «القانون الدولي يفتقر إلى أدوات فعالة لردع الانتهاكات السيبرانية، مقارنة بما هو قائم في مجال النزاعات المسلحة التقليدية»[73].

ثانيًا: الآفاق المستقبلية لتنظيم الحروب السيبرانية الصامتة

أمام هذه التحديات، يبرز اتجاه فقهي عربي ودولي يدعو إلى تطوير القواعد القائمة بدلًا من استبدالها، من خلال تفسير مبادئ القانون الدولي التقليدية تفسيرًا ديناميكيًا يراعي خصوصية الفضاء السيبراني[74]، ففي هذا السياق، يرى عدد من الباحثين العرب أن مبادئ السيادة وعدم التدخل وعدم استخدام القوة لا تزال صالحة من حيث الجوهر، لكن ينبغي إعادة صياغة تطبيقاتها بما يتناسب مع الواقع الرقمي الجديد[75].

ويتجسد اتجاه آخر في الدعوة إلى إبرام اتفاقية دولية خاصة بالأمن السيبراني، تُحدد على نحو واضح الأفعال السيبرانية المحظورة، ومعايير الإسناد، وضوابط الرد المشروع، وآليات التعاون الدولي[76]، ويؤكد عبد الرحمن أن «اعتماد معاهدة دولية شاملة للأمن السيبراني بات ضرورة ملحة، على غرار اتفاقيات نزع السلاح التقليدية، لتفادي انزلاق الدول نحو سباق تسلح سيبراني غير منضبط»[77].

كما يبرز دور الجهود الإقليمية العربية في هذا المجال، سواء في إطار جامعة الدول العربية أو المجالس الإقليمية المتخصصة، من أجل وضع استراتيجيات مشتركة للأمن السيبراني وتعزيز التعاون في مواجهة الهجمات الرقمية[78]، ويرى بعض الباحثين العرب أن بناء موقف عربي موحد من شأنه أن يعزز القدرة التفاوضية للدول العربية في المحافل الدولية المعنية بوضع قواعد السلوك في الفضاء السيبراني[79].

ومن الآفاق المهمة كذلك تعزيز بناء القدرات الوطنية في المجال السيبراني، من خلال تطوير البنى التحتية التقنية، وتأهيل الكوادر البشرية، وسن تشريعات داخلية متوافقة مع المعايير الدولية[80]، ويؤكد أحمد فتحي سرور أن «التنظيم الدولي وحده لا يكفي ما لم تُدعّم الدول قدراتها الذاتية لحماية فضائها السيبراني»[81].

كما يُعوَّل على ترسيخ قواعد عرفية دولية من خلال الممارسة المتكررة للدول واقترانها بالاعتقاد بالإلزام القانوني، ولا سيما في ظل صعوبة التوصل إلى معاهدة شاملة في المدى القريب[82]، وفي هذا الإطار، يمكن أن تسهم المبادئ غير الملزمة، كالتقارير الصادرة عن فرق الخبراء الحكوميين في الأمم المتحدة، في بلورة معايير سلوك مقبولة دوليًا[83].

---

71 علوان، القانون الدولي العام في عالم متغير، المرجع السابق، ص 304.
72 عبد السلام، القانون الدولي واستخدام القوة، المرجع السابق، ص218.
73 عبد السلام، القانون الدولي واستخدام القوة، المرجع السابق، ص 220.
74 أبو هيف، القانون الدولي العام، المرجع السابق، ص 528.
75 عبد الرحمن، الأمن السيبراني والقانون الدولي، المرجع السابق، ص 175.
76 سليمان، "الأمن السيبراني وإشكالية التنظيم الدولي"، المرجع السابق، ص30.
77 عبد الرحمن، الأمن السيبراني والقانون الدولي، المرجع السابق، ص 178.
78 أحمد يوسف أحمد، "الأمن السيبراني في الوطن العربي: التحديات والفرص"، مجلة شؤون عربية، العدد 186 2021: ص45.
79 أحمد، "الأمن السيبراني في الوطن العربي"، المرجع السابق، ص 48.
80 سرور، "الحرب السيبرانية وتحديات الأمن القومي العربي"، المرجع السابق، ص 78.
81 سرور، "الحرب السيبرانية وتحديات الأمن القومي العربي"، المرجع السابق، ص80.
82 Schmitt, Tallinn Manual 2.0, Previous reference, p 9.
83 United Nations, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security 2015, para. 13.

ويخلص جانب من الفقه العربي إلى أن مستقبل تنظيم الحروب السيبرانية الصامتة يتوقف على مدى قدرة المجتمع الدولي على تحقيق توازن دقيق بين متطلبات الأمن القومي للدول، وضرورة الحفاظ على طابع الفضاء السيبراني كفضاء مفتوح يخدم التنمية والتواصل الإنساني[84]، فالإفراط في القيود قد يعيق التطور التكنولوجي، في حين أن غياب التنظيم قد يؤدي إلى فوضى رقمية تهدد السلم الدولي.

وعليه، فإن الحروب السيبرانية الصامتة تضع القانون الدولي أمام اختبار حقيقي لمرونته وقدرته على التطور. فهي تكشف في آن واحد عن قصور القواعد القائمة، وعن إمكان تطويرها واستكمالها بما يواكب التحولات الرقمية المتسارعة. ومن ثم، فإن استشراف آفاق تنظيمها لا يقتصر على اقتراح حلول قانونية فحسب، بل يمتد إلى الدعوة لبناء ثقافة دولية جديدة قوامها التعاون والثقة المتبادلة في الفضاء السيبراني، بما يسهم في حماية السلم والأمن الدوليين في العصر الرقمي.

الخاتمة

خلص هذا البحث إلى أن الحروب السيبرانية الصامتة تمثل أحد أبرز مظاهر التحول في طبيعة الصراعات الدولية في العصر الرقمي، حيث لم تعد القوة تُمارس بالضرورة عبر الوسائل العسكرية التقليدية، بل أضحت تُمارس أيضًا من خلال أدوات رقمية خفية قادرة على إحداث آثار استراتيجية عميقة في البنى التحتية الحيوية للدول، وفي استقرارها السياسي والاقتصادي والاجتماعي. وقد كشف البحث أن هذا النمط من الصراعات يفرض تحديات جدية على قواعد القانون الدولي العام، ولا سيما مبدأ عدم استخدام القوة الذي يشكل حجر الزاوية في النظام القانوني الدولي المعاصر.

وأظهر البحث أن غياب تعريف دولي موحّد للحروب السيبرانية الصامتة، وتعدد صورها، وصعوبة إسنادها إلى دول بعينها، كلها عوامل أسهمت في تعقيد تكييفها القانوني وإخضاعها للقواعد القائمة. كما بيّن أن الفقه الدولي، العربي والأجنبي، لا يزال منقسمًا حول ما إذا كانت هذه الحروب تُعد في جميع صورها استخدامًا للقوة بالمعنى المقصود في المادة (4/2) من ميثاق الأمم المتحدة، أم أنها تظل – في كثير من الحالات – دون هذه العتبة، مع بقائها أفعالًا غير مشروعة تمس مبادئ السيادة وعدم التدخل.

وفي ضوء ذلك، يتضح أن الحروب السيبرانية الصامتة لا تشكل مجرد تحدٍّ تقني، بل تمثل اختبارًا حقيقيًا لمرونة القانون الدولي وقدرته على التكيف مع التحولات العميقة في طبيعة التهديدات المعاصرة. ومن ثم، فإن التعامل معها يقتضي مقاربة قانونية متوازنة، تحافظ على جوهر مبادئ القانون الدولي، وفي مقدمتها حظر استخدام القوة، مع تطوير آليات تفسيرها وتطبيقها بما ينسجم مع خصوصيات الفضاء السيبراني.

أولًا: النتائج

أسفر هذا البحث عن جملة من النتائج، يمكن إجمالها فيما يأتي:

1. حداثة مفهوم الحروب السيبرانية الصامتة وعدم استقراره فقهيًا أو دوليًا، رغم تزايد حضوره في الممارسات الدولية، بما يجعل تحديد معالمه وضبطه القانوني أمرًا ملحًا.

2. تميّز هذه الحروب بخصائص نوعية، أبرزها الخفاء، وصعوبة الإسناد، والطابع العابر للحدود، وتعدد الأهداف، وانخفاض الكلفة، وهو ما يجعلها أداة جذابة للإكراه بين الدول دون الانزلاق إلى مواجهة عسكرية مباشرة.

3. وقوع أغلب صور الحروب السيبرانية الصامتة في المنطقة الرمادية بين السلم والنزاع المسلح، إذ لا ترقى إلى مستوى القوة المسلحة، لكنها في الوقت ذاته تمثل خرقًا لمبادئ أساسية في القانون الدولي، كاحترام السيادة وعدم التدخل.

4. استمرار صلاحية مبدأ عدم استخدام القوة من حيث الجوهر لتنظيم السلوك الدولي في الفضاء السيبراني، شريطة تفسيره تفسيرًا ديناميكيًا يراعي طبيعة الوسائل الرقمية وآثارها الواقعية.

[84] عبد الرحمن، الأمن السيبراني والقانون الدولي، المرجع السابق، ص 182.

5. قصور الإطار القانوني الدولي القائم عن الإحاطة الشاملة بظاهرة الحروب السيبرانية الصامتة، ولا سيما في ما يتعلق بتحديد المعايير الفاصلة بين القوة المحظورة والأفعال دون العتبة، وبآليات الإسناد والمساءلة.

ثانيًا: المقترحات

في ضوء النتائج المتقدمة، يقترح البحث ما يأتي:

1. العمل على بلورة تعريف دولي موحّد للحروب السيبرانية الصامتة أو للعمليات السيبرانية العدائية الخطيرة، في إطار الأمم المتحدة، بما يسهم في تقليص الغموض المفاهيمي وتوحيد مواقف الدول.

2. الدفع نحو إبرام اتفاقية دولية للأمن السيبراني تُحدّد الأفعال المحظورة، وتضع قواعد للإسناد، وتُرسّخ آليات للتعاون الدولي في التحقيق والاستجابة للهجمات السيبرانية.

3. إنشاء أو دعم آليات دولية فنية مستقلة تحت مظلة الأمم المتحدة، تتولى المساعدة في التحقيق في الهجمات السيبرانية الكبرى، بما يعزز الثقة ويحد من تسييس مسألة الإسناد.

4. تفعيل التعاون العربي في مجال الأمن السيبراني عبر جامعة الدول العربية والمنظمات الإقليمية، لوضع استراتيجيات مشتركة وبناء موقف عربي موحّد في المفاوضات الدولية ذات الصلة.

5. تعزيز التشريعات الوطنية وبناء القدرات التقنية والبشرية في الدول العربية، بما يضمن حماية أفضل للبنى التحتية الحيوية، ويُيسّر التفاعل الإيجابي مع الجهود الدولية لتنظيم الفضاء السيبراني.

قائمة المصادر والمراجع

أولاً :المصادر والمراجع العربية

1. محمد عبد الرحمن، *الأمن السيبراني والقانون الدولي*، القاهرة: دار النهضة العربية، 2021.
2. أحمد فتحي سرور، "الحرب السيبرانية وتحديات الأمن القومي العربي"، *مجلة السياسة الدولية*، العدد 214، 2018.
3. عبد الكريم علوان، *القانون الدولي العام في عصر العولمة*، عمّان: دار الثقافة، 2020.
4. علي صادق أبو هيف، *القانون الدولي العام*، الإسكندرية: منشأة المعارف، 2010.
5. محمد مجدي عبد السلام، *القانون الدولي واستخدام القوة*، القاهرة: دار الفكر الجامعي، 2019.
6. عبد الله سليمان، "الأمن السيبراني وتطور مفهوم القوة في القانون الدولي"، *مجلة الحقوق*، جامعة الكويت، العدد 2، 2020.
7. عبد الله عبد العزيز الهاجري، "الهجمات السيبرانية ومبدأ عدم استخدام القوة"، *مجلة الدراسات القانونية*، جامعة الكويت، العدد 1، 2021.
8. أحمد يوسف أحمد، "الأمن السيبراني في الوطن العربي: التحديات والفرص"، *مجلة شؤون عربية*، العدد 186، 2021.
9. عبد الله عبد العزيز الهاجري، "الفاعلون من غير الدول في الفضاء السيبراني"، *مجلة الدراسات القانونية*، جامعة الكويت، العدد 2، 2022.

ثانياً : المراجع الأجنبية

1. Richard A. Clarke and Robert Knake, *Cyber War: The Next Threat to National Security and What to Do About It* ،New York: Ecco, 2010.
2. Thomas Rid, *Cyber War Will Not Take Place* ،Oxford: Oxford University Press, 2013.

3. Michael N. Schmitt (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* ،Cambridge: Cambridge University Press, 2017.
4. Michael J. Mazarr, *Mastering the Gray Zone* ،Carlisle: U.S. Army War College Press, 2015.
5. Frank G. Hoffman, "Hybrid Warfare and Challenges" ،*Joint Force Quarterly*2009 ،52 العدد ،.
6. David E. Sanger, *Confront and Conceal* ،New York: Crown, 2012.
7. Rain Ottis, "Analysis of the 2007 Cyber Attacks against Estonia" ،*NATO CCD COE Proceedings*2008 ،.
8. Jack Goldsmith and Tim Wu, *Who Controls the Internet?* ،Oxford: Oxford University Press, 2006.
9. Susan W. Brenner, *Cybercrime and the Law* ،Boston: Northeastern University Press, 2010.
10. Michael N. Schmitt, "Cyber Operations and the Jus ad Bellum Revisited" ،*Villanova Law Review*2011 ،3 العدد ،56 المجلد ،.
11. Gary P. Corn, "Cyber National Security: Navigating Gray Zone Challenges" ،*Journal of National Security Law & Policy* ،9 المجلد ، 2018.
12. James Crawford, *State Responsibility: The General Part* ، Cambridge: Cambridge University Press, 2013.
13. United Nations, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*2015 ،.
14.

ثالثاً :الوثائق الدولية

1. ميثاق الأمم المتحدة، 1945.
2. قضية نيكاراغوا ضد الولايات المتحدة (المحكمة الدولية للعدل، 1986).