

العدوان في القانون الدولي والهجمات السيبرانية بين الدول

Aggression in international law and cyber-attacks between states



الدكتور/ دخلافي سفيان^{2,1}

Dr./ Dekhlafi Sofiane

¹ جامعة تيزي وزو، (الجزائر)

University of Tizi Ouzou, (Algeria)

² المؤلف المراسل (author correspondent): sofiane.dekhlaifi@ummto.dz

تاريخ الاستلام: 2022/10/09 تاريخ القبول للنشر: 2023/01/22 تاريخ النشر: 2023/09/28



مراجعة الهقال: اللغة العربية: أ.د. / كمال بن عمر (جامعة الوادي) اللغة الإنجليزية: د. / محمد أكرم عربات (جامعة سطيف 2)

ملخص:

أصبح الفضاء السيبراني ساحة صراع جديدة بين الدول، تستعمل فيه الهجمات السيبرانية كوسيلة بديلة للتحايل على الحظر المفروض على استخدام القوة في العلاقات الدولية بدون مبرر، وقد ازدادت هذه الهجمات في السنوات الأخيرة في زمن السلم سواء من حيث عددها أو من حيث شدتها وآثارها الوخيمة على الدول المستهدفة، بل أصبحت تشكل تهديدا للسلم والأمن الدوليين، وأمام غياب اتفاقية دولية حول الموضوع، فإن مسألة تأطيرها في القانون الدولي تعد ضرورة ملحة وذات أولوية، وذلك من خلال تبني نظام قانوني خاص بها يتماشى مع القانون الدولي ومبادئه السارية المفعول، كمبدأ حظر استخدام القوة، وحظر العدوان، وهذا يتطلب توسيع مفهوم العدوان ليشمل الهجمات السيبرانية نظرا للتشابه بينها وبين الهجمات التقليدية من حيث طبيعتها باعتبارها أسلحة غير حركية تستهدف إحداث نفس الآثار في الواقع الملموس، وقد تتجاوز أحيانا آثار الهجمات التقليدية، بحيث يمكن أن تشكل من الناحية القانونية عدوانا يرتب المسؤولية الدولية للدولة المعتدية إلى جانب المسؤولية الجنائية للأفراد.

الكلمات المفتاحية: حظر استخدام القوة؛ العدوان؛ الفضاء السيبراني؛ الهجمات السيبرانية.

Abstract:

Cyberspace has become a new conflict between States, using cyberattacks as an alternative means of circumventing the unjustified prohibition of the use of force in international relations. These attacks have increased in recent years in peacetime, both in terms of their number and severity and their adverse impact on the target States. international peace and security, and in the absence of an international convention on the subject international law ", the question of its framing in international law is an urgent and priority necessity, Through the adoption of its own legal regime consistent with international law and its applicable principles as the principle of prohibiting the use of force and the prohibition of aggression, which requires extending the concept of aggression to cyberattacks because of their similarity to conventional attacks in nature as non-

motor weapons aimed at producing the same effects in concrete fact, The effects of conventional attacks may sometimes exceed, so that they can legally constitute aggression that entails the aggressor State's international responsibility as well as the criminal responsibility of individuals.

Key words: Prohibition of the use of force; aggression; cyberspace; cyberattacks.

مقدمة:

تقوم العلاقات الدولية في الوقت الراهن أساساً على التعايش السلمي بين الدول المتساوية في السيادة، وهي محمية بالتزام عدم التدخل في شؤونها الداخلية والخارجية، وأي نزاع دولي يتم حله عن طريق الحلول السلمية، ومع ذلك مازالت الحروب تشكل الأسلوب المفضل لحل النزاعات الدولية رغم حظر استخدام القوة بموجب ميثاق الأمم المتحدة، ولم يعد يقتصر هذا الأسلوب على استخدام الجنود والآليات المتحركة، بل تطور إلى أساليب أخرى تتم في الفضاء الإلكتروني غير المرئي.

فقد أدى التقدم السريع الحاصل في مجال المعلومات والاتصالات إلى حدوث تغيرات إيجابية وسلبية كبيرة في جميع المجالات، فلم يعد يقتصر دور هذا التطور على خدمة البشرية من خلال تطوير وتحسين أداء البنية التحتية، وإنما ظهر الجانب السلبي الذي أصبح يشكل تهديداً صريحاً لسيادة الدول ولأمنها القومي بسبب الهجمات السيبرانية التي تستهدف مصالحها الحيوية والإستراتيجية، فقد أصبح الفضاء السيبراني اليوم مجالاً جديداً للصراع بين الدول مثله مثل المجال البري والبحري والجوي، والفضاء الخارجي، بحيث تلجأ بعض الدول في زمن السلم إلى الفضاء الإلكتروني لشن هجمات معقدة ضد دول أخرى ترقى إلى مستوى النزاع المسلح من حيث الآثار أو تجري في سياقها، وذلك بواسطة استخدام الكمبيوتر أو الشبكات أو الأنظمة ذات الصلة بهدف تعطيل أو تدمير أو التحكم في البنية التحتية للكمبيوتر أو تدمير سلامة البيانات أو سرقة المعلومات المحمية، من أجل إحداث اضطرابات في عمل الأنشطة والخدمات العامة والخاصة للدولة المستهدفة، ومن هذا المنظور يشكل هذا الفضاء عاملاً قوياً لتهديد السلم والأمن الدوليين.

أصبحت الهجمات السيبرانية المرتكبة وقت السلم تثير مخاوف الدول خاصة عندما تتجاوز آثارها المساس بالبيانات في أجهزة الكمبيوتر إلى خلق تأثير في العالم الحقيقي، وما يترتب عن ذلك من أضرار جسيمة للدولة المستهدفة، وقد أثبت الواقع أن عدداً من الدول كانت ضحايا لهجمات سيبرانية ضخمة متفاوتة من حيث الدرجة والضرر وجهت الاتهامات فيها إلى دول (العظامات، 2015، ص 17-18)، وهو ما دفع حلف شمال الأطلسي إلى الإعلان أكثر من مرة أن هناك مخاطر وشيكة لتهديدات غير تقليدية، وهي تمثل خطراً محدقاً وعدواناً وشيكاً، ومن أهمها الصواريخ الباليستية النووية الموجهة، بالإضافة إلى الهجمات السيبرانية التي تصيب أماكن إستراتيجية وحساسة، وهذه الأخيرة تعتبر الأهم والخطر. كما أعلنت الولايات المتحدة الأمريكية أنها قد تقوم بعمل عسكري للدفاع عن النفس أو الانتقام في حالة شن هجمات عليها ترعاها دول أخرى. مثل هذه المواقف وأمام المخاطر الكبيرة المحتملة الناجمة عن الهجمات

السيبرانية المرتكبة من طرف دولة ضد دولة أخرى وقت السلم خاصة في ظل غياب نصوص خاصة في القانون الدولي العام حول الموضوع، تثار إشكالية في غاية الأهمية تتعلق بـ:

مدى إمكانية تكييف هذه الهجمات في القانون الدولي باعتبارها عدواناً؟

وسنركز في هذا المقال على الهجمات السيبرانية الدولية التي ترتكها دولة ضد دولة أخرى وقت السلم، وبالتالي لن يتناول جرائم الإنترنت التي يحكمها القانون الجنائي الوطني كجرائم استغلال الأطفال في المواد الإباحية، والتصيد الاحتيالي، ولن يتناول الإرهاب السيبراني الذي تقوم به الجماعات المسلحة العابرة للحدود لحسابها الخاص.

حيث سنخصّص المبحث الأول حول واقع القانون الدولي فيما يتعلق بالعدوان والهجمات السيبرانية، أما المبحث الثاني فسنخصصه لمدى إمكانية تكييف الهجوم السيبراني بين الدول كعدوان طبقاً لقواعد القانون الدولي السارية.

المبحث الأول:

واقع القانون الدولي فيما يتعلق بالعدوان والهجمات السيبرانية

يقوم نظام الأمم المتحدة على حظر اللجوء إلى القوة أو التهديد بها في العلاقات الدولية، ويعتبر استخدام القوة الذي يكون على درجة عالية من الخطورة عدواناً يهدد السلم والأمن الدوليين (المطلب الأول)، ومع ظهور تكنولوجيات المعلومات والاتصالات في الفضاء السيبراني برزت تهديدات وتحديات قانونية جديدة بسبب الهجمات السيبرانية الخطيرة المرتكبة وقت السلم من طرف دولة ضد دولة أخرى في هذا الفضاء، خاصة في ظل غياب نصوص قانونية خاصة في القانون الدولي حول الموضوع (المطلب الثاني).

المطلب الأول: مفهوم العدوان في القانون الدولي العام

يملك مجلس الأمن الدولي وحده الترخيص باستخدام القوة في إطار نظام الأمن الجماعي، باستثناء حالة الدفاع الشرعي، فأى هجوم يحدث خارج الحالات التي يأذن بها مجلس الأمن، وحالات الدفاع الشرعي يعتبر لجوء غير شرعي للقوة (الفرع الأول)، وبالتالي يمكن تكييفه من طرف مجلس الأمن على أنه عدوان من دولة على دولة أخرى (الفرع الثاني).

الفرع الأول: حظر اللجوء إلى القوة

يعدّ حظر التهديد باستعمال القوة أو استخدامها في القانون الدولي السلمي-أي في غير وقت الحرب (الغنيمي، 1993، ص298) - قاعدة عرفية أمرة تم تقنينها في المواثيق الدولية (C.I.J., 27 juin 1986,)، وهو التزام في مواجهة كافة الدول (الموسى، 2004، ص15) erga omne، وتم تكمله هذا الالتزام بمبدأ آخر هو عدم جواز التدخل في شؤون الدول، ويعتبر ميثاق بريان كيلوج الذي وقعته خمسة عشر دولة في 27 أوت 1928 الذي منع الحرب كوسيلة للسياسة الوطنية، نقطة التحول من قانون الحرب JUS AD BELLUM إلى قانون ضد الحرب (AKOTO, 2015, p203 JUS CONTRA BELLUM)، وقد

تم تقنين مبدأ حظر استخدام القوة في المادة 2 الفقرة 4 من ميثاق الأمم المتحدة التي تعتبر حجر الزاوية في قانون الحرب المعاصر، حيث نصت على أن "يتمنع أعضاء الهيئة في علاقاتهم الدولية عن التهديد باستعمال القوة أو باستخدامها ضد سلامة الأراضي أو الاستقلال السياسي لأية دولة، أو على أي وجه آخر لا يتفق ومقاصد الأمم المتحدة".

إن أي تدخل في شؤون دولة أخرى مصحوب بوسيلة إكراه (القوة) يشكل انتهاكا لحظر اللجوء إلى القوة في العلاقات الدولية (C.I.J., 27 juin 1986, p205-29)، ومن ثم يجب على الدول الامتناع عن التدخل بقواتها العسكرية وأعوانها على إقليم دولة أخرى دون رضاها (C.I.J., 27 juin 1986, p228).

طرح تفسير نص المادة 4/2 من ميثاق الأمم المتحدة نقاشات كبيرة خاصة فيما يتعلق بنوع القوة المحظورة، هل يتعلق الحظر بالقوة العسكرية فقط، أم أنه يشمل وسائل الإكراه الاقتصادية، والسياسية والإيديولوجية؟، فإذا كانت غالبية التفسيرات تشير إلى أن المقصود من القوة في نص المادة 4/2 هي القوة العسكرية، إلا أن تفسيرات المادة 4/2 على ضوء لوائح الجمعية للأمم المتحدة خاصة اللائحة رقم 2625 بشأن العلاقات الودية والتعاون بين الأمم، واللائحة رقم 22/42 بشأن تعزيز فعالية مبدأ الامتناع عن استعمال القوة أو التهديد باستعمالها في العلاقات الدولية التي أيدت هذا الطرح، أضافت أن مبدأ عدم جواز التدخل في شؤون الدول (المادة 2/7 من ميثاق الأمم المتحدة) الذي يكمل مبدأ حظر اللجوء إلى القوة يطبق على صور أخرى من الإكراه (C.I.J., 27 juin 1986, p191)، وما يعزز هذا التفسير أكثر هو أن مصطلح القوة جاء في الفقرة 4 من المادة 2 عاما أي دون تحديد لنوعها، ولو كان قصد واضعي ميثاق الأمم المتحدة القوة "المسلحة" لأضافوا مصطلح "المسلحة" إلى جانب مصطلح "القوة" كما هو عليه الحال في المادة 51 من الميثاق نفسه، وبالتالي، فالحظر الوارد في المادة 4/2 يشمل جميع أنواع القوة والضغوط بما فيها الاقتصادية والسياسية كذلك (بوسلطان، من حفظ السلم عن طريق النصوص القانونية إلى ثقافة السلم، 2012)، وسواء أكانت مباشرة أم غير مباشرة، وحتى تلك التي لا تصل إلى درجة استعمالها، كالتهديد باستخدامها (بوسلطان، 2002، ص174)، فاللجوء إلى القوة ليس مشروعا في كل صوره (الغنيحي، 1993، ص299) (Alain, 1994, p880).

من الواضح أن الفقرة 4 من المادة 2 من ميثاق الأمم المتحدة لم تنص صراحة على الهجمات السيبرانية وهذا راجع بطبيعة الحال إلى حداثة الموضوع الذي لم يكن قد ظهر إلى الوجود عند تحرير الميثاق؛ غير أن هذه الفقرة عالجت مسألة المتغيرات والمشاكل التي يمكن أن تحدث مستقبلا والتي تشكل تهديدا باستعمال القوة أو استخدامها في أي مجال من مجالات ممارسة السيادة الوطنية، بما فيها الفضاء السيبراني الذي يعد ساحة جديدة للصراعات، بحيث يتعين البحث في كل حالة ما إذا كان استخدام "القوة" يتوافق أو لا مع مقاصد الأمم المتحدة" (Alain, 1994, p881)، ومن ثم يمكن إدراج حظر أي هجمات لا تتوافق مع مقاصد الأمم المتحدة ضمن مفهوم هذه الفقرة (AKOTO, 2015, p205)، بغض النظر عن طبيعتها.

الفرع الثاني: تكييف اللجوء إلى القوة كعدوان.

عرّفت الجمعية العامة للأمم المتحدة العدوان في اللائحة رقم 3314 الصادرة بتاريخ 14 ديسمبر 1974 على أن "استعمال القوة المسلحة من قبل دولة ما ضد سيادة دولة أخرى، أو ضد سلامتها الإقليمية أو استقلالها السياسي بأي شكل يتنافى مع ميثاق الأمم المتحدة مثلما قرر في هذا الميثاق"، مما يعني أن مجال تطبيق الفقرة 4 من المادة 2 من ميثاق الأمم المتحدة يقتصر فقط على حظر التهديد باستعمال القوة أو استخدامها ضد سلامة الأراضي أو الاستقلال السياسي لأية دولة أو على أي وجه آخر لا يتفق ومقاصد "الأمم المتحدة"، "ويقرر مجلس الأمن ما إذا كان قد وقع تهديد للسلم أو الإخلال به، أو كان ما وقع عملا من أعمال العدوان (...)" (المادة 39 من ميثاق الأمم المتحدة).

يعدّ تعريف العدوان الوارد في اللائحة 3314 أداة توجيهية ودليلا يستعين به مجلس الأمن -وفقا للميثاق- في مسألة وجود عمل من أعمال العدوان، مما يعني أن المجلس ليس ملزما بما ورد في التعريف حرفيا عند النظر بالمسائل المعروضة أمامه، بل إنه يحتفظ بسلطة كاملة في تقدير توافر العدوان من عدمه، ومن ثم، فإنه يجوز له أن يقرر بأن أعمالا أخرى تشكل عدوانا وفقا لأحكام الميثاق (خلف، 2010، ص35).

يشترط لتكييف أي عمل عدائي بأنه عدوان وفقا لتعريف الجمعية العامة، ومن ثم تطبيق قواعد المسؤولية الدولية للدولة، ارتكابه من طرف أحد أجهزة الدولة-شرط عدم وجود ظروف تحول دون عدم قانونية السلوك المخالف للالتزامات الدولية للدولة-، أو من طرف جهات فاعلة غير حكومية خاضعة بصورة كاملة ومطلقة للدولة التي تمارس رقابة فعلية على مرتكبي أفعال الاعتداء من خلال التعليمات والتوجيهات الصادرة عن أجهزة الدولة إلى هذه الجهات (116-109 p, 27 juin 1986, C.I.J.), كما تتحمل الدولة المسؤولية الدولية في حالة اعترافها أو اعتمادها اللاحق للأفعال المعنية.

وباعتبار العدوان انتهاكا للمادة 4/2 من الميثاق، فهو بذلك يعد عملا دوليا غير مشروع يتم عن طريق استخدام القوة المسلحة من طرف دولة ضد دولة أخرى دون مبرر، وقد جاءت المادة 3 من اللائحة 3314 بقائمة على سبيل المثال لا الحصر للأفعال التي يمكن أن تشكل عدوانا إذا قرر مجلس الأمن ذلك وفقا للمادة 39 من الميثاق، فاستخدام القوة بالمخالفة للمادة 4/2 من الميثاق قرينة بسيطة قابلة لإثبات العكس على وجود عدوان، فالعبرة بالتقييم اللاحق لمجلس الأمن حسب الظروف المحيطة بالوضع، كما تتضمن المادة 2 من اللائحة 3314 بندا بسيطا، بحيث يتطلب انتهاك المادة 4/2 حدا كافيا من الخطورة لتكييف الأعمال العدائية كعدوان، كما يشترط أيضا وجود قصد أو نية الاعتداء أو إحداث الضرر بالدولة المستهدفة (AKOTO, 2015, pp 213-215).

إنّ التعريف الوارد في المادة 3 من اللائحة 3314 يتعلق بالعدوان المباشر، بينما تفسير محكمة العدل الدولية لم يأخذ بحرفية النص بل استعملته لتعريف العدوان غير المباشر، حيث اعتبرت هذا التعريف قاعدة عرفية دولية لحظر العدوان غير المباشر، وهو "إرسال من قبل دولة أو نيابة عنها عصابات أو جماعات مسلحة، أو القوات غير النظامية أو المرتزقة الذين يشاركون في أعمال عسكرية ضد

دولة أخرى تبلغ في خطورتها الأعمال المذكورة أعلاه، أو الانخراط بأي شكل من الأشكال في مثل هذا الإجراء".

يتضح من هذا التفسير أن الأمر يتعلق بأعمال تدخل خارجي دون استعمال للقوة العسكرية، لكنها ذات خطورة مشابهة لخطورة العدوان المباشر (C.I.J., 27 juin 1986, p195)، وأهم ما يميزها هو أن الدولة المعتدية لا ترتكب أعمال العدوان بنفسها، وإنما تقوم بها بواسطة أطراف ثالثة ليسوا أعوانا لها سواء بحكم القانون أو الواقع، ويبدو أنهم يتصرفون بمبادرة منهم (C.I.J., 27 juin 1986, p110)، بحيث يمكن إثبات مشاركة الدولة في الأعمال العدائية من خلال الدعم المالي (C.I.J., 27 juin 1986, p107)، والتنظيم، والمساعدة والحث والتمويل والتشجيع، أو التسامح مع الأنشطة التخريبية أو الإرهابية (C.I.J., 27 juin 1986, p205). إن حدوث هجوم مسلح من طرف دولة على دولة أخرى يستتبع ردة فعل من الدولة المستهدفة، ومن مجلس الأمن الذي يتعين عليه التحرك لوقف ذلك الهجوم، غير أن الممارسة أثبتت أن هذا الأخير لم يكيف أي تهديد باستخدام القوة أو استخدامها بأنه عدوان إلا في حالات قليلة، وإنما لجأ لاستعمال أوصاف أخرى كتهديد السلم أو الإخلال به، بل وفي حالات أخرى حيث تم اللجوء إلى القوة العسكرية- ولأسباب سياسية- لم يتخذ أي قرار بشأنها، غير أن هذا لا يعني عدم وجود عدوان من الناحية الواقعية (المادة 2 من اللائحة 3314)، وهو ما يمكن أن ينطبق على الأنواع الأخرى من الهجمات المحتملة إذا ما توافرت على شروط العدوان، بحيث لا يعتبر عدوانا إلا أشد الأشكال وأخطرها للاستخدام غير المشروع للقوة (Jean-Pierre, PELLET Alain, FORTEAU Mathias, 2005, p17)، بحيث يجب أن يصل استخدام القوة إلى حد معين من الشدة، فلا يعتبر مثلاً حادث حدودي بسيط عدواناً (C.I.J., Affaire du temple de Préah Vihear , 1962 p6)، فوحده استخدام القوة العسكرية الأشد خطورة يمكن أن يكيف على أنه عدوان مسلح.

والجدير بالذكر أن نص المادة 39 من الميثاق لم يضع تعريفاً محدداً للعدوان، وبالتالي مقيدا لسلطة مجلس الأمن، بل تركته واسعاً حتى يتمكن مجلس الأمن في أعمال سلطته التقديرية في تكيف أي تصرف من شأنه تعريض سلامة الدول للخطر بما في ذلك الهجمات الإلكترونية (العظامات، 2015، ص11-12). وما يدعم هذا الموقف تعريف العدوان الوارد في المادة 8 مكرر من النظام الأساسي للمحكمة الجنائية الدولية، الذي نجده قد حصر العمل العدواني في استعمال القوة المسلحة من جانب دولة ما ضد سيادة دولة أخرى أو سلامتها الإقليمية أو استقلالها السياسي، أو بأي طريقة أخرى تتعارض مع ميثاق الأمم المتحدة (المادة 2/8 من النظام الأساسي للمحكمة الجنائية الدولية). وبالتالي يبدو أن هذا التعريف قد تجاهل صور العدوان الأخرى، ولم يساير التطورات المرتبطة بالتكنولوجيات الجديدة للحرب، كالعدوان الإلكتروني الذي لا يقل خطورة عن العدوان المسلح، بل وأشد خطورة منه في بعض الحالات (العصادي، 2021، ص28). ومع ذلك، فقد أشارت المادة 8 مكرر في متنها إلى القرار (3314) الصادر عن الجمعية العامة للأمم المتحدة، وهو ما يجعله يحتمل التأويل وإمكانية إدراج الهجمات السيبرانية ضمن التعريف، وذلك إما بفتح المجال لتطبيق المادة 4 من القرار (3314) التي تسمح لمجلس الأمن بإدراج أعمال جديدة إلى قائمة الأعمال العدوانية الواردة في المادة 8 مكرر/2، وإما بإدراج أعمال

عدوانية جديدة بالقياس مع القائمة المتضمنة في المادة 8 مكرر، بحيث يسمح لقضاة المحكمة بأن يبحثوا في أوجه التشابه بين الأعمال العدوانية المسلحة، وأعمال العدوان الحديثة (الهجمات الإلكترونية)، مثال لذلك قياس غزو دولة ما لدولة أخرى بقيام دولة ما بتركيب فيروس على الشبكات المعلوماتية العسكرية لدولة أخرى (خلوي، 2020، ص 127)، كما يمكن إدراج الهجمات الإلكترونية ضمن مفهوم العدوان عن طريق تبني قضاة المحكمة للتفسير الواسع لمصطلح (المسلحة) كعنصر ملازم للقوة في تعريف العدوان، وذلك بأن تحصر المحكمة مجال هذا المصطلح في هجمات تعطيل الأنظمة العابرة للحدود التي يترتب عنها أضرار مادية وخسائر في الأشخاص والممتلكات، كونها تشكل انتهاكا صارخا لميثاق الأمم المتحدة (خلوي، 2020، ص 130).

المطلب الثاني: غياب نصوص قانونية دولية خاصة بالهجمات السيبرانية

ظهرت الهجمات السيبرانية حديثا مع تطور استخدام الفضاء السيبراني الذي يعد مساحة افتراضية لأجهزة كمبيوتر مترابطة بعضها ببعض مشكّلة ما يعرف بالشبكة، بحيث أصبحت الشركات الخاصة، والإدارات العامة، وإدارة النقل الجوي، والطرق والسكك الحديدية، ومحطات توليد الطاقة والمياه، وأسلحة الحرب الجديدة كالطائرات بدون طيار، والصواريخ النووية، تعمل جميعها باستخدام أجهزة كمبيوتر متصلة بالشبكات المنتشرة، لدرجة أنها تعرض الدول لأخطار متعددة الأشكال وجديدة ناتجة عن ما يعرف "بالهجمات السيبرانية".

ويمكن وصف هذه الهجمات على أنها "الهجمات المنسوبة للدولة ضد شبكات الكمبيوتر لدولة أخرى من أجل إحداث أضرار مادية أو غير مادية متفاوتة في درجة الخطورة بالدولة المستهدفة". تتميز الهجمات السيبرانية بطابعها السري، بحيث أصبحت تتحدى المفاهيم التقليدية للحدود، والقوة، والتدخل في شؤون الدول، فلم تعد القوة الحركية ضرورية لإحداث أضرار جسيمة بالدولة المستهدفة، أو للتدخل في شؤونها الداخلية والخارجية، لذا فقد أصبح الفضاء السيبراني أرضا مفضلة للاشتباكات بين الدول، ومجالا خامسا للمواجهة بينها، حيث يمكن التأثير بسهولة في ميزان القوة حتى من طرف البلدان الصغيرة التي يمكنها الوقوف في وجه قوة عظيمة، فلم يعد الأمن الوطني لأي دولة مهما كانت قوتها في منأى عن تهديدات هذا الفضاء، وقد ظهرت الأبعاد العسكرية للهجمات السيبرانية في عدد من الحالات، فقد تعرضت استونيا سنة 2007 لهجمات إلكترونية واسعة أحدثت إخلالا كبيرا بالحياة الاقتصادية لهذا البلد، كما قامت إسرائيل في السنة نفسها بشن هجمات سيبرانية من أجل تحييد منظومة دفاع الطيران السورية والقيام بعمليات قصف لتجهيزات نووية سرية في سوريا.

رغم خطورة الوضع بسبب التهديدات الكبيرة للهجمات السيبرانية التي تشنها الدول ضد دول أخرى على السلم والأمن الدوليين، ومع ذلك، حتى الآن لم تؤخذ هذه الهجمات في الاعتبار بموجب القانون الدولي (Laura, 2014, p27)، فلا توجد اتفاقية دولية خاصة بالهجمات السيبرانية التي تشنها الدول.

تخضع الهجمات السيبرانية إلى الإطار العام للقانون الدولي، الذي يفرض سيطرة محدودة عليها خاصة في وقت السلم، بينما يفرض تحكما أكبر فيما يتعلق بالهجمات السيبرانية عندما يتم استخدامها

من قبل القوات المتحاربة أثناء النزاعات المسلحة وذلك بموجب قواعد القانون الدولي الإنساني (Laura, 2014, p9-10)، لاسيما المادة 36 من البروتوكول الإضافي الأول لسنة 1977 الملحق باتفاقيات جنيف الأربع لسنة 1949.

إنّ أحكام القانون الدولي الإنساني تطبق فقط على الهجمات السيبرانية التي ترتكب في إطار النزاعات المسلحة، ولا تشمل الهجمات التي تتم زمن السلم، فقد تلجأ أي دولة إلى استبدال الهجمات الحركية التي تتم بأساليب ووسائل حرب تقليدية بهجمات سيبرانية (Laura) (Les, Daniel, 2011, p57)، cyberttaques dans les conflits armées (2014)، يمكن تكييفها على أنها عدوان على دولة أخرى بطريقة غير مادية، ومع ذلك لا تنطبق عليها أحكام القانون الدولي العام بما فيها أحكام القانون الدولي الإنساني السارية المفعول (Szoke-Pellet, 2017/2018)، وبالتالي فهناك ثغرة في نظام الأمم المتحدة يمكن استغلالها من طرف الدول لشن عدوان إلكتروني دون تبعات دولية سواء من حيث المسؤولية الدولية الناجمة عن ذلك، أو من حيث الإجراءات المضادة الجماعية.

يرجع سبب وجود هذا الفراغ القانوني إلى عدم الاتفاق على مستوى الجماعة الدولية؛ فقد فشلت الدول في الاتفاق على تعريف مشترك للهجمات السيبرانية سيكون أساسا لأي نظام قانوني للموضوع في المستقبل، فلا يوجد قبول مؤكد لمصطلح "الحرب الإلكترونية" أو "الهجوم الإلكتروني"، مما يبقي على الغموض التام في تعريف الهجوم الإلكتروني (Clémentine, 2014, p4).

لم يتكيف القانون الدولي العام بعد مع الهجمات السيبرانية، فلا يمكن أخذها بعين الاعتبار إلاّ من خلال قراءة موسعة للقانون الدولي العام، فهناك من الناحية القانونية فجوة بين واقع القانون الدولي العام الذي يفتقر إلى قواعد حول الموضوع بسبب غياب اتفاقية دولية خاصة، مما جعل الأجهزة الرئيسية لمنظمة الأمم المتحدة كالجمعية العامة ومجلس الأمن ومحكمة العدل الدولية تمتنع عن الخوض في موضوع الهجمات السيبرانية، فلا تنظر محكمة العدل الدولية مثلا إلاّ في النزاعات بين الدول (المواد 33، 36/3 من نظام روما). أو المسائل القانونية المتعلقة بالقانون الدولي (المادتين 1/65، 96 من نظام روما)، بينما الهجمات السيبرانية لا ينظمها القانون الدولي، وبالتالي لا يمكن للدول أو المنظمات الدولية اللجوء إلى المنظمة الأممية في حالة وجود نزاع حول الموضوع، ومن جهة أخرى، هناك تطور ممارسات الدول في هذا المجال، من خلال الاستخدام المتزايد للهجمات السيبرانية بعضها ضد بعض.

إنّ وجود فراغ قانوني حول تكييف الهجمات السيبرانية كعدوان لم يمنع منظمة الأمم المتحدة من دعوة الدول إلى الاعتراف بأهمية وخطورة هذه الهجمات وبضرورة اتخاذ إجراءات مناسبة للحد منها، فقد طالب الاتحاد الدولي للاتصالات سنة 2010 بإنشاء معاهدة حول السلام على الإنترنت "cyberpaix" من أجل تجنب التصعيد بين الدول والإخلال بالسلام الذي قد يؤدي إلى حرب سيبرانية، وذلك من خلال التزام الدول بحماية رعاياها من هذه الهجمات، والتزامها بعدم إيواء أو حماية مستخدمي الإنترنت لأغراض إرهابية على إقليمها، والالتزام بعدم شن هجمات على دول أخرى (Hamadoun, 2010).

إنّ افتقار القانون الدولي إلى قواعد قانونية خاصة حول الهجمات السيبرانية لم يمنع الدول من تكييف بعض الهجمات التي حدثت في العالم بأنها عدوان، فقد وصف مسؤول القيادة الأمريكية

الإلكترونية في استونيا سنة 2007، أن ما تعرضت له استونيا "بهجوم مسلح حقيقي في الفضاء السيبراني معتبرا أنها تواجه عدوانا حقيقيا، وباعتبار استونيا عضو في منظمة شمال الأطلسي كان لديها الوقت في 2007 للاحتجاج بالمادة 5 من اتفاقية منظمة حلف شمال الأطلسي (Loïc, 2012, p120).

ظلت الهجمات الإلكترونية إلى غاية 2007 منخفضة وضد أهداف محددة جدا، بحيث تتم في الغالب بهدوء في أعمال تقليدية كسرقة المعلومات والبيانات، والتجسس عن طريق التنصت أو الاعتراض، وعرقلة أداء الخدمات من خلال حرمان المستخدمين من الوصول على خدمات معينة في الإنترنت دون إحداث أضرار مادية (AKOTO, 2015, p13-14)، لذا كانت الدول تميل إلى تكييفها على أنها تدخل في الشؤون الداخلية، أو انتهاك لمبدأ عدم التدخل (Szoke-Pellet, 2017/2018, p33).

لقد ظهرت استخدامات جديدة للهجمات السيبرانية أكثر شدة وأكثر انتشارا في العالم، وبأهداف مختلفة، بحيث أصبحت هذه الهجمات وسيلة مفضلة - نظرا لتكلفتها القليلة وصعوبة اكتشاف هوية منفذيها أو القائمين بها أو المتواطئين معهم سواء أكانوا دولاً أو كيانات من غير الدول- تستخدم وقت السلم والحرب بهدف إخضاع الدول عن طريق استهداف بنيتها الإلكترونية المدنية والعسكرية، فأهداف هذه الهجمات غير محددة كسرقة المعلومات أو التجسس، وإنما قد تستهدف شل وتعطيل عمل الأجهزة الحكومية والمرافق العمومية، كالهجمات الإلكترونية التي تعرضت لها استونيا وتكررت في جورجيا وإيران وأوكرانيا والعديد من الدول، وهو ما يطرح مسألة تشبيهها وإدراجها ضمن مفهوم العدوان في القانون الدولي.

المبحث الثاني:

ضرورة توسيع مفهوم العدوان إلى الهجمات السيبرانية

أصبحت الهجمات السيبرانية التي ترتكب بشكل مستقل عن أي نزاع مسلح أحد انشغالات المجتمع الدولي، خاصة مع انتشارها الواسع وازدياد شدتها، مما أدى إلى ظهور اتجاه قانوني-سياسي حديث يصف هذه الهجمات بالأعمال العدائية، ويعتبرونها هجمات مسلحة واستعمالا للقوة طبقا للفقرة 4 من المادة 2 من ميثاق الأمم المتحدة، بل يكييفونها في حالات معينة على أنها عدوان، ويسوقون في ذلك عدة مبررات لتوسيع مفهوم العدوان ليشمل الهجمات السيبرانية، سواء بسبب تشابه هذه الهجمات مع الهجوم المسلح الحركي التقليدي وقدرتها على قلب موازين القوى في العالم (المطلب الأول)، أو بالنظر إلى شدتها وآثارها الوخيمة على الأشخاص والدول المستهدفة (المطلب الثاني).

المطلب الأول: الهجمات السيبرانية سلاح قوي في ميزان العلاقات الدولية

تعدّ الهجمات السيبرانية في نظر بعض القانونيين وبعض الدول هجمات مسلحة كالهجمات الحركية التقليدية (الفرع الأول) لها من القوة والتأثير في العلاقات الدولية ما يجعلها تصنف ضمن أقوى الأسلحة الجديدة المستخدمة من طرف الدول بعضها ضد بعض (الفرع الثاني).

الفرع الأول: الهجمات السيبرانية كهجوم مسلح

تعدّ الشيفرات والفيروسات والديدان وأحصنة طروادة والقنابل المنطقية وغيرها من الفيروسات الخبيثة من الوسائل المتطورة المستخدمة من طرف دولة لشن هجمات سيبرانية وقت السلم ضد دولة أخرى، بحيث يمكن تكييفها في بعض الحالات على أنها "أسلحة" (Loïc, 2012, p123) بسبب قوتها التدميرية للبنى التحتية المدنية والعسكرية، فأتار هذه الهجمات لا يبقى على المستوى الافتراضي وإنما تصبح واقعا محسوسا، فبعدما كانت الهجمات العسكرية التقليدية وحدها من يسبب شلل في قدرات العدو، أصبحت اليوم الهجمات في الفضاء السيبراني شكلا جديدا من أشكال القوة (الصباحي، 2016) قادرا في حد ذاته ودون حاجة للقوة العسكرية المتحركة على إحداث شلل تام في القطاعات المستهدفة سواء أكانت عسكرية أم مدنية، وبالتالي فالهجمات السيبرانية الموجهة ضد الدول غرضها في الغالب الوصول إلى أهداف إستراتيجية، مما يفيد أن القائمين بها دول أو كيانات أخرى تعمل لصالح الدول.

شكلت الهجمات السيبرانية على استونيا وجورجيا وإيران نقطة تحول رئيسية في التعامل مع الهجمات السيبرانية بفعل الأدوات الجديدة التي تم استخدامها لشل هذه الدول، فقد تعرضت استونيا خلال شهر أبريل 2007 إلى عدوان غير مباشر بواسطة هجمات سيبرانية (هجمات التشيع) استهدفت المواقع الحكومية والخاصة الحيوية لإدارة الدولة (Laura, Les cyberattaques dans les conflits armés, 2014, p51)، أثرت على أداء أجهزة الدولة.

وتجدر الإشارة إلى أن استونيا وكثيرا من دول منظمة حلف شمال الأطلسي اتهمت روسيا بالوقوف وراء هذه الهجمات بالنظر إلى السياق الذي ارتكبت فيه، بحيث كان هناك توتر دبلوماسي حاد بين البلدين بسبب قرار استونيا بتغيير موقع تمثال الجندي البرونزي في تالين الذي يخلد مجد الجيش الأحمر، فالطابع المفاجئ والمنسق للهجمات، وكذلك حجمها، كل هذه العوامل توحى بأن هذا من عمل الدول.

وفي تطور آخر، تم الكشف عن طريقة أخرى أكثر شدة لاستخدام الهجمات السيبرانية، حيث تعرضت إيران لعدوان سري من طرف الولايات المتحدة الأمريكية سنة 2010 استخدمت فيه فيروس "ستكسنت" Stuxnet الإلكتروني عن طريق جهاز USB ضد البرنامج النووي الإيراني بغرض السيطرة على النظام الحاسوبي للمجمع النووي "بنطنز"، وبالأخص برنامج التحكم في أجهزة الطرد المركزي من أجل إحداث أضرار مادية بالبنية التحتية الإيرانية من خلال تعطيل وتدمير أجهزة الطرد المركزي عن طريق تغيير سرعة دورانها (AKOTO, Les cyberattaques étatiques constituent-elles des actes d'agression en vertu du droit international public, 2015, p17). وقد نجحت الولايات المتحدة في إحداث أضرار مادية معتبرة بالمجمع تمثلت في تدمير 100 جهاز طرد مركزي، مما يعني أن هناك تغييرا في وسائل الهجمات السيبرانية، فبعدما كانت هذه الهجمات تنطوي على مجرد أعمال تخريبية كالتجسس والتضليل الإعلامي، أصبحت تستهدف القيام "بأعمال تدميرية" لإحداث أضرار مادية جسيمة برعايا أو بممتلكات الدولة الضحية رغم أن الدول ليست في حالة حرب (Szoke-Pellet, 2017/2018, p38).

هناك وجه آخر للهجمات السيبرانية ظهر سنة 2008 أثناء حرب أوسيتيا الجنوبية بعدما طالبت هذه المنطقة الانفصالية باستقلالها عن روسيا، حيث شنت جورجيا هجوما مسلحا على روسيا لاستعادة المنطقة، وقدرت روسيا بنشر قواتها في هذه المنطقة باسم عملية السلام، وبالموازاة مع الحرب التقليدية على الواقع استخدمت روسيا هجمات سيبرانية لشل نظام المعلومات والاستخبارات والقيادة (Dominique, 2013, p32-49) الجورجية أثناء قيام قواتها العسكرية التقليدية بتدمير البنى التحتية الجورجية ماديا (LIMONIER Kévin, GERARD Colin, 2017,p9)، وهو ما يعرف "بالنزاعات الهجينة" Conflits hybride. وحسب منظمة شمال حلف الأطلسي، تمزج النزاعات الهجينة بين الحرب التقليدية وغير التقليدية، وبين الحرب النظامية وغير النظامية، وبين حرب المعلومات والحرب السيبرانية (Dugoin-Clément, 2016, p85)، وبالتالي يمكن اقتران استخدام الهجمات السيبرانية مع العمليات العسكرية التقليدية بغرض تدمير القدرات الإلكترونية للعدو وإحداث آثار تدميرية على أرض الواقع.

وقد كانت أوكرانيا مسرحا لحرب هجينة واسعة النطاق سنة 2014، حيث تعرضت لهجوم سيبراني استهدف المدنيين بالموازاة مع الحرب الحركية التقليدية بين القوات الأوكرانية والثوار الانفصاليين المدعومين من روسيا (Dugoin-Clément, 2016, p85-86)، كما استعملت روسيا في حربها ضد أوكرانيا بداية من فيفري 2022 الوسائل العسكرية وغير العسكرية كالهجمات في الفضاء السيبراني لزعة الحكومة في أوكرانيا، كما قامت هذه الأخيرة بهجمات سيبرانية مضادة على أجهزة ومواقع روسية لزعة المؤسسات وتعطيل الخدمات، وإحداث أكبر قدر ممكن من الفوضى (دنكر، 2022).

حسب تفسير محكمة العدل الدولية للمادة 4/2 من ميثاق الأمم المتحدة، فإن دعم دولة "لنشاطات عسكرية تخريبية أو إرهابية داخل دولة أخرى" (C.I.J, Affaire des Activités militaires et paramilitaires au Nicaragua et contre celui-ci , 27 juin 1986, p205) يشكل انتهاكا لحظر استخدام القوة، ومن ثم يمكن تشبيه الهجمات السيبرانية التي تعرضت لها كل من استونيا وجورجيا (وحتى أوكرانيا) بأعمال "تخريب" أو "تدمير" ضد "السلامة الإقليمية أو الاستقلال السياسي" لهاتين الدولتين (AKOTO, Les cyberattaques étatiques constituent-elles des actes d'agression en vertu du droit international public ?, 2015, p217).

يتضح من خلال ما سبق، أن هناك تطورات كبيرة في مجال الاستخدام غير المشروع للفضاء الإلكتروني ضد المصالح الحيوية للدول؛ فالهجمات السيبرانية لم تعد تقتصر على مجرد عمليات سرية للتدخل في الشؤون الداخلية من خلال أعمال التجسس وسرقة المعلومات والتضليل الإعلامي، بل أصبحت هذه العمليات تستعمل سواء وقت السلم أو بالاقتران مع نزاع مسلح (هجمات سيبرانية هجينة) كسلاح فعال بغرض إحداث تدمير مادي للبنى التحتية للدول، وهو ما ينتج عنه أضرار جسيمة بالأشخاص والأعيان قد تتجاوز الأضرار الناجمة عن الهجمات الحركية التقليدية (AKOTO, Les cyberattaques étatiques constituent-elles des actes d'agression en vertu du droit international public, 2015, p22).

الفرع الثاني: تشابه الهجمات السيبرانية مع الهجمات المسلحة من حيث القوة

أحدثت الهجمات السيبرانية التي تعرضت لها استونيا سنة 2007 صدمة لدى العديد من الدول، التي أدركت من جهة ضعف التحضير لمواجهة مثل هذه الهجمات (Frédéric, 2014, p9)، ومن جهة أخرى تزايد هذه الهجمات وقوتها في التأثير على الواقع المحسوس، بحيث أصبحت تشكل تهديدا فعليا للأمن الوطني لجميع الدول، بل تهديدا للسلم والأمن الدوليين (AKOTO, Les cyberattaques étatiques) constituent-elles des actes d'agression en vertu du droit international public ? : Deuxième partie, (2015, p230).

فبعد نجاح الهجمات السيبرانية في استونيا وجورجيا، تعرضت أوكرانيا سنة 2013 إلى هجمات مماثلة دفعت الحكومة إلى رفض الانضمام إلى اتفاق الشراكة مع الاتحاد الأوروبي، كما تسببت هذه الهجمات في اندلاع أعمال شغب انتهت باستقالة الحكومة وتعيين حكومة جديدة، كما طالبت العديد من المقاطعات في أوكرانيا التي تضم عددا كبيرا من السكان الناطقين بالروسية إلى طلب إجراء استفتاء للانضمام إلى روسيا. وقد كانت مقاطعة "القرم" أول مقاطعة تنفصل عن أوكرانيا وتنضم إلى روسيا، كما عبرت مقاطعات أخرى عن رغبتها في الانضمام إلى روسيا منها مقاطعة دونباس التي تعرضت سنة 2014 إلى حرب هجينة أو مختلطة استخدمت فيها الهجمات السيبرانية إلى جانب وسائل الحرب التقليدية (Clément, 2016, p 85,86).

إن الهجمات السيبرانية المنسوبة إلى روسيا ليست في الواقع سوى أمثلة، فالروس ليسوا وحدهم من يلجأ إلى هذا النوع الجديد من الهجمات، بل نجد كلا من إسرائيل والولايات المتحدة الأمريكية والصين قامت باستخدام هجمات إلكترونية ضد دول أخرى ومنظمات تقاوم السيطرة الاستعمارية. إدراكا من الدول بخطورة الموقف خاصة مع تكرار الهجمات السيبرانية في عدة دول، بدأت تضع استراتيجيات للدفاع عن سيادتها في الفضاء السيبراني لحماية أمنها الوطني والبنية التحتية الحيوية من أي اضطرابات أو تخريب قد يعرض حياة السكان للخطر، فالفضاء السيبراني أصبح يمثل تحديا استراتيجيا باعتباره منطقة للغزو والسيطرة والمراقبة والاستعادة، بحيث يكون من الضروري على الدولة فرض حدودها وسيادتها وقوانينها، لأنه يشكل فوق ذلك تهديدا لأمنها الوطني ولمصالح الأمة (Frédéric, 2014, p 9,10).

يشكل التحكم في المعلومات تحديا بالغ الأهمية، بحيث توفر القدرة على جمع المعلومات وتحليلها ومعالجتها ميزة استراتيجية للعدو وتجعله يشك في مصداقية معلوماته الخاصة، من خلال تعطيل الاتصالات بشكل مباشر، والتأثير على قدراته العملية التي تعتمد عليها الشبكات لتنسيقها وعملها. وفي هذا الإطار تعتبر الولايات المتحدة الأمريكية والصين في طليعة التقدم التكنولوجي والوعي بأهمية الفضاء السيبراني وبضرورة تبني استراتيجيات مناسبة -خاصة العسكرية- لمواجهة التحديات الناتجة عن الاستخدام الواسع لهذا الفضاء، وذلك بإدراج الهجمات لاسيبرانية ضمن هذه الاستراتيجيات.

ويتجلى هذا الوعي لدى الدول أيضا من خلال إنشاء المراكز السيبرانية، ولاسيما العسكرية التي تشهد على استعداد الدول لاستخدام الهجمات السيبرانية لأغراض عسكرية دفاعية أو هجومية (Szoke-Pellet, 2017/2018, p46)، فقد أنشأت الجزائر سنة 2004 المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني الذي يتوفر على مصلحة الإعلام الآلي لرصد ومراقبة وتتبع عمليات الاختراق والقرصنة المعلوماتية وكذا اكتشاف المعلومات المسروقة وتفكيك البرامج المعلوماتية، كما تم في سنة 2008 إنشاء مركز الوقاية من جرائم الإعلام الآلي للدرك الوطني، من أجل تأمين الأنظمة المعلوماتية والحفاظ عليها، ولاسيما تلك المستعملة في المؤسسات الرسمية والبنوك. وفي سنة 2011 أنشأت المصلحة المركزية لمكافحة الجريمة المعلوماتية التابعة لمديرية المن الوطني، كما أنشأت سنة 2015 الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها (عطية، 2020، ص 113-115).

وفي الولايات المتحدة الأمريكية أنشأت سنة 2010 "القيادة الإلكترونية الأمريكية"، و"وحدة العمليات العسكرية الإلكترونية" التابعة لوكالة الأمن القومي (NSA) التي قررت زيادة عدد العاملين فيها من 900 إلى 4900 خلال السنوات القادمة، وهو ما يعكس اهتمام الولايات المتحدة الأمريكية المتزايد بالهجمات السيبرانية.

ونظرا لخطورة الوضع خاصة بعد تعرض استونيا لهجمات السيبرانية، قررت منظمة شمال حلف الأطلسي في قمة لشبونة سنة 2010 تطوير القدرة على مواجهة هذه الهجمات بناء على طلب دولة عضو، كما تم التأكيد على ذلك خلال قمة شيكاغو سنة 2015، بحيث تم إنشاء "مركز التميز في الدفاع الإلكتروني لحلف شمال الأطلسي بتالين (استونيا) بهدف تحسين القدرات والتعاون وتبادل المعلومات داخل الحلف استعدادا للدفاع عن شبكاته ضد التهديدات والهجمات السيبرانية المتزايدة التعقيد التي يواجهها (l'OTAN).

يتضح من خلال ما سبق تزايد اهتمام المجتمع الدولي بالهجمات السيبرانية بسبب تزايد قوتها واستخدامها في شتى المجالات، ومن هنا تظهر الحاجة إلى تمديد نطاق مفهوم العدوان ليشمل هذه الهجمات بحيث ينظمها القانون الدولي، وقد أدركت الدول هذه الحاجة، فقد أكدت بشكل واضح كل من الولايات المتحدة الأمريكية سنة 2011 وفرنسا سنة 2013 أنه يمكن اعتبار الهجوم السيبراني على نطاق واسع كعمل حرب، وتحفظ بحقها في الرد بكل الوسائل (Frédéric, 2014, p15).

وقد أبدت روسيا والصين رغبتهما في التعاون من أجل تطوير "قواعد القانون الدولي" رغم الاختلاف القوي في الآراء في الوقت الحاضر مما يعرقل مثل هذا المشروع، ومع ذلك فمن الضروري للدول وضع نظام قانوني في ضوء تطور الهجمات السيبرانية والفضاء الإلكتروني الذي ينطوي على تحديات جيوسياسية تشابك بشكل وثيق مع الاعتبارات السياسية والاقتصادية والاجتماعية والثقافية. هذه التحديات التي يجب أن تؤخذ بعين الاعتبار لأنها تسمح بمعالجة كل هذه المسائل بكل تعقيداتها (Frédéric, 2014, p20)، فقد أصبح الفضاء الإلكتروني "قضية تنافس القوى بين الجهات الفاعلة" و"مسرح للمواجهة" بوسائل جد متطورة تتمثل في الهجمات السيبرانية باعتبارها "سلاح قوي" استخداماته تتصاعد بشكل متسارع بين الدول في مواجهة بعضها البعض.

لذا، وبالنظر إلى اعتبار الهجمات السيبرانية كأسلحة متطورة تستخدم وقت السلم من طرف دولة ضد دولة أخرى، وبالنظر إلى تطور أهداف هذه الأسلحة وانتشارها الواسع في العالم يتعين توسيع مفهوم العدوان ليشملها باعتبارها عملا حربيا.

المطلب الثاني: تشابه الهجمات السيبرانية مع الهجمات التقليدية من حيث الشدة والآثار.

تشابه الهجمات السيبرانية مع الهجمات التقليدية من حيث الشدة (الفرع الأول) والآثار الناجمة عن كليهما (الفرع الثاني) مما يجعل إدراجها ضمن مفهوم العدوان ضرورة عملية لمواجهتها.

الفرع الأول: شدة الهجمات السيبرانية

يشترط لتكييف عمل عدائي بأنه عدوان أن يكون على "درجة كافية من الشدة".

يمكن وصف استخدام القوة السيبرانية باعتبارها سلاحا بأنه عدوان عندما يتجاوز شدة معينة، ويكون له خطورة معينة، بالقياس على ما جاء في حكم محكمة العدل الدولية في قضية الأنشطة العسكرية في نيكاراغوا وضدها سنة 1986 بقولها هناك "أخطر أشكال استخدام القوة (تلك التي تشكل عدوان عسكري) وأخرى أقل وحشية" (C.I.J, Affaire des Activités militaires et paramilitaires au Nicaragua et contre celui-ci, 27 juin 1986, p191).

إنّ استخدام الهجمات السيبرانية -باعتبارها سلاحا من طرف دولة ضد دولة أخرى بغرض القيام بنشاطات تخريبية أو تدميرية يتعارض مع المفهوم الحديث للفقرة 4 من المادة 2 من ميثاق الأمم المتحدة، فالتخريب كقاعدة عامة يؤدي إلى زعزعة استقرار حكومة قائمة، ويمكن تفسيره على أنه عمل ضد الاستقلال الإقليمي أو السياسي للدولة المستهدفة كما حدث في استونيا سنة 2007 وجورجيا سنة 2008، بحيث تم منع هذه الدول من ممارسة سلطتها على جزء من فضاءها الإلكتروني الخاضع لسيادتها ومنع تقديم الخدمات للمواطنين، وهو ما يمكن تشبيهه بالأعمال التخريبية (AKOTO, Les cyberattaques étatiques constituent-elles des actes d'agression en vertu du droit international public ? , 2015, p217)، وبالنتيجة يجب أن يخضع اللجوء إلى الهجمات السيبرانية لنفس نظام الأسلحة التقليدية كونه يشكل عدوانا عندما يتجاوز شدة معينة.

إنّ ظهور أسلحة جديدة كالأسلحة النووية والكيميائية والإشعاعية والبيولوجية بعد تحرير المادة 4/2 من ميثاق الأمم المتحدة يقتضي تفسير وتحليل هذه المادة على ضوء هذه التطورات، فاستخدام الهجمات السيبرانية من طرف دولة ضد دولة أخرى يمكن تكييفه على أنه استخدام غير مشروع للقوة، فقد أعلنت محكمة العدل الدولية أن "ميثاق الأمم المتحدة لم يمنع ولم يسمح صراحة باستخدام سلاح بصفة خاصة" (C.I.J, Affaire des Activités militaires et paramilitaires au Nicaragua et contre celui-ci, 27 juin 1986), فاستخدام أي سلاح تقليدي أو حديث من طرف دولة ضد سلامة الأراضي أو الاستقلال السياسي لأية دولة أو على أي وجه آخر لا يتفق ومقاصد "الأمم المتحدة" يعد عملا غير مشروع دوليا، فالعبرة بطبيعة النتائج المباشرة المترتبة عن استخدام القوة خاصة الخسائر البشرية والتدمير المادي وليست بوسائل استخدام القوة (AKOTO, Les cyberattaques étatiques constituent-elles des actes d'agression en vertu du droit international public ? : Deuxième partie, 2015), فاستبدال

الدول للوسائل التقليدية بوسائل حديثة (الهجمات السيبرانية) لتحقيق نفس الأهداف لا يغير من تكييف العمل على أنه انتهاك لمبدأ حظر استخدام القوة؛ فتدمير المجمع النووي العراقي ومفاعل "أوزيراك" الخاص به بواسطة هجمات حركية تقليدية إسرائيلية (غارات جوية) سنة 1981 لا يختلف عن تدمير آلاف أجهزة الطرد المركزي في منشأة "نطنز" النووية الإيرانية بواسطة هجمات إلكترونية إسرائيلية - أمريكية سنة 2010.

إنّ شنّ حرب في الفضاء السيبراني من خلال أنظمة الكمبيوتر والبرامج الحاسوبية والبيانات لم تعد تتطلب المواجهة المباشرة بين القوات المسلحة، ولا عبور الحدود لغزو بلد؛ فتقييم العمل الحربي يتم عادة من حيث قتل المقاتلين أو الخسائر والدمار الذي لحق بالعدو، ومن هذا المنظور تتشابه الهجمات السيبرانية مع الهجمات التقليدية، فتشويش الاتصالات والهجمات على أنظمة التحكم في الحركة الجوية أو السيطرة على خطوط الأنابيب وشبكات توزيع الغاز، أو حتى على مصانع الإنتاج، وتصنيع المنتجات الأساسية للحياة الاقتصادية مثل الكيمياء الصناعية واستهداف أنظمة التحكم في البنى التحتية الحساسة وما يترتب عن ذلك من عواقب ضارة بالسكان المدنيين وبالمجتمع والأمن القومي لبلد ما، يمكن أن تعتبر أعمال حرب، إذا كانت الأوامر بارتكاب مثل هذه الهجمات صادرة عن دولة، بحيث تكون جزءا من إستراتيجية حرب الكمبيوتر الهجومية (Solange, 2011, p63).

إنّ اعتبار الهجمات السيبرانية أسلحة، واستخدامها يشكل لجوء للقوة، يجعلها تحتفظ بالوصف ذاته عندما ترتكب وقت السلم إذا تجاوزت حدا معيناً من الشدة بهدف الهيمنة، وهي بذلك ترتب نفس الآثار الوخيمة الناجمة عن الهجمات الحركية التقليدية (Szoke-Pellet, 2017/2018, p51)، فالهجمات السيبرانية عندما تستخدم كسلاح هجومي قد تسعى إلى تحقيق نفس الأهداف التي تسعى إليها الهجمات الحركية التقليدية، بحيث يمكن استخدامها كأداة مثالية لتحقيق نفس أهداف الهيمنة (AKOTO, Les cyberattaques étatiques constituent-elles des actes d'agression en vertu du droit international public, 2015, p1)، فالاختلاف الوحيد بينها، هو أنه إذا كانت الهجمات التقليدية الواردة في اللائحة رقم 3314 الصادرة عن الجمعية العامة للأمم المتحدة سنة 1973 تتجسد بالقصف والاجتياح وغيرها، فإن الهجمات السيبرانية تتجسد بواسطة عمليات غير حركية، كالاستحواذ أو السيطرة على الشبكات والاضطرابات والانقطاعات (Szoke-Pellet, 2017/2018, p52).

علاوة على ذلك، يمكن أن تقترن الهجمات السيبرانية الهجومية بالاستراتيجيات العسكرية الكلاسيكية من أجل إضعاف دفاعات الخصم وخداعه والمساهمة في تغيير قراراته، تحييد وحتى شل مراكز الاستراتيجيات، أو حتى منع وسائل الاتصالات، فكلما كانت الدول متقدمة كلما ارتبطت قدرتها العسكرية والاقتصادية بتكنولوجيا المعلومات، مما يجعلها غير محصنة من الهجمات الإلكترونية، وبالتالي تكون أكثر ضعفاً، مما يعني أن الفضاء السيبراني ساحة صراع مفتوحة على كل الاحتمالات بين الدول بغض النظر عن قوتها.

إنّ أجهزة الكمبيوتر التي يتم التحكم فيها عن بعد بعد السيطرة عليها بواسطة برامج حاسوبية أطلقها أوعاها الجيش ستكون مشابهة للمقاتلين المتسللين المتحكم فيهم عن بعد، لذلك يمكن أن تعتبر

قرصنة الكمبيوتر كسلاح حرب (Solange, 2011, p63)، بحيث تصبح الإنترنت وأجهزتها خلال الحرب وحدة عسكرية هجومية (Solange, 2011, p 65)، تستطيع تسخير ملايين الأشخاص كعملاء مخفيين للهيمنة وإخضاع العدو، وهو الهدف الرئيسي للهجمات الحركية.

من الواضح، أن الهجمات السيبرانية عندما تستخدم من طرف دولة أو برعايتها كأسلحة ضد دولة أخرى تشكل لجوء واستخداما غير مشروع للقوة طبقا للمادة 3 من لائحة الجمعية العامة للأمم المتحدة 3314، التي عرفت العدوان بأنه " استخدام أي أسلحة من طرف دولة ضد أراضي دولة أخرى"، فالمادة 3 لم تضع قائمة محدودة للأفعال التي تشكل عدوانا، بل تركت المجال مفتوحا لتكييف أي فعل غير مشروع بما فيها الهجمات السيبرانية يستهدف سلامة أراضي دولة أخرى أو استقلالها السياسي، وهو ما يتوافق مع تعريف اللجوء إلى القوة الذي قدمته محكمة العدل الدولية بقولها " أي تدخل غير قانوني في شؤون دولة أخرى مصحوب بوسيلة الإكراه التي هي القوة يشكل انتهاكا لحظر استخدام القوة في العلاقات الدولية" (AKOTO, Les cyberattaques étatiques constituent-elles des actes d'agression) (en vertu du droit international public ? , 2015, p204).

الفرع الثاني: تشابه الهجمات السيبرانية مع الهجمات التقليدية من حيث الآثار

تعتبر الأسلحة وسائل تستخدمها القوات المسلحة في النزاعات المسلحة وفي الحروب العدوانية ضد الدول، فالدبابات والطائرات والسفن الحربية، والبنادق والمدافع الرشاشة والمسدسات والصواريخ تعتبر وسائل قتال تستخدمها الدول للهجوم أو الدفاع عن نفسها.

تصنف الهجمات السيبرانية من وجهة نظر الجهات الفاعلة في القانون الدولي على أنها أسلحة مثلها مثل الوسائل التقليدية للهجوم الحركي (Szoke-Pellet, 2017/2018, p49)؛ فالهجمات السيبرانية هي أسلحة حسب الوجهة، أي حسب الاستخدام الذي تستخدم فيه، بغض النظر عما إذا كانت لها آثار حركية أو لا، فإذا ما استخدمت للهجوم أو الدفاع عن الشبكات والبنى التحتية لدولة ما، فهي أسلحة مثل غيرها من الأسلحة التقليدية، فالهجمات السيبرانية هي "سلاح يستخدم لتنفيذ التدمير المادي للبنى التحتية التي تعتمد على تقنيات المعلومات وتسبب في أضرار جانبية يمكن أن تكون جسيمة ولا يمكن السيطرة عليها (Dominique, 2013, p49).

كما تعتبر الهجمات السيبرانية أسلحة من قبل الخبراء في المجال، فقد اعتبرها الأستاذ "شميت" Schmitt استخداما للقوة إذا كانت أبعادها وتأثيراتها مماثلة لتلك التي كان يمكن الحصول عليها بعد استخدام القوة المسلحة (AKOTO, Les cyberattaques étatiques constituent-elles des actes d'agression en vertu du droit international public ? , 2015)، وهو نفس الطرح الذي تبناه دليل "تالين" (القاعدة 11 من دليل تالين المطبق سنة 2013)، والذي اعتبرها "عمليات إلكترونية هجومية أو دفاعية والتي يهدف من خلالها بصورة معقولة التسبب بالإصابة أو وفاة الأشخاص أو الإضرار أو تدمير الأعيان الأهداف"، وقد اعتبرتها اللجنة الدولية للصليب الأحمر والهلال الأحمر على أنها من جهة، استخدام عدواني للفضاء السيبراني يمكن أن تترتب عنه عواقب إنسانية وخيمة، ومن جهة أخرى قد تشكل هذه الهجمات في حد ذاتها -باعتبارها وسائل وأساليب للحرب- نزاعات مسلحة حقيقية، كما

اعتبرتها العديد من الدول كالولايات المتحدة الأمريكية وروسيا والصين وفرنسا أسلحة جديدة للحرب (Solange, 2011, p62)، بل ينظر إليها في بعض الأحيان على أنها أسلحة "مثالية" بسبب خصائصها الفريدة (إخفاء الهوية، السرعة، التقدير) (Laura, Les cyberattaques dans les conflits armés, 2014, p50)، قد تسبب في أثار وخيمة سواء على الأشخاص أو الأعيان.

ومن هذا المنظور، يبدو أن تصور المندوبين إلى مؤتمر سان فرانسيسكو سنة 1945 الذي انصب فقط على القوة العسكرية بأسلحة حرب معروفة وقت تحرير الميثاق، مما جعل الهجمات السيبرانية خارج مجال تطبيق المادة 4/2 باعتبارها استخداما للقوة غير الحركية، أصبح قديما لا يتماشى مع التطورات التكنولوجية والقانونية الراهنة لأنه لا يأخذ في الحسبان ظهور أسلحة جديدة بعد تحرير الميثاق (AKOTO, Les cyberattaques étatiques constituent-elles des actes d'agression en vertu du droit international public ? : Deuxième partie, 2015, p218)، وهي أسلحة غير مرئية لكنها فتاكة ومدمرة مثلها مثل أي سلاح حركي.

بالرجوع إلى أحكام القانون الدولي، فإن تصنيف الوسائل والأساليب المستخدمة في الحروب كأسلحة لا يخضع إلى ما إذا كانت ذات طابع حركي أو لا؛ فقد تعتبر أسلحة رغم عدم وجود أي تأثير حركي لها، ومن ثم يمكن تصور حدوث هجمات بأسلحة غير حركية، فالأسلحة النووية والأسلحة الكيميائية تعتبر وسائل حرب محظورة دوليا على الرغم من أنها لا تتوافق مع الهجمات التقليدية، مما يعني أنه يمكن أيضا اعتبار الهجمات الإلكترونية التي تتم بواسطة أجهزة الكمبيوتر وسائل للتدمير (Solange, 2011, p62) وأسلحة قادرة على أن تشكل استخداما للقوة مثلها مثل أي سلاح آخر حتى في غياب أي تأثير حركي لها. وقد أكدت محكمة العدل الدولية هذا الطرح في قضية مشروعية التهديد بالأسلحة النووية أو استخدامها سنة 1996 بقولها "أن اللجوء إلى القوة يمكن أن يكون أي استخدام للقوة بواسطة أي سلاح (حتى غير حركي)، وبناء على هذا يمكن اعتبار أي هجوم إلكتروني سلاحا، وبالتالي يعتبر لجوء إلى القوة (حتى غير حركي) ويخضع استخدامه لأحكام ميثاق الأمم المتحدة، بالنظر إلى آثارها السلبية في الواقع المحسوس.

وتجدر الملاحظة، أن الهجوم السيبراني واسع النطاق الذي يؤدي إلى شلل تام في الدولة المستهدفة، مما يعني أنه على قدر عال من الخطورة والقوة، وهو ما لا يمكن تحقيقه إلا من خلال هجوم تقليدي واسع النطاق باستخدام القوة بشكل كبير ومكثف، من جيوش نظامية ومعدات وآليات عسكرية حركية ثقيلة، ومن هنا تظهر أكثر عناصر التشابه بين الأسلوبين، وهو ما يتوافق مع مفهوم دليل تالين الذي أكد على "أن الهجوم السيبراني يشكل استخداما للقوة إذا كانت أبعاده والآثار مشابهة لتلك التي يمكن الحصول عليها بعد استخدام الأسلحة الحركية (Szoke-Pellet, 2017/2018, p219)، غير أنه يمكن تصور أن قوة الهجوم السيبراني بسبب سرعة تنفيذه وبسرية ونظافة وبأقل تكلفة، وبالنظر إلى شدته العالية جدا وآثاره الوخيمة على الدولة الضحية قد تتجاوز في بعض الحالات قوة وآثار الهجوم التقليدي.

ومن الناحية الواقعية يمكن استخدام هجمات إلكترونية من طرف دولة لتنفيذ عدوان ضد دولة أخرى، "فالتشويش على الاتصالات وهجمات الكمبيوتر على أنظمة مراقبة الطيران أو التحكم في خطوط

الأنابيب (...) يمكن اعتبارها أعمالاً حربية (Solange, 2011, p63)، واستخداماً للقوة نظراً لآثارها الحركية (N.Schmitt, 2012, p19)، أو غير الحركية كالأضرار الناتجة عن الهجوم على المواقع التي تقدم الخدمات الأساسية عن السكان (AKOTO, Les cyberattaques étatiques constituent-elles des actes d'agression en vertu du droit international public, 2015, p220)، بل أكثر من ذلك، فالهجمات السيبرانية الضخمة والهائلة والهجمات المضادة وإن لم تحدث بعد بسبب الردع السيبراني - إلا أنه يمكن تصور حدوث مثل هذه السيناريوهات في المستقبل، لذا من الخطأ التقليل من أهمية التهديدات الإلكترونية المحتملة في ميزان القوى بين الدول وفي تفاعل تحالفاتها وتوازناتها الجيوسياسية (AKOTO, Les cyberattaques étatiques constituent-elles des actes d'agression en vertu du droit international public, 2015, p64).

يتضح مما سبق، أن هناك تشابهاً بين الهجمات السيبرانية والهجمات الحركية في شدتها وآثارها، وهما شرطان ضروريان لاعتبار الهجوم السيبراني استخداماً للقوة بشكل خطير بما يكفي لتكييفه بأنه عدوان، فليست كل حالات اللجوء إلى القوة تكيف على أنها عدوان، ولكن فقط تلك التي تنطوي على درجة معينة من الشدة والتي يمكن تقديرها من خلال شدة آثارها في الواقع المحسوس بالمقارنة مع شدة وآثار الهجمات الحركية التقليدية. وفي هذا الإطار فقد اعتبرت محكمة العدل الدولية أن "مجرد اشتباكات على الحدود بين دولتين لا تشكل عدواناً (C.I.J., Affaire du temple de Préah Vihear, 1962, p195)، بينما الهجوم على كامل إقليم الدولة يمكن وصفه عدواناً، وهنا بالتحديد تشابه الهجمات السيبرانية واسعة النطاق عبر بلد بأكمله مع الهجوم التقليدي على كامل إقليم الدولة، فإذا توقفت شبكات المعلومات الحيوية عن العمل، سيصاب مجتمع المعلومات بالشلل وسرعان ما يفرق في الفوضى (AKOTO, Les cyberattaques étatiques constituent-elles des actes d'agression en vertu du droit international public, 2015, p1).

الخاتمة:

لقد عبرت الدول سنة 1945 عن رغبتها الملحة في استئصال الحرب من العلاقات الدولية باعتبارها عملاً دولياً غير مشروع، وقد كرست ذلك في المادة 4/2 من ميثاق الأمم المتحدة، حيث لم يعد بإمكان الدول استخدام القوة مباشرة دون مبرر، وإلا اعتبر ذلك انتهاكاً للالتزام دولي في مواجهة الكافة يستتبع مسؤوليتها الدولية.

أمام هذا الحظر، ومع تطور تكنولوجيا المعلومات والاتصالات ظهر ما يعرف بالفضاء السيبراني كمجال خامس للتنافس والصراع بين الدول، حيث لجأت بعض الدول للتحايل على الحظر المكرس في المادة 4/2، وذلك باللجوء المكثف والمتصاعد إلى الهجمات السيبرانية وقت السلم ضد دول أخرى، بحيث لم تعد هذه الهجمات تستهدف أعمالاً بسيطة وعادية كالتجسس وسرقة المعلومات، بل أصبحت تستخدم كوسيلة للحرب أو ضمن أساليب الحرب لشل الدول الأخرى وزعزعة استقرارها، وإلحاق أضرار مادية وغير مادية جسيمة بها سواء بشكل مستقل أو مرافق لهجوم حركي.

أصبحت الهجمات السيبرانية بديلا فعالا للهجمات التقليدية المباشرة، وهذا راجع من جهة إلى خصائصها الفريدة، والتي جعلت منها سلاحا سريا قليل التكلفة، وتصعب نسبته إلى الدولة، ومن جهة أخرى، عدم تأطير هذه الهجمات في القانون الدولي، على الرغم أنه من الممكن في بعض الحالات تطبيق القواعد والمبادئ العامة للقانون الدولي، كحالة ثبوت ارتكاب هجوم سيبراني من طرف دولة ضد دولة أخرى، وخلف ذلك الهجوم آثارا تتشابه مع الآثار التي يمكن أن يخلفها أي هجوم حركي، بحيث يمكن اعتباره استخداما غير مشروع للقوة، ومن ثم تكييفه على أنه عدوان إذا بلغ شدة معينة.

إنّ واقع القانون الدولي مازال غامضا حول الموضوع، خاصة مع غياب اتفاقية دولية، لذا يتعين وضع اتفاقية دولية خاصة بالفضاء السيبراني عامة والهجمات السيبرانية خاصة، مع ضرورة توسيع مفهوم العدوان ليشمل هذه الهجمات من جهة، وتدخل مجلس الأمن الدولي واستعمال صلاحياته الواردة في الفصل السابع من ميثاق الأمم المتحدة لتقييم الحالات المتعلقة بالهجمات السيبرانية التي يمكن أن تشكل عدوانا، ووضع معايير واضحة لتكييفها وفقا لموقف محكمة العدل الدولية المعبر عنه في رأيها بشأن مشروع التهديد بالأسلحة النووية أو استخدامها لسنة 1996، ووفقا للتفسيرات الحديثة للمادة 4/2 من ميثاق الأمم المتحدة التي تتماشى مع ضرورة إدراج الهجمات السيبرانية الجديدة ضمن حظر استخدام القوة، واعتبارها عدوانا إذا بلغت شدة معينة، وهو ما يستتبع تطبيق قواعد المسؤولية الدولية.

الإحالات والمراجع:

1. *Cyberattaque et cyberdéfense 2011 éditions Lavoisier.*
2. *Les cyberattaques dans les conflits armés 2014 éditions L'Harmattan.*
3. *Les cyberattaques étatiques et la notion d'agression en droit international, MÉMOIRE DANS LE CADRE DU MASTER 2 DROIT INTERNATIONAL PUBLIC 2017/2018 AIX-MARSEILLE UNIVERSITÉ FACULTÉ DE DROIT ET DE SCIENCE POLITIQUE UNIVERSITÉ FACULTÉ DE DROIT ET DE SCIENCE POLITIQUE.*
4. *Les cyberattaques, armes de guerres en temps de paix 2013 éditions Esprit.*
5. *droit international public 1994 Paris LGDJ.*
6. AKOTO, E. (2015). *Les cyberattaques étatiques constituent-elles des actes d'agression en vertu du droit international public ?*, 2, 203.
7. AKOTO, E. (2015). *Les cyberattaques étatiques constituent-elles des actes d'agression en vertu du droit international public. Première partie, REVUE DE DROIT D'OTTAWA OTTAWA LAW REVIEW*, 46 (01).
8. C.I.J. (27 juin 1986). *Affaire des Activités militaires et paramilitaires au Nicaragua et contre celui-ci. (Nicaragua c. États-Unis d'Amérique).*
9. C.I.J. 1962 *Affaire du temple de Préah Vihear Cambodge c. Thaïlande.*
10. Clémentine, B. (2014). *Appréhender la cyberguerre en droit international, Quelques réflexions et mises au point. La Revue des Droits de l'Homme, éditions Revue du centre de recherche et d'études sur les droits fondamentaux*, 4-24.
11. Frédéric, D. (2014). *La géopolitique pour comprendre le cyberspace*, 2014, n°152. éditions Hérodote.

12. Hamadoun, T. (2010). *La seule façon de gagner la cyberguerre, c'est de l'éviter ; Le Monde Technologies*. Consulté le 8 10, 2022, sur <https://www.lemonde.fr/Technologies/article/2010/02/03/La-seule-façon-de-gagner-la-cyberguerre-c'est-de-l-eviter-1300757-651865.ht>
13. Jean-Pierre, PELLET Alain, FORTEAU Mathias 2005 *La Charte des nations unies commentaire article par article (3 ème édition)* paris éditions Economica.
14. l'OTAN Site officiel de l'OTAN, dossier « cyberdéfense ».
15. *La guerre hybride en Ukraine* 2016 *Revue de défense nationale* 793.
16. Laura, B. (2014). *Les cyberattaques dans les conflits armés*. éditions L'Harmattan.
17. *Les cyberattaques étatiques constituent-elles des actes d'agression en vertu du droit international public ? : Deuxième partie* 2015 *REVUE DE DROIT D'OTTAWA* 02.
18. LIMONIER Kévin, GERARD Colin 2017 *La guerre hybride russe dans le cyberspace* éditions Hérodote.
19. Loïc, S. (2012). *L'usage de la force dans le cyberspace et le droit international*. *Annuaire de droit français internationa*.
20. N.Schmitt, M. (2012). *Koh Speech and Tallinn Manual*. *Harvard international law journal*, Online , 54.
21. Solange, G.-H. (2011). *Menaces, conflits dans le cyberspace et cyberpouvoir*. *Revue Sécurité et Stratégie*.
22. إدريس عطية. (2020). مكانة الأمن السيبراني في منظومة الأمن الوطني الجزائري. مجلة مصداقية، 01 (02)، 115-113.
23. جمال العظلمات. (2015). جريمة العدوان في الهجمات الالكترونية في نطاق القانون الدولي العام. 4، 21، 17-18.
24. خالد خلوي. (2020). جريمة العدوان في ظل نظام روما الأساسي، أطروحة دكتوراه. كلية الحقوق والعلوم السياسية، قسم الحقوق، تيزي وزو: جامعة مولود معمري.
25. مبادئ القانون الدولي العام، الجزء الثاني 2002 الجزائر دار الغرب للنشر والتوزيع.
26. محمد بوسلطان. (2012). من حفظ السلم عن طريق النصوص القانونية الى ثقافة السلم. تاريخ الاسترداد 20 9، 2022، من انسانيات: <https://doi.org/10.4000/insaniyat.8099>
27. محمد خليل الموسى. (2004). استخدام القوة في القانون الدولي المعاصر. عمان: دار وائل للنشر.
28. محمد دنكر. (2022). اسوأ الاختراقات الالكترونية عام 2022. تاريخ الاسترداد 10 8، 2022، من entertainment-media/www.alaraby.co.uk/https://www.google.com/amp/s
29. محمد طلعت الغنيمي. (1993). الوسيط في قانون السلام. الاسكندرية: منشأة المعارف.
30. مريم امحمد المبروك العصادي. (2021). اختصاص المحكمة الجنائية الدولية بجريمة العدوان، رسالة ماجستير، جامعة الزاوية، 2021. كلية القانون، قسم القانون العام.
31. نسرين الشحات الصباحي. (2016). الأبعاد العسكرية للقوة السيبرانية على الأمن القومي للدول، دراسة حالة إسرائيل. تاريخ الاسترداد 2022، من المركز الديمقراطي العربي: <http://democraticac.de/?p=30962>

References:

1. Idrīs 'Aṭīyah. (2020). *Makānat al-amn alsybrāny fī manzūmat al-amn al-Waṭanī al-Jazā'irī*. *Majallat mişdāqīyat*, 01 (02), 113-115.
2. Jamāl al-ẓmāt. (2015). *Jarīmat al-'Adwān fī alhjmāt al-iliktrūnīyah fī niṭāq al-qānūn al-dawlī al-'āmm*. 4, 21, 17-18.
3. Khālīd khlwy. (2020). *Jarīmat al-'Adwān fī ẓill Niẓām Rūmā al-asāsī, utrūhat duktūrāh. Kullīyat al-Ḥuqūq wa-al-'Ulūm al-siyāsīyah, Qism al-Ḥuqūq, Tīzī Wuzū : Jāmi'at Mawlūd Mu'ammarī*.
4. Mabādi' al-qānūn al-dawlī al-'āmm, al-juz' al-Thānī 2002 aljzā'rdār al-Gharb lil-Nashr wa-al-Tawzī'.
5. Muḥammad Būsultān. (2012). *min ḥifẓ al-silm 'an ṭarīq al-nuṣūṣ al-qānūnīyah ilā Thaḳāfat al-silm. Tārīkh alāstrdād 20 9, 2022, min ansānyāt : https : // doi. org / 10. 4000 / insaniyat. 8099*.
6. Muḥammad Khalīl al-Mūsá. (2004). *istikhdām al-qūwah fī al-qānūn al-dawlī al-mu'aşir. 'Ammān : Dār Wā'il lil-Nashr*.
7. Muḥammad dnkr. (2022). *asw' al-ikhtirāqāt al-iliktrūnīyah 'ām 2022. Tārīkh alāstrdād 10 8, 2022, min https : // www. google. com / amp / s / www. alaraby. co. uk / entertainment-media*.
8. Muḥammad Ṭal'at al-Ghunaymī. (1993). *al-Wasīṭ fī Qānūn al-Salām. al-Iskandarīyah : Munsha'at al-Ma'ārīf*.
9. Maryam Imḥammad al-Mabrūk al'şādy. (2021). *Ikhtīṣāş al-Maḥkamah al-jinā'īyah al-Dawlīyah bjrymh al-'Adwān, Risālat mājisṭūr, Jāmi'at al-Zāwīyah,, 2021. Kullīyat al-qānūn, Qism al-qānūn al-'āmm*.
10. Nisrīn al-Shahḥāt alşbāḥá. (2016). *al-ab'ād al-'askarīyah lil-quwwah alsybrānyh 'alá al-amn al-Qawmī lil-duwal, dirāsah ḥālat Isrā'īl. Tārīkh alāstrdād 2022, min al-Markaz al-dīmuqrāṭī al-'Arabī : ttp : // democraticac. de /? p=30962*.

