

عن إشكالية الدفاع الشرعي في مواجهة الجوسسة الرقمية في السياق الدولي About the Problematic of the Legitimate Defense against the Digital Espionage over the International Sphere

سميرة حصايم *

جامعة جيجل - الجزائر

s.hassaim@univ-jijel.dz

تاريخ النشر: 2025/12/30

تاريخ القبول: 2025/10/09

تاريخ الارسال: 2025/01/10

ملخص:

إن الجوسسة الرقمية من المنظور الدولي وبالنظر إلى ما يترتب عليها من أثار وخيمة، يمكن أن تمس في حالات عدة وبشكل مباشر البنية التحتية للدولة المستهدفة، تشكل بحق، وفقا لحدود معيارية استعمالا للقوة بمفهوم الهجوم المسلح، في بيئة وبوسيلة الكترونية، ليرتب عن ذلك أحقية ممارسة الدفاع الشرعي في مجال يغطي غياب الضوابط القانونية لممارسة هذا الحق، الذي ينبثق من تأسيسات مختلفة في ظل عدم التدرج بالأولوية لمصادر القانون الدولي، لذلك تهدف الدراسة تبين التأسيس الممكن اعتماده لتبرير ممارسة هذا الحق. لما كان الدفاع الشرعي يشكل استثناء لحظر استخدام القوة فإن استعماله لمواجهة القوة الالكترونية يتطلب وضع ضوابط قانونية تستجيب للتأثيرات التي تمارسها الهجمات الرقمية المتباعدة الآثار في ظل الرقمنة المؤسسية، انطلاقا من تصنيفها في نطاق استخدام القوة، والتي يترتب عن عدم استقائها لهذا الوصف إمكانية اتخاذ التدابير المضادة في مواجهة العمل غير المشروع دوليا.

كلمات مفتاحية: الجوسسة.الهجمات الالكترونية.مبادئ تالين، الدفاع الشرعي.التدابير المضادة.

Abstract:

Considering to the disastrous effects of the digital espionage over the international sphere, which can affect the infrastructure of the target State; it is really considered a force use under the armed attack in an environment and using an electronic instrument according to certain standards, to be eligible to exercise the legitimate defense in field, that cover the absence of the legal control to exercise this right which emerges from several establishments under the non-graduation priority concerning the sources of the international Law.

Since the legitimate defense constitutes an exception to the prohibition use of force; its use to face the electronic force requires legal controls that responds to the impacts of the several digital attacks under the institutional digitization, on the basis of its classification on the scope of the force use, and its non-compliant status can lead to take the countermeasures to face the internationally wrongful acts.

Keywords: Espionage- Electron sat tacks- Tallin Principles-Legitimate defense- Counter measures.

مقدمة

يفرض تطبيق القانون الدولي على العلاقات بين الدول سلطة الدولة السيادية ومسؤولياتها عن التحكم في بناها التحتية والأساسية، وممارستها وفق الأطر القانونية التي تمنحها القدرة، بل وحتى الحق أو السلطة في مواجهة أي استخدام للقوة.

يعد الدفاع الشرعي أحد أبرز الحقوق المقترنة بالدولة، والتي فرضت ثبوتيتها انطلاقاً من العرف الدولي، وصولاً إلى تكريسه في المواثيق الدولية، لارتباطه بالحق المشروع للدولة في البقاء، ككيان قانوني وسياسي. ينطلق الحديث عن استخدام حق الدفاع الشرعي وجوباً، ووفقاً لتأطير قانوني لزوياه، بأسبقية استخدام القوة، حيث أبرزت المادة الثانية الفقرة الرابعة من الميثاق الأممي كمنطلق قانوني يحمل في طياته أهداف ومقاصد أممية في حظر أي استعمال للقوة، وأكثر من ذلك التهديد بها؛ إلا أنه مصاغ في نطاق استثنائي لمنع استخدامها، ليدخل في هذا النطاق مسمى "الدفاع الشرعي".

لم تعد القوة في زماننا هذا تمارس بالأساليب التقليدية، حيث يشهد العالم تغيرات عدة، في ظل التطور الهائل لوسائل التكنولوجيا والأمن المعلوماتي، والتحديثات والاختراعات اليومية، شاملة لجوانب مختلفة. فقد تمكن الفضاء الإلكتروني فعلياً من تغيير طبيعة الصراع الدولي والاستخدام التقليدي للقوة نتيجة هذه التطورات التي وضعت في يد الدول والفاعلين من غيرها تشكيلة جديدة من الأسلحة الهجومية والدفاعية، في نطاق مقتضيات هذا الفضاء، الذي انتقلت فيه الحرب من التقليدية إلى الافتراضية، لتنفيذ هجمات إلكترونية أو سيرانية لأغراض تصدرها العسكرية أو الأمنية.

بسطت بدورها القوة الإلكترونية تأثيراتها على التجسس بما يحمله من معنى وطورته إلى التجسس الرقمي لتدخله في نطاق الحرب المعلوماتية أو الرقمية، التي تستخدم للإضرار بمصالح الدول، انطلاقاً من استهدافها لمعلومات سرية عن طريق اختراق الشبكات أو المواقع، وصولاً لتنفيذ هجمات إلكترونية. إن أهمية الموضوع ترتبط بكون الجوسسة الرقمية عملية مركبة، تتضمن فعل التجسس كسلوك غير مشروع للوصول إلى البيانات بداية، والذي أصبحت أهدافه مسطرة في المساس بالبنية التحتية للدول المستهدفة، عن طريق ممارسة الهجمة الإلكترونية لاحقاً، قصد ترتيب أضرار متعددة الأوجه بمختلف مراكزها، والتي قد تتساوى إلى حد بعيد أو تتجاوز تلك الأضرار التي تسببها الحرب التقليدية.

ولما كان حق الدفاع الشرعي يرتبط أساساً باستخدام القوة، وإن كان ذلك بصفة استثنائية، طبقاً لما ورد في المادة الثانية من الميثاق، التي جاءت مطلقة لمصطلح القوة، دون تقييده، - من جهة - ووجود عدوان أو هجوم مسلح طبقاً للمادة 51 والتي ربطت القوة بالهجوم المسلح - من جهة أخرى؛ ولما كانت الجوسسة الرقمية تشكل النموذج البارز للهجمات الإلكترونية، والتي تعد من السمات المميزة لحرب المعلومات والحرب السيبرانية كقوة إلكترونية، فضلاً عن ذلك التبنّي الاصطلاحي للمفاهيم التي ضبّطت وجودها في القانون الدولي

بشكل عام، تثار إشكالية الدفاع الشرعي لمواجهة الهجوم الإلكتروني، كقوة حديثة في الفضاء الإلكتروني، وبشكل خاص في صورة الجوسسة الرقمية، بالنظر لخصوصياتها.

تهدف الدراسة إلى تبيان الجوانب القانونية الدولية الممكن تبنيها لممارسة أحقية الدفاع الشرعي لمواجهة الجوسسة في العالم الرقمي، انطلاقاً من نصوص الميثاق، بشكل خاص، وقواعد القانون الدولي ذات الصلة المعتمدة لضبط التأطير القانوني للمسألة، لذلك تبحث المداخلة في إمكانية تأسيس الدفاع الشرعي لمواجهة الجوسسة الرقمية على القواعد الدولية القائمة، أو بتعبير آخر مدى كفاية القواعد الدولية السارية للتأطير القانوني للدفاع الشرعي لمواجهة الجوسسة الرقمية؟.

تقتضي الإجابة على الإشكالية ضرورة الجمع بين المنهجين: الوصفي والتحليلي، لاعتبار جزئيات الدراسة المستخلصة تفرض تحليل قانوني لضوابط عدة، وقياسها على الأوضاع المشتركة الأثر، إستجابة لمتطلبات البحث التي تدور بشكل أساسي في حلقة تحديد ما إذا كانت عمليات الجوسسة الرقمية تدخل في إطار مفهوم القوة المحظورة في القانون الدولي، والتي تخول للدولة أو الدول المعتدى عليها ممارسة حقها في الدفاع الشرعي وفقاً للميثاق الأممي، والقائم على ضرورة ثبوت العملية العسكرية بالمعنى الوارد في المادة 51، بالأخص أن هذه المادة لا تقدم مدلولاً واضحاً لمفهوم الهجوم المسلح أو العسكري.

لذلك يتطلب البحث في إمكانية التأسيس القانوني لممارسة الدفاع الشرعي لمواجهة عمليات الجوسسة الرقمية ضرورة تسليط الضوء على مفهوم هذه العمليات من منظور النص الأممي لحظر استخدام القوة، من خلال التطرق إلى المحددات القانونية للدفاع الشرعي، في نطاق عمليات الجوسسة الرقمية (أولاً)، ومدى بلوغ هذه العمليات لمستوى الهجوم المسلح، باعتباره من متطلبات ممارسة حق الدفاع الشرعي (ثانياً).

أولاً: المحددات القانونية للدفاع الشرعي في نطاق عمليات الجوسسة الرقمية

يقتضي البحث عن المحددات القانونية للدفاع الشرعي في نطاق عمليات الجوسسة الرقمية بيان دخول هذه العمليات في مجال استعمال القوة (1)، بالتالي اللجوء إلى الأحقية الطبيعية للدفاع الشرعي، كاستثناء لاستعمال القوة في مواجهة الجوسسة الرقمية (2).

1. دخول الجوسسة الرقمية في مجال استعمال القوة

إن الحكم بدخول الجوسسة الرقمية في مجال استعمال القوة يتطلب منا بداية تحديد ضابط القوة في عمليات الجوسسة (1.1)؛ ثم الأساس القانوني لاعتبارها استخداماً للقوة في القانون الدولي (2.1)؛ وهي المسألة التي تطرح منطقياً عدم مشروعية هذه العمليات (3.1).

1.1- تحديد ضابط القوة في مفهوم الجوسسة الرقمية

يعكس التجسس الرقمي عملية اختراق الشبكة المعلوماتية، نتيجة القوة الإلكترونية، بغرض الوصول إلى مجموع البيانات الرقمية السرية، لبلوغ الهدف المسطر لغاية التجسس، الذي قد يصل لنطاق عمليات التعطيل أو التدمير لمراكز ذات أهمية لدى الخصم.

فالتجسس الرقمي في السياق الدولي هو استعمال الوسائل التقنية الحديثة من قبل دولة ما، للولوج غير المصرح به إلى أنظمة البيانات أو المعلومات السرية (عسكرية، أمنية، سياسية، اقتصادية أو علمية) لدولة أخرى، قصد الإضرار بها والتقويض بأمنها، ما يشكل تدخلا في شؤونها الداخلية، ووسيلة إكراه تؤثر في قراراتها وتوجهاتها في المجالات المختلفة، بالتالي التأثير في سياستها كدولة ذات سيادة.

تعتبر الجوسسة الرقمية من بين صور الهجمات الالكترونية، التي تشكل اعتداءات تستهدف نظم المعلومات أو البيانات والبرامج الحاسوبية، من خلال الدخول فيها، لرصد الأعمال والأنشطة واستخلاص المعلومات، قصد توظيفها وفقا للأهداف المسطرة.

هذا وتعرف الهجمات الالكترونية على أنها: الأعمال العدائية المنتهجة عبر استعمال أجهزة الكمبيوتر أو النظم والشبكات ذات الصلة، لغرض تعطيل أو تحطيم الأنظمة أو البيانات الالكترونية أو ممتلكات أو المناصب ذات الأهمية للخصم¹.

ينصرف التجسس الرقمي في حالات عدة إلى إحداث تغييرات في المعلومات المبرمجة على الحواسيب الآلية، لتنفيذ هجمات إرهابية على مواقع رئيسية لدولة معينة، لتدخل بذلك في إطار الإرهاب المعلوماتي. فالتجسس الرقمي من صور الإرهاب الالكتروني، الذي يحدث أثارا مدمرة وأضرار وخيمة لمحطات التحكم، وشبكات الاتصال والأجهزة الرقمية، لدوافع سياسية أو عرقية أو دينية أو غيرها، ليمتد بذلك إلى اعتباره عدوان أو تخويف أو تهديد مادي أو معنوي باستخدام الوسائل الالكترونية، الصادر من الدول أو الجماعات أو الأفراد بغير حق².

وبذلك يتضح جليا ارتباط الجوسسة الرقمية باستخدام القوة الالكترونية، الناتجة عن تطور التقنيات في عصر المعلوماتية؛ فقد أصبحت هذه القوة حقيقة أساسية بجل مظاهرها، بما فيها الداعمة للعمليات الحربية والمجالات السياسية والاقتصادية³.

ولما كانت الجوسسة الرقمية تقود بداية لاستعمال مصطلح "القوة"، وإن كانت في شكلها الالكتروني، للتعبير عنها، فإن المسألة تحيلنا في نطاق القانون الدولي لدراسة موقفه تجاه استخدام القوة عموما. جاء ميثاق الأمم المتحدة مانعا لاستعمال القوة، وحتى التهديد بها في العلاقات الدولية، طبقا لما جاء في الفقرة الرابعة من المادة الثانية منه.

فإذا كان تعريف القوة عادة يستند إلى أثارها، من مساسها بالاستقلال السياسي للدولة وسلامة أراضيها، فإن هذه الفرضية لا تنطبق على جرائم الفضاء الرقمي، أين يمكن لدولة أن تقوم بالاعتداء على غيرها، من خلال هجوم من شأنه تعطيل بناها التحتية، بالتالي تعطيل المظاهر الحياتية فيها، لاعتمادها بشكل واسع على التطور الالكتروني الحديث⁴.

والجدير بالذكر أن ميثاق الأمم المتحدة يتسم بالفراغ بشأن التعريف باستخدام القوة، وبالرغم من اعتبار جانب مهم من فقه القانون الدولي أنه ينصرف إلى القوة العسكرية فحسب، وهو ما استقر عليه العرف الدولي،

فإنه ثمة جانب آخر يوسع من تعريفها، ليشمل مختلف الضغوطات التي تشكل تهديدا ومساسا بالاستقلال السياسي للدولة، وأن تقييد هذا التعريف في استعمال القوة العسكرية أو المسلحة فحسب، من شأنه تبرير أعمال وتصرفات عدة⁵.

في الحقيقة يتعين على الدول وضع مفهوم لاستخدام القوة، التي تتزايد تعقيداتها في الفضاء الإلكتروني، لتبرير استخدامها بشكل قانوني، لذلك، وانطلاقا من التوجه الموسع لمفهوم القوة، وبناءا على عدم التدرج بالأولوية لمصادر القانون الدولي من جهة، وموقف محكمة العدل الدولية من جهة أخرى، التي اعتبرت في رأيها الاستشاري، بشأن مشروعية التهديد أو استخدام الأسلحة النووية أن المادة الثانية أعلاه، تحظر استخدام القوة بغض النظر عن السلاح المستخدم⁶، تطرح معها مسألة دعم توجه إدخال الجوسسة الرقمية في إطار مفهوم القوة المحظورة في الميثاق الاممي.

ومع ذلك يبقى مفهوم القوة في نطاق الحرب السيبرانية يتميز بمدلولاته عن مفهومها وفقا لواضعي الميثاق في استخدام القوة وانتهاك أمن الدولة، وعلى ضوء الأشكال المتعددة للحروب الإلكترونية، والتي تشكل استخداما غير مشروعاً للقوة، يتم استخدام الفضاء الرقمي كساحة صراع من خلال المساس أو التأثير على الجوانب الاقتصادية الاجتماعية وغيرها، والتي لا تتطور عموما إلى استخدام الفضاء الرقمي كقوة مسلحة، إنما تتجسد صراعاتها بوسائل متعددة منها الاختراقات والتجسس المعبر عنها بحروب الفضاء الإلكتروني المدمرة، من خلال اختراق العمليات العسكرية ذات التقنيات العالية التي تستهدف الحياة المدنية والبنى التحتية.

أدى الهجوم الذي تعرضت له محطة نظام الايرانية النووية سنة 2009 والمعلن عنه من قبل الولايات المتحدة سنة 2011 باستخدام برنامج Stuxnet إلى تعطيل عمليات حساسة والحاق أضرار في عمليات تخصيب اليورانيوم والذي يعد سابقة في حقل الهجمات الإلكترونية؛

وتعرضت جمهورية استونيا عام 2011 إلى هجوم سيبراني من روسيا الاتحادية عن طريق إغراق المواقع الإلكترونية بالبيانات غير اللازمة، التي استهدفت المواقع الحكومية والصحف والمستشفيات وخدمات الإطفاء وكذا المصارف والجامعات لشل الحكومة الاستونية⁷؛ كما أجبرت قوة الهجوم الرقمي الذي استهدفت به إيران الأنظمة الرقمية لشركة أرامكو سنة 2017 استبدال مجمل الشبكة الإلكترونية المتعامل بها، والذي رتب تغييرا كبيرا للأجهزة العاملة.

2.1 - الأساس القانوني لاعتبار الجوسسة الرقمية استخداما للقوة في القانون الدولي

إن البحث عن الأساس القانوني للمسائل ذات الطابع الدولي، يقودنا للاستعانة بنص المادة الثامنة وثلاثون من النظام الأساسي لمحكمة العدل الدولية، التي ترجع إليها المحكمة وتطبقها بخصوص مصادر القانون الدولي، بالأخص أنها لم تشر صراحة إلى الأولوية في التطبيق بخصوص ما ورد فيها، وهو الأمر الذي يعطي ذات القيمة القانونية للنتائج المتوصل إليها، أي كان الأساس المعتمد عليه، سواء كان نص اتفاقي أو عرفي، أو مبادئ قانونية، وحتى الاجتهاد القضائي والمذاهب الفقهية.

لذلك ومع غياب الاتفاقيات الدولية والعرف الدولي بخصوص اعتبار الهجمات الالكترونية الواقعة في سياق الجوسسة الرقمية من صور استخدام القوة والتهديد بها، يقودنا الأمر آليا للرجوع إلى الاجتهاد القضائي للمحكمة بخصوص موضوع البحث.

عاجت محكمة العدل الدولية نص الفقرة الرابعة المادة الثانية من الميثاق (مشار إليه سابقا) من زاويتين، حيث أكدت في الزاوية الأولى - بعد أن أوضحت في حكمها أن مبدأ حظر استخدام القوة أضحي قاعدة عرفية تلزم الكافة، بغض النظر عن مسألة العضوية في منظمة الأمم المتحدة- أن مضمون هذه المادة ينطبق على أي استخدام للقوة، بغض النظر عن طبيعة الأسلحة المستخدمة، على أن يرقى من حيث النطاق والتأثير إلى مستوى النزاع المسلح. في حين اهتمت في الزاوية الثانية بالحالات التي لا تعد استخداما للقوة، بالمعنى التقليدي، بين الأطراف المتحاربة، على غرار إرسال قوات من قبل دول أخرى، أو تقديم الدعم أو العون غير المباشر لهم، والذي أدخلته في سياق استخدام القوة، كنقطة تحول كاشفة في إطار مسؤولية الدول عن ممارساتها الخاطئة، المباشرة منها وغير المباشرة.

وعليه يتضح من قرار المحكمة الاستعداد الجدي لها لضم فئات أخرى، بخلاف الهجمات العسكرية التقليدية، الأمر الذي يفتح المجال لإمكانية تطبيق ذات الفرضية على الصور المختلفة للهجمات الالكترونية، واعتبارها من حالات استخدام القوة.

بالموازاة وفي إطار الوثائق الدولية ذات الصلة، جاء دليل تالين⁸ داعما لتوجه محكمة العدل الدولية، حيث اعتبر أن الهجمات على الشبكات الرقمية تشكل استخداما للقوة ضد سيادة الدولة الإقليمية، والتي تعد عملا غير مشروع دوليا.

والجدير بالذكر أن مبادئ تالين بشأن القانون الدولي المطبق على الحروب السيبرانية تعد دليل ضمن إصدارين لسنة 2013 وسنة 2017 طوره خبراء القانون الدولي، بالتالي لا تشكل اتفاقية دولية، وأن الرجوع إليها في البحث مرتبط أساسا بعدم التدرج الوارد في المادة 38 من النظام الأساسي لمحكمة العدل الدولية بخصوص مصادر القانون الدولي.

3.1 - في عدم مشروعية الجوسسة الرقمية

على الرغم من اتجاه فقه القانون الدولي، على غرار الفقيه ستون Ston و وولف Wolf إلى الدفاع عن مشروعية الجوسسة الرقمية استنادا إلى اعتبارات عدة⁹، فإن منطلق الدراسة ومقتضات الموضوع في ظل التطورات التكنولوجية الراهنة تدفعنا لمساندة الاتجاه المدافع عن عدم مشروعية عمليات التجسس الرقمي؛ والذي تبني خطوته الأولى في محاولته الجدية في دحض الحجج والأسانيد التي اعتمد عليها الاتجاه القائل بمشروعية هذه العمليات.

حيث يعتبر التجسس رقمي من الأعمال غير المشروعة دولياً، باعتباره من السلوكيات المستهجنة المنبوذة والمخالفة للأخلاق المتعارف عليها دولياً¹⁰، بالأخص أنها هادفة لكسب مادي، من خلال الإضرار بمصالح الدولة الضحية من جوانب عدة.

إن غياب قاعدة قانونية اتفاقية تحظر التجسس الرقمي بشكل مباشر، لا يعني أنه سلوك مشروع، حيث نجد بعض الاتفاقيات الدولية توعي من خلال استقراءها بعدم مشروعية ذات السلوك، على غرار اتفاقية فينا للعلاقات الدبلوماسية؛ واتفاقية الأمم المتحدة لقانون البحار التي تشير إلى إلزامية احترام القواعد القانونية في دولة المجال، - بالأخص أن أغلبية القوانين الداخلية تحظر التجسس الإلكتروني- والامتناع عن جمع المعلومات فيه بوسيلة غير مشروعة، والذي يعد عمل غير مقبول؛ وبما أن هذا العمل من أهداف التجسس، فإن ذلك يقود آلياً إلى أن هذه الاتفاقيات تحظر هذا السلوك؛ وتضفي عليه عدم المشروعية؛

في ذات الاتجاه وإذا كانت اتفاقية لاهاي لسنة 1907، التي عدت المحظورات الدولية، دون الإشارة إلى التجسس، يبدو جلياً منها، أن ذلك لا يعني دخول السلوك في نطاق المشروعية، كون الاتفاقية عدت المحظورات على سبيل المثال فحسب، وإن اتجهت في نصها إلى اعتبار أن الحصول على المعلومات في ساحة الحرب جائز، مع ذلك لا يمكن الأخذ به للقول بمشروعية التجسس، فالاتفاقية تنطبق في إطار العمليات العدائية فحسب.

هذا وإذا كانت اتفاقية الفضاء الخارجي التي تؤكد على الاستخدام السلمي لهذا المجال لفائدة الشعوب، وانطلاقاً من إلزام الدول باستخدامه، بمراعاة قواعد القانون الدولي، بما يحفظ السلم والأمن الدولي، فإن الجوسسة الرقمية باستخدام الأقمار الصناعية يتعارض مع ذلك، بالأخص أن العملية تحقق أهداف دولة أو دول بعينها، لا فائدة للشعوب.

والجدير بالذكر أنه يمكن الاعتماد على اتفاقية بودابست التي وضعت من قبل مجلس أوروبا سنة 2001¹¹ كاتفاقية دولية إقليمية تحاول معالجة الجرائم الإلكترونية، والتي تعد الأكثر حداثة في مواجهة تحدي الجرائم السيبرانية عموماً، في تبيان عدم مشروعية الجوسسة الرقمية من خلال نص المادة الثانية التي تعتبر الدخول المتعمد إلى الأنظمة الإلكترونية يشكل دخول غير مشروع أو غير قانوني.

هذا وقد تضمنت اتفاقية بودابست بنود معنية بالتجريم والتعاون الدولي لمكافحة الجرائم السيبرانية دون إدخالها في مجال استعمال القوة لممارسة حق الدفاع الشرعي.

وقد ذهب خبراء تالين في القاعدة الخامسة من مبادئ تالين، أنه على الدول منع استعمال البنية الأساسية السيبرانية أو الإلكترونية، التي تخضع لسيطرتها في إطار الفضاء الرقمي، في أعمال من شأنها المساس بالحقوق السيادية لدول أخرى؛ وتعد الجوسسة الرقمية من بين هذه الأعمال المنتهكة للسيادة.

انطلاقاً مما سبق، يعد قيام أي دولة بتدريب وتمويل جماعة نظامية متخصصة باختراق الحواسيب والشبكات المعلوماتية ومنحها برامج معدة لتنفيذ لعمليات التجسس الرقمي عمل غير مشروع، يدخل في سياق استخدام القوة.

في الحقيقة أن غياب اتفاقية دولية تتضمن نصوص صريحة لتقييد التجسس العادي والرقمي بين الدول، راجع أساساً لحرصها على التكتّم بخصوص إمكانياتها، لذلك يصعب مناقشة هذا الأمر دون الكشف عن معلومات متعلقة بقدراتها؛ بالإضافة إلى اعتبار التجسس من أنشطة الاستخبارات الداخلة في نطاق المصالح الأمنية الأساسية للدولة، فإنه من البديهي أن لا ترغب أي منها في تقييد إمكانياتها في هذا المجال، لحماية نفسها بأي آلية وان كانت غير قانونية¹².

والجدير بالذكر أن الاعتبارات أعلاه، لم تمنع الدول من تقييد وحظر الجوسسة في نطاق القانون الداخلي.

2. الأحقية الطبيعية للدفاع الشرعي كاستثناء لاستعمال القوة في مواجهة الجوسسة الرقمية

لم يأتي مبدأ حظر استخدام أو استعمال القوة في العلاقات الدولية على صورة الإطلاق، حيث وردت عليه استثناءات يكون فيها اللجوء لاستخدام القوة عملاً مشروعاً، منها حالة الدفاع الشرعي، الواردة في نص المادة 51 من الميثاق، كحق من الحقوق الطبيعية للدول، التي لا تقبل التنازل عنها، والذي تمارسه الدول بشكل فردي أو جماعي، وفق ضوابط تقيّد اللجوء إليه.

فقد جاء في نص المادة 51 أنه : لا يوجد في نص الميثاق ما ينقص أو يضعف الأحقية الطبيعية للدول، فرادى كانت أو جماعات، في الدفاع عن نفسها، في حالة ما إذا اعتدت قوة مسلحة على أحد أعضاء الأمم المتحدة، إلى غاية أن يتخذ مجلس الأمن التدابير اللازمة لحفظ السلم والأمن الدوليين، على أن يتم تبليغ المجلس فوراً بالتدابير المتخذة استعمالاً لهذا الحق؛ هذا ولا تؤثر تلك التدابير، بأي حال من الأحوال، فيما لمجلس الأمن - بمقتضى سلطاته وفقاً للميثاق - من الحق في أن يتخذ ما يراه ضروري من الأعمال، لحفظ السلم والأمن الدولي أو إعادته إلى نصابه.

نشير إلى أنه، فضلاً عن اعتبار الدفاع الشرعي حقاً طبيعياً، واستثناء عن المبدأ العام الذي يقضي بحظر ومنع استعمال القوة في العلاقات الدولية، يعتبر بذلك سبباً من أسباب الإباحة، فضلاً عن ذلك، يشكل نظاماً قانونياً يترتب عنه انتفاء المسؤولية الدولية، رغم بقاء الفعل مجرماً.

يرتبط الدفاع الشرعي بوقوع فعل الهجوم أو العدوان المسلح، باعتباره العامل المنشط والمنشئ له، لذلك كان ولا يزال محل تأويلات، نابعة من غياب التدقيق في توجهات المصطلح، وقد أظهرتها بشكل خاص، الممارسات العملية التي بلغت حد الاعتقاد على الاحتمالية في نطاق ما يسمى "بالدفاع الشرعي الاستباقي" أو "الوقائي"، والمرتبطة أساساً بالتفسير الموسع لفعل الهجوم، ليستغرق معها الهجمات الاحتمالية أيضاً.

في حقيقة الأمر لا يزال الدفاع الشرعي الوقائي موضوع نقاش¹³، حيث أنه يتطلب دراسة معايير التهديدات الوشيكة والاستجابات الفورية، مع احترام مبدأ الضرورة والاستجابة المناسبة مع الهجوم الإلكتروني.

هذا وقد يكون للهجمات الالكترونية نمطا متصلا بالقدرات الهجومية وكذا الدفاعية للدولة، حيث قامت الصين برد العدوان تجاه الولايات المتحدة اثر استهداف مواقعها العسكرية المتعلقة بتطوير المقاتلات، بمهاجمة مواقع أمريكية الكترونية قدرت حصيلتها 2 مليار دولار.

ثانيا: في مدى بلوغ الجوسسة الرقمية لمستوى الهجوم المسلح لإعمال الدفاع الشرعي

نظرا لكون التدرع باستعمال حق الدفاع الشرعي لتبرير استخدام القوة من الممارسات الخطيرة في العلاقات الدولية، أخضع هذا الحق لجملة من القيود، لإضفاء المشروعية على ممارسته، إذ يُفترض وقوع اعتداء مسلح، غير مشروع، من طرف دولة ما على دولة أخرى، لذلك نبحت بداية في إمكانية اعتبار الجوسسة الرقمية هجوما مسلحا (1)، وهو الفرض الذي لا يتحقق في جميع الحالات، ليحيلنا إلى أحقية ممارسة التدابير المضادة (2).

1. في إمكانية اعتبار الجوسسة الرقمية هجوما مسلحا

يرتبط اعتبار عمليات الجوسسة الرقمية ضمن الهجمات العسكرية توفر ضابط الهجوم المسلح فيها (1.1) بتوفر معايير ترتقي بالتجسس الرقمي لمستوى الهجوم العسكري (1.2).

1.1- ضابط الهجوم المسلح ضمن الجوسسة الرقمية

يرتبط إعمال الدفاع الشرعي بوجود هجوم مسلح أو عدوان، فإذا كان الهجوم التقليدي يقترن باتخاذ سلوك حركي ايجابي، فإن للتجسس الرقمي عمل ايجابي بدوره، يتمثل بالضغط على لوحة المفاتيح لاختراق البيانات، من أجل الحصول على معلومات يتم توظيفها لاستهداف مؤسسات الدولة، أو شخصيات لها مكانة فيها، وهو الأمر الذي يؤدي إلى عواقب وخيمة عادة.

تستند إمكانية إدخال الجوسسة الرقمية ضمن سياق الهجومي، إلى معطيات عدة في نطاق القانون الدولي الإنساني¹⁴، انطلاقا من المادة الثانية المشتركة من اتفاقيات جنيف، التي تفتح مجال لاستغراق العمليات الهجومية المختلفة، كونها لم تربط هذه العمليات بالسلاح، وهو الأمر الذي قد يفتح المجال لربط الهجمات الالكترونية، بما فيها التجسس الرقمي بمضمون هذه المادة، بشرط أن يترتب عنها أضرار وأثار على الفرد والممتلكات، بالأخص أن الفقرة الأولى من المادة التاسعة وأربعون من البرتوكول الإضافي الأول، لم تقيد أعمال العنف بالوسائل الحركية، بل بالتبعات المترتبة عنها؛ فالقانون الدولي الإنساني عموما، يهتم بالآثار التي تحدثها الهجمات أكثر من الفعل ذاته، وهو ما يمنح له مرونة لاحتواء الهجمات الحديثة الرقمية.

يتضح أن الهجوم الرقمي يشكل عملية سيبرانية هجومية أو دفاعية، عند وصول استخدام القوة فيها لدرجة عالية، وإلى مستوى شديد الخطورة، بحيث يترتب عليها خسائر في الأرواح، وإصابات للأشخاص، فضلا عن ذلك إلحاق الضرر بالممتلكات أو تدميره¹⁵، لتدخل بذلك في نطاق أعمال العنف المنصوص عليها في المادة 49 أعلاه، وفي إطار عواقب وتوابع السلوك أو العملية الهجومية دون طبيعتها.

هذا وتفرض المادة السادسة وثلاثون من البرتوكول الإضافي الأول تطبيقها في هذا المقام، والتي تلزم الدول عند التعامل مع الأدوات أو الأسلحة الحديثة، ضرورة النظر وبشكل قانوني في مدى توافقها مع الالتزامات

الدولية الأخرى؛ فالمادة لم تحدد وسائل أو أدوات الحرب المنصوص عليها، حيث أن السلاح ينصرف إلى القدرة أو الاستطاعة الهجومية ذات إمكانية لاستهداف هدف عسكري؛ أما الأداة فتتمثل فيما يعتمد عليه لتحقيق الغرض، وهو ما يؤكد جليا أن البعد الأساسي للمادة هو منع استخدام أي أداة جديدة، بما فيها الهجمات الالكترونية، والتي يمكن أن يعتبر استخدامها انتهاكا للقانون.

سايرت محكمة العدل الدولية ذات التوجه، في رأيها الاستشاري المتعلق بالأسلحة النووية (المشار إليه سابقا الفقرتان 35-36)، والذي جاء وجوديا بعد الاتفاقيات الإنسانية، حيث صرحت أنه لا يمكن استبعاد انطباق قواعد ومبادئ هذه الاتفاقيات، كون ذلك لا يطابق الخاصية الإنسانية، وأنها تنطبق على مختلف النزاعات والأسلحة المخترعة في الماضي والحاضر والتي ستظهر في المستقبل أيضا.

ذات الفرضية جاءت في إطار دليل تالين لعام 2012 بشكل صريح، مؤكدا إمكانية اعتبار الهجمة الالكترونية بمثابة هجوم، ما ينطبق على التجسس الرقمي الداخل في نطاقه، فتكييف الفعل بأنه داخل في نطاق العنف يعتمد على الآثار أو التبعات الناتجة عنه، لا على طبيعة الفعل أو أداة القيام به.

تعد الهجمات الالكترونية من بين الصعوبات التي تواجه تطبيقات القانون الدولي الإنساني، إلا أن هنالك توافق عام يشير إلى أن هذا القانون يتصف بالمرونة والمتجسد في شرط مارتينيز¹⁶ - الضامن للمستوى الأدنى من الحماية - والذي يتيح مواجهة التحديات التي تطرحها الأسلحة الحديثة.

وقد أشار بدوره دليل تالين، أنه وبوجود هذا الشرط، والذي يعكس القانون الدولي العرفي، لا وجود لفراغ قانوني بخصوص الهجمات على شبكات المعلوماتية؛ كما أن محكمة العدل الدولية في رأيها الاستشاري بشأن الأسلحة النووية أوضحت أن ذات الشرط، أثبت بأنه وسيلة فعالة للتصدي للتطورات السريعة في مجال التكنولوجيات العسكرية .

1.2 - في تحديد معايير ارتفاع القوة في الجوسسة الرقمية لمستوى الهجوم المسلح

وضع جان بكتيه " Jan Paktie " دليل تقييمي لبلوغ استخدام القوة مستوى الهجوم المسلح، وذلك عندما تكون هذه القوة ذات نطاق ومدة وكثافة كافية؛ وانطلاقا من ذلك حاول الفقه وضع نماذج ثلاث في سياق اعتبار الهجمات الالكترونية من الهجمات المسلحة¹⁷:

- أولها: السبيل القائم على الأدوات: يقوم على البحث في مدى تحقق الضرر المترتب عن الهجمة الالكترونية من خلال الهجوم المسلح، مثال ذلك: الهجمات الالكترونية التي تؤدي إلى إفساد الشبكات الكهربائية المحمية في إطار القانون الدولي الإنساني، والذي يشكل في النزاعات المسلحة التقليدية هجوما مسلحا يتحقق بالقصف.

- ثانيها: السبيل القائم على التأثيرات: يقوم على تقييم الضرر المترتب عن الهجمة الالكترونية مقارنة بالذي يحدثه الهجوم الحركي، مثال ذلك تعطيل التجارة في الدولة الضحية، نتيجة التلاعب بالبيانات المصرفية، وهو ذات الضرر الناتج عن الهجوم المسلح.

- ثالثها: سبيل المسؤولية الصارمة: ترتبط بشكل خاص بالهجمات على أنظمة البنية الأساسية، أو المرافق العامة في الدولة المستهدفة، فالهجمات الالكترونية على البنية التحتية تشكل فعليا هجمات مسلحة. لذلك، وبناء على ما ورد أعلاه، فإذا ترتب عن التجسس الرقمي، والذي يدخل في نطاق الهجمات الالكترونية، أحد هذه السبل، يعد بمثابة الهجوم المسلح، والذي يفتح المجال لتفعيل أو ممارسة حق الدفاع الشرعي.
- حدد "مايكل سميث" بدوره، معايير من شأنها تحديد مدى بلوغ الهجمات الالكترونية، بما فيها التجسس الرقمي، مستوى الهجوم المسلح لممارسة حق الدفاع الشرعي والمتمثلة في¹⁸:
- معيار شدة الدمار: حيث يقوم هذا الشرط على أساس أن حجم الدمار الناتج عن الهجمات الالكترونية، مساوية أو مماثلة للهجمات المسلحة المهددة بخسائر على الأشخاص والأعيان.
- معيار إمكانية تقدير الضرر: لقيام هذا الشرط وبلوغ الهجمات الالكترونية حد الهجمات المسلحة يتطلب وقوع ضرر فعلي أو وشيك الوقوع؛ مع العلم أن الضرر لا يعتبر واضحا في سياق الهجمات الالكترونية، لذلك كلما تم إحصاء البيانات والمواقع المستهدفة، تم إدراجها في نطاق استخدام القوة الخطرة.
- معيار قرب تحقق التبعات: يقوم هذا الشرط على وجود علاقة بين الهجوم الالكتروني الصادر من الدولة، والضرر الحاصل، مع مراعاة ما يطرحه الانفصال الزمني بين الهجمة وما ينتج عنها.
- معيار العلاقة السببية: أي وجود رابطة سببية بين الفعل أو السلوك والنتيجة المحققة، اخذين بعين الاعتبار أن التجسس الرقمي لا تتحقق النتائج الفورية فيه.
- معيار الاجتياح أو تجاوز حدود الدولة المستهدفة: وهو المعيار القائم بشكل واضح في الهجمات المسلحة التقليدية باختراق الحدود الإقليمية للدولة، في حين أنه ينصب على اختراق مواقع مهمة لأنظمة الكترونية للدولة المستهدفة.
- ارتباط الدولة بالهجمات: ترتبط الدولة بالعمليات العسكرية بشكلها التقليدي، أما التجسس الرقمي تقوم به الدولة بشكل مباشر، عن طريق أجهزتها، أو بصفة غير مباشرة عن طريق وكلاء، بالتالي تحتاج عمليات معقدة للوصول إلى إسنادها.
- الجدير بالذكر أن المعايير أعلاه لم يتم وضعها حصرا، لذلك يمكن للدول الاعتماد على معايير أخرى لتكثيف الهجمات الالكترونية عامة، كاستخدام للقوة ودخولها ضمن مدلول الهجوم العسكري.
- وقد أدى عدم التدقيق في تحديد المعايير -أعلاه- قانونا، ظهور ممارسات دولية في اعتبار هجمات الكترونية، بالرغم من جسامتها، بأنها لا ترقى أساسا إلى درجة أو مستوى العمليات أو الاعتداءات العسكرية، بما يتفق مع المادة 51 من الميثاق، على غرار عملية "ستوكس نت" سنة 2010 التي أدت إلى تخريب ما يقارب 1000 طرد مركزي إيراني نووي.

هذا وقد أقر خبراء تالين في المادة 16 الاعتماد على معيار النطاق والأثر في تحديد ما إذا كانت الهجمة الالكترونية ترقى إلى مستوى عمليات الاستعمال غير المشروع للقوة، وكذا إدخالها ضمن الهجمات العسكرية، في ذات السياق، والتي تبرر ممارسة حق الدفاع الشرعي نتيجة الأضرار الجسيمة المترتبة عنها، استناد إلى رأي محكمة العدل الدولية في قضية النشاطات العسكرية في نيكارغوا¹⁹، على أساس أنه الأنسب في ذلك.

هذا وإذا ما انطلقنا من مقتضيات المادة الثامنة مكرر من نظام روما الأساسي للمحكمة الجنائية الدولية في تعريفها لجريمة العدوان، وفي صدد البحث عن تكييف التجسس الرقمي وفق هذه الجريمة، يمكن القول أنها تنطبق على الهجمات الالكترونية التي تهدد بدورها الاستقلال السياسي للدولة المعتدى عليها وسلامتها الإقليمية، فضلا عن ذلك؛ فعلى الرغم من أن نطاق تحميل المسؤولية محدد في ذات المادة، فإن نطاق الأشخاص الذين يحتمل أن يكونوا مسؤولين عن ارتكاب الهجمات الالكترونية، أكبر بكثير من الحرب التقليدية، لذلك فالمحكمة الجنائية الدولية بإمكانها أن تشكل إطار قابل للتطبيق لمساءلة الحروب الحديثة²⁰.

في حقيقة الأمر ومن المفروض أن ينصرف الهجوم المسلح الذي يعد من مقتضيات الدفاع الشرعي وفقا للتفسير الضيق للمصطلح إلى الهجوم الفعلي دون المحتمل، استنادا إلى اتفاقية فينا لقانون المعاهدات، المعبرة بشكل صريح على وجوب الأخذ باللفظ والمعنى العادي عند تفسير الاتفاقيات الدولية. في حين أظهر التوجه الممارساتي أو العملي، ومعه جانب فقهي الأخذ بالمدلول الواسع للمصطلح، ليقر بذلك حق الدفاع الشرعي ضد السلوكيات التي لا تصل حد العدوان المسلح، لمنع هجوم وشيك يهدد الدولة²¹، انطلاقا من الأخذ بالنص الكاشف لحق الدفاع الشرعي أي المادة 51 من الميثاق، التي لا تعد حسب ذات الاتجاه منشأة لهذا الحق.

وتطبيقا للمادة الثالثة عشر من دليل تالين يحق للدولة الضحية ممارسة حقها في الدفاع الشرعي نتيجة هجمات التجسس الالكتروني الرقمي، بالنظر إلى حجمها وأثارها وفقا للقاعدة السادسة عشر من الدليل؛ على أن يبلغ مجلس الأمن بذلك ليتخذ ما يراه ملائما وفقا لسلطاته التقديرية في تكييف الأوضاع، مع العلم أن إخطار أو إبلاغ مجلس الأمن يدخل في نطاق الطبيعة الاستثنائية لحق الدفاع الشرعي عموما، والوارد في الميثاق، والتي تستلزم بالضرورة وفقا لهذا التكييف فرض نوع من الرقابة اللاحقة على التدابير التي تتبناها الدولة أثناء ممارسته، فالدولة التي تتمسك به تلتزم حتما بإبلاغ المجلس فورا بما تتخذه من الإجراءات والتدابير المناسبة لممارسة حقها هذا.

ولما كان الدفاع الشرعي يشكل استثناء لاستخدام القوة في العلاقات الدولية، فإن توجهات الدول في إطار التعاون الدولي، والذي يتخذ الشكل الاتفاقي، وفي إطار مكافحة الجرائم السيبرانية عموما، والتوجه نحو سلمية حل المنازعات وفقا للميثاق الاممي، لم تشر اتفاقية بودابست لسنة 2001 إلى الدفاع الشرعي لمواجهة الهجمات الالكترونية عموما، لعدم اعتبارها ضمن مجال استعمال القوة، مكتفية بالتجريم الموضوعي ومسؤولية الأشخاص، والجزاءات والتدابير المعنوية، فضلا عن تدابير التعاون بين الدول في مجال مكافحة هذه الجرائم.

2. في احتمالية عدم بلوغ التجسس الرقمي لمستوى الهجوم المسلح لاتخاذ التدابير المضادة

يرتبط ممارسة الدفاع الشرعي قانونا وفقا لمتطلبات المادة 51 من الميثاق بالهجوم المسلح، الذي يرتب آثار واضحة المعالم في الدولة الضحية، إلا أن هذه الآثار قد يختلف حجمها لاعتبار الهجمة تدخل في سياق استخدام القوة طبقا للفقرة 04 المادة الثانية من الميثاق، وعدم بلوغها مستوى الهجوم المسلح بالتالي عدم مشروعية الدفاع الشرعي؛ فالأعمال التي لا ترقى إلى تصنيف الهجمة الالكترونية على أنها تدخل في مفهوم القوة، لا يحق معها ممارسة الدفاع الشرعي، إنما يعطي للدولة المستهدفة خيارات أخرى لمواجهة العمل غير المشروع دوليا²²، على غرار التدابير المضادة.

والجدير بالذكر أن محكمة العدل الدولية من خلال رأيها الاستشاري في قضية النشاطات العسكرية²³ فصلت بين الأعمال الأكثر خطورة لاستخدام القوة، والتي تصل إلى درجة الهجوم المسلح أين يحق معها تفعيل حق الدفاع الشرعي، والأشكال الأقل خطورة، التي لا يجوز معها ممارسة هذا الحق، إنما تفعيل الإجراء المضاد انطلاقا من عدم مشروعية الفعل.

لم تحدد ذات المحكمة الحد الفاصل بين الفعل الخطر والأقل خطورة لاستعمال القوة، فاتحة الباب بذلك لتفسيرات الدول، وهو ما ظهر أيضا في دليل تالين، بالضبط في القاعدة التاسعة منه، التي نصت على جواز لجوء الدولة المصابة بالفعل غير المشروع دوليا اعتماد تدابير مضادة متناسبة، بما فيها الداخلة في الفضاء الالكتروني أو السيبراني.

هذا وتعرف التدابير المضادة على أنها رد فعل الدولة على التصرف غير المشروع، شريطة استقاء شروط إجرائية وموضوعية²⁴ كضرورة الطلب من الدولة المعنية تصويب الإخلال الدولي ووقف سلوكها غير المشروع، والوفاء بالتزاماتها الدولية، ضف إلى ذلك إخطارها بأي قرار يتم اللجوء إليه، مع مراعاة مبدأ تناسب التدابير المضادة مع الضرر الحاصل.

جاء في المادة 49 من مبادئ تالين أن التدابير المضادة تشكل تدابير قسرية، تعتمد عليها الدولة المتضررة في مواجهة الدولة المتسببة للضرر وحدها، من أجل حثها على احترام التزاماتها ووقف السلوك غير المشروع دوليا، باعتبارها تدابير قانونية ضد دولة مرتكبة لانتهاكات حقوق الإنسان، والالتزامات المعنية تجاه المجتمع الدولي.

لذلك تبقى بدورها التدابير المضادة تثير صعوبات مرتبطة أساسا بتحديد مسألة ما إذا كانت الهجمات الرقمية تخول الدولة المستهدفة استخدامها لهذه التدابير وذلك في إطار مشروع مسؤولية الدول عن الأعمال غير المشروعية دوليا، خصوصا إذا لم ترتقي إلى المقصيات المطلوبة في ظل الغموض وعدم التحديد الذي يميز العديد من المفاهيم في القانون الدولي وهي التدابير التي تحتاج إلى دراسة خاصة لتحديد إطارها القانوني في مواجهة الجرائم الالكترونية عموما.

الخاتمة

يتضح من خلال الدراسة أن:

- إمكانية التأسيس القانوني لأحقية ممارسة الدفاع الشرعي في مواجهة الجوسسة الرقمية يتطلب ضوابط ومحددات قانونية، تنطلق من توسيع مفاهيم عدة على غرار: القوة والهجوم المسلح، والذي يحتاج إلى ضبط معايير اللجوء لهذا الحق بشكل يستجيب لخصوصيات القوة في عمليات التجسس الإلكتروني، بالنظر إلى النتائج التي يمكن أن تترتب عليها.
- إشكالية القواعد القانونية التي يمكن من خلالها ضبط اللجوء للدفاع الشرعي وفقا للمتطلبات القانونية المنظمة في ميثاق الأمم المتحدة على عمليات الجوسسة الرقمية تميزها خصوصيات أفردتها طبيعة هذه الهجمات، على ضوء ما تطرحه المستجدات الدولية ذات الصلة، بتطورات طارئة على مفاهيم أفرزتها العلاقات الدولية من منظور القانون الدولي .
- نصوص ميثاق الأمم المتحدة عامة، وبشكل خاص في أحكام الدفاع الشرعي، وبالرغم من استعمال المصطلحات المرنة، تحتل بل وتستوعب احتواء حالات عدة، ومع ذلك تبقى تتطلب نوعا من التعديل أو التحيين استجابة لما تطرحه المتغيرات على ساحة العلاقات الدولية.
- إن التجسس الإلكتروني وبالنظر إلى تطور نطاق استعماله، وما ينجم عليه من انعكاسات، يمكن أن تؤثر في العديد من الحالات وبشكل مباشر بالبنية الأساسية لمؤسسات الدولة المندمجة في النظام الرقمي، يشكل وبحق مظهر لاستخدام القوة بالمعنى المرافق للهجوم المسلح في بيئة الكترونية، ليرتبط عن ذلك الحق في ممارسة الدفاع الشرعي، في نطاق حدود مبنية معياريا، سواء من خلال خبراء تالين، أو الفقه المهتم بموضوع تحديد المعايير المعتمد عليها لبلوغ الهجوم الدرجة المطلوبة من الأضرار، والتي تتجاوز الحد الفاصل بين النزاعات المسلحة، وحالات السلم، لممارسة حق الدفاع الشرعي.
- في الحقيقة إن عدم التدرج بخصوص الأولوية في التطبيق ضمن مقتضيات المادة 38 من النظام الأساسي لمحكمة العدل الدولية، يعمل على فتح مجالات وأفاق واسعة لإيجاد حلول من شأنها وضع أطر لإشكالات عدة تطرحها العلاقات الدولية المتطورة، وبشكل خاص ما يتعلق باستعمالات القوة وكيفية التعامل معها؛ ومع ذلك يبقى الاجتهاد القضائي والفقه سبل استدلالية للوصول إلى القواعد القانونية الواجبة التطبيق وفقا لهذا النظام.
- إن عدم بلوغ عمليات الجوسسة الرقمية لمفهوم الاعتداء المسلح وفقا للمعايير المقبولة دوليا يضع الدول المعتدى عليها أمام خيارات أخرى، أهمها التدابير المضادة التي تعطي للدولة المستهدفة حق الرد على الاعتداء غير المشروع دوليا.

- إن الحرب الالكترونية عموماً تفرض واقع أكثر من استخدام قواعد قانونية محددة ومتعامل بها مسبقاً، لذلك تحتاج لمعالجة عامة ووفقاً لقواعد خاصة، وبغياها، فإن المعايير التي يحتمل تطبيقها مستمدة بشكل أساسي من قواعد القانون الدولي الإنساني ونصوص ميثاق الأمم المتحدة.
- في الحقيقة إن التوصيات المتوصل إليها من خلال هذا الموضوع، وبغض النظر عن تلك المتعلقة بضرورة تعديل نصوص الميثاق حتى تستجيب لمجرى العلاقات الدولية المعاصرة، والمشار إليها في اغلب دراسات القانون الدولي، فإن الإشكالية تطرح بشكل واسع التوصيات التالية:
- ضرورة الاهتمام بالدور الذي يمكن أن يلعبه الفقه وكذا الاجتهاد القضائي في إيجاد حلول يمكن من خلالها تطبيق قواعد القانون الدولي على حالات تطرحها التطورات الدولية المعاصرة والمستقبلية.
- إن التعقيدات والإشكالات التي تطرحها الهجمات الالكترونية تقتضي دراسة كل حالة على حدى في ضوء نطاقها، لوضع تصور عام حول المعايير أو بالأحرى الضوابط الواجب الاستناد إليها لتبرير الأحقية في اللجوء للدفاع الشرعي من عدمه.
- أمام التحديات التي تواجه الفضاء السيبراني عموماً لا بد من وضع مبادئ دولية تستجيب لمقتضيات ممارسة الدفاع الشرعي لمواجهة الجوسسة الرقمية، من خلال إصدار ثالث لمبادئ تالين، لما لا، يتم من خلاله وضع الحدود الفاصلة مع التدابير المضادة، وضوابط تستجيب لتأثيرات الجوسسة في الفضاء الرقمي.
- إبرام اتفاقيات دولية تستجيب لمقتضيات البيئة الرقمية، وما تطرحه من اعتبارات تدخل ضمن استعمال القوة، بعد رفع الاهتمامات المتوصل إليها والتعقيدات وكذا الحلول المطروحة في نطاق الدراسات الفقهية، أو أمام الهيئات القضائية الدولية في خطوة لمواصلة مجهودات اتفاقية بودابست التي اعتبرتها من الاعمال غير المشروعة وضرورة ادراجها ضمن استعمالات القوة وفق ضوابط محددة بدقة.
- لما كان الدفاع الشرعي عموماً يشكل استثناء عن منع تبني القوة، فإن استعماله وبشكل خاص عن القوة الالكترونية يتطلب وضع ضوابط قانونية تستجيب للتأثيرات التي تمارسها الهجمات الرقمية.

الهوامش:

¹ - شريف نسيم، دليل تالين: الهجمات الالكترونية وحظر استخدام القوة، نوفمبر 2017، تم الاطلاع عليه بتاريخ 25 أبريل 2024 على الساعة العاشرة على الموقع:

https://accronline.com/article_detail.aspx?id=28958

² - نجاري بن حاج علي فايزة، جريمة التجسس الالكتروني، مجلة دراسة استراتيجية، العدد 11، السداسي الأول، 2019 ص 66.

³ - سميرة شرايطية، السيادة السيبرانية في الصين: بين متطلبات القوة وضروريات الأمن القومي، المجلة الجزائرية للأمن والتنمية، 2020، ص 398.

- زينب رياض جبر، التجسس الرقمي في ضوء قواعد القانون الدولي العام، المركز العربي، للنشر والتوزيع، القاهرة، 2023، ص 28.

- ⁴ - Etude approfondie sur le phénomène de la cybercriminalité et les mesure prise par les Etats membres, la communauté internationale et le secteur privés pour y faire face Vienne25628 FEVRIER 2013 P12, vu le 28 Septembre 2024 à 10h00 ; in : https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/UNODC_CCPCJ_EG4_2013_2_F.pdf,.
- ⁵ - راجع في هذا الاتجاه: شريف نسيم، مرجع سابق.
- ⁶ - محكمة العدل الدولية، موجز الأحكام والفتاوى الصادرة عن المحكمة، 1992-1969، مشروعية التهديد بالأسلحة النووية واستخدامها، 08 جويلية 1996، ص 116، الفقرات 35-36، على الموقع الإلكتروني للمحكمة: www.cij-cij.org
- ⁷ - أنظر في ذلك: سامر نمر سالم، مرجع سابق، ص 123.
- ⁸ - قام بإعداده مجموعة من فقهاء القانون الدولي، نشر الإصدار الأول منه عام 2013، ويحتوي على 95 قاعدة قانونية إرشادية لعمل أو سلوك الدول في سياق الحرب الإلكترونية، وصدر الإصدار الثاني منه في العام 2017، ويحتوي على 154 قاعدة، يعد أكثر اتساعاً من الإصدار الأول ويحسم في جوانب عدم الاتفاق لما جاء في الإصدار الأول.
- ⁹ - أنظر في حجج هذا الاتجاه: زينب رياض جبر، مرجع سابق، ص 108 - 117.
- ¹⁰ - محمود سليمان موسى، التجسس الدولي والحماية الدولية للدفاع الوطني وأمن الدولة، منشأة المعارف، الإسكندرية، 2001، ص 187.
- ¹¹ - Conseil de l'Europ, convention sur la cybercriminalité, Budapest 23.XI.2001 , in : <https://www.europarl.europa.eu>
- ¹² - زينب رياض جبر، مرجع سابق، ص 114.
- ¹³ - سامر نمر سالم الجاروشة، الجرائم السيبرانية وحقوق الإنسان، دار النهضة العربية، القاهرة، 2023، ص 47-48.
- ¹⁴ - أنظر في تفاصيل ذلك: زينب رياض جبر، مرجع سابق، ص 140 وما بعدها.
- ¹⁵ - Michael Schmitt , Classification of cyber conflit, journal of conflict & Security Law(2012), Vol 17, N° 2,pp, 245-260
- ¹⁶ - Erik Kodar, Applying the law of armed conflict to cyber attacks : From the MARTENS clause to additional protocol, ENDC Proceedings, Volume15,2012,pp 107-132(109) ,29/09/2024at 10h, in:; <https://ksk.edu.ee>
- ¹⁷ - زينب رياض جبر، مرجع سابق، ص 128.
- ¹⁸ - Michael Schmit, Tallin manual on the international law applicable to cyber warfare ;CAMBRIDGE University press, 2013, p64
- ¹⁹ - محكمة العدل الدولية، القضية المتعلقة بالأنشطة العسكرية والشبه العسكرية في نيكارغوا وضدها (نيكارغوا ضد الولايات المتحدة الأمريكية)، حكم صادر في 27 يونيو 1987 موجز الأحكام والفتاوى والأوامر الصادرة عن المحكمة 1991-1948.
- الفقرتين 210-211، ص 219، على الموقع الإلكتروني للمحكمة: www.cij-cij.org
- ²⁰ - JONATHAN A.OPHARDT, Cyber warfare and the crime of aggression : The need for individual accountability on tomorrow's battlefield; Duke law & Technology review;N°3,2010 p
- ²¹ - سيف غانم السويدي، مدى مشروعية الدفاع الشرعي الاستباقي وفقاً لأحكام قواعد القانون الدولي المعاصر، مجلة الأمن والقانون، العدد 02، 2008، ص 244.
- ²² - عماد حسن محمد إبراهيم، التدابير المضادة ومدى مشروعيتها في مواجهة الهجمات السيبرانية المعادية في القانون الدولي العام، مجلة البحوث القانونية والاقتصادية، كلية الحقوق جامعة المنوفية، المجلد 54، العدد 03، أكتوبر 2021، ص 198.
- ²³ - محكمة العدل الدولية، القضية المتعلقة بالأنشطة العسكرية والشبه العسكرية في نيكارغوا، مرجع سابق، ص 2019.
- ²⁴ - عماد حسن محمد إبراهيم، مرجع سابق، ص 199 وما بعدها.