حدود استخدام الفضاء الالكتروني في ضوء القانون الدولي

إيمان هاتف نايف تفاح
الجامعة الإسلامية /لبنان

المستخلص:

مع الانتشار لاستخدام الفضاء الالكتروني في التعاملات المختلفة سواء ما يتعلق بالنقل للمعلومات أو ما يتصل بالحفظ لمختلف البيانات فإنه تظهر المخاطر الخاصة بالهجمات الالكترونية التي تنعكس على أمن المعلومات وكذلك التهديد المباشر للسلم والأمن للدول، فما يحدث من تجسس وتخطي للحماية واختراقات لمواقع مؤسسات أمنية ووزارات خاصة بالبيئة والكهرباء وكذلك المياه وشبكات الاتصال وغيرها أمر من شأنه أن يهدد أمن الدولة والبنية التحتية الخاصة بها.

إن مخاطر الاستخدام الخاطئ للفضاء الإلكتروني ترتبط بالأمور والجوانب السياسية إذ أن من شان معرفة اسرار الدول والمعلومات الخاصة بمواطنيها عن طريق التجسس الالكتروني أن يحقق ميزة وتفوق بين الدول، ويترتب عليه تهديد أمن الدول وسيادتها من خلال اتدخل في شؤونها والمساس بسلامتها سياسًا واقتصاديًا.

الكلمات المفتاحية: أمن الدول- التجسس إلكترونيًا- سيادة الدولة.

Abstract

With the widespread use of cyberspace for various transactions, whether related to the transfer of information or the storage of various data, the risks of cyber-attacks emerge, posing a direct threat to the peace and security of states. Espionage, bypassing protection, and breaches of the websites of security institutions and ministries concerned with the environment, electricity, water, communications networks, and other sectors can threaten state security and infrastructure.

The risks of misusing cyberspace are linked to political matters and aspects, as learning state secrets and the private information of their citizens through cyber espionage can lead to an advantage and superiority among states. This can also threaten the security and sovereignty of states through interference in their affairs and compromising their political and economic integrity.

Keywords: State security - cyber espionage - State sovereignty.

المقدمة

تُعد المبادئ الأساسية للقانون الدولي الإنساني مرجعًا لتقييم مدى انطباقها على الحرب السيبرانية والفضاء الالكتروني. يُعد هذا الموضوع من القضايا القانونية المعاصرة التي لم تنل بعد حظها الكافي من الدراسة ضمن إطار القانون الدولي العام، رغم تصاعد أهميتها في ضوء التقدم التكنولوجي المتسارع في ميدان الفضاء.

إن الاستخدامات المتزايدة للتكنولوجيا في الفضاء الخارجي، سواء لأغراض مدنية أو عسكرية، أفرزت تحديات قانونية تتطلب ضبطًا دقيقًا يضمن الاستخدام الآمن والمشروع وفق قواعد القانون الدولي. حيث يهدف البحث إلى توضيح مدى فاعلية النظام القانوني الدولي في مواكبة التطورات التقنية في الفضاء، ورصد أوجه القوة والقصور في التشريعات الحالية ذات الصلة.

ومن أبرز هذه المبادئ ما يُعرف بشرط مارتنز، الذي تم إقراره بدايةً ضمن اتفاقيتي لاهاي في أواخر القرن التاسع عشر، ثم تأكد حضوره في البروتوكولات الإضافية اللاحقة. هذا الشرط يُقر بأن في غياب نصوص قانونية صريحة، يظل الأفراد محميين بأحكام العرف، وبالاعتبارات الإنسانية، وبما يقتضيه الضمير الجمعي. ورغم وضوح الصيغة، يظل الجدل قائمًا بشأن ما إذا كانت هذه المبادئ تشكّل قواعد قانونية واجبة التطبيق، أم أنها مجرد معايير أخلاقية توجيهية. وقد حسمت محكمة العدل الدولية في رأيها المتعلق بشرعية التهديد بالأسلحة النووية أو استخدامها أهمية هذا الشرط، معتبرة إياه قاعدة فعالة تواكب التقدم التكنولوجي في الميدان العسكري، وتؤكد استمرارية قابليته للتطبيق.[١]

ويُلاحظ أن السياقات المعاصرة، خصوصًا مع تعقيد أدوات الصراع وتطورها التكنولوجي، تفرض تحديات جديدة على المعايير الإنسانية، ما يزيد من أهمية هذا الشرط كأداة قانونية مرنة تواكب المتغيرات. فالفكرة الجوهرية التي بُني عليها هذا المبدأ تؤكد أن عدم النص على الحظر لا يعني بالضرورة الإباحة، إذا كان الفعل يتعارض مع جوهر القيم الإنسانية.

كما يُعد شرط مارتنز امتدادًا طبيعيًا للمبادئ العامة للقانون الدولي الإنساني، حيث يؤدي دورًا محوريًا في معالجة الثغرات القانونية والتعامل مع المستجدات التي لم تُتناول مسبقًا. وهو يستمد قوته من طبيعته الإنسانية العامة، التي تسمح بتطبيقه في أي ظرف، سواء استند إلى نص مكتوب أو إلى عرف دولي مستقر، ما يجعله ملزمًا حتى للدول التي لم تصادق على الاتفاقيات ذات الصلة.

[١] المادة (٣٦) من البروتوكول الإضافي الأول الملحق باتفاقيات جنيف لسنة ١٩٧٧.

أولاً: أهمية البحث:

برزت أهمية هذا البحث في ظل التقدم المتسارع لتكنولوجيا الفضاء الخارجي، وما يرافقه من تحولات نوعية في أنماط استخدامها، سواء لأغراض سلمية أو غير سلمية. فقد بات لتلك التكنولوجيا أثر مباشر على حياة الأفراد وأمنهم، مما يستدعي تأطير استخدامها ضمن قواعد قانونية واضحة تحول دون إساءة توظيفها.

كما أن توغل تقنيات الفضاء في البنية التحتية للحياة اليومية يعزز الحاجة إلى إطار قانوني دولي يضمن الاستخدام الآمن والمسؤول، ويحد من المخاطر الإنسانية التي قد تترتب على توجيه هذه التقنيات نحو أهداف عدائية أو غير مشروعة.

ثانيًا: أهداف البحث:

لتتبع الأساس القانوني المنظم لاستخدام الفضاء الخارجي، من خلال الرجوع إلى نصوص الاتفاقيات الدولية ذات الصلة، وقرارات ومبادئ الأمم المتحدة، فضلًا عن الوثائق التي تُعالج تطبيق قواعد القانون الدولي الإنساني في سياق الاستخدامات غير السلمية للفضاء

ثالثًا: المنهجية:

اعتمدت المنهج التحليلي: ويعتمد على تحليل المضمون القانوني لتلك النصوص والاتفاقيات، بهدف فهم أبعادها وتقييم مدى قدرتها على ضبط الاستخدامات الفضائية، واستكشاف نقاط القوة والقصور فيها.

رابعًا: الإشكالية:

نتيجة المخاطر وموضوع البحث الذي يتصل بالفضاء الإلكتروني وأثر الاستخدامات غير المنضبطة له فإن إشكالية البحث تتمثل في الإجابة على التساؤل:

ما هو دور وموقف القانون الدولي من استخدام الفضاء الالكتروني سواء أكان استخدام لأغراض سلمية أم عدائية؟

خامسًا: خطة البحث:

من أجل الإجابة على الإشكالية فإنني قسمت البحث إلى مبحثين الأول ببيان ضوابط استخدام الفضاء الإلكتروني والثاني خاص ببيان الانحرافات الإجرامية الناجمة عن الاستخدام غير المنضبط للفضاء الإلكتروني.

المبحث الأول:

ضوابط استخدام الفضاء الإلكتروني وموقف القانون الدولي

يحظى مبدأ الالتزام بالقواعد القانونية في النزاعات المسلحة بإجماع فقهاء القانون الدولي الإنساني، سواء من حيث ضرورة تطبيقها أو عدم تأثرها بدرجة النزاع أو طبيعة تطوره. ومن أبرز هذه القواعد ما جاء في البروتوكول الإضافي الأول لاتفاقيات جنيف لعام ١٩٧٧، الذي يقر بوجوب اعتبار أي شخص مشكوك في صفته القتالية مدنيًا حتى يثبت العكس.

ولا تقتصر هذه القواعد على حماية المدنيين من آثار النزاع، بل تتطلب أيضًا التقيد بشرعية الاستهداف، من خلال التمييز الدقيق بين المقاتلين ومن يملكون القدرة على المشاركة في الأعمال العدائية، وبين من لا علاقة لهم بالنزاع. كما يُشترط الفصل الواضح بين الأهداف العسكرية المباحة والأعيان المدنية المحمية. ويجد هذا المبدأ جذوره في المفاهيم القانونية التقليدية التي تؤكد أن الحرب نزاع بين دول، لا بين أفراد، وأن صفة العداء لا تُنسب إلى الأشخاص بصفتهم المدنية، بل فقط حينما ينخرطون فعليًا في العمليات القتالية.[٢].

المطلب الأول: الحماية المقررة في القانون الدولي واستخدام الفضاء الالكتروني

الفرع الأول: الحدود والمحظورات:

يُعد حظر الهجمات العشوائية من المبادئ الأساسية التي تؤكد عليها قواعد القانون الدولي الإنساني، ويشمل ذلك أي هجوم لا يُوجَّه نحو هدف عسكري محدد، أو تُستخدم فيه وسائل أو أساليب قتال تفتقر إلى القدرة على التحديد الدقيق، سواء من حيث التوجيه أو الأثر، ما يؤدي إلى إصابة مواقع عسكرية ومدنية وأفراد مدنيين دون تمييز.

ويتصل بهذا الحظر مبدأ التناسب، الذي يفرض قيودًا على العمليات العسكرية، بحيث يُمنع تنفيذ أي هجوم قد تترتب عليه خسائر في صفوف المدنيين أو أضرار في الأعيان المدنية بشكل غير متناسب مع الميزة العسكرية المتوقعة. ويستمد هذا المبدأ قوته من القانون الدولي العرفي، ويُطبق في جميع النزاعات المسلحة، بغض النظر عن طابعها الدولي أو غير الدولي.[٣].

يُعد مبدأ الضرورة العسكرية من الركائز الجوهرية في القانون الدولي الإنساني، حيث يجيز استخدام القوة ضمن حدود ما هو غير محظور، وبالقدر الذي تفرضه الحاجة لتحقيق هدف مشروع في إطار النزاع، والمتمثل في شل قدرة العدو كليًا أو جزئيًا، مع تقليل الخسائر البشرية

[٢] الفقرة (١) من المادة (٥٠) من البروتوكول الإضافي الأول الملحق باتفاقيات جنيف لسنة ١٩٧٧.
[٣] الفقرة (٤) من المادة (٥١) من البروتوكول الإضافي الأول الملحق باتفاقيات جنيف لسنة ١٩٧٧.

والمادية إلى أدنى حد ممكن. وبناءً عليه، لا يُسمح بتدمير ممتلكات العدو أو الاستيلاء عليها، إلا إذا كانت طبيعة العمليات الحربية تستوجب ذلك بشكل حتمي.[٤].

يمثل مبدأ الإنسانية أحد المبادئ العامة في القانون الدولي الإنساني، ويُعد مكمّلًا لمبدأ الضرورة العسكرية بل ومتداخلًا معه، إذ يفرض قيودًا على استخدام القوة من خلال حظر إلحاق معاناة أو إصابات لا تبررها متطلبات القتال. وبموجب هذا المبدأ، يُمنع اللجوء إلى أساليب أو وسائل قتال لا تُحظرها نصوص أخرى بشكل صريح، انطلاقًا من أن حرية أطراف النزاع في اختيار أدوات الحرب ليست مطلقة، بل تخضع لقيود تهدف إلى حماية الكرامة الإنسانية والتقليل من الأضرار غير الضرورية.[٥] يُحظر أيضًا استخدام الأسلحة، القذائف، المواد، ووسائل التدمير التي قد تؤدي إلى إحداث إصابات أو معاناة غير مبررة.[٦].

الفرع الثاني: تقييم دور الفضاء الإلكتروني في العلاقات الدولية

تطبيق قواعد القانون الدولي المتعلقة بالنزاعات المسلحة في الواقع يُعد تحديًا كبيرًا، حيث يعتمد بشكل أساسي على توازن الصلاحيات الممنوحة للقوات العسكرية أثناء العمليات، والتي تشمل حماية الذات من جهة، وحماية المدنيين والفئات غير المشاركة في الأعمال العدائية والأعيان المدنية من جهة أخرى.

في هذا المطلب، سنتناول مقاربات مختلفة بين سلوك الأفراد العسكريين في ظل الظروف الفعلية للنزاعات المسلحة وما يترتب عليها من انتهاكات جسيمة، وبين كيفية الاستفادة الأمثل من الفضاء الإلكتروني في النزاعات المسلحة ضمن بيئة عمل تراعي الالتزام بقواعد القانون الدولي الإنساني.[٧] "شريطة أن تُتخذ الإجراءات أو التدابير المعنية لغياب أي خيار بديل متاح، استنادًا إلى مبدأ الضرورة." [٨] وقد يشكل هذا الفعل في حدّ ذاته انتهاكًا لمبدأ حظر إلحاق آلام غير مبررة، وهو المبدأ الذي يحظر أي مساس غير مشروع بالسلامة الجسدية أو النفسية، أو بحياة المقاتلين الذين يُعدّ استهدافهم بالعنف المشروع جائزًا قانونًا [٩].

---

[٤] الفقرة (ب) الفقرة (٥) من المادة (٥١) وكذلك المادة (٥٧) من البروتوكول الإضافي الأول الملحق باتفاقيات جنيف لسنة ١٩٧٧.

[٥] الفقرة (٣) من المادة (٥٧) من البروتوكول الإضافي الأول الملحق باتفاقيات جنيف لسنة ١٩٧٧.

[٦] الفقرة (١) من المادة (٣٥) من البروتوكول الإضافي الأول الملحق باتفاقيات جنيف لسنة ١٩٧٧.

[٧] المصدر السابق ص ١٣٥.

[٨] هشام بشري المدخل القانوني الدولي الإنساني ط ١ المركز القومي للإصدارات القومية القاهرة ٢٠١٢ ص ٨٩.

[٩] سلوان جابر هاشم حالة الضرورة العسكرية في القانون الدولية الإنساني ط ١ المؤسسة الحديثة للكتاب لبنان ٢٠١٣ ص ١٠٥.

تظهر الإشكالية في التعامل السلبي مع الهجمات السيبرانية بوضوح في الميدان، حيث يواجه الجنود صعوبات جمّة في الالتزام بمبدأ التناسب. فهذا المبدأ، الذي يقتضي موازنة الأثر العسكري المتوقع مع الأضرار المحتملة، خاصة على المدنيين والممتلكات المدنية، يصبح تطبيقه معقّدًا في ظل تغيّر المعطيات العسكرية باستمرار، تبعًا لتبدّل الخطط والتطورات العملياتية لدى الطرفين. وفي الحالات التي تكون فيها هذه المتغيرات غير قابلة للتنبؤ، يصعب على البرمجيات الإلكترونية تنفيذ ذلك المبدأ بدقة. إذ إن معادلة التناسب بحد ذاتها تتطلب تقديرًا عاليًا ومهارة فائقة حتى في النزاعات التقليدية، حيث تظل الأولوية للقوات تحقيق النصر العسكري، مع التزام قانوني موازٍ بتقليص الضرر وتجنّب التدمير المفرط. ومن هنا، فإن تحقيق هذا التوازن المعقّد يتطلب قائدًا متمرسًا يجيد ضبط المعادلة، وهو ما يزيد صعوبة المشهد عندما يتعلق الأمر بالفضاء السيبراني.[١٠].

هذا وتبرز هنا إشكالية أخرى بالغة الأهمية تتعلق بقدرة البرمجيات على التقدير السليم للسلوكيات الاجتماعية في الميدان. فالتقييم الدقيق لهذه التصرفات يتطلب خبرة إنسانية يصعب برمجتها إلكترونيًا، لا سيما في المواقف المعقدة التي قد يظهر فيها سلوك مدني أو جماعة من المدنيين كردّ فعل تلقائي ناتج عن الخوف أو الهلع أثناء العمليات العسكرية، مما قد يبدو للوهلة الأولى تهديدًا محتملاً للقوات. في مثل هذه الحالات، لا بد من تدخل بشري قادر على التمييز بين السلوك الخطر فعلاً وتلك الأفعال التي لا تمثل خطرًا حقيقيًا، بل تنبع من ردود فعل طبيعية في أوقات النزاع. ومن هذا المنطلق، لا يجوز للجندي أن يستخدم القوة إذا كان لديه شك في طبيعة التصرف، لأن ذلك ينعكس مباشرة على تقييم القصد الجنائي في حال المساءلة القانونية. فثبوت المسؤولية الجنائية يتطلب توافر نية إجرامية قائمة على إدراك وحرية في اتخاذ القرار. وقد أكّد النظام الأساسي للمحكمة الجنائية الدولية على هذه المسألة بوضوح، حيث نصّ على أن المسؤولية لا تُثبت إلا عند تحقق الأركان المادية للجريمة مقرونة بالقصد والعلم، موضحًا أن القصد يتحقق عندما يتعمّد الشخص سلوكه أو نتائجه، وأن العلم يعني إدراك الشخص بوجود ظروف معينة أو نتائج مرجحة الوقوع في السياق الطبيعي للأحداث.[١١].

بعد أن تناولنا سابقًا التحديات المرتبطة بتطبيق المبادئ الإنسانية على الهجمات السيبرانية، تبرز هنا إشكالية أخرى بالغة الأهمية تتعلق بقدرة البرمجيات على التقدير السليم للسلوكيات الاجتماعية

[١٠] هنري ميروفيتز مبدأ الآلام التي لا مبرر لها دراسات في القانون الدولي الإنساني دار المستقبل العربي القاهرة ٢٠٠٩ ص ٢٢.

[١١] أحمد الأنور قواعد وسلوك القتال دراسات في القانون الدولي الإنساني دار المستقبل العربي القاهرة ٢٠٠٠ ص ٣١٩.

في الميدان. فالتقييم الدقيق لهذه التصرفات يتطلب خبرة إنسانية يصعب برمجتها إلكترونيًا، لا سيما في المواقف المعقدة التي قد يظهر فيها سلوك مدني أو جماعة من المدنيين كردّ فعل تلقائي ناتج عن الخوف أو الهلع أثناء العمليات العسكرية، مما قد يبدو للوهلة الأولى تهديدًا محتملاً للقوات. في مثل هذه الحالات، لا بد من تدخل بشري قادر على التمييز بين السلوك الخطر فعلاً وتلك الأفعال التي لا تمثل خطرًا حقيقيًا، بل تنبع من ردود فعل طبيعية في أوقات النزاع. ومن هذا المنطلق، لا يجوز للجندي أن يستخدم القوة إذا كان لديه شك في طبيعة التصرف، لأن ذلك ينعكس مباشرة على تقييم القصد الجنائي في حال المساءلة القانونية. فثبوت المسؤولية الجنائية يتطلب توافر نية إجرامية قائمة على إدراك وحرية في اتخاذ القرار. وقد أكّد النظام الأساسي للمحكمة الجنائية الدولية على هذه المسألة بوضوح، حيث نصّ على أن المسؤولية لا تُثبت إلا عند تحقق الأركان المادية للجريمة مقرونة بالقصد والعلم، موضحًا أن القصد يتحقق عندما يتعمّد الشخص سلوكه أو نتائجه، وأن العلم يعني إدراك الشخص بوجود ظروف معينة أو نتائج مرجحة الوقوع في السياق الطبيعي للأحداث.

المطلب الثاني: بعض الإيجابيات المترتبة على توظيف الفضاء السيبراني في النزاعات المسلحة

الفرع الأول: ضوابط ومعايير تطبيق القانون الدولي

تطبيق القانون الدولي الإنساني أثناء النزاعات لا يعد مسألة نظرية فحسب، بل يرتكز على احترام معايير قانونية محددة، تتطلب من الأطراف المتنازعة الالتزام بها بغضّ النظر عن مشاعرهم أو انفعالاتهم الشخصية. فالجندي، على سبيل المثال، ملزم بعدم المساس بحياة المدني، مهما كانت مشاعره تجاهه، في حين يسمح له القانون باستهداف المقاتل حتى إن لم يُبدِ أي عدوانية. ومن هذا المنطلق، فإن توظيف التكنولوجيا الحديثة في بيئات ميدانية معقّدة قد يسهم في تعزيز الالتزام بهذه القواعد، نظرًا لقدرتها على تقليص أثر الانفعالات البشرية التي قد تنشأ نتيجة الخوف أو الكراهية أو الإرهاق أو حتى غريزة البقاء. لذلك، فإن الاستخدام المنظّم للهجمات السيبرانية قد يقدم بديلًا أكثر اتزانًا وموضوعية، يعزّز من احترام المبادئ الإنسانية في سياق العمليات العسكرية[١٢].

يُثار أحيانًا اعتراض مفاده أن اعتماد الهجمات السيبرانية في النزاعات المسلحة قد يُعد ممارسة تفتقر إلى العدالة، غير أن هذا الرأي يصعب تعميمه أو التسليم به. فالحروب، بطبيعتها، لم تكن يومًا ميدانًا للتكافؤ الكامل بين الأطراف. إذ من غير المنطقي أن يُمنع طرف من استخدام قدراته الجوية أو البحرية لأن خصمه لا يملك الوسائل ذاتها، أو يفتقر إلى أدوات دفاعية توازيها،

[١٢] المادة (٣٠) من النظام الأساسي للمحكمة الجنائية الدولية.

كالأنظمة المضادة للطائرات. وبالتالي، فإن مبدأ العدالة في سياق النزاع المسلح لا يُقاس بتوازن الوسائل، بل بمدى التزام استخدامها ضمن الأطر القانونية المعتمدة.[١٣].

ولا يساور الشك أن إدماج التقنيات المتقدمة، ومن بينها الهجمات السيبرانية، في سياق النزاعات المسلحة قد يحدّ بدرجة كبيرة من تدخل العوامل البشرية التي قد تميل أحيانًا إلى تجاوز القواعد القانونية، أو اتخاذ قرارات محكومة بمصالح آنية بحتة. ورغم ما تثيره الهجمات السيبرانية، شأنها شأن بعض أنواع الأسلحة الأخرى، من إشكالات تتعلق بمدى انطباق قواعد القانون الدولي الإنساني وقانون حقوق الإنسان، فإن تنفيذ ضربات على أهداف عسكرية من مواقع بعيدة عن ميدان المواجهة يسلّط الضوء على إشكالية قانونية دقيقة تتصل بتحديد الإطار القانوني الحاكم في تلك الظروف، لا سيما ما يتعلق بتحديد السيادة القانونية بين النظامين الدوليين المعنيين.[١٤].

الفرع الثاني: تقييم دور القانون الدولي في مواجهة الهجمات السيبرانية:

انطلاقًا مما سبق، فإن تقييم دور التقنيات الإلكترونية الحديثة، وعلى رأسها الهجمات السيبرانية، في سياق النزاعات المسلحة، ينبغي أن يتم بمقارنتها بالواقع البشري وظروف القتال الفعلية، لا من خلال معايير مثالية أو تصورات نظرية مجردة. فالمقارنة العادلة تقتضي مراعاة ما يحيط بالعمليات العسكرية من التباسات وتعقيدات. كما أن القواعد الحالية للقانون الدولي الإنساني، التي ترتكز في جزء كبير منها على مبدأ اتخاذ التدابير الاحتياطية الممكنة، تفتح المجال أمام استخدام الوسائل التقنية المتطورة كوسائل قد تسهم في تحسين القدرة على احترام تلك الاحتياطات عند تنفيذ العمليات العسكرية.[١٥] وفي حال جرى تطوير الأنظمة التقنية بشكل يمكّنها من تجاوز الأداء البشري في الامتثال لقواعد القانون الدولي الإنساني، من خلال قدرتها على تحليل المعلومات واستشعار الحاجة إلى وقف الهجوم عند ظهور مؤشرات على مخالفته لتلك القواعد، فإن ذلك قد يمنحها تفوقًا نوعيًا على بعض الوسائل التقليدية، التي تفتقر إلى المرونة في اللحظات الحاسمة، كما هو الحال في الهجمات المدفعية أو الصاروخية التي لا يمكن العدول عنها بعد تنفيذها. ومع

---

[١٣] هناك سياسة في مجال الدفاع مفادها امتلاك دولة ما القوة العسكرية سوف يخيف عددًا محتملًا وتمنعه في الهجوم عليها وهذا المفهوم يُعد جوهريًا في سياسته الولايات المتحدة الأمريكية ولعل أهم وسيلة للروع هو مجرد الأسلحة النووية إلا أنها لم تستعمل منذ نهاية الحرب العالمية الثانية – محمد يسري هل يصبح السلاح النووي سببًا في تحقيق السلام موقع إلكتروني ٢٠١٨/٨/١ /http://raseefzz.com.

[١٤] تعرف الحروب على أنها: (مجموعة من العمليات الاجتماعية السلبية حيث تتسم بطابع الصراع التدميري العنيف حيث تستخدم القوة المسلحة كل وسائل لإلحاق الضرر والأذى بالطرف الآخر) – موقع إلكتروني ٢٠١٨/٨/٣ WWW.marefa.org.

[١٥] القانون الدولي الإنساني وفتوى محكمة العدل الدولية بشأن مشروعية التهديد بالأسلحة النووية أو استخدامها اللجنة الدولية للصليب الأحمر موقع إلكتروني ٢٠١٨/٨/١٠ -WWW.icrc.org.

ذلك، فإن مجرد توفر هذه القدرات المتقدمة لا ينبغي أن يُفهم على أنه مبرر كافٍ أو مسـوغ دائم لاستخدامها تحت ذريعة الضرورة العسكرية.

المبحث الثاني:

الانحرافات الاجرامية الالكترونية وموقف القانون الدولي

رغم أهمية ضبط السلوكيات المنحرفة في السياق الدولي، ولا سيما ما يتعلق باستخدام القوة أو تجاوز الأطر القانونية المنظمة لها، فإن التعامل مع هذه الظواهر لا ينبغي أن يتم وفق مقاربة جامدة أو متشددة. بل يتطلب الأمر إيجاد توازن دقيق بين مشروعية اللجوء إلى القوة في بعض الحالات، وبين تفادي الانزلاق إلى ممارسات مفرطة تتجاوز ما يتيحه القانون الدولي، لتصل إلى مستويات محظورة تمثل انتهاكًا صريحًا للمعايير القانونية والأخلاقية في العلاقات بين الدول[١٦].

ويُطرح هنا تساؤل جوهري يتعلق بفهم دلالة مصطلح "القوة"، وما إذا كان المقصود به ينحصر في استخدام الوسائل العسكرية التقليدية ضمن سياق عدوان أو هجوم مسلح تنفّذه دولة ما، سواء عبر قواتها النظامية أو من خلال مجموعات منظمة تعمل تحت إشرافها أو تحظى بدعم مباشر منها.[١٧] وهنالك من يرى أن تحديد "القوة" فقط بالقوة العسكرية ليس له أساس قانوني كافٍ، بل يجب أن يشمل أيضًا الضغوط الاقتصادية والسياسية، حيث يمكن لهذه الوسائل أن تفرض تأثيرًا كبيرًا يعادل تأثير القوة المسلحة في بعض الظروف[١٨].

في الواقع، فإن الاعتماد على المعيار الأول الذي يحدد القوة المسلحة بناءً على العنصر الحركي لا يتناسب مع العديد من صور استخدام القوة في الحروب، بغض النظر عن شرعية تلك الحروب، مثل الهجمات البيولوجية أو الجرثومية، وكذلك الهجمات السيبرانية التي تشكل محور بحثنا. ومن جهة أخرى، فإن التوسع في تطبيق المعيار الثاني قد يؤدي إلى اتساع مفهوم استخدام القوة وتهديدها ليشمل أشكالًا من الإكراه الاقتصادي والسياسي، مما قد يتعارض مع أهداف ميثاق الأمم المتحدة وفقًا لرأي معظم الفقهاء، حيث يفتح هذا التوسع المجال لتبرير العدوان ويمنح شرعية لاستخدام القوة المضادة تحت ستار الدفاع الشرعي.[١٩].

هناك من يعارض الاتجاهين السابقين في تفسير "القوة"، حيث يوسّع هذا الرأي المفهوم ليشمل ليس فقط كافة أشكال القوة المسلحة، بل أيضًا أي صور أخرى تتسبب في انتهاك أو تأثير واضح على الأمن القومي لدولة ما. [٢٠].

---

[١٦] المادة (٤٢) من ميثاق الأمم المتحدة.
[١٧] الفقرة (٤) من المادة (٢) من ميثاق الأمم المتحدة.
[١٨] علاء الدين حسين مكي خماس استخدام القوة في القانون الدولي المطابع العسكرية بغداد ١٩٨٢ ص ٦٧.
[١٩] المصدر السابق ص ٦٨.
[٢٠] المصدر السابق نفس الصفحة.

المطلب الأول: المواجهة القانونية الدولية للحروب السيبرانية

الفرع الأول: ضوابط استخدام القوة فى ظل الحرب السيبرانية

في ضوء ما تم استعراضه، تبرز عدة أطر تفسيرية مرتبطة بالحرب السيبرانية، لاسيما ما يتعلق بمفهوم القوة. فقد أصبح الفضاء الإلكتروني عنصرًا محوريًا في تعزيز القوة واستثمار عناصرها الأساسية ضمن العلاقات الدولية، حيث بات التفوق في هذا المجال أحد العوامل الحاسمة لتنفيذ العمليات العسكرية المؤثرة على الأرض والبحر والجو والفضاء الخارجي. وتعتمد القدرة القتالية في الفضاء الإلكتروني على أنظمة التحكم والسيطرة التكنولوجية، مما يقتضي إعادة تعريف مفهوم القوة، بحيث يمكن تحديدها على أنها: "مجموعة من الوسائل والموارد المادية وغير المادية، المرئية وغير المرئية، التي تمتلكها الدولة، والتي يستخدمها صانع القرار لتنفيذ أفعال تؤثر في مصالح الدولة وسلوك الكيانات السياسية الأخرى[٢١].

تتألف عناصر القوة في العلاقات الدولية من توازن بين القدرات التكنولوجية والسكانية والاقتصادية والصناعية والقوة العسكرية وإرادة الدولة. هذه العناصر تعزز قدرة الدولة على ممارسة الإكراه أو الإقناع أو التأثير السياسي على الدول الأخرى لتحقيق أهدافها، سواء كانت مشروعة أو غير مشروعة. مع تطور مفهوم القوة، تغيرت طبيعة الحرب من الحروب التقليدية إلى حروب تستهدف سباق التقدم التكنولوجي وسرقة الأسرار الاقتصادية والعلمية والتحكم بالمعلومات، مما يؤثر بشكل كبير على الاقتصاد والبنية التحتية دون الحاجة إلى استخدام الأسلحة التقليدية. هذا التطور يؤكد على أهمية التكامل بين القوة الصلبة والناعمة في تحقيق الأهداف الدولية.

يتضح مما تم عرضه سابقًا أن مفهوم القوة في سياق الحرب السيبرانية يكتسب معاني جديدة تختلف عن تلك التي حددها واضعو ميثاق الأمم المتحدة للمفهوم التقليدي للقوة [٢٢] يمكن فهم الاستخدام غير المشروع للقوة في سياق الحرب السيبرانية على أنه يتضمن انتهاكًا للأمن القومي لدولة أخرى، ويعد ذلك بمثابة تطبيق فعلي لمفهوم القوة. في هذا الإطار، يمكن أن تشمل الحروب السيبرانية مختلف مستويات الصراع التي قد تشكل تهديدًا غير قانوني للقوة. الفضاء الإلكتروني يُستخدم أحيانًا كأداة لصراعات منخفضة الشدة، تركز على التأثير في مجالات اقتصادية، ثقافية، أو اجتماعية، دون أن يتحول إلى صراع مسلح أو حرب إلكترونية شاملة. قد تتجسد هذه

[٢١] سراب أحمد ثامر الهجمات على شبكات الحاسوب في القانون الدولي الإنساني أطروحة دكتوراه جامعة النهرين – كلية الحقوق بغداد ٢٠١٥ ص ١٠٧.

[٢٢] جوزيف ناي المنازعة الدولية – مقدمة للنظرية والتاريخ ترجمة احمد أمين الجمل ومجدي كامل الجمعية المصرية لنشر المعرفة والثقافة العالمية القاهرة ١٩٩٧ ص ٨٢.

الصراعات من خلال أساليب متنوعة مثل الحرب النفسية، الاختراقات الإلكترونية، التجسس، وسرقة البيانات، بالإضافة إلى حرب الأفكار. على سبيل المثال، تعرضت روسيا للاتهام بالتورط في القرصنة الإلكترونية خلال الانتخابات الأمريكية، حيث كان يُزعم أنها دعمت المرشح الجمهوري دونالد ترامب ضد منافسته الديمقراطية هيلاري كلينتون.[٢٣].

تتمثل إحدى أساليب الحروب السيبرانية في تحويل الفضاء الإلكتروني إلى ساحة موازية أو مكملة للصراعات التقليدية على الأرض. ومن الأمثلة على ذلك الهجوم السيبراني الذي شنته إسرائيل في ٦ ديسمبر ٢٠٠٧ على الدفاعات الجوية السورية في موقع يُعتقد أنه منشأة نووية في دير الزور، مما أدى إلى تعطيل هذه الدفاعات وتمكين الطائرات الإسرائيلية من استهداف الموقع دون الكشف عن الهجوم.[٢٤].

النمط الثالث من الحروب السيبرانية يظهر في الصراعات الإلكترونية التي تحدث بشكل مستقل. ورغم أن تأثيرات هذه الحروب قد لا تكون مدمرّة على غرار الهجمات التقليدية، حيث تقتصر بعض الهجمات على تعطيل العمليات العسكرية أو التأثير على البنية التحتية المدنية، إلا أن هناك أمثلة بارزة على ذلك، مثل الهجوم الذي تعرضت له إستونيا في عام ٢٠٠٧. الهجوم الذي شنته روسيا عبر إغراق المواقع الإلكترونية بحجم ضخم من البيانات غير الضرورية، استهدف العديد من المواقع الحكومية والمؤسسات الحيوية مثل الصحف، الجامعات، المستشفيات، المصارف، وخدمات الطوارئ، بهدف تعطيل الحكومة الإستونية.

هذا النوع من الهجمات يثير إشكالية في تحديد ما إذا كان يمكن تصنيفه كاستخدام للقوة، وبالتالي مدى مشروعيته. هذه القضية تفتح النقاش حول تطبيق المبادئ القانونية للأمم المتحدة التي تمنع استخدام القوة أو التهديد بها في العلاقات الدولية، باستثناء حالات الدفاع الشرعي أو القرارات الصادرة عن مجلس الأمن بموجب الفصل السابع من الميثاق. تصبح المشكلة أكثر تعقيدًا عندما نتعامل مع الهجمات السيبرانية التي قد لا تقتصر على الأبعاد العسكرية بل قد تشمل أبعادًا اقتصادية أو ثقافية، مما يجعل تصنيفها كعمل عدواني مسلح أمرًا غير واضح.

في هذا السياق، سنركز على الهجمات السيبرانية ضمن النزاعات المسلحة، وهي النزاعات التي تستدعي استخدام القوة من قبل الأطراف المعنية، سواء كانت نزاعات دولية أو غير دولية. من

---

[٢٣] الفقرة (٤) من المادة (٢) من ميثاق الأمم المتحدة.

[٢٤] إفادات وكالة الاستخبارات الأمريكية بتدخل روسيا في الانتخابات الرئاسية الأمريكية لدعم (دونالد ترامب) وأن روسيا وراء الهجمات الإلكترونية والقرصنة المعلوماتية التي طالت حسابات البريد الإلكتروني لمرشحة الحزب الديمقراطي (هيلاري كلينتون) – ٢٠١٨/٨/١٠ موقع إلكتروني/ WWW.SaSapost.com.

هنا، يصبح من الضروري فهم مدى تطبيق قواعد القانون الدولي الإنساني في هذه الحالات، وما إذا كانت العمليات السيبرانية تتماشى مع المعايير القانونية المتعلقة بالنزاعات المسلحة.

الفرع الثاني: شمولية مبادئ وقواعد القانون الدولي الإنساني

يتصل دور القانون الدولي الإنساني بالحروب، حيث نشأ هذا القانون نتيجة للتطور المستمر لأساليب القتال ووسائله. مع تقدم التكنولوجيا، تظهر تحديات جديدة في تطبيق هذا القانون، خصوصًا فيما يتعلق بتكييفه مع الهجمات السيبرانية كأحد أشكال الحروب الحديثة. لم تُدرج هذه الهجمات ضمن الاتفاقيات القديمة مثل اتفاقيات لاهاي أو اتفاقيات جنيف، مما يثير تساؤلات حول كيفية تطبيق القواعد القائمة على هذه الظاهرة الجديدة.

ومع تزايد استخدام الفضاء الإلكتروني من قبل الدول في النزاعات المسلحة، يواجه القانون الدولي الإنساني اختبارًا حقيقيًا. ذلك أن القواعد التي تم تقنينها قبل ظهور الهجمات السيبرانية لم تأخذ في اعتبارها هذا النوع من الصراع، مما يخلق فراغًا قانونيًا يتطلب بحثًا معمقًا في مدى صلاحية تطبيق القواعد الحالية عليه. في هذا السياق، توضح المادة ٣٦ من البروتوكول الإضافي الأول لاتفاقيات جنيف ضرورة فحص مشروعية استخدام أي سلاح أو أسلوب حرب جديد لضمان توافقه مع القوانين الدولية.

تُتيح المادة ٣٦ من البروتوكول الإضافي الأول للدول تطوير واستخدام أسلحة حديثة أو أساليب قتال جديدة غير مغطاة في القانون الدولي الإنساني، لكنها تشترط أن تتم مراجعتها قانونيًا قبل استعمالها لضمان توافقها مع القواعد الدولية. هذه المادة لا تمنع الدول من اقتناء أو تطوير وسائل جديدة، بل تفرض التحقق من مطابقتها للقانون الدولي، مما يعكس التزام الدول بالقواعد العرفية التي تنظم العمليات العدائية بنية حسنة.

ومن جهة أخرى، يعتبر شرط مارتنز آلية فعّالة لمواجهة التغيرات التكنولوجية في أساليب القتال، حيث تم تضمينه لأول مرة في اتفاقية لاهاي الثانية عام ١٨٩٩. ينص على أنه عندما لا تكون هناك معاهدة أو قاعدة عرفية تنطبق، يجب حماية المدنيين والعسكريين استنادًا إلى المبادئ الإنسانية والضمير العام. استنادًا لهذا المبدأ، يمكن تحريّم الأسلحة التي تتعارض مع المبادئ الإنسانية الأساسية.

يضع القانون الدولي الإنساني مجموعة من القواعد التي تهدف إلى تقليل تأثيرات النزاعات المسلحة، سواء كانت دولية أو غير دولية، من خلال تنظيم وسائل وأساليب القتال. هذه القواعد لا تمنع القتال، بل تحدد الأطر التي يجب أن يتم فيها لتقليل الأضرار. ويعترف القانون الدولي بضرورة وجود مستوى معين من العنف والخسائر أثناء الأعمال العدائية، مع توفير حلول لسد

الثغرات القانونية في الحالات غير المتوقعة. تُؤكد المبادئ الأساسية للقانون على التمييز بين الأهداف العسكرية والمدنية، والتناسب في استخدام القوة، وأهمية اتخاذ الاحتياطات لتقليل الأضرار.[٢٥]

يتطلب مبدأ التمييز، وفقًا للمادة ٤٨ من البروتوكول الإضافي الأول لعام ١٩٧٧، أن تميز أطراف النزاع بين المدنيين والأعيان المدنية من جهة، والمقاتلين والأهداف العسكرية من جهة أخرى في جميع الأوقات. كما تنص المادة ٥١ على حظر استهداف السكان المدنيين أو استخدام العنف أو التهديد به لإثارة الذعر بينهم. إضافة إلى ذلك، تنص المادة ٥٢ على عدم جواز الهجوم على الأعيان المدنية أو استخدامها في أعمال الردع العسكرية. كما تحظر المادة ٥٥ استخدام أساليب قتال تتسبب في أضرار كبيرة وطويلة الأمد للبيئة الطبيعية، مما يعرض صحة السكان أو استدامتهم للخطر. وتوفر المادة ٥٦ حماية للمرافق والمنشآت التي تحتوي على مخاطر خطيرة.

هذه المبادئ، التي تُكرّس حماية المدنيين والأعيان المدنية، تجد تطبيقًا واسعًا في القانون الدولي الإنساني والقانون الدولي العرفي، وتعمل على توجيه قواعد الهجوم بما يتماشى مع مبدأي الضرورة والتناسب. أكدت محكمة العدل الدولية في رأي استشاري عام ١٩٦٦ أن القانون الدولي الإنساني يقوم على مبدأين أساسيين: الأول يحظر جعل المدنيين أهدافًا للهجوم، والثاني يحرّم استخدام الأسلحة التي تسبّب آلامًا غير مبررة. هذه المبادئ تظل قابلة للتطبيق في مختلف أشكال الحروب، بما فيها الهجمات السيبرانية.[٢٦].

الفضاء السيبراني يشترك فيه العسكريون والمدنيون على حد سواء، مما يطرح تحديات كبيرة في ضمان استهداف الهجمات السيبرانية للأهداف العسكرية فقط، مع الحفاظ على حماية المدنيين والأعيان المدنية المحمية بموجب القانون الدولي الإنساني. نظرًا للطبيعة المترابطة للنظم الحاسوبية في الفضاء السيبراني، تتداخل الأنظمة العسكرية مع المدنية، مما يجعل من الصعب تنفيذ هجوم سيبراني يقتصر تأثيره على هدف عسكري دون التأثير على البنية المدنية.

الهجمات السيبرانية تتمتع بقدرة دقيقة على استهداف الأهداف العسكرية، ولكن التداخل بين النظم قد يؤدي إلى آثار جانبية غير مقصودة. في بعض الحالات، من المستحيل استهداف البنية العسكرية دون التأثير على البنية المدنية، خاصة إذا كانت البنية تحتية تستخدم لأغراض مزدوجة، مما يعقد تطبيق مبدأ التناسب. في هذه الحالات، تصبح الأعيان المدنية التي تُستخدم في

---

[٢٥] أحمد عبيس الفتلاوي، الهجمات السيبرانية: مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر، مجلة المحقق الحلي للعلوم القانونية والسياسية، جامعة بابل – كلية القانون العدد الرابع، السنة الثامنة، ٢٠١٦، ص ٥١

[٢٦] المادة (٣٦) من البروتوكول الإضافي الأول الملحق باتفاقيات جنيف لسنة ١٩٧٧.

الأغراض العسكرية أهدافًا مشروعة بموجب القانون الدولي، وبالتالي تفقد الحماية التي يمنحها القانون الدولي الإنساني.[٢٧]

تتمثل الإشكالية في أن العديد من البنى التحتية الإلكترونية المستخدمة حاليًا لها طبيعة مزدوجة، حيث يُتوقع أن تستمر هذه الظاهرة في المستقبل. على سبيل المثال، يمكن أن تتقاسم شبكات الاتصالات العسكرية جزءًا من الكابلات مع البنية التحتية المدنية. كما تعتمد الأسلحة الحديثة على بيانات نظام تحديد المواقع العالمي (GPS)، الذي يُستخدم أيضًا في التطبيقات المدنية مثل الملاحة. إضافة إلى ذلك، أصبحت منصات التواصل الاجتماعي مثل فيسبوك وتويتر أدوات رئيسية لنقل معلومات عسكرية في النزاعات الحديثة. علاوة على ذلك، تتزايد الجيوش في الاعتماد على الأنظمة التجارية الجاهزة مثل الحواسيب التجارية، ما يجعل الشركات المصنعة لهذه المعدات هدفًا عسكريًا محتملًا.

المطلب الثاني: المسؤولية الدولية وقوانين الحرب:

الفرع الأول: إشكالية الحرب في ظل الفضاء السيبراني

وهنا يثور تساؤلًا هامًا: من يتحمل المسؤولية الجنائية عن الانتهاكات الجسيمة لقوانين الحرب؟ مع تقدم تكنولوجيا القتال، تظل المسؤولية القانونية تقع على عاتق البشر في النهاية، حيث يظل الإنسان هو من يوجه ويستخدم هذه الوسائل مهما تطورت. حتى مع تطور الذكاء الاصطناعي، سيظل الإنسان هو نقطة البداية في اتخاذ القرارات.

في الماضي، كانت الدولة هي المسؤولة الوحيدة عن الجرائم الدولية التي يرتكبها الأفراد باسمها، لكن مع تزايد فظاعة الجرائم المرتكبة ضد الإنسان وكرامته، أصبح من الممكن تحميل الأفراد، بصفتهم أشخاصًا طبيعيين، المسؤولية الجنائية الدولية عن أعمالهم. وقد أسفرت هذه التطورات القانونية عن تأسيس المحكمة الجنائية الدولية في أواخر القرن الماضي للنظر في الجرائم التي يرتكبها الأفراد.

الحديث عن المسؤولية الجنائية يشمل القادة العسكريين والرؤساء الذين يتحملون المسؤولية عن الانتهاكات التي تتمثل في مخالفات لقوانين الحرب واتفاقيات جنيف، مثل المجازر وجرائم الحرب التي ارتكبتها قوات الاحتلال في فلسطين في الأحداث الأخيرة في ٧ أكتوبر ٢٠٢٣، وما

[٢٧] مايكل شميدت، الحرب بواسطة شبكات الاتصال: الهجوم على شبكات الكمبيوتر والقانون في الحرب، المجلة الدولية للصليب الأحمر، ٢٠٠٢، ص١٢٠

تعرض لـه سـكـان شـمال غزة من تهديدات الموت ودمار واسـع يتعارض مع مبادئ القانون الدولي.[٢٨]

تتمثل إشكالية خصوصية الهجمات السيبرانية في تأثيراتها والأهداف التي تستهدفها، والتي تتصل بالبنية التحتية للدول؛ حيث تعد البنية التحتية عنصرًا حيويًا لضمان تطور المجتمع الحديث، وتعد جزءًا أساسيًا من الأمن القومي للدول نظرًا لتأثيرها المباشر على حياة الأفراد. ومن هنا تبرز أهمية حماية هذه البنية من التهديدات المتنوعة، وعلى رأسها الهجمات السيبرانية. سنتناول في هذا السياق تعريف الهجمات السيبرانية ونسلط الضوء على أبرز أشكالها المستهدفة لهذه البنية.

البنية التحتية الحرجة تتضمن الأهداف الاستراتيجية والمرافق الحيوية التي تعد أساسية لاستمرار عمل الدولة. استهداف هذه البنية يؤدي إلى تعطيل أنشطة الدولة وقدرتها على أداء وظائفها الأساسية في العديد من المجالات. وهي تشمل الخدمات الأساسية التي يتسبب تعطيلها أو تدميرها في أضرار كبيرة للصحة العامة، السلامة، التجارة، والأمن القومي، بل قد تؤثر على هذه المجالات جميعها في وقت واحد. من هذه القطاعات المهمة: الاتصالات، الطاقة، النظام المصرفي، النقل، الصحة العامة، الزراعة، الغذاء، المياه، المواد الكيميائية، الملاحة البحرية، والخدمات الحكومية الحيوية. [٢٩].

تشمل البنية التحتية الحرجة عناصر مادية مثل المنشآت والمرافق، إلى جانب عناصر افتراضية تتضمن الأنظمة والبيانات. تتفاوت أهمية هذه البنية الحيوية من دولة لأخرى

الفرع الثاني: صور الهجمات السيبرانية ضد البنى التحتية الحرجة:

تشير تقارير الوكالات الدولية المتخصصة إلى زيادة الهجمات السيبرانية التي استهدفت أنظمة حيوية مثل الطاقة، الاتصالات، النقل، الأنظمة المالية، والقطاع الكيميائي الحيوي، وخصوصًا الرعاية الصحية خلال جائحة كوفيد-١٩. شملت هذه الهجمات أيضًا الهيئات الحساسة التي تعتمد على الفضاء السيبراني لتخزين البيانات والمعلومات المتعلقة ببنيتها التحتية. وقد تسببت هذه الهجمات في أضرار مادية جسيمة، مما أدى إلى خسائر كبيرة في الأرواح والمال تتجاوز تلك الناتجة عن الاستهداف العسكري المباشر، خاصة في مناطق النزاعات المسلحة.

---

[٢٨] اللجنة الدولية للصليب الأحمر، الحرب السيبرانية: القانون الدولي الإنساني يوفر طبقة إضافية من الحماية، ١٠ أيلول ٢٠١٩، ص ٥٩

[٢٩] الاتحاد الدولي للاتصالات التقرير النهائي المسألة ٢٢/١ تأمين شبكات المعلومات والاتصالات: أفضل الممارسات من أجل بناء ثقافة الأمن السيبراني الدراسة الرابعة ٢٠٠٦- ٢٠١٠ متاح على الرابط التالي: https://www.itu.int/dms-pub/itu-d/opb/stg/D-STG-SG01.22-2010-MSW-A.DOCX تاريخ الزيارة ٨ أكتوبر ٢٠٢١ على الساعة 15:45.

١) الهجمات السيبرانية على قطاع الرعاية الصحية:

تعاني البنى التحتية الصحية في جميع أنحاء العالم، سواء في فترات السلم أو النزاعات المسلحة، من تهديدات الهجمات السيبرانية، خاصة خلال فترات الأوبئة مثل كوفيد-١٩. هذه الهجمات تستهدف تعطيل أنظمة الكمبيوتر، وسلاسل التوريد الطبية، والأجهزة الطبية، مما يهدد بتوقف تقديم الرعاية الصحية ويشكل خطرًا كبيرًا على حياة المرضى والطواقم الطبية. كما تعطل هذه الهجمات توزيع المستلزمات الأساسية وتساهم في انتشار المعلومات المضللة.

تستهدف الهجمات السيبرانية شبكات الرعاية الصحية الأولية والطوارئ بهدف الابتزاز المالي. على سبيل المثال، في أعقاب هجوم "وانا كراي" في مايو ٢٠١٧، الذي استهدف قطاع الصحة في المملكة المتحدة، تكبدت الخدمات الصحية خسائر تقدر بنحو ٩٢ مليون جنيه إسترليني، نتيجة تعطيل الخدمات وتكاليف تكنولوجيا المعلومات. الهجوم، الذي نفذته مجموعة قراصنة من كوريا الشمالية، أثر على ٨٠ مؤسسة صحية وأدى إلى إلغاء حوالي ١٩,٠٠٠ موعد طبي خلال أسبوع. في ألمانيا، أسفرت أول حالة وفاة جراء هجوم سيبراني في مستشفى بمدينة دوسلدورف عن وفاة امرأة بعد أن تم نقلها إلى مستشفى آخر بسبب تعطل النظام في المستشفى الأصلي [٣٠].

٢) الهجمات السيبرانية على قطاع التجارة الإلكترونية والمؤسسات المالية:

تعد التجارة الإلكترونية والقطاع المالي جزءًا أساسيًا من البنية التحتية الحيوية للدولة، نظرًا لما يحتويه من بيانات حساسة وحرجة. ومن هنا، فإنها تواجه تهديدًا حقيقيًا نتيجة للاستخدام الضار للتكنولوجيا، مما قد يؤدي إلى تعطيل الخدمات المقدمة، وتقويض الثقة والأمن، ويعرض الاستقرار المالي على المستويين العالمي والقومي للخطر. وتشير تقارير البنك الدولي المتعلقة بالتسويق إلى أن القطاع المالي يشهد ثاني أكبر عدد من الهجمات السيبرانية، بعد القطاع الصحي [٣١].

أفاد صندوق النقد الدولي، استنادًا إلى دراسات البنك الدولي التي أُعدت في ٢٠١٨، أن الهجمات السيبرانية على القطاع المالي في ٥٠ دولة تسببت في خسائر تقدر بنحو ٩% من صافي دخل البنوك على مستوى العالم. [٣٢].

---

[٣٠] شارلوت ميتشل امرأة أول وفاة بسبب هجوم إلكتروني على الرعاية الصحية بعد أن أُجبرت مستشفى ألمانية على إبعادها عندما قام المتسللون بإلغاء تنشيط أجهزة الكمبيوتر الخاصة بهم صحيفة الدايلي ميل البريطانية ١٨ سبتمبر ٢٠٢٠ متاح على الرابط التالي:
https://www.dailymail.co.uk/ تاريخ الزيارة ٩ أكتوبر ٢٠٢١ على الساعة 32:20.

[٣١] تيم مورر أرثر نيلسون التهديد السيبراني العالمي تقرير التمويل والتنمية صندوق النقد الدولي مارس ٢٠٢١ ص٢٥.

[٣٢] محمد إسماعيل الأمن السيبراني في القطاع المصرفي صندوق النقد العربي موجز سياسات ع الرابع جوان س ٢٠١٩ ص١.

في فبراير ٢٠١٦، تعرض بنك بنغلاديش المركزي لهجوم سيبراني كبير، المعروف بعملية "لازاروس"، حيث تم استهداف محاولة لسرقة مليار دولار. تم توجيه الاتهام إلى كوريا الشمالية كمسؤولة عن الهجوم، الذي شكل تحذيرًا جدياً للقطاع المالي بضرورة اتخاذ الحيطة تجاه الهجمات السيبرانية التي تشكل تهديدًا حقيقيًا لاستقرار النظام المالي، مما قد يؤدي إلى أزمات مالية وفقدان الثقة العامة إذا لم تتم معالجتها بشكل فعال. (٣٣).

٣) الهجمات السيبرانية على محطات الطاقة النووية والكهرباء والمياه والمنشئات الخطرة:

يتعرض هذا القطاع بشكل مستمر للهجمات السيبرانية، سواء كانت المحطات مخصصة للأغراض السلمية أو العسكرية، مما يهدد حياة المدنيين والبيئة المحيطة. على سبيل المثال، في عام ٢٠٠٣، تعرض مفاعل "ديفيد بيس" في أوهايو، الذي يُستخدم لتوليد الطاقة، لعملية اختراق استهدفت أنظمة التحكم الإلكترونية، مما كان من شأنه أن يتسبب في انفجار كارثي. إلا أن أنظمة الأمان المتطورة في المفاعل قامت بتفعيل آلية الإطفاء التلقائي، مما حال دون وقوع كارثة كبيرة، وفقًا لتأكيدات المسؤولين الأمريكيين. (٣٤).

يعد هذا القطاع عرضة بشكل دائم للهجمات السيبرانية، سواء كانت المنشآت موجهة للاستخدام المدني أو العسكري، ما يهدد حياة المواطنين والبيئة المحيطة. على سبيل المثال، في ٢٠٠٣، استهدف هجوم سيبراني مفاعل "ديفيد بيس" في أوهايو، الذي يستخدم في توليد الكهرباء، حيث اخترق أنظمة التحكم في المفاعل مما كان قد يؤدي إلى كارثة انفجارية. ومع ذلك، تمكنت أنظمة الأمان من تفعيل عملية الإطفاء التلقائي، وهو ما حال دون وقوع أي أضرار جسيمة، حسبما أشار المسؤولون الأمريكيون.

أفادت شركة "مايكروسوفت" بتاريخ ٦ يناير ٢٠٢٠ بأنها نجحت في تعطيل عدد من النطاقات الإلكترونية التي استُخدمت من قِبل مجموعة تسلل إلكتروني تُعرف باسم "ثاليوم"، والمتهمة بشن هجمات استهدفت الحصول على معلومات مرتبطة بمرافق نووية. وتشير التقديرات إلى أن المجموعة تعمل من داخل كوريا الشمالية، حيث وجّهت أنشطتها نحو موظفين في إدارات حكومية، مراكز أبحاث، أكاديميين، وأشخاص معنيين بقضايا تتعلق بمنع انتشار الأسلحة النووية، وكان معظم ضحايا الهجمات من الولايات المتحدة، اليابان، وكوريا الجنوبية.

---

(٣٣) تيم مورر أرثر نيلسون التهديد السيبراني العالمي المرجع نفسه ص٢٤.

(٣٤) أحمد عبيس نعمة الفتلاوي الهجمات السيبرانية مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر المرجع السابق ص ٦٢٥.

٤) الهجمات السيبرانية على قطاع الاتصالات وحركة الملاحة البرية والبحرية والجوية:

يتعرض قطاع الاتصالات ووسائل النقل البرية والبحرية والجوية لهجمات سيبرانية متكررة تهدف إلى تعطيل أنظمة الرصد والمراقبة، واختراق شبكات التحكم الخاصة بمسارات الملاحة، ما قد يؤدي إلى خلل في برمجيات الإقلاع والهبوط للطائرات ويزيد من احتمالات وقوع حوادث تصادم. كما تشمل هذه الهجمات اختراق شبكات الهاتف وتعطيل مراكز توزيع الخدمة أو شبكات الهواتف المحمولة، مما يؤدي إلى توقف التواصل بين الأفراد. كذلك، تُستهدف الحسابات الشخصية للمستخدمين على منصات التواصل الاجتماعي مثل فيسبوك، إنستغرام، وواتساب، ما يُشكل تهديدًا لخصوصية المستخدمين وأمنهم الرقمي. [٣٥] .

يتزايد مستوى التهديد خلال فترات النزاعات المسلحة، حيث تُستهدف شبكات النقل والمواصلات بهدف تهيئة البيئة لهجوم ميداني، كما حدث قبيل التصعيد الروسي الأوكراني في عام ٢٠١٥. وفي بعض الحالات، تأتي الهجمات السيبرانية بالتوازي مع العمليات العسكرية كجزء من استراتيجية الحرب، كما ظهر جليًا في الهجوم على إستونيا في مايو ٢٠٠٧، حين تعطلت مؤسسات الدولة بشكل شبه كامل، بما في ذلك المواقع الإلكترونية لرئاسة الوزراء والبرلمان.

عند مراجعة الإطار القانوني الدولي الحالي، يتضح غياب نصوص صريحة ومباشرة تنظم حماية البنية التحتية الحرجة من الهجمات السيبرانية أو تصنّف طبيعة هذه الاعتداءات بشكل واضح. إلا أن هذا الغياب لا يعني أن القانون الدولي يخلو تمامًا من الأحكام التي يمكن أن تنطبق على هذا النوع من الهجمات، بل توجد مبادئ وأعراف يمكن البناء عليها قانونيًا لمعالجة هذه الظاهرة [٣٦] تم التوصل إلى إجماع واسع حول تطبيق أحكام القانون الدولي التقليدي على الفضاء السيبراني، مما يزيل أي شكوك حول وجود نقص قانوني في هذا المجال. هذا التوجه يؤكد أن الأنشطة السيبرانية، رغم تطورها التقني، تخضع للأطر القانونية الدولية المعمول بها.

يفرض القانون الدولي لحقوق الإنسان على الدول التزامات ملزمة في حالات السلم والحرب، تركز على احترام الحقوق الأساسية للإنسان، حيث تُعد هذه الحقوق قواعد آمرة لا يمكن التنازل

---

[٣٥] أميرة عبد العظيم محمد عبد الجواد المخاطر السيبرانية وسبل مواجهتها في القانون الدولي العام مجلة القانون والشريعة ع٣٥ الجزء ٣ س ٢٠٢٠ ص ٤٣٣.

[٣٦] كوردولا دروغيه ما من فراغ قانوني في الفضاء السيبراني اللجنة الدولية للصليب الأحمر ١٦ أوت ٢٠١١ متاح على الرابط التالي: https://www.icrc.org تاريخ الزيارة ١٥ أكتوبر ٢٠٢١ على الساعة 12:37.

عنها أو انتهاكها [٣٧] أبرز هذه الحقوق هو الحق في الحياة. [٣٨]تتضمن حقوق الإنسان الأساسية الحق في الصحة، المياه، الغذاء، والبيئة السليمة، فضلاً عن حماية الحق في التنقل، الخصوصية، والملكية الفكرية، وهي حقوق معترف بها بموجب الإعلان العالمي لحقوق الإنسان والعهدين الدوليين للحقوق السياسية والمدنية، والاقتصادية والاجتماعية والثقافية لعام ١٩٦٦، إضافة إلى الآليات الدولية ذات الصلة. وعليه، فإن استهداف المنشآت الحيوية مثل المستشفيات، محطات توليد الطاقة، المياه، الكهرباء، المصارف، الجامعات، ووسائل النقل، يعتبر انتهاكًا لهذه الحقوق. وفقًا لنص المادة ٥ من العهد الدولي للحقوق الاقتصادية والاجتماعية والثقافية، فإن أي نشاط يهدف إلى إهدار هذه الحقوق يُعد غير مشروع دوليًا، مما يترتب عليه مسؤولية دولية [٣٩].

بناءً على ما تم توضيحه، فإن الحماية القانونية للبنية التحتية الحرجة تستند إلى حماية الحقوق الأساسية التي تتعرض للتأثر نتيجة استهداف هذه البنى.

[٣٧] انظر المادة ٥٣ اتفاقية فينا لقانون المعاهدات ٢٣ ماي ١٩٦٩ ٢٧ جانفي ١٩٨٠.

[٣٨] المادة ٣ من الإعلان العالمي لحقوق الإنسان ١٠ ديسمبر ١٩٤٨ المادة ٦ من العهد الدولي الخاص بالحقوق السياسية والمدنية ١٦ ديسمبر ١٩٦٦.

[٣٩] انظر المواد ١ ٢ ٣ مشروع لجنة القانون الدولي بشأن مسؤولية الدول عن الفعل الضار غير المشروع دوليًا الجمعية العامة للأمم المتحدة الوثيقة رقم: A/RES/56/83 ٢٨ جانفي ٢٠٠٢ ص ٢.

الخاتمة

الحمد لله الذي وفّقني لإتمام هذا البحث، وما كان لي أن أبلغ غايته لولا عون الله وتوفيقه. تناول هذا البحث موضوع "الحدود الخاصة بالاستخدام للفضاء الالكتروني في ضوء موقف القانون الدولي"، وهو من الموضوعات البالغة الأهمية في ظل التطورات التقنية المتسارعة وتزايد الاعتماد على الفضاء في مختلف جوانب الحياة.

بدأت الدراسة بتحديد المفاهيم الأساسية المتعلقة بالتكنولوجيا عمومًا، وتكنولوجيا الفضاء على وجه الخصوص، ثم انتقلت إلى استعراض أوجه الاستخدام الدولي لتلك التكنولوجيا، سواء في الأغراض المدنية أو العسكرية. كما تم تسليط الضوء على الجهود القانونية المبذولة على المستوى الدولي، ولا سيما من قبل الأمم المتحدة، لضمان الاستخدام السلمي والمنضبط لتكنولوجيا الفضاء الخارجي، من خلال الاتفاقيات الدولية، والمبادئ والقرارات الأممية، والهيئات المعنية بشؤون الفضاء. وفي نهاية البحث، تم التطرق إلى دور القانون الدولي الإنساني في الحد من مخاطر الاستخدامات العسكرية للتقنيات الفضائية.

وبعد هذا العرض والتحليل، أمكن التوصل إلى عدد من النتائج المهمة، من أبرزها:

أولاً: النتائج

١. تكنولوجيا الفضاء تُشير إلى أحدث ما توصل إليه العلم من أدوات وتقنيات يمكن تسخيرها في أنشطة الفضاء الخارجي.

٢. شهدت تكنولوجيا الفضاء تطورًا ملحوظًا في العقود الأخيرة، وامتدت تطبيقاتها إلى مجالات سلمية متعددة وكذلك إلى استخدامات عسكرية.

٣. تُستخدم هذه التكنولوجيا في تنفيذ العديد من الأهداف الإنمائية للأمم المتحدة، مما يؤكد حضورها في الخطط التنموية العالمية.

٤. يشمل الاستخدام غير السلمي لتكنولوجيا الفضاء مجالات متعددة، من أبرزها: تنفيذ الهجمات السيبرانية، وأنشطة التجسس الرقمي، وتوجيه الأسلحة الذكية عن بُعد، مما يزيد من تعقيد التهديدات الأمنية.

٥. ساهم التطور المتسارع لتكنولوجيا الفضاء في تعزيز أهمية ضبط استخدامها قانونيًا، نظرًا لتأثيرها المباشر – سواء في الأغراض السلمية أو العسكرية – على الأمن والاستقرار المدني على الأرض.

٦. بالنظر إلى توغل هذه التكنولوجيا في مختلف القطاعات الحيوية، فإن إساءة استخدامها لأغراض غير سلمية تمثل تحديًا إنسانيًا يستوجب تحركًا دوليًا جادًا لضمان الحماية القانونية الكافية.

ثانيًا: التوصيات

١. ضرورة تعزيز مساهمة تكنولوجيا الفضاء في تحقيق أهداف التنمية المستدامة ٢٠٣٠، من خلال تفعيل دور الدول الأعضاء في الأمم المتحدة وربط سياسات الفضاء بالأجندة التنموية العالمية.

٢. التأكيد على أهمية إدماج قواعد القانون الدولي الإنساني ضمن الإطار القانوني المنظم للاستخدامات العسكرية لتكنولوجيا الفضاء، مع توسيع نطاق الوعي بها من قبل الدول والمنظمات الدولية والمجتمع الأكاديمي.

٣. الدعوة إلى تطوير قواعد قانونية جديدة تُنظّم استخدام تكنولوجيا الفضاء خلال النزاعات المسلحة، بالاستناد إلى المبادئ الراسخة في القانون الدولي الإنساني، وبما يواكب التطورات التكنولوجية الراهنة.

المراجع

١. اتفاقية فينا لقانون المعاهدات ٢٣ ماي ١٩٦٩ ٢٧ جانفي ١٩٨٠.

٢. أحمد الأنور قواعد وسلوك القتال دراسات في القانون الدولي الإنساني دار المستقبل العربي القاهرة ٢٠٠٠

٣. أحمد عبيس الفتلاوي، الهجمات السيبرانية: مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر، مجلة المحقق الحلي للعلوم القانونية والسياسية، جامعة بابل – كلية القانون العدد الرابع، السنة الثامنة، ٢٠١٦،

٤. الإعلان العالمي لحقوق الإنسان ١٠ ديسمبر ١٩٤٨ المادة ٦ من العهد الدولي الخاص بالحقوق السياسية والمدنية ١٦ ديسمبر ١٩٦٦.

٥. أفضل الممارسات من أجل بناء ثقافة الأمن السيبراني الدراسة الرابعة ٢٠٠٦- ٢٠١٠ متاح على الرابط التالي: https://www.itu.int/dms-pub/itu-d/opb/stg/D-STG-SG01.22-2010-MSW-A.DOCX تاريخ الزيارة ٨ أكتوبر ٢٠٢١ على الساعة 15:45.

٦. البروتوكول الإضافي الأول الملحق باتفاقيات جنيف لسنة ١٩٧٧.

٧. تيم مورر أرثر نيلسون التهديد السيبراني العالمي تقرير التمويل والتنمية صندوق النقد الدولي مارس ٢٠٢١

٨. جوزيف ناي المنازعة الدولية – مقدمة للنظرية والتاريخ ترجمة احمد أمين الجمل ومجدي كامل الجمعية المصرية لنشر المعرفة والثقافة العالمية القاهرة ١٩٩٧

٩. سراب أحمد ثامر الهجمات على شبكات الحاسوب في القانون الدولي الإنساني أطروحة دكتوراه جامعة النهرين – كلية الحقوق بغداد ٢٠١٥

١٠. سلوان جابر هاشم حالة الضرورة العسكرية في القانون الدولية الإنساني ط ١ المؤسسة الحديثة للكتاب لبنان ٢٠١٣

١١. عبد العظيم محمد عبد الجواد المخاطر السيبرانية وسبل مواجهتها في القانون الدولي العام مجلة القانون والشريعة ع٣٥ الجزء ٣ س ٢٠٢٠

١٢. علاء الدين حسين مكي خماس استخدام القوة في القانون الدولي المطابع العسكرية بغداد ١٩٨٢

١٣. القانون الدولي الإنساني وفتوى محكمة العدل الدولية بشأن مشروعية التهديد بالأسلحة النووية أو استخدامها اللجنة الدولية للصليب الأحمر موقع إلكتروني ٢٠١٨/٨/١٠ -WWW.icrc.org.

١٤. كوردولا دروغيه ما من فراغ قانوني في الفضاء السيبراني اللجنة الدولية للصليب الأحمر ١٦ أوت ٢٠١١ متاح على الرابط التالي: https://www.icrc.org تاريخ الزيارة ١٥ أكتوبر ٢٠٢١ على الساعة 12:37.

١٥. اللجنة الدولية للصليب الأحمر، الحرب السيبرانية: القانون الدولي الإنساني يوفر طبقة إضافية من الحماية، ١٠ أيلول ٢٠١٩

١٦. مايكل شميدت، الحرب بواسطة شبكات الاتصال: الهجوم على شبكات الكمبيوتر والقانون في الحرب، المجلة الدولية للصليب الأحمر، ٢٠٠٢،

١٧.محمد إسماعيل الأمن السيبراني في القطاع المصرفي صندوق النقد العربي موجز سياسات ع الرابع جوان س ٢٠١٩

١٨.محمد يسري هل يصبح السلاح النووي سببًا في تحقيق السلام موقع إلكتروني ٢٠١/٨/١/ http://raseefzz.com.

١٩.مشروع لجنة القانون الدولي بشأن مسؤولية الدول عن الفعل الضار غير المشروع دوليًا الجمعية العامة للأمم المتحدة الوثيقة رقم: A/RES/56/83 ٢٨ جانفي ٢٠٠٢ ص ٢.

٢٠.النظام الأساسي للمحكمة الجنائية الدولية.

٢١.هشام بشري المدخل القانوني الدولي الإنساني ط ١ المركز القومي للإصدارات القومية القاهرة ٢٠١٢

٢٢.هنري ميروفيتز مبدأ الآلام التي لا مبرر لها دراسات في القانون الدولي الإنساني دار المستقبل العربي القاهرة ٢٠٠٩