تكييف الهجمات السيبرانية في ضوء أحكام القانون الدولي

دخلافي سفيان[1]،
[1] أستاذ محاضر قسم "أ"، جامعة تيزي وزو، الجزائر.
البريد الإلكتروني: dekhlafisofiane76@gmail.com

الملخص:

تتناول الدراسة موضوع الهجمات السيبرانية باعتباره موضوع جديد له ارتباطات بعدة فروع للقانون، كما أنه موضوع محل نقاش واختلاف بين الدول والباحثين من عدة جوانب، ولعل أبرزها المسؤولية الدولية عن هذه الهجمات التي تحدث في الفضاء الإلكتروني كمجال خامس لممارسة السيادة الوطنية إلى جانب المجالات الأربع الأخرى (البرية، البحرية، الجوية، الفضاء الخارجي)، فالفضاء الإلكتروني يقدم للأفراد وللدول وللمجتمع الدولي برمته خدمات كبيرة، ولكن بمقابل ذلك فقد أصبح هذا الفضاء يشكل ساحة جديدة للصراع الدولي، وعامل تهديد للأمن القومي للدول، وللسلم والأمن الدوليين، فقد تتسبب هذه الهجمات في نزاعات مسلحة داخلية أو دولية على أرض الواقع، أو قد تتحول إلى حرب سيبرانية شاملة تؤدي إلى أضرار جسيمة بالأشخاص والأعيان، وهو ما يطرح مسألة في غاية الأهمية تتعلق بالإطار القانوني الواجب التطبيق على هذه الهجمات الجديدة خاصة في ظل عدم وجود اتفاقية دولية خاصة حول الموضوع، وذلك من خلال البحث عن تكييفها وفقا للقانون الدولي العام والقانون الدولي الإنساني الساري المفعول.

الكلمات المفتاحية:

الهجمات السيبرانية، القانون الدولي العام، القانون الجنائي الدولي، القانون الدولي الإنساني.

تاريخ إرسال المقال: 2022/09/14، **تاريخ قبول المقال:** 2022/11/16، **تاريخ نشر المقال:** 2022/12/31.

لتهميش المقال: دخلافي سفيان، "تكييف الهجمات السيبرانية في ضوء أحكام القانون الدولي"، المجلة الأكاديمية للبحث القانوني، المجلد 13، العدد 02، السنة 2022، ص ص303-323.

المقال متوفر على الرابط التالي: https://www.asjp.cerist.dz/en/PresentationRevue/72

المؤلف المراسل: دخلافي سفيان؛ dekhlafisofiane76@gmail.com

Adaptation of cyberattacks in the light of international law

Summary:

The study addresses cyber-attacks as a new topic with linkages to several branches of law, as well as a topic of debate and divergence between States and researchers in several respects, perhaps most notably international responsibility for such attacks occurring in cyberspace as a fifth area for the exercise of national sovereignty along with the other four areas (Land, marine, air, outer space), cyberspace provides significant services to individuals, States and the international community as a whole But conversely, this space has become a new arena for international conflict, a threat to States' national security and to international peace and security, which may cause internal or international armed conflicts on the ground or may turn into an all-out cyber warfare that causes serious harm to persons and objects, This raises a very important issue concerning the legal framework applicable to these new attacks, especially in the absence of a special international convention on the subject by seeking to adapt them in accordance with general international law and applicable international humanitarian law.

Keywords:

Cyberattacks, public international law, international criminal law, international humanitarian law.

Adaptation des cybers attaques à la lumière du droit international

Résumé :

L'étude aborde les cyber attaques comme un nouveau sujet lié à plusieurs branches du droit, ainsi qu'un sujet de débat et de divergence entre les États et les chercheurs à plusieurs égards, peut-être plus particulièrement la responsabilité internationale de telles attaques survenant dans le cyberespace en tant que cinquième zone pour l'exercice de la souveraineté nationale avec les quatre autres zones (terre, mer, air, espace extra-atmosphérique), le cyberespace fournit des services importants aux individus, Mais inversement, cet espace est devenu une nouvelle arène pour les conflits internationaux, une menace pour la sécurité nationale des États et pour la paix et la sécurité internationales, qui peut provoquer des conflits armés internes ou internationaux sur le terrain ou qui peut se transformer en une cyber guerre totale causant de graves dommages aux personnes et aux objets, ce qui soulève une question très importante concernant le cadre juridique applicable à ces nouvelles attaques, en particulier en l'absence d'une convention internationale spéciale sur le sujet en cherchant à les adapter conformément au droit international général et au droit international humanitaire applicable.

Mots-clés :

Cyber attaques, droit international public, droit pénal international, droit international humanitaire.

مقدمة

تعتمد مجتمعات اليوم بشكل متزايد على الفضاء الإلكتروني في مختلف المجالات[1]، كما تعتمد عليه الدول في ممارسة سيادتها داخليا وخارجيا، فكل الهيئات والمؤسسات الحكومية تستخدم هذا الفضاء لتنفيذ مهامها الداخلية وإدارة علاقاتها الدولية، مما جعل العلاقات الخاصة والعامة أكثر ارتباطا وتأثرا به، حيث أثرت التكنولوجيا الرقمية على حياة الأفراد والدول معا، بل أصبح تطور أي دولة–إن لم نقل وجودها– واستمرارها رهن الفضاء الإلكتروني.

مع سيطرة الفضاء الإلكتروني على تفاصيل إدارة وتسيير شؤون الدولة العسكرية منها والمدنية ظهر خطر محدق جديد يتمثل في إمكانية لجوء الدول في مواجهة بعضها البعض إلى استهداف المرافق الحيوية والبنى التحتية وإحداث أضرار بشرية أو مادية جسيمة للعدو انطلاقا من الفضاء السيبراني دون حاجة إلى اللجوء إلى وسائل الحرب التقليدية، فأبرز ما يميز هذا الفضاء هو أنه غير محسوس وغير حركي، حيث أن استخدامه في العلاقات الدولية كأسلوب إخضاع يتميز بالسرعة، وقلة التكلفة، ولا يتطلب قوات ومعدات عسكرية سواء أكانت برية أو بحرية أو جوية.

ساهمت خصائص الفضاء الإلكتروني في انتشار الهجمات السيبرانية[2] سواء وقت السلم أو أثناء الحرب، والتي أصبحت تشكل تهديدا متصاعدا لسيادة الدول ولمصالحها الحيوية، وقد تتعدى آثارها إلى تهديد للسلم

---

[1] حول تعريف الفضاء السيبراني، انظر:
Canada, Ministère des travaux publics et des services gouvernementaux, La banque de données terminologiques et linguistiques du gouvernement du canada, Terminus plus, 2014 sub verbo « cyberspace », en ligne : www.btb.termiumplus.gc.ca/tpv2alpha/alpha-fra.html?_lang=_fra&i=1&index=alt&__inex=alt&srchtxCYBERESPACE&comencsrch.x=7&comencsrch.y=4[Termium Plus] (« [m]onde numérique construit par des ordinateurs et des réseaux d'ordinateurs, dans lequel coexistent des gens et des ordinateurs, et qui englobe toutes les zones d'activité en ligne[…] Depuis 1993, « cyberespace » a subi une extension de sens : restreint au début à la réalité virtuelle, il englobe aujourd'hui les communications sur Internet, comme en anglais »)

[2] استخدمنا في هذا المقال مصطلح الهجمات السيبرانية (Cyber Attack) بالنظر إلى المحيط الذي تجري فيه العمليات السيبرانية (Cyber Operations) الناشئة عن أداء أنظمة الكترونية مهمتها متابعة وجمع المعلومات التي تعمل الكترونيا وتحليلها ومن ثم اتخاذ إجراءات محددة لمهاجمتها عن طريق أنظمة الكترونية أخرى مخصصة لهذا الغرض، حول تعريف الهجمات السيبرانية: أحمد عبيس نعمة الفتلاوي، "الهجمات السيبرانية: مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر"، مجلة المحقق المحلي للعلوم القانونية والسياسية، العدد 4، جامعة بابل، 2016، ص ص 615–617؛ منى عبد الله السمحان، "متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود"، مجلة كلية التربية، جامعة المنصورة، العدد 11، 2020، ص 10؛ انظر أيضا:

والأمن الدوليين، وما عزز هذه الهجمات، ضعف شبكات المعلومات وسهولة اختراقها، وإمكانية الحصول على الأسلحة السيبرانية من خلال الإنترنت المظلم[3]، وصعوبة تحديد موقع وهوية مرتكبي هذه الهجمات، إلى جانب فعاليتها في الواقع، ما جعل الدول الكبرى تلجأ إليها لتحقيق التقدم على الخصوم في جميع مجالات الصراع.

تهدف الهجمات السيبرانية التي تنطلق من فضاء افتراضي إلى خلق تأثير في موازين القوة في العالم المحسوس، بحيث تشكل هذه الهجمات وسيلة جديدة للسيطرة على الفضاءات الأخرى (البرية، والبحرية والجوية والفضاء الخارجي) للدول المستهدفة، وذلك من خلال استهداف أنظمة الكومبيوتر للسيطرة على الحركة البرية والبحرية والجوية ومحطات الطاقة النووية، ومحطات الكهرباء، والبنية التحتية المدنية والعسكرية بشكل عام عن طريق برامج خبيثة أو غيرها من الوسائل[4]، وهو ما يترتب عنه آثار جسيمة على الدول المستهدفة، وقد تصل تداعياتها إلى تهديد السلم والأمن الدوليين.

لقد أصبح الفضاء الإلكتروني يشكل ساحة جديدة للصراع بين الدول سواء وقت السلم أو الحرب، ويكرس عقيدة جديدة مفادها من يسيطر على هذا الفضاء فإنه يسيطر على المجالات الأخرى خاصة الاقتصادية والعسكرية، وبذلك يستطيع حسم الصراع لصالحه، فالهجمات السيبرانية تكون عبر الدخول في الشبكات الإلكترونية والسيطرة عليها أو تدميرها، لشل قدرات الدولة ونشاطها وتعطيل عمل مؤسساتها، مما قد يتسبب في زهق أرواح الأبرياء، وتدمير للأعيان، فالهدف من الهجوم السيبراني هو تعطيل وظيفة شبكة الكومبيوتر، لتحقيق أغراض سياسية أو تتعلق بالأمن القومي[5]، أو حتى تهديد بالسلم والأمن الدوليين.

إن توسع الهجمات السيبرانية وانتشارها بشكل رهيب، وما ينتج عنها من آثار وخيمة على الإنسانية، يطرح مسألة البحث عن نظام قانوني يؤطرها خاصة في ظل وجود فراغ قانوني حولها ويهدف هذا المقال إلى تسليط الضوء على إشكالية مدى انطباق قواعد القانون الدولي العام والقانون الدولي الإنساني على الهجمات السيبرانية؟

ولمعالجة هذه الإشكالية يتعين علينا أولا التطرق إلى تكييف الهجمات السيبرانية طبقا لأحكام القانون الدولي العام **(المبحث الأول)**، ثم نبحث تكييفها وفقا للقانون الدولي الإنساني **(المبحث الثاني)**.

Québec, Office québécois de la langue française, Bibliothèque virtuelle, Québec, Gouvernement du Québec 2002, en ligne : www.oqlf.gouv.qc.ca/ressources/bibliotheque/dictionnaires/Internet/Fiches/2075010.html

[3] نور أمير الموصلي، الهجمات السيبرانية في ضوء القانون الدولي الإنساني، بحث مقدم استكمالا لمتطلبات نيل درجة ماجستير التأهيل والتخصص في القانون الدولي الإنساني، الجامعة الافتراضية السورية، 2021، ص1.

[4] EVELYNE AKOTO, Les cyberattaques étatiques constituent-elles des actes d'agression en vertu du droit international public ? : première partie, Revue de droit d'OTTAWA, n°2, 2015, pp. 11-12.

[5] نور أمير الموصلي، الهجمات السيبرانية في ضوء القانون الدولي الإنساني، مرجع سابق، ص ص 15-16.

المبحث الأول: تكييف الهجمات السيبرانية وفقا للقانون الدولي العام

لم ينظم القانون الدولي صراحة مسألة الهجمات السيبرانية سواء وقت السلم ، وهذا راجع إلى الاستخدام الحديث نسبيا لشبكات الإنترنت، بينما قواعد القانون الدولي التي تحكم العلاقات الدولية يرجع تاريخها إلى ما قبل وجود الفضاء السيبراني، وبالتالي فقواعده قد لا تتلاءم والتكنولوجيات الجديدة للحرب[6]، غير أن الاستخدام الواسع للفضاء السيبراني كساحة صراع جديدة[7] بين الدول يؤدي إلى مزيد من التهديدات للسلم والأمن الدوليين، وفي ظل غياب نصوص قانونية خاصة في القانون الدولي العام حول هذه الهجمات، سنبحث مسألة تكييفها وفقا للمبادئ الأساسية للقانون الدولي العام، وهي مبدأ السيادة (المطلب الأول)، ومبدأ حظر استخدام القوة أو التهدّيد باستخدامها (المطلب الثاني).

المطلب الأول: الهجمات السيبرانية ومبدأ السيادة

تعد الهجمات السيبرانية إحدى الوسائل الحديثة والأكثر استخداما لحسم الصراعات بين الدول، نظرا لسرعتها وسهولة استعمالها وقلة تكلفتها، بحيث يمكن لأي دولة أن تعطل المنشآت والبنى التحتية العسكرية و/أو المدنية[8] لدولة أخرى بالضغط على بعض الأزرار، ومن ثم إخضاعها دون استخدام الوسائل التقليدية للحرب.

ارتبط مفهوم السيادة مع البدايات الأولى لنشأة الدولة بالمفهوم الحديث وتنظيم المجتمع الدولي، وتعد معاهدة وستفاليا لسنة 1648 أول صك دولي وضع الأسس لهذا المفهوم الذي عرف عدة تطورات للتكيف مع الأوضاع الجديدة الناتجة عن التطور الذي عرفه المجتمع الدولي في مختلف المجالات، فالسيادة تقليديا لها مدلول سياسي ويقصد بها "السلطة العليا للدولة في الداخل واستقلالها عن غيرها في الخارج"[9]، أما من الناحية القانونية، فالسيادة هي "المصطلح الدولي الذي يدل على الأهلية القانونية للدولة باعتبارها صفة تتميز بها الدولة عن غيرها من أشخاص القانون الدولي"[10]، تسمح لها بممارسة اختصاصاتها على الصعيدين الداخلي والدولي على

---

[6] عمر محمد أعمر، الحرب الإلكترونية في القانون الدولي الإنساني، دراسات، علوم الشريعة والقانون، المجلد 46، عدد3، 2019، ص 136.

[7] Walter Peretti, La souveraineté à l'épreuve des cyberattaques « supply chain », Conférence des Grandes Ecoles, 28 septembre 2021, en ligne : https://www.cge.asso.fe/liste-actualites/La-souveraineté- à- lepreuve- des- cyberattaques- supply- chain/

[8] حول الآثار العسكرية والمدنية الناجمة عن الهجمات السيبرانية انظر: نور أمير الموصلي، الهجمات السيبرانية في ضوء القانون الدولي الإنساني، مرجع سابق، ص ص 18-20.

[9] محمد طلعت الغنيمي، الغنيمي الوسيط في قانون السلام، منشأة المعارف، الإسكندرية، 1993، ص319، ص 322.

[10] محمد طلعت الغنيمي، الغنيمي الوسيط في قانون السلام، مرجع سابق، ص ص 317 -318.

حد سواء[11]، وبإدارة شؤونها دون تدخل من أي دولة أو دول أخرى في إطار أحكام القانون الدولي[12] التي قبلتها بإرادتها الحرة، ويعد مبدأ السيادة حجر الزاوية للقانون الدولي خاصة مع قابليته لمسايرة التطورات الحاصلة في الحياة الدولية، وقد تم الاعتراف به وتكريسه في ميثاق الأمم المتحدة الذي نص على أن "تقوم الهيئة على مبدأ المساواة في السيادة بين جميع أعضائها".[13]

لم يعد مفهوم السيادة يقتصر على المفهوم السياسي التقليدي ولا حتى القانوني، بل تطور وتكيف مع التقدم التكنولوجي وظهور الفضاء السيبراني كمجال خامس إلى جانب المجال البري والبحري والجوي والفضاء الخارجي، فظهر مفهوم السيادة السيبرانية[14]، الذي يعني بسط الدولة سيطرتها وولايتها القضائية على الفضاء الرقمي المتمثل بشبكة الإنترنت[15]، ومن ثم حماية أمنها القومي من مخاطر التهديدات الجديدة المرتبطة بالفضاء السيبراني الذي لا يعرف حدودا جغرافية بين الدول.

ويرتبط مفهوم السيادة السيبرانية ارتباطا وثيقا بمفهوم الأمن السيبراني باعتباره مجموع الوسائل التقنية والإدارية التي يتم استخدامها لمنع الاستخدام غير المصرح به، وسوء استغلال واستعادة المعلومات الالكترونية ونظم الاتصالات والمعلومات التي تحتويها بهدف ضمان توافر واستمرارية عمل نظم المعلومات، وتأمين حماية وسرية البيانات الشخصية واتخاذ جميع التدابير اللازمة لحماية المواطنين والمستهلكين من المخاطر في الفضاء السيبراني [16]، وبالتالي أي هجوم تقوم به دولة ضد الشبكات الإلكترونية لدولة أخرى

---

[11] حازم محمد عتلم، أصول القانون الدولي العام، القسم الثاني أشخاص القانون الدولي، دار النهضة العربية، القاهرة، 2001، ص ص 344-345.

[12] المرجع نفسه، ص 347؛ أحمد وافي، الحماية الدولية لحقوق الإنسان ومبدأ السيادة، دار هومة، الجزائر، 2005، ص 49.

[13] المادة 2 الفقرة 1 من ميثاق منظمة الأمم المتحدة.

[14] هناك من يستعمل مصطلح آخر هو "السيادة الرقمية"، انظر:
Travaux parlementaire, Sénat, Le devoir de souveraineté numérique, 1 octobre 2022, en ligne : http://www.senat.fr/rap/r19-007-1/r19-007-17.html

[15] حسام جاسم محمد أحمد الدليمي، التطور التكنولوجي وأثره في سيادة الدول، رسالة ماجستير، كلية القانون والعلوم السياسية، جامعة الأنبار، العراق، 2018، ص 114؛ انظر أيضا: فاطمة بيرم، "السيادة الوطنية في ظل الفضاء السيبراني والتحولات الرقمية: الصين نموذجا"، المجلة الجزائرية للأمن الإنساني، العدد 1، 2020، ص 789.

[16] حول تعريف الأمن السيبراني انظر: فاطمة بيرم، "السيادة الوطنية في ظل الفضاء السيبراني والتحولات الرقمية: الصين نموذجا"، مرجع سابق، ص 795.

بغرض إحداث اضطرابات في عمل الأنشطة والمرافق العمومية والخاصة للدولة المستهدفة[17]، والمساس بمصالحها[18]، يشكل انتهاكا لسيادتها[19].

وعرفه الاتحاد الدولي للاتصالات بأنه مجموع الأدوات والسياسات، وضوابط الأمن والمبادئ التوجيهية، ونهج إدارة المخاطر والإجراءات والتدريب، وأفضل الممارسات وآليات الضمان والتكنولوجيات التي يمكن استخدامها في حماية البيئة السيبرانية وأصول المؤسسات والمستعملين، وتشمل أصول المؤسسات والمستعملين أجهزة الحوسبة الموصولة بالشبكة، والموظفين، والبنية التحتية والتطبيقات والخدمات وأنظمة الاتصالات، ومجموع المعلومات المنقولة و/ أو المحفوظة في البيئة السيبرانية[20]، فالأمن السيبراني هو الجهد المستمر لحماية شبكات وبيانات المؤسسات والأفراد من الاستخدام غير المصرح به أو أي أذى أو اختراق يلحق بالشبكة[21]، غير أن مفهوم السيادة السيبرانية يختلف عن مفهوم الأمن السيبراني، حيث يهدف هذا الأخير إلى حماية البنية التحتية والعمليات المتصلة بالإنترنت، بينما تركز السيادة السيبرانية على المعلومات والمحتوى الذي توفره الإنترنت كامتداد طبيعي للسيادة الوطنية في الفضاء الإلكتروني.[22]

لم تعد القوة العسكرية التهديد الوحيد للدول وللمجتمع الدولي، بل أصبح امتلاك الدول للقوة الإلكترونية يمثل أكبر تهديد لسيادة الدول المستهدفة سواء في المجال العسكري، أو الاقتصادي، أو الثقافي، أو السياسي[23]، خاصة في ظل الحكومة الإلكترونية، وذلك من خلال استهداف مختلف الأنظمة المعلوماتية للدول

---

[17] EVELYNE AKOTO, Les cyberattaques étatiques constituent-elles des actes d'agression en vertu du droit international public ? : Première partie, op. cit, p. 1.

[18] Bories Clémentine, « Appréhender la cyberguerre en droit international. Quelques réflexions et mise point », édition La revue des Droits de l'Homme, juin 2014§5.

[19] Vincent Sébastien, « Qui s'y frotte, s'y pique. Une stratégie intégrale pour réduire la subversion cyber », Revue défense nationale, p. 42, en ligne : https://www.defna.com/e-RDN/vue-article-chier.php?carticle=482&cidcahier=1291

[20] التوصية (04/2008) 1205.ITU-T-X الصادرة عن الاتحاد الدولي للاتصالات، ص ص 2-3، على الموقع:
https://www.itu.int>rec>T-RE-X.1205-200804.I

[21] محمد سعد محمود، الحرب السيبرانية: أدواتها وقودها خسائرها، ص 2، على الموقع:
https://www.Noor-Book.com

[22] سميرة شرايطية، "السيادة السيبرانية في الصين بين متطلبات القوة وضروريات الأمن القومي"، المجلة الجزائرية للأمن والتنمية، المجلد 09، العدد 16، جانفي 2020، ص 404.

[23] محمد عاطف إمام ابراهيم، الفضاء الإلكتروني وأثره على الأمن القومي للدول: الحروب الإلكترونية نموذجا، المركز الديمقراطي العربي، أفريل 2022 على الموقع:
https://democraticac.de/?page-id=60141

بغرض السيطرة أو تدمير البيانات والمنشآت المرتبطة بها بأكبر سرعة، وبأقل تكلفة وعبئا من ناحية المساءلة والتبعات.[24]

تشكل الهجمات السيبرانية التي ترتكبها دول على البنى التحتّية الرقمية والتقنيات والمحتويات الرقمية والاتصالات انتهاكا للسيادة السيبرانية للدولة المستهدفة، والتي تعد امتدادا لسيادتها الإقليمية على البنى التحتية السيبرانية التي تغطيها سيادتها الإقليمية، وعلى المنشآت العسكرية والاقتصادية والسياسية والثقافية والاجتماعية المرتبطة بهذا الفضاء[25]، فالدولة لها حق سيادي في إدارة شبكة الانترنت الخاصة بها التي يجب أن تعمل بشكل مستقل ودون الخضوع لدول أخرى[26]، وفي الرقابة على مختلف الهيئات والمؤسسات والمنشآت والأنشطة المتواجدة على إقليمها طبقا للقانون الدولي[27]، وأي مساس بالبنية التحتية الإلكترونية كشبكات الاتصال ومحطات توليد الطاقة وتزويد المواطنين بالحاجيات الأساسية[28]، وغيرها هو انتهاك لسيادتها، بل أن مبدأ السيادة يفرض واجبا على الدول في منع استخدام البنية التحتية الإلكترونية التي تقع على إقليم الدولة وتخضع لسيطرتها في النشاطات التي تستهدف السيادة السيبرانية لدول أخرى، كما أن سيادة الدولة لا تكون على البنى التحتية الإلكترونية الموجودة على إقليمها فقط، وإنما تمتد إلى البنى التحتية التي هي تحت سيطرتها والموجودة على أقاليم دول أخرى.[29]

يتضح من خلال ما سبق، أن الهجمات السيبرانية التي تشنها دولة على الفضاء الافتراضي لدولة أخرى هو مساس بأمنها السيبراني، وهو ما يشكل انتهاكا لسيادتها على مختلف المنشآت والأجهزة المرتبطة بهذا الفضاء التي تقع تحت سيطرتها، ومن ثم فهو عمل دولي غير مشروع، وبالتالي فحماية مختلف الأنشطة (التجارية، والمدنية، وغيرها) يشكل مفتاح للأمن الوطني في المستقبل[30].

---

[24] صلاح حيدر عبد الواحد، حروب الفضاء الإلكتروني؛ دراسة في مفهومها وخصائصها وسبل مواجهتها، رسالة ماجستير، كلية الآداب والعلوم، قسم العلوم السياسية، جامعة الشرق الأوسط، 2021، ص 20.

[25] Cyberespace, relations internationales et pays émergents : évolution ou révolution, Mémoire présenté comme exigence partielle de la maitrise en science politique, Université du Québec à Montréal, octobre 2015, p. 49.

[26] سميرة شرايطية، السيادة السيبرانية في الصين بين متطلبات القوة وضروريات الأمن القومي، مرجع سابق، ص 404.

[27] أحمد عبيس نعمة الفتلاوي وزهراء عماد محمد، "تكييف الهجمات السيبرانية في ضوء القانون الدولي"، مجلة الكوفة للعلوم القانونية والسياسية، المجلد 44، العدد 1، كلية القانون والعلوم السياسية، جامعة الكوفة، العراق، 2020، ص 57.

[28] - Walter Peretti, La souveraineté à l'épreuve des cyberattaques « supply chain ». op. cit.

[29] علي محمد كاظم الموسوي، المشاركة المباشرة في الهجمات السيبرانية، المؤسسة الحديثة للكتاب، لبنان، 2019، ص 2.

[30] Cyberespace, relations internationales et pays émergents : évolution ou révolution, op. cit, p. 50.

المطلب الثاني: الهجمات السيبرانية ومبدأ حظر استخدام القوة والتهديد باستخدامها

تعد معاهدة وستفاليا في نظر كثير من الفقهاء بداية تشكل القانون الدولي التقليدي القائم على مبدأ المساواة في ممارسة السيادة المطلقة من غير قيد أو حد يحدها، وهو ما أدى إلى اندلاع عدة حروب كمظهر طبيعي لهذه السيادة وأداة لتنفيذ السياسة الوطنية[31]، وخلق حالة من الفوضى واللااستقرار في العلاقات الدولية.

ساهم اندلاع الحربين العالميتين وما نتج عنهما من ويلات ودمار على الإنسانية جمعاء في ترسيخ الاعتقاد بضرورة تحريم الحرب كوسيلة لتسوية النزاعات الدولية، ولهذا الغرض تم إنشاء منظمة الأمم المتحدة، حيث نص ميثاقها على حظر استخدام القوة والتهديد باستخدامها في العلاقات الدولية بأية طريقة تتنافى ومقاصد الأمم المتحدة المتمثلة في الحفاظ على السلم والأمن الدوليين[32]، بحيث أصبح التدخل أو التهديد باستعمال القوة أو باستخدامها ضد سلامة الأراضي أو الاستقلال السياسي لأية دولة مخالف للقانون الدولي باعتباره عملا غير مشروع[33] باستثناء حالتين: حالة الدفاع عن النفس، وحالة تدخل مجلس الأمن الدولي للمحافظة على السلم والأمن الدولي تطبيقا لنص المادة 42 من الميثاق.

ويتوافق تحريم اللجوء إلى القوة بقاعدة أخرى في الميثاق، وهي قاعدة عدم التدخل في الشؤون الداخلية أو الخارجية لدولة أخرى[34]، وهو ما أكدته محكمة العدل الدولية في عدة قضايا[35]، كما يكرس ويكمل مبدأ عدم جواز التدخل في سيادة الدولة على إقليمها[36]، فالتدخل عمل غير مشروع دوليا لما فيه من اعتداء على سيادة واستقلال الدول، كما أنه يشكل اعتداء خطيرا على النظام العام الدولي في المجتمع المعاصر.

إن استعمال القوة أو التهديد باستعمالها يتنافى مع أهداف مقاصد الرامية إلى حفظ السلم والأمن الدوليين، وقد ورد في نص الفقرة 4 من المادة 2 من الميثاق مصطلح "القوة" دون اقترانه بأي مصطلح آخر، أي دون

---

[31] عبد الواحد محمد الفار، القانون الدولي العام، دار النهضة العربية، القاهرة، 1994، ص 431.

[32] المادة 2 الفقرة 4 من ميثاق منظمة الأمم المتحدة.

[33] Vladimir Szoke-Pellet, Les cyberattaques étatiques et la notion d'agression en droit international, MÉMOIRE DANS LE CADRE DU MASTER 2 DROIT INTERNATIONAL PUBLIC, AIX-MARSEILLE UNIVERSITÉ FACULTÉ DE DROIT ET DE SCIENCE POLITIQUE, 2017/2018, p. 14.

[34] المادة 2 الفقرة 7 من ميثاق منظمة الأمم المتحدة.

[35] محكمة العدل الدولية، قضية الأنشطة العسكرية وشبه العسكرية في نيكاراغوا وضدها، نيكاراغوا ضد الولايات المتحدة الأمريكية)، 27 جون 1986، موجز الأحكام والفتاوى الصادرة عن محكمة العدل الدولية 1948-1991، منشورات الأمم المتحدة، نيويورك، 1999، ص 212، على الموقع:https://www.icj-cij.org/ar

[36] أميرة حناشي، مبدأ السيادة في ظل التحولات الدولية الراهنة، رسالة ماجستير، كلية الحقوق، جامعة منتوري، قسنطينة، 2008، ص 90.

تحديد لنوع القوة المستعملة، حيث جاءت الفقرة مطلقة لتشمل كل أشكال القوة، وهذا بخلاف المواطن الأخرى لاستعمال المصطلح في الميثاق، أين يقترن بمصطلح "المسلحة" كما ورد في الديباجة والمادة 44 من الميثاق، وبناء عليه، فإن مفهوم القوة لا ينحصر فقط بالقوة العسكرية، وإنما يشمل كل أنواع التهديد بغض النظر عن الوسيلة المستخدمة طالما أن النية عدائية[37]، بحيث يتخذ التدخل باستعمال القوة أو التهديد باستعمالها صورا مختلفة منها التدخل العسكري، أو التدخل المالي، أو التدخل بقصد التخريب، وقد يتخذ التدخل شكلا فرديا أو جماعيا، وقد يكون صريحا ومباشرا، أو خفيا ومقنعا[38]، كما يحدث في الهجمات السيبرانية.

أدت التطورات التكنولوجية في المجال الإلكتروني إلى ظهور عدة مفاهيم جديدة، منها مفهوم "القوة السيبرانية"، حيث أصبح التفوق في المجال الإلكتروني عنصرا حيويا في تنفيذ عمليات ذات فعالية على الأرض وفي البحر والجو والفضاء الخارجي من خلال اعتماد القدرة القتالية في الفضاء الإلكتروني على نظم التحكم والسيطرة التكنولوجية[39]، غير أنه يجب التمييز في هذا الإطار بين استخدام الهجمات السيبرانية التي لها نفس الأغراض العسكرية مع الهجمات التقليدية[40]، والمتمثلة أساسا في استهداف البنية التحتية العسكرية للدول، وأمن المعلومات العسكرية، وبين الهجمات السيبرانية الأخرى التي ليس لها هدف عسكري كالحرب الإعلامية، ونشر الإشاعات والتحويلات المالية بصورة غير شرعية، فوحدها القوة السيبرانية لأغراض عسكرية والتي لها نفس التداعيات الناجمة عن استخدام القوة العسكرية التقليدية من قتل على نطاق واسع، وتدمير للطبيعة وللبنية التحتية للدولة، وسرقة المعلومات والبيانات العسكرية والتلاعب بها، والسيطرة على الأنظمة العسكرية التي تدخل ضمن مفهوم الفقرة 4 من المادة 2 من ميثاق الأمم المتحدة.[41]

إن معيار تكييف الهجمات السيبرانية وفقا للمادة 4/2 يتعلق بالآثار والأضرار الناتجة عنها وليس بالوسيلة المستعملة، وهو ما أكدت عليه محكمة العدل الدولية في رأيها الاستشاري حول مشروعية التهديد بالأسلحة

---

[37] علي فاضل علي سليمان، "حق الدفاع الشرعي على الهجمات السيبرانية"، مجلة جامعة تكريت للحقوق، السنة 4، المجلد 4، العدد 4، الجزء 1، 2020، ص 8.

[38] أحمد محمد رفعت، القانون الدولي العام، مكتبة علاء الدين، الإسكندرية، 2001، ص196.

[39] يحي ياسين سعود، "الحرب السيبرانية في ضوء القانون الدولي الإنساني"، المجلة القانونية، المجلد (4)، العدد (4)، كلية الحقوق–جامعة القاهرة، مصر، ص 87، على الموقع:
https://jlaw.journals.ekb.eg/article_45192_52d735c1a23cca2bf7dbbe56c4eb6846.pdf

[40] Vladimir Szoke-Pellet, Les cyberattaques étatiques et la notion d'agression en droit international, op. cit., p. 7.

[41] إيهاب خليفة، ما هو موقف ميثاق الأمم المتحدة من استخدام القوة السيبرانية في التفاعلات الدولية؟، 24 أكتوبر 2019، على الموقع: https://Futureuae.com>ar-AE> Item

النووية أو استخدامها، حيث خلصت المحكمة إلى أن القانون الواجب التطبيق على المسألة المعروضة عليها والذي له أكبر صلة مباشرة هو القانون المتصل باستعمال القوة والوارد في ميثاق الأمم المتحدة إلى جانب القانون الواجب التطبيق على النزاع المسلح، كما لاحظت المحكمة أن التطبيق الصحيح للقانون يكون من خلال الأخذ بعين الاعتبار الخصائص الفريدة للأسلحة النووية، ولا سيما قدرتها التدميرية، وقدرتها على التسبب في آلام الإنسانية لا حصر لها، وقدرتها على إيقاع الضرر بالأجيال المقبلة، ومن ثم أكدت بأنه ليس في تلك الأحكام ما يشير إلى أسلحة معينة، فالفقرة 4 من المادة 2 تحظر "أي استعمال للقوة بصرف النظر عن الأسلحة المستخدمة"[42]، وبناء على هذا الرأي، أكدت بعض الدول أن "تجاوز حد استخدام القوة لا يتوقف على الوسائل الرقمية المستخدمة، ولكن على آثار العملية السيبرانية"، ومن ثم فالعملية السيبرانية التي تنفذها دولة ضد دولة أخرى تنتهك حظر استخدام القوة إذا كانت آثارها مماثلة (أو تتجاوز) الآثار الناجمة عن استخدام الأسلحة التقليدية"[43]، وفي هذه الحالة تنطبق أحكام القانون الدولي الإنساني المتعلقة بحماية الأشخاص والأعيان أثناء النزاعات المسلحة.

وبناء على ما سبق، يدخل في مفهوم القوة الوارد في المادة 2 الفقرة 4 من ميثاق الأمم المتحدة، الهجمات السيبرانية واسعة النطاق ضد السكان المدنيين أثناء النزاعات المسلحة أو خارجها، كإغلاق أجهزة الكمبيوتر التي تتحكم في محطات المياه والسدود التي ينتج عنها الفيضانات في المناطق المأهولة بالسكان، وكذلك الحوادث الهندسية المميتة والمتعمدة، مثل :المعلومات الخاطئة التي تغذيها أجهزة الكمبيوتر للطائرات، وانهيار في محطات الطاقة النووية وانطلاق المواد المشعة في المناطق ذات الكثافة السكانية العالية، التي تتسبب في آثار وخيمة على السكان المدنيين تتجاوز في شدتها آثار الحروب التقليدية، وقد اعتبر أن الهجمات الإلكترونية الخطرة تمثل هجوما مسلحا[44]، حتى ولو لم يكن هناك إصابات بالأشخاص مثل الهجمات التقليدية التي لا ينتج عنها إصابات أو خسائر في الممتلكات، ولا يوجد أي سبب للوصول إلى استنتاج مختلف فيما يتعلق بالهجمات"

---

[42] محكمة العدل الدولية، مشروعية التهديد بالأسلحة النووية أو استخدامها، الرأي الاستشاري الصادر في 8 جويلية 1996، موجز الأحكام والفتاوى الصادرة عن محكمة العدل الدولية 1992-1996، منشورات الأمم المتحدة، نيويورك، 1998، ص 2016 على الموقع: https://www.icj-cij.org/a

[43] التعليق على الفقرة 1 من شرح القاعدة 69 من دليل "تالين" بشأن القانون الدولي المطبق على الحروب السيبرانية، أعد من قبل مجموعة من الخبراء الدوليين، 2013، ترجمة علي محمد كاظم الموسوي، 2017، على الموقع:
https//www.academia.edu

[44] SIMONET Loïc, « L'usage de la force dans le cyberespace et le droit international », Annuaire de droit français international, n° 58, 2012, p. 126.

السيبرانية "ضد النظم المدنية[45]، "إذ من الصعب الإقرار بشرعية الهجمات السيبرانية فذلك لا يعفي الدول من مسؤولية التدخل وفقا للفقرة 4 من المادة 2 من ميثاق الأمم المتحدة، في حال أدت الهجمات السيبرانية إلى آثار مادية ملموسة في الأعيان المدنية أو العسكرية".[46]

بينت محكمة العدل الدولية في قضية نيكاراغوا ضد الولايات المتحدة الأمريكية والمتعلقة بالأنشطة العسكرية وشبه العسكرية في سنة 1986، أن المادة 51 لا تشير إلى أسلحة محددة وأن مفهوم الأسلحة ينطبق على" أي استخدام للقوة، وبغض النظر عن حقيقة أن الهجمات "السيبرانية "لا تستخدم الأسلحة الحركية التقليدية، فإن ذلك لا يعني بالضرورة أنها لا يمكن أن تكون" مسلحة"، ويمكن اعتبار استخدام أي جهاز ينتج عنه خسائر كبيرة في الأرواح أو تدمير واسع للممتلكات مستوف لشروط الهجوم" المسلح"، ويدعم هذا الاستنتاج تأكيد مجلس الأمن على ذلك الحق في الدفاع عن النفس ردا على هجمات 11 سبتمبر 2001 على الولايات المتحدة[47].

وفي هذا الإطار فقد اعتبر حلف شمال الأطلسي الهجمات السيبرانية المتلاحقة التي تعرضت لها جمهورية استونيا سنة 2007 والتي أدت إلى تعطيل كامل لشبكات الاتصال الإلكترونية فيها، بمثابة هجوم مسلح يهدد دول الحلف جميعا، وقد أكد الحلف أن أي هجوم سيبراني يؤدي إلى تطبيق البند الخامس من ميثاق الحلف الذي يعتبر أي عدوان على عضو في الحلف بمثابة عدوان على جميع أعضاء الحلف.[48]

كما ذكر دليل" تالين" الذي أعدته اللجنة الدولية التابعة لحلف شمال الأطلسي والمكونة من خبراء قانونيين وعسكريين سنة 2013، أنه يمكن استخدام القوة العسكرية الحقيقية في حالة تم شن هجوم الكتروني على دولة وأدى هذا الهجوم لخسائر بالأرواح البشرية.[49]

---

[45] المؤتمر الدولي الثاني والثلاثون للصليب الأحمر والهلال الأحمر، جنيف، سويسرا، 8-10 ديسمبر 2015، تقرير عن القانون الدولي الإنساني وتحديات النزاعات المسلحة المعاصرة، وثيقة أعدتها اللجنة الدولية للصليب الأحمر؛ عمر محمد أعمر، الحرب الإلكترونية في القانون الدولي الإنساني، مرجع سابق، ص 139.

[46] Shin; Beomchul, The Cyber Warfare and the Right of Self-Defense: Legal Perspectives and the Case of the United States, IFANS, Vol. 19, No1, June 2011, p. 111.

[47] Ibid, p. 138 ; Voir aussi : SIMONET Loïc, « L'usage de la force dans le cyberespace et le droit international », op. cit., p. 128.

[48] أحمد عبيس نعمة الفتلاوي، الهجمات السيبرانية: مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر، مرجع سابق، ص 624؛ حول موقف حلف شمال الأطلسي من الهجمات السيبرانية التي قد تحدث مستقبلا ضد أحد أعضائه، انظر:

Communiqué du sommet de Bruxelles publié par les chefs d'Etats et de gouvernement participant à la réunion du conseil de l'atlantique nord tenue à Bruxelles le 14 juin 2021, sur le site électronique : https://www.nato.int/cps/fr/natohq/new

[49] الفصل 14 من دليل تالين.

المبحث الثاني: تكييف الهجمات السيبرانية وفقا للقانون الدولي الإنساني

يطبق القانون الدولي الإنساني–أو ما يسميه العسكريون قانون الحرب[50]، أو قانون النزاعات المسلحة– على مجموع قواعد القانون الدولي التي تهدف إلى حماية ضحايا تلك النزاعات[51]، وذلك من خلال تقييد خيار الأطراف في النزاع سواء بالنسبة لطرق أو وسائل أو أهداف المعارك في الميدان[52]، فالقانون الدولي الإنساني يحكم سير الأعمال العدائية، ويهدف إلى حماية الأشخاص "المتواجدين بين أيدي أطراف النزاع"[53] المسلح كالأسرى والمدنيين، كما يهدف إلى حماية الممتلكات من آثار النزاعات المسلحة التقليدية.

شهدت السنوات الأخيرة تطورا ملحوظا في اللجوء إلى تكنولوجيات الحرب الجديدة، خاصة منها الهجمات السيبرانية في سياق النزاعات المسلحة، وهو ما أدى بكثير من الباحثين إلى تكييفها على أنها نزاع مسلح (المطلب الأول) يخضع لمبادئ القانون الدولي الإنساني (المطلب الثاني).

المطلب الأول: الهجمات السيبرانية بوصفها نزاع مسلح

يثير الموضوع محل البحث مسألة في غاية الأهمية، تتعلق بوصف الهجمات السيبرانية كجزء من نزاع مسلح، فالقانون الدولي الإنساني هو مجموعة من القواعد القانونية التي تسعى للحد من آثار النزاعات المسلحة لأسباب إنسانية، وبالتالي فإن مجال انطباق القانون الدولي الإنساني هو النزاع المسلح.

بداية نشير إلى أن مسألة انطباق القانون الدولي الإنساني على الهجمات السيبرانية هي محل خلاف في النقاشات الجارية بتفويض من الأمم المتحدة بين أعضاء فريق العمل المفتوح العضوية الذي أنشأته الجمعية العامة والذي يمارس مهامه جنبا إلى جنب مع فريق الخبراء الحكوميين، وكلا الفريقين مكلف بمهام منها دراسة

---

[50] يشمل مفهوم قانون الحرب *Jus in bello* "قوانين وأعراف الحرب"، التي تطبق عند نشوب الحرب، وهو ما يعرف بقانون لاهاي استنادا إلى اتفاقيتي لاهاي لسنة 1899 و1907 حول قوانين وأعراف الحرب البرية والبحرية، التي بينت حقوق وواجبات المحاربين خلال الأعمال العدائية، وكذلك القيود المفروضة على وسائل القتال؛ إلى جانب هذا القانون، هناك ما يعرف بقانون جنيف استنادا إلى اتفاقيات جنيف لسنة 1864 و1949 الذي يعنى بحماية بعض ضحايا النزاعات المسلحة.

حول التمييز بين قانون لاهاي وقانون جنيف، انظر:

M. CYR DJIENA WEMBOU et D. FALL, « Le droit international humanitaire : Théorie générale et réalités africaines », Paris, L'Harmattan, 2000, pp. 47-48.

[51] M. MAHOUVE, La répression des violations du droit international humanitaire au niveau national et international, R.D.I.D.C, troisième trimestre 2005, pp. 229-230.

[52] Pietro VERRI, Dictionnaire du droit international des conflits, CICR, 1988, p. 49.

[53] Stelios PERRAKIS, « Le droit international humanitaire et ses relations avec les droits de l'homme. Quelques considérations », in P.TAVERNIER et J-M. HENCKAERTS, Droit international humanitaire coutumier enjeux et défis contemporains, Bruxelles, Bruylant, 2008, p.118.

"كيفية انطباق القانون الدولي الإنساني على استخدام الدول لتكنولوجيات المعلومات والاتصالات"[54]، وقد اتفقت الدول الأعضاء في فريق الخبراء الحكوميين عامي 2013 و2015 على أن أحكام القانون الدولي، لاسيما ميثاق الأمم المتحدة، قابلة للتطبيق في بيئة تكنولوجيا المعلومات والاتصالات، وأشارت إلى المبادئ القانونية الدولية المعمول بها، بما في ذلك حسب الاقتضاء، مبادئ الإنسانية والضرورة والتناسب والتمييز[55]، بحيث يمكن أن تكون الهجمات السيبرانية جزء من حرب سيبرانية إذا ما استخدمت في إطار نزاع مسلح لتحقيق أهداف عسكرية.[56]

إن عدم وجود نص صريح في القانون الدولي حول الهجمات السيبرانية، لا يعني عدم انطباق القواعد العامة لقانون لاهاي التي تنظم وسائل وأساليب الحرب –بما فيها استخدام الأسلحة– والقواعد العامة لقانون جنيف لحماية الفئات الضعيفة والأعيان المدنية أثناء النزاعات المسلحة على هذه الهجمات[57]، حيث جاءت هذه القواعد لتشمل كافة التطورات ذات الصلة، ومن ثم ينطبق القانون الدولي الإنساني على الهجمات السيبرانية التي تشكل جزء من نزاع مسلح باستخدام الوسائل التقليدية للحرب وتكون متصلة به، كما ينطبق على العمليات السيبرانية التي تصل في حد ذاتها إلى مستوى النزاع المسلح من حيث الآثار الناجمة عنها في ظل غياب العمليات الحركية[58].

يعرف دليل "تالين" الهجوم السيبراني بموجب القانون الدولي الإنساني بوصفه" عملية الكترونية سواء هجومية أو دفاعية يتوقع أن تتسبب في إصابة أو قتل أشخاص أو الأضرار بأعيان أو تدميره، كما قد يشكّل توقف أحد الأعيان عن العمل ضررا ماديا[59]، فالهجمات السيبرانية تشكل وسيلة وأسلوبا للقتال في الوقت

---

[54] قرار الجمعية العامة للأمم المتحدة رقم 73/27 " التطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي" وثيقة الأمم المتحدة 73/27/A/RES، 11 ديسمبر 2018، الفقرة 5؛ وقرار الجمعية العامة للأمم المتحدة رقم 73/266، "الارتقاء بسلوك الدول المسئول في الفضاء الإلكتروني في سياق الأمن الدولي"، وثيقة الأمم المتحدة، A/RES/73/266، 2 جانفي 2019، الفقرة 3.

[55] قرار الجمعية العامة للأمم المتحدة فريق الخبراء الحكوميين، المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي: مذكرة من الأمين العام" وثيقة الأمم المتحدة 174/70/A، 22 جويلية 2015، الفقرتان 24 و28 (د).

[56] يحي ياسين سعود، الحرب السيبرانية في ضوء القانون الدولي الإنساني، مرجع سابق، ص 85.

[57] « Le droit international humanitaire et les cyberopérations pendant les conflits armés », position du CICR, novembre 2019, p.7, en ligne : https://www.icrc-ihl-and-cyber-operations-during-armed-conflict-fr(1)pdf

[58] يحي ياسين سعود، الحرب السيبرانية في ضوء القانون الدولي الإنساني، مرجع سابق، ص 90، ص 302.

[59] المادة 92 من دليل تالين.

نفسه[60]، ومن ثم يمكن اعتبار الفيروسات والديدان الإلكترونية سلاحا – مثل الأجهزة والمفاعلات النووية– يستخدم لتنفيذ الاختراق أو الهجوم السيبراني[61]، وفي هذه الحالة يمكن تطبيق قواعد ومبادئ القانون الدولي الإنساني السارية على هذه الهجمات بوصفها حرب سيبرانية[62]، وقد اعتبر الدليل " الهجوم الإلكتروني بمثابة استخدام للقوة إذا كان أثر هذا الهجوم عند مقارنته بالاستخدام الفعلي للقوة مساويا له، أو قريبا منه" .[63]

وتعتبر اللجنة الدولية أيضا أنّ العملية التي تهدف إلى تعطيل عين ما –حاسوب أو شبكة حاسوبية–، على سبيل المثال تشكّل هجوما بموجب القواعد بشأن إدارة العمليات العدائية، سواء تم تعطيل العين عن طريق وسائل حركية أو سيبرانية، فأي عملية تستهدف تعطيل أو ضرب البنى التحتية المدنية والعسكرية تخضع لقواعد القانون الدولي الإنساني بغض النظر عن الوسيلة المستخدمة في ذلك، فالعبرة بالنتائج المادية على الأرض وليس بالوسيلة المستعملة.

ومن صور استخدام العمليات السيبرانية أثناء النزاعات المسلحة، عمليات التجسس، وتحديد الأهداف، والعمليات المعلوماتية الرامية إلى التأثير على معنويات العدو وإرادته إزاء القتال، وقطع نظم اتصالات العدو أو تضليلها أو التشويش عليها، وتعطيل محطات الرادار، والمنشآت النووية، ولعل أخطر الهجمات السيبرانية المرتكبة أثناء النزاعات المسلحة أو خارج سياق هذه النزاعات والتي لها آثار وخيمة على المدنيين، تلك الهجمات التي تستهدف البنى التحتية التي يستعملها المدنيون على غرار محطات توليد الكهرباء، ونظم الرعاية الصحية، وبرامج المساعدة الإنسانية، ومخططات الإسعاف، وتعد الهجمات السيبرانية المتبادلة حاليا بين كل من روسيا وأوكرانيا بالموازاة مع الحرب الدائرة بينهما على الأرض أكبر تهديد للأمن والسلام في العالم، وتحديا كبيرا للمجتمع الدولي ينذر بحرب سيبرانية عالمية.

وتجدر الإشارة إلى أن القانون الدولي الإنساني لا يضفي الشرعية على استخدام القوة سواء كانت حركية أو سيبرانية، فلا يجوز أن يفسر أي نص ورد في هذا الملحق "البروتوكول" أو في اتفاقيات جنيف لعام 1949

---

[60] نور أمير الموصلي، الهجمات السيبرانية في ضوء القانون الدولي الإنساني، مرجع سابق، ص ص 20– 21.

[61] يحي مفرح الزهراني، "الأبعاد الاستراتيجية والقانونية للحرب السيبرانية"، مجلة البحوث والدراسات، العدد 23، السنة 14، 2017، ص 239.

[62] Bories Clémentine, « Appréhender la cyberguerre en droit international. Quelques réflexions et mise point », op. cit., p. 5.

[63] المادة 69 من دليل تالين.

على أنه يجيز أو يضفي الشرعية على أي عمل من أعمال العدوان أو أي استخدام للقوة يتعارض مع ميثاق الأمم المتحدة".[64]

إن الأضرار الناجمة عن الهجمات السيبرانية كفيلة بأن تجعل الهجوم الإلكتروني يرتقي إلى مستوى الهجوم المسلح، فالوفيات والإصابات في صفوف الفئات المحمية الناجمة عن تعطيل أنظمة دعم الحياة التي يتحكم فيها جهاز الكومبيوتر، وانقطاع التيار الكهربائي بشكل كامل، وكذلك تعطيل أجهزة الكومبيوتر التي تتحكم في محطات المياه والسدود مما ينتج عنه فيضانات في المناطق المأهولة بالسكان دليل كاف لاعتبار الهجوم السيبراني قوة وعدوان.[65]

وبناء على ما سبق، فإن الهجمات السيبرانية تعطل المصالح الإستراتيجية والحيوية للدول على الرغم من أنها لا يتم فيها احتلال الأراضي والغزو المباشر إلا أن أبعادها التدميرية وأضرارها تجعلها أشد من العدوان المسلح في بعض الأحيان، بحيث أنها تؤدي إلى حدوث ضحايا وكوارث إنسانية، وهو ما يطرح بشدة موضوع المسؤولية الدولية عن هذه الهجمات.

المطلب الثاني: خضوع الهجمات السيبرانية لمبادئ القانون الدولي الإنساني

يخضع استخدام وسائل الحرب الإلكترونية لنفس المبادئ التي تحكم سير الأعمال العدائية بالأسلحة التقليدية[66]، باعتبار أن القانون الدولي الإنساني واسع بما فيه الكفاية ليساير التقدم الحاصل في التكنولوجيا، فمن أبرز مواطن قوة القانون الدولي الإنساني–كما ذهبت إليه محكمة العدل الدولية– أنه وضع بطرق تجعله قابلا للتطبيق على كافة أشكال وأنواع الأسلحة بما فيها الأشكال والأنواع المستقبلية، فالقانون الدولي الإنساني يحد من العمليات السيبرانية أثناء النزاعات المسلحة مثلما يحد من استخدام أي أسلحة ووسائل وأساليب حرب أخرى– جديدة كانت أو قديمة – أثناء نزاع مسلح[67]، حيث يمكن في هذا الإطار أن نشير إلى أنه تم تبني التطورات الحديثة التي قد تحدث في وسائل وأساليب القتال في المستقبل في المادة 36 من البروتوكول الإضافي الأول الملحق باتفاقيات جنيف الأربعة لعام 1949 التي نصت على أن "يلتزم أي طرف سام متعاقد عند دراسة أو تطوير أو اقتناء سلاح جديد أو أداة للحرب، أو إتباع أسلوب للحرب، بأن يتحقق مما إذا كان ذلك محظورا في

---

[64] الفقرة 2 من ديباجة البروتوكول الإضافي الأول لسنة 1977 الملحق باتفاقيات جنيف لسنة 1949.

[65] علي فاضل علي سليمان، "حق الدفاع الشرعي على الهجمات السيبرانية"، مجلة جامعة تكريت للحقوق، السنة 4، المجلد 4، العدد 4، الجزء 1، 2020، ص 9.

[66] Vladimir Szoke-Pellet, Les cyberattaques étatiques et la notion d'agression en droit international, op. it., p. 8.

[67] تيلمان رودنهاورز، "الحرب السيبرانية والقانون الدولي الإنساني"، المجلة الدولية للصليب الأحمر، فيفري 2021، على الموقع: https://www.icrc.org/ar/document

جميع الأحوال أو في بعضها بمقتضى أحكام هذا الملحق (البروتوكول) أو أية قاعدة أخرى من قواعد القانون الدولي الإنساني التي يلتزم بها الطرف السامي المتعاقد"، وبناء على ذلك، تخضع الهجمات السيبرانية لمبادئ القانون الدولي الإنساني التي تحكم سير العمليات القتالية باعتبارها وسائل وأساليب حديثة للقتال عندما تستخدم في النزاعات المسلحة[68]، مع استثناء الأجهزة والبنية التحتية التي تشكل أهدافا عسكرية من الحماية، ولكن حق أطراف النزاع في اختيار أساليب ووسائل القتال غير مطلق بل يخضع للقيود التي يفرضها القانون الدولي الإنساني[69]، وهو ما يعرف بمبدأ "تقييد حق أطراف النزاع في اختيار الوسائل والأساليب التي يرغبون في استخدامها"، حتى لا يتم الإضرار بالمدنيين والأعيان المدنية، أما في حالة عدم وجود نزاع مسلح قائم فقد ترتقي الهجمات السيبرانية لتكون نزاعا مسلحا بالنظر إلى أثرها على حياة المدنيين[70]، ومن ثم تنطبق قواعد ومبادئ القانون الدولي الإنساني على الهجمات السيبرانية التي تستهدف الأشخاص المتمتعين بحماية خاصة، والأعيان المدنية، باعتبارها وسيلة وأسلوب للحرب ما تنتج نفس الآثار الذي يمكن أن تنتج عن الأسلحة التقليدية من دمار وانقطاع الخدمات الحيوية والأضرار أو الإصابة أو الوفاة.

كما يمكن الاستناد إلى المبادئ الأساسية الأخرى للقول بخضوع الهجمات السيبرانية للقانون الدولي الإنساني، ولعل أهم هذه المبادئ: مبدأ التمييز بين المدنيين والمقاتلين[71]، و"شرط مارتنز"[72]، الذي يعتبر من قبيل القانون العرفي[73]، بحيث ورد في ديباجة اتفاقية لاهاي لعام 1899، وفي صلب البروتوكول الإضافي الأول لعام 1977، وفي ديباجة البروتوكول الثاني لعام 1977، والذي جاء فيه: "في حالة عدم وجود قاعدة معينة في القانون الاتفاقي، يظل المدنيون والمقاتلون تحت حماية وسلطان مبادئ القانون الدولي كما استقر بها العرف ومبادئ الإنسانية وما يمليه الضمير العام".

---

[68] نور أمير الموصلي، الهجمات السيبرانية في ضوء القانون الدولي الإنساني، مرجع سابق، ص 31.

[69] المادة 53 من البروتوكول الإضافي الأول الملحق باتفاقيات جنيف الأربعة لعام 1949.

[70] يحي مفرح الزهراني، الأبعاد الاستراتيجية والقانونية للحرب السيبرانية، مرجع سابق، ص 242.

[71] Oriane Barat-Ginies, Existe-t-il un droit international du cyberespace?, La Découverte, 2014, n°1, p. 213.

[72] وضع البروفسور فيودوروفيتش مارتنز المندوب الروسي لدى مؤتمر لاهاي للسلام سنة 1899 هذا الشرط بعد ما فشل المندوبون في مؤتمر السلام في الاتفاق على مسألة مركز المدنيين الذي يحملون السلاح ضد قوات الاحتلال، حيث رأت الدول العسكرية الكبرى أنه يجب أن يعامل هؤلاء المدنيون بوصفهم جنودا غير نظاميين يخضعون لعقوبة الإعدام، في حين رأت الدول الأخرى أنه يجب معاملتهم بوصفهم محاربين نظاميين، ونتيجة لذلك الخلاف قام المندوب الروسي "مارتنز" بطرح رأيه الذي أصبح يعرف بشرط "مارتنز".

[73] نيلس ميلزر، القانون الدولي الإنساني، اللجنة الدولية للصليب الأحمر، 2016، ص 119.

وقد أكدت محكمة العدل الدولية في رأيها الاستشاري الصادر بشأن مشروعية التهديد بالأسلحة النووية أو استخدامها من جهة على "شرط مارتنز" الذي لا يمكن الشك في استمرار وجوده وقابليته للتطبيق، وبأن هذا الشرط يعد وسيلة فعالة لمواجهة التطور السريع في التكنولوجيا العسكرية، ومن ثم فإن مبادئ القانون الدولي الإنساني تنطبق على جميع أشكال الحروب، وعلى جميع الأسلحة –بما في ذلك تلك المستقبلية" التي لم يتمكن المجتمع الدولي من حظرها أو تقييد استخدامها، فمبادئ وقواعد القانون الدولي الإنساني قد وضعت قبل الأسلحة النووية، ومع ذلك لا يوجد شك حول انطباق القانون الدولي الإنساني على هذه الأسلحة الفتاكة، وعلى تقنيات أي أسلحة ناشئة[74]، وليس هناك ما يدعو للتمييز بين الأسلحة النووية والهجمات السيبرانية، من حيث الزمن الذي استحدثت فيه[75]، ومن حيث الآثار المدمرة الناتجة عنهما، بل أن آثار الهجمات السيبرانية قد تكون أكثر جسامة وأكثر ضررا إذا استهدفت المحطات النووية على نطاق واسع، وهو ما جعل محكمة العدل الدولية تركز في رأيها على الطبيعة التدميرية للسلاح وعلى الأضرار اللاحقة بالبشرية الناتجة عن استخدامه بصرف النظر عن الوسيلة في حد ذاتها.

وبالتالي، فعدم وجود قواعد مكتوبة في القانون الدولي الإنساني خاصة بالهجمات السيبرانية لا يعني أنها مباحة طالما أنها تتعارض مع مبادئ الإنسانية وما يمليه الضمير العام باعتبارها مبادئ تقييدية، وهنا تظهر أهمية "شرط مارتنز" باعتبارها جزء من الأهمية الجوهرية لمبادئ القانون الدولي الإنساني التي تقدم الحل بالاستقراء للحالات المستجدة وتسهم في سد ثغرات القانون وتساعد في تطوره مستقبلا بتبيان المسار الذي ينبغي إتباعه، وهي تمثل في هذا الإطار القانوني أبسط الأسس الإنسانية التي يمكن أن تطبق في كل زمان ومكان وتحت جميع الظروف[76]، فالقانون الدولي الإنساني تعامل مع التطورات والتغيرات السابقة في التكنولوجيا المستخدمة في النزاعات المسلحة، بمعنى أن القانون القائم قادر على التعامل مع هذه التطورات الجديدة دون الحاجة إلى إشعار أو وضع قواعد قانونية خاصة بالفضاء السيبراني.[77]

وقد أشارت محكمة العدل الدولية في رأيها الاستشاري حول مشروعية التهديد بالأسلحة النووية أو استخدامها بصورة ضمنية إلى انطباق مبادئ القانون الدولي الإنساني على الهجمات السيبرانية رغم اختلاف

---

[74] نيلس ميلزر، القانون الدولي الإنساني، اللجنة الدولية للصليب الأحمر، مرجع سابق، ص 119.

[75] نور أمير الموصلي، الهجمات السيبرانية في ضوء القانون الدولي الإنساني، مرجع سابق، ص 32.

[76] يحي ياسين سعود، الحرب السيبرانية في ضوء القانون الدولي الإنساني، مرجع سابق، ص 91.

[77] كوردولا دروغيه، ما من فراغ قانوني في الفضاء السيبراني، اللجنة الدولية للصليب الأحمر، 2011، على الموقع:
https://www.icrc.org/ar/doc/resources/documents/interview/2011/cyber-warfare-interview-2011-08-16.htm

ميدانها عن باقي ميادين الحروب التقليدية الأخرى[78] بقولها "عن مبادئ وقواعد القانون الدولي الإنساني المنطبق في النزاع المسلح تنطبق على كل أشكال الحرب وكل أنواع الأسلحة...بما في ذلك تلك المستقبلية".

إن العمليات السيبرانية سواء ارتكبت في السلم أو في الحرب- شأنها شأن أي أسلحة أو وسائل أو أساليب حرب أخرى جديدة كانت أم قديمة-، تخضع في تنظيمها للقانون الدولي الإنساني الذي يوفر شريحة إضافية من الحماية ضد آثار الأعمال العدائية، بحيث تنطبق مبادئ القانون الدولي الإنساني التي تحكم سير ووسائل الأعمال العدائية، بما فيها مبادئ التمييز والضرورة، والتناسب على جميع العمليات العسكرية سواء كانت حركية أو ذات طابع سيبراني، فيجب على أطراف النزاع المسلح التمييز بين المدنيين والمقاتلين، وبين الأعيان المدنية والأهداف العسكرية[79]، ومن ثم يكون توجيه العمليات العسكرية نحو الأهداف العسكرية دون غيرها[80]، وهذا ينطبق على جميع الأنشطة العسكرية سواء أكانت حركية أو سيبرانية، فالهجمات السيبرانية يجب أن تقتصر على الأعيان العسكرية، والأعيان ذات الاستخدام المزدوج، -الأعيان المدنية التي تستخدم لأغراض عسكرية في الوقت نفسه- طوال هذا الاستخدام .[81]

ويجب على أطراف النزاع المسلح الموازنة بين الضرورة العسكرية والاعتبارات الإنسانية لتحقيق "الميزة العسكرية" بأقل تكلفة في الأرواح والأعيان[82]، فيكون استخدام القوة بالقدر اللازم لتحقيق الهدف المقصود والمشروع من النزاع المسلح وهو إخضاع العدو بصورة كاملة أو جزئية وبأقل قدر ممكن من التضحية في الأرواح والموارد، وبالتالي يمنع في هذا الخصوص تدمير ممتلكات العدو أو حجزها، إلا إذا كانت ضرورات الحرب تقتضي حتماً هذا التدمير والحجز، ويرتبط بما سبق مراعاة مبدأ التناسب، أي حظر الهجوم الذي قد يتوقع منه أو يسبب بصورة عرضية خسائر في أرواح المدنيين أو إصابات بينهم أو أضرار بالأعيان المدنية، أو قد يسبب مجموعا من هذه الخسائر والأضرار تكون مفرطة مقارنة بالميزة العسكرية التي يحققها ذلك الهجوم، وقد تضمن دليل "تالين" قاعدة تحظر الهجمات الإلكترونية التي قد تسبب خسائر كبيرة في الأرواح أو الأعيان

---

[78] يحي مفرح الزهراني، الأبعاد الاستراتيجية والقانونية للحرب السيبرانية، مرجع سابق، ص 242.

[79] Oriane Barat-Ginies, Existe-t-il un droit international du cyberespace?, op. it., p. 215.

[80] المادة 48 من البروتوكول الإضافي الأول لعام 1977 الملحق باتفاقيات جنيف الأربعة لعام 1949؛ حول مبدأ التمييز بين المدنيين والمقاتلين وبين الأعيان المدنية والأهداف العسكرية، انظر: نيلس ميلزر، القانون الدولي الإنساني، اللجنة الدولية للصليب الأحمر، 2016، ص ص 77-98.

[81] القاعدة 39 من دليل "تالين".

[82] المادة 2/52 من البروتوكول الإضافي الأول لعام 1977 الملحق باتفاقيات جنيف الأربعة لعام 1949.

مقارنة بالنتائج العسكرية التي تحققها تلك الهجمات[83]، وتجدر الإشارة أن الهجمات السيبرانية على الأعيان ذات الاستخدام المزدوج تشكل تحديا للقانون الدولي الإنساني بالنظر إلى صعوبة التمييز بين الجزء من الشبكة الإلكترونية الذي يستخدم لأغراض عسكرية، والجزء الذي يستخدم لأغراض مدنية، وبالتالي تصبح الشبكة بأكملها هدفا عسكريا، وهو ما قد يترتب عنه أضرارا للسكان المدنيين في حالة المساس بالبنية التحتية المدنية التي لا غنى عنها لبقاء السكان المدنيين[84].

ويتمتع السكان المدنيون والأعيان المدنية، والأشياء التي لا غنى عنها لبقاء السكان المدنيين بحماية خاصة بموجب القانون الدولي الإنساني[85]، بحيث تكفل مبادئ القانون الدولي الإنساني حماية قوية للبنية التحتية المدنية الحيوية ضد آثار الهجمات السيبرانية في أثناء النزاعات المسلحة، ويجب ألا تستخدم الأسلحة والهجمات العشوائية، وتحظر الهجمات غير المتناسبة، كما يجب على المتحاربين احترام وحماية الوحدات والمنشآت الطبية والعاملين فيها في جميع الأوقات، وبالتالي فإن الهجمات السيبرانية ضد الأشخاص والأعيان المحمية أثناء النزاع المسلح تمثل في معظم الأحوال انتهاكا للقانون الدولي الإنساني[86]، كما ينطبق القانون الدولي الإنساني على البيانات المدنية المتعلقة بالأعيان التي لا تتمتع بحماية خاصة، مثل بيانات الضرائب والسجلات المصرفية على أساس مبدأ "تمتع السكان المدنيين بحماية عامة من آثار الأعمال العدائية"[87]، وأي استثناء لهذه البيانات من الحماية التي يوفرها القانون الدولي الإنساني، من شأنه أن يؤدي إلى ثغرة كبيرة في نظام هذه الحماية[88].

خاتمة

يعد الفضاء السيبراني ساحة من ساحات الصراع الجديدة بين الدول سواء أثناء السلم أو خلال النزاعات المسلحة، والتي تستخدم فيها الهجمات السيبرانية كوسيلة حاسمة لإخضاع الدول، من خلال استهداف البنى

---

[83] يحي ياسين سعود، الحرب السيبرانية في ضوء القانون الدولي الإنساني، مرجع سابق، ص 94.

[84] Elena Volkova, Protection des infrastructures de santé contre les cyberattaques dans les conflits armés, en ligne : https://en.calameo.com/books/006401546497064e46e94 », p. 8.

[85] حمدان إيمان، التكنولوجيات الجديدة والقانون الدولي الإنساني (الحرب السيبرانية)، ماجستير في القانون الدولي الإنساني، الجامعة الافتراضية السورية، 2020، ص 9.

[86] الحرب السيبرانية: القانون الدولي الإنساني يوفر طبقة إضافية من الحماية، بيان ألقته السيدة "فيرونيك كريستوري"، كبيرة مستشاري الحد من التسلح في اللجنة الدولية أمام "الفريق العامل المفتوح العضوية المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي" – نيويورك، 10 سبتمبر 2019، على الموقع:
https://www.icrc.org/ar/document/cyber-warfare-ihl-provides-additional-layer-protection

[87] المادة 1/51 من البروتوكول الإضافي الأول لسنة 1977 الملحق باتفاقيات جنيف لسنة 1949.

[88] حمدان إيمان، التكنولوجيات الجديدة والقانون الدولي الإنساني (الحرب السيبرانية)، مرجع سابق، ص 9.

التحتية سواء أكانت العسكرية منها أو المدنية، مما يترتب عنها آثار وخيمة عابرة للحدود، قد تصل إلى حد تهديد السلم والأمن الدوليين، ولعل أبرز دليل على ذلك الحرب السيبرانية الدائرة اليوم بين روسيا وأوكرانيا، من ثم تطرح مسألة تكييف هذه الهجمات بقوة في ظل غياب اتفاقية دولية خاصة حول الموضوع، وقد توصلنا إلى جملة من النتائج والاقتراحات التي نراها ضرورية لتقوية النظام القانوني لتأطير الهجمات السيبرانية المرتكبة من طرف دولة ضد دولة أخرى سواء وقت السلم أو أثناء الحرب.

للفضاء الإلكتروني عدة إيجابيات في مختلف المجالات، لكنه قد يشكل عامل توسيع لنطاق التهديدات والأخطار المحدقة على المجتمع الدولي برمته بسبب الهجمات السيبرانية المنفذة من طرف الدول أو الجهات الفاعلة من غير الدول وقت السلم أو خلال النزاعات المسلحة، فقد تلجأ الدول زمن السلم إلى تنفيذ هجمات سيبرانية ضد دولة أخرى بغرض سرقة لمعلومات أو التجسس أو إثارة الاضطرابات والفوضى فيها، وهو ما يشكل تدخلا في شؤونها الداخلية، ومن ثم انتهاكا لسيادتها، كما تعد الهجمات السيبرانية واسعة النطاق التي تتسبب في أضرار جسيمة للسكان المدنيين والأعيان المدنية –سواء زمن السلم أو أثناء النزاعات المسلحة– استخداما للقوة بأسلحة غير حركية، والتي قد تتجاوز في حجمها وآثارها في بعض الحالات الأضرار الناجمة عن استخدام القوة بالوسائل الحركية، ومن ثم تدخل ضمن مجال الحظر الوارد في المادة 2 الفقرة 4 من ميثاق الأمم المتحدة، وهو ما يتيح للدول فرادى أو في إطار جماعي اتخاذ التدابير والإجراءات اللازمة لوقف تلك الهجمات، وإثارة المسؤولية الدولي للدولة المعتدية.

يترتب على تكييف بعض الهجمات السيبرانية الشديدة التي ترتكب زمن السلم، أو تلك التي ترتكب بالموازاة مع نزاع مسلح بوسائل تقليدية، وجوب تطبيق قواعد ومبادئ القانون الدولي الإنساني، التي تفرض التزامات محددة على أطراف النزاع بهدف حماية الفئات الضعيفة والأعيان المدنية والطبية، بحيث أن أي انتهاك لها يرتب المسؤولية الدولية للدولة التي ارتكبت الهجمات.

وعليه، فإن الأحكام القانونية الدولية السارية المفعول والقابلة للتطبيق على الهجمات السيبرانية المرتكبة من طرف الدول ضد دول أخرى، موزعة بين قواعد ومبادئ القانون الدولي العام وقواعد ومبادئ القانون الدولي الإنساني، غير أن هذه الأحكام في حاجة إلى تعزيز وتقوية بما يتلاءم وطبيعة وخصائص الهجمات السيبرانية كهجمات سريعة يصعب إسنادها إلى الدول، وهذا عن طريق إبرام اتفاقية دولية في إطار الأمم المتحدة خاصة بموضوع الفضاء السيبراني وشاملة لكل جوانبه بما فيه الهجمات السيبرانية والمسؤولية الدولية للدول، والمسؤولية الجنائية الدولي للأفراد، بالإضافة إلى التعاون الدولي في المجال الإلكتروني بغرض الكشف عن الدول المعتدية.