المجلة الإلكترونية الشاملة متعددة التخصصات
العدد الثاني والأربعون (شهر ١١) ٢٠٢١

عنوان الدراسة

إشكاليات ممارسة حق الدفاع الشرعي الوقائي عن النفس رداً على الهجوم الإلكتروني المسلح "الوشيك"

Problematics of practicing the right to anticipatory self-defense in response to an imminent armed cyber-attack

اسم الباحث: شريف نسيم قلته بخيت

الدرجة العلمية: باحث دكتوراه مرحلة إعداد رسالة، كلية الاقتصاد والعلوم السياسية جامعة القاهرة

الإيميل: Sherif_angel2000@yahoo.com

ملخص

هدفت الدراسة مناقشة إمكانية ممارسة حق الدفاع الشرعي الوقائي في القانون الدولي ردا على هجوم إلكتروني مسلح وشيك. وواقع الأمر، تواجه هذه الممارسة عملياً ثلاثة تحديات رئيسية، وهما: تحدى النطاق الزمني الصارم لمعيار كارولين، وتحدى تكييف عتبة جسامة الهجوم الإلكتروني المسلح الوشيك، وتحدى الإسناد. وفى سياق تلك التحديات، خاصة تحدى نطاق الزمنى الصارم؛ اقترح مجموعة من الفقهاء ما يسمى اقتراب نافذة الفرصة الأخيرة الممكنة، وذلك لتأصيل ممارسة مشروعة لحق دفاع شرعي "استباقى" ردا على الهجوم الإلكتروني المسلح الوشيك. وخلصت الدراسة إلى صعوبة تأصيل ممارسة لحق دفاع شرعي وقائي أو استباقى لرد الهجوم الإلكتروني المسلح الوشيك.

الكلمات المفتاحية: حق الدفاع الشرعي الوقائي، الجسامة، نافذة الفرصة الأخيرة، الوشيك، الإسناد، الهجوم المسلح، هجوم إلكتروني

Abstract

The study aimed to discuss the possibility of practicing the right to anticipatory self-defense in international law in response to an imminent armed cyber-attack. In practice, this practice faces three main challenges: the challenge of the strict time-scale of the Caroline criterion, the challenge of adapting the gravity threshold of the imminent armed cyber-attack, and the challenge of attribution. In the context of those challenges, especially the challenge of the strict time scale; A group of jurists suggested the approach of the last possible window of opportunity, in order to establish a legitimate practice of the right to "preemptive" defense in response to the imminent armed cyber-attack. The study concluded that it is difficult to establish a practice of right to anticipatory or preemptive self-defense to respond to an imminent armed cyber- attack.

Key words: Anticipatory self-defence, Gravity, Last window of Opportunity, Imminent, Attribution, Armed attack, Cyber-attack

مقدمة

تعد مشروعية حق الدفاع الشرعي الوقائي عن النفس من أكثر الموضوعات التي دار بشأنها جدالا فقهيا. ويكمن جوهر هذا الجدل في مدى توافق حق الدفاع الشرعي الوقائي مع نص المادة 51 التي نصت صرحة، بأن ممارسة حق الدفاع الشرعي يكون رداً على هجوم مسلح قائم وليس "وشيكا". ومع ذلك، يرى الجانب الفقهي المؤيد لحق الدفاع الشرعي الوقائي أن نص المادة 51 لا يتعارض مع الممارسة العرفية المشروعية لحق الدفاع الوقائي السابقة على تأسيس الميثاق.

وبالإضافة إلى الحجج الفقهية الداعمة لمشروعية حق الدفاع الشرعي الوقائي؛ يستمد هذا الحق مشروعيته أيضا من اعتبار موضوعي مؤداه عدم معقولية أن تقف الدول مكتوفة اليد لردع هجوم مسلح وشيك ضدها خاصة مع التطور الهائل في الأسلحة الهجومية، ينذر بتبعات شديدة الكارثية على أمنها ومصالحها القومية.

واستناداً إلى هذه الحجج الفقهية والموضوعية الداعمة لمشروعية حق الدفاع الشرعي الوقائي؛ يؤيد جانب لا يستهان به من الفقهاء خاصة "خبراء دليل تالين" ممارسة حق الدفاع الوقائي ضد الهجمات الإلكترونية المسلحة الوشيكة. ومع ذلك، تواجه هذه الممارسة عملياً بعض التحديات أهمها على الإطلاق تحدى النطاق الزمنى الصارم الذى كرسته عقيدة "كارولين" لمفهوم "الوشيك". وهو التحدي الذى يجعل من المستحيل عملياً الرد على هجوم إلكتروني مسلح وشيك بسبب سرعته الرهيبة والخاطفة. كما تواجه هذه الممارسة بتحديين آخرين وهما: تحدى تكييف عتبة جسامة الهجوم الوشيك، أو تحدى مستوى التيقن من أن الغرض والنوايا الحقيقية للهجوم الإلكتروني الوشيك هو إحداث خسائر مادية فادحة. ويكمن التحدي الثاني، في إسناد الهجوم الإلكتروني المسلح الوشيك.

ويمكن القول أن هذين التحديين ذات ارتباط وثيق بتحدي النطاق الزمنى الصارم لمفهوم "الوشيك". إذ سيكون من المفترض أن تكون الدولة الضحية قد كيفت عتبة الجسامة وبنت إسناداً صحيحا لهجوم وشيك خاطف لا يستغرق حتى يصل إلى هدفه إلا بضع ثواني محدودة.

وإزاء التحديات التي تواجه ممارسة حق الدفاع الشرعي الوقائي ردا على الهجوم الإلكتروني المسلح الوشيك وبخاصة تحدى النطاق الزمنى الصارم للوشيك؛ قدم جانب من الفقه القانون الدولي ما يسمى "اقتراب نافذة الفرصة الأخيرة الممكنة" يسعى من خلاله إلى تكريس ممارسة مشروعية لحق الدفاع الوقائي رداً على الهجوم المسلح الوشيك. وتستند هذه الممارسة المشروعية عملا بالاقتراب على ضرورة توسيع النطاق الزمنى الصارم لمفهوم الوشيك أو منحه درجة كافية من المرونة حتى يتسنى للدول الرد-بشكل استباقي- على الهجمات الإلكترونية الوشيكة أثناء مراحل التحضير لها أو في مراحلها التمهيدية وليس بعد انطلاقها بلا عودة بشكل خاطف. واستناداً أيضا إلى المرونة الزمنية لمفهوم الوشيك يمكن التغلب نسبياً على تحديي الجسامة والإسناد.

وبناء على ما تقدم، تتمحور المشكلة البحثية لهذه الدراسة في مناقشة أبرز الإشكاليات والتحديات التي تواجه ممارسة حق الدفاع الشرعي الوقائي عن النفس في القانون الدولي العرفي ردا على هجوم إلكتروني مسلح "وشيك". وأيضا، مناقشة ما مدى إمكانية تأصيل ممارسة مشروعة وموضوعية لحق دفاع شرعي وقائي عن النفس عملاً باقتراب نافذة الفرصة الأخيرة.

وتنقسم هذه الدراسة إلى ثلاثة مباحث:

الأول- حق الدفاع الشرعي الوقائي في القانون الدولي العرفي

الثاني: تحديات ممارسة حق الدفاع الشرعي الوقائي ردا على الهجوم الإلكتروني المسلح الوشيك

الثالث: الهجوم الإلكتروني الوشيك واقتراب نافذة الفرصة الأخيرة الممكنة

المبحث الأول: حق الدفاع الشرعي الوقائي في القانون الدولي العرفي

أولا: مفهوم حق الدفاع الشرعي الوقائي وشروط ممارسته

يُستمد مفهوم حق الدفاع الشرعي الوقائي Anticipatory Self-Defence وشروط ممارسته ومشروعيته أيضا، كممارسة عرفية راسخة قبل تأسيس الميثاق من حادثة "كارولين" أو ما بات يعرف بعقيدة "كارولين". ففي العام 1837، صاخ وزير الخارجية الأمريكية دانيال ويبستير Daniel Webster تعريف الدفاع الشرعي الذى تطور لقانون دولي عرفي وذلك على خلفية ما يعرف بحادثة كارولين Caroline Incident. إذ كانت كارولين سفينة أمريكية تحاول نقل الإمدادات إلى المتمردين الكنديين واعترضت القوات البريطانية رحلة كارولين وأطلقت عليها النار مما أدى إلى إشعالها وإسقاطها من فوق شلالات نياجرا. وفى أعقاب الحادث، قال ويبستير إن تصرف بريطانيا لا يعد دفاعاً عن النفس؛ لأن الدفاع عن النفس له ما يبرره فقط، إذا كانت ضرورة الدفاع عن النفس فورية، ساحقة، ولا تترك خيارا لوسائل أخرى، ولا لحظة للتداول. كما كان بإمكان بريطانيا التعامل مع الموقف بطريقة أكثر دبلوماسية. ومن هنا، وضعت عقيدة ويبستير أو كارولين، مجموعة من الضوابط المقيدة لممارسة الحق وهى الاستجابة الضرورية والفورية في حال استنفاذ جميع الوسائل السلمية لحل النزاع، وأن تكون هذه الاستجابة متناسبة أيضا[1].

وتأسيساً على عقيدة "كارولين"، يعرف الفقهاء حق الدفاع الشرعي الوقائي باستخدام القوة بغرض الدفاع عن النفس كسبيل وحيد أو كملاذ أخير أو كضرورة لدرء هجوم مسلح وشيك Imminent ساحق جسيم مع مراعاة تناسب الرد مع جسامة العدوان. وتأسيساً على هذا التعريف الذى هو محل إجماع فقهى والمتسق مع التفسير الضيق لعقيدة كارولين، تحكم مشروعية ممارسة حق الدفاع الشرعي الوقائي ثلاثة ضوابط أو قيود رئيسية: أن يكون لرد هجوم مسلح "وشيك" ساحق لم ينطلق فعليا أو لم يوجه فعليا إلى الدولة المستهدفة بالهجوم لكن هناك العديد من الملابسات والشواهد الجازمة بقرب وقوع هذا الهجوم كإعلان حالة الحرب وحشد قوات عسكرية ضخمة على حدود الدولة المستهدفة. أن يكون استخدام القوة

[1] Guiora, A.N.(2008), "Anticipatory Self-Defence and International Law- A Re-Evaluation", ***Journal of Conflict & Security Law***, Vol. 13 No. 1, pp. 8.9.

لرد هذا الهجوم الوشيك ضرورة بعد انقطاع أية سبل أخرى أمام الدولة المستهدفة أو الضحية لرد هذا الهجوم. تناسب الرد مع جسامة الهجوم والتهديد[2].

ورغم ما تبدو شروط أو ضوابط ممارسة حق الدفاع الشرعي الوقائي بسيطة وواضحة. إلا أنه في بعض الأوقات قد يصعب التيقن منها وبخاصة شرط "الهجوم الوشيك". ومراعاة البعض الآخر وتحديدا التناسب في الرد. ويعد شرط أو مفهوم "الوشيك" والذى هو أساس ممارسة حق الدفاع الشرعي الوقائي من أكثر الشروط إشكالية. فالمفهوم ليس له تعريف محدد أو دقيق في القانون الدولي. وفى بعض الأحيان قد يكون من غير الواضح متى يكون هذا الهجوم وشيك، أو كيف وبأي وسائل تبرر الدولة المستهدفة بشكل معقول وجود هجوم خطير وشيك يستهدفها. وفى سياق ذلك، رأت محكمة العدل الدولية في مناسبة نظرها لقضية "مشروع جابيتشيكوفو-ناغيماروس Gabčikovo-Nagymaros Project" بين المجر وسلوفاكيا عام 1977. أن مفهوم الوشيك مرادفا "للفورية" أو القرب "Proximity وأنه يتجاوز مفهوم "الإمكانية أو الاحتمالية "Possibility. واستنادا إلى ذلك، حددت المحكمة نطاق مفهوم الوشيك بشكل صارم حيث يقع على عاتق الدولة المتذرعة بحق الدفاع الشرعي الوقائي في المقام الأول عبء إثبات وجود تهديدات مسلحة خطيرة حقيقية فورية أو قريبة الحدوث وليست محتملة. واتساقاً أيضا مع المفهوم الصارم للوشيك، لا مناص أمام إثبات هذا الهجوم الوشيك وبشكل معقول إلا من خلال مجموعة مواقف وشواهد وأجواء قوية تدل على نية واستعدادات نهائية من قبل المعتدى لشن هجوم مسلح وشيك أو اقتراب تصعيد عسكري لا لبس فيه ضد الدولة الضحية. وفى هذا الصدد، يرى بعض الفقهاء أن جسامة الصفة العسكرية الحركية وذلك من حيث الانتشار والحشد والاستعداد المكثف للقوة العسكرية على حدود الدولة المستهدفة يعد بمثابة أكثر الشواهد الجازمة على وجود هجوم وشيك يستهدف الدولة الضحية. إذ في بعض الأحيان قد يُفسر التهديد بالحرب والتصريحات الشديد العداء على أنها هجمات وشيكة لكنها دون تحرك عسكري مكثف حقيقي يمكن تفسيرها بالمحتملة وليست الوشيكة .[3]

---

[2] Dunlap, C.J.(2013), "Anticipatory Self-Defense and The Israeli-Iranian Crisis: Some Remarks", ***ILSA Journal of International & Comparative Law***, Vol.19, No.2, p.327.

[3] Mastrolembo, R.(2019), "Imminence and States' rights to Anticipatory self-Defence: Responding to Contemporary Security Threats and Divergence in Legal Diplomacy", ***Canberra Law Review***, Vol.16, No.1, pp. 144.145.

أما فيما يتعلق بشرط التناسب فيمثل إشكالية حقيقية لأن الدولة المستهدفة ستكون بصدد الرد على هجوم مسلح وشيك لم يقع بعد. وبالتالي، فتقدير حجم القوة المستخدمة ونوعيتها لتناسب جسامة الهجوم أمر غاية في الصعوبة وسيختلف من حالة إلى حالة ووفقا لتطورات الموقف. وعليه، يرى جانب من الفقه أن الدولة الضحية يجب تقييد استخدام القوة إلى أقصى حد ممكن وتوجيهها فقط ضد الأهداف والمعدات العسكرية التي تجزم بأنها في وضع استعداد لتوجيه هجمات. وفى المقام الأخير، سيقع على الدولة الضحية عبء إثبات عدم خرقها لشرط التناسب عبر أدلة متنوعة على درجة عالية من الإقناع والموثوقية. وينسحب هذا الأمر أيضا على عبء إثبات هجوم مسلح وشيك[4].

ثانيا: الجدل الفقهي حول مشروعية حق الدفاع الشرعي الوقائي

اختلف الفقه الدولي في مدى مشروعية الدفاع الشرعي الوقائي. فهناك من يرى عدم مشروعيته، وهم من أنصار التفسير النصي أو المقيد للمادة 51، ويستندون في ذلك بأن المادة 51 من الميثاق هي الإطار القانوني الوحيد ذات الصلة بمسالة حق الدفاع الشرعي عن النفس بشكل عام، وتفسيرها بشكل صحيح يحظر أي عمل استباقي للدولة في الدفاع عن نفسها. فالمادة 51، قد استخدمت بوضوح عبارة "حالة وقوع أو حدوث Occurs هجوم مسلح" ولم تستخدم كلمة وشيك. فضلا عن أن الغرض الرئيسي للمادة هو تقييد استخدام القوة بشكل أحادي أو جماعي إلى أبعد حد ممكن لضمان السلم والأمن الدوليين. ويستند أنصار التفسير النصي، والمعارضين بشكل عام إلى فرضية رئيسية وهي الصعوبة الشديدة في وضع معايير موضوعية لتقييم "الهجوم المسلح الوشيك" حيث عادة ما يترك التقييم لتقدير الدولة المعنية. مما يفسح المجال على نحو واسع لإساءة استخدام تلك السلطة التقديرية، كما يصعب الوفاء بمتطلب التناسب ما دام الهجوم لم يقع بعد[5].

---

[4] Lubell, N.(2015) "The Problem of Imminence in an Uncertain World", in: Weller, M, ed, ***The Oxford Handbook of The Use of Force in International Law***, Oxford University Press, p. 717.

[5] ينظر:

- Dunlap, C.J., ibid, p.325.
- Nilsson, C.(2008), ***The Legality of Anticipatory Self-Defence in International Law***, Master Thesis: University of Lund, pp. 31.32.
- Shiryaev, Y.(2008), "The Right of Armed Self-Defense in International Law and Self-Defense Arguments Used in the Second Lebanon War", ***Acta Societatis Martensis***, No.3, p. 82.

وينتهي المعارضون لحق الدفاع الشرعي الوقائي إلى أن حق الدفاع الشرعي منذ إنشاء عصبة الأمم وحتى الآن مقيد بضرورة وقوع مسلح على إقليم الدولة، مستندين في ذلك إلى أن الممارسة الدولية منذ عام 1945 وحتى الآن تقصر حق الدفاع الشرعي على وقوع هجوم مسلح[6].

أما المدافعون أو من يرون بمشروعية حق الدفاع الشرعي الوقائي، فسيتندون على أن حالة الدفاع الشرعي لا تتوقف عند وقوع هجوم أو اعتداء مسلح، بل تمتد أيضا إلى حالة الاعتداء الوشيك، أو حالة التهديد بالعدوان، لأن المادة 51 من الميثاق أقرت الحق الطبيعي في الدفاع عن النفس دون قيد. فالمادة 51 تتضمن القانون الدولي العرفي كما هو موضح في معيار كارولين والتي تسمح بالدفاع عن النفس بشكل وقائي. فوفقا لمبدأ كارولين تستطيع الدول الرد على "هجوم أو تهديد وشيك" عندما لا يترك لحظة للتداول أو أية تأجيل قد يؤدى إلى عدم قدرة الدولة على الرد بفاعلية شريطة تيقن الدولة بناء على دليل موثوق أو شواهد مادية قوية بأن هجوم يتم الإعداد له ضدها. كما أن مشروعية هذا الحق ليست وليدة ميثاق الأمم المتحدة، بل أقرتها الأعراف الدولية وقرارات المحاكم استناداً إلى حالة الضرورة التي لا يكون معها مجال أو وقت لاختيار وسيلة أخرى لدفع الخطر، شريطة أن يكون الخطر جديا ووشيك الوقوع، وأن تكون الإجراءات الوقائية التي تمارسها الدولة دفاعاً عن النفس معقولة ومحددة بضرورة الحماية فقط. وبناء على ذلك، يميز أنصار حق الدفاع الشرعي الوقائي بين مفهومي "التهديد الوشيك" و "التهديد المحتمل"، فاستخدام القوة ضد الأخير غير مشروع عامة[7].

ويعد Hans Kelsen، من أبرز الداعمين للتفسير الواسع للمادة 51، حيث يؤكد أن الدفاع الشرعي الوقائي قانوني إذا كان التهديد وشيك أو حقيقي. ويرى جانب آخر من المدافعين عن الدفاع الوقائي أن

---

[6] - شامية، أحمد زهير، والجاسم، طارق (2014)، "الدفاع الشرعي الوقائي ومدى مشروعيته في العلاقات الدولية"، **مجلة جامعة البعث**، المجلد 36- العدد 6، ص. 175.

[7] ينظر:

Hoisington, M.(2009), "Cyberwarfare and the Use of Force Giving Rise to the Right of Self-Defense", ***Boston College International and Comparative Law Review***, Vol.32, Article 16, pp. 449.450.

- Barak, D.R.(2018), ***Underground Warfare***, Oxford University Press, pp. 132.133.

- شامية، أحمد زهير، والجاسم، طارق، مرجع سابق، ص ص 172. 173.

المادة 51 تغطى التهديدات الوشيكة، على أساس أنه لا يوجد هجوم مسلح وليد اللحظة بل كل هجوم مسلح يسبقه إعداد وهو ما يتوجب حق الدفاع الوقائي[8].

والمؤيدون لحق الدفاع الشرعي الوقائي يستندون على نحو عام على ثلاثة حجج أساسية:

الأولى- هي نص المادة 51 ذاته التي لم تنشأ حقا للدفاع عن النفس، بل حافظت على "الحق الأصيل" للدول في الدفاع عن النفس الذي سبق تأسيس الميثاق ذاته في العام 1945، والذي تضمن الاعتراف بحق الدول في الدفاع عن النفس ضد أية هجوم وشيك وذلك وفقا لمعيار كارولين. فلغة المادة التي جاءت صراحة بعبارة "في حال حدوث هجوم مسلح" لا ترد، وفقا للداعين، عليها قيود بشان "الحق الأصيل" للدول، بل تنصرف ببساطة إلى نوع الحق العام المحفوظ. فعلى الرغم من أن محكمة العدل الدولية في رأيها الاستشاري بشأن مشروعية الدفاع ضد الأسلحة النووية لم تعطى رأيا جازماً في هذا الشأن؛ إلا أن المحكمة قد أقرت بحق الدول في الدفاع عن نفسها باستخدام الوسائل اللازمة عندما يكون بقاءها على المحك. وهو أمر في غاية المنطقية لتبرير الدفاع الشرعي الوقائي في حالات الضرورة القصوى. فالمادة 51 لا ينبغي أن تفسر بشكل متعسف على نحو يقيد استعمال حق الدفاع بشرط حدوث هجوم مسلح فعلى قد يهدد بقاء الدولة.

والثانية- تكمن في التفسير الواسع لمفهوم "الهجوم المسلح" الذي يتضمن "الهجوم الوشيك". فالهجوم المسلح لا يشترط أن يكون الهجوم الذي تم القيام به بالفعل وأحدث أضرار مادية جسيمة بالدولة الضحية، بل عادة ما يتم تنفيذ الهجوم على مراحل فحشد القوات المسلحة على الحدود على سبيل المثال هو في الواقع الخطوة الأولى لشن هجوم مسلح فعلى.

والثالثة- هي ممارسة الدول منذ العام 1945، والتي تشير إلى قبول عام لفكرة حق الدفاع الشرعي الوقائي كعرف. ومن الأمثلة على ذلك، حصار كوبا في العام 1962، ضرب إسرائيل للمنشآت النووية العراقية في العام 1981، والقصف الأمريكي على ليبيا في العام 1998. لذلك، يرى المدافعون، أن

[8] Pank, S.C.(2014), "What is the Scope of Legal Self-Defense In International Law? Jus ad Bellum with a Special View to New Frontiers for Self-Defense", **Specialeafhandling** 19, p.34.

أنصار التفسير النصي الضيق للمادة 51، كسند لرفض حق الدفاع الشرعي الوقائي يتجاهلون تطور العرف الدولي بشأن حق الدفاع الشرعي[9].

المبحث الثاني: تحديات ممارسة حق الدفاع الشرعي الوقائي ردا على الهجوم الإلكتروني المسلح الوشيك

أولاً: تحدى النطاق الزمنى الصارم لمعيار كارولين

كرس معيار كارولين ممارسة حق الدفاع الشرعي الوقائي في حالة واحدة وهى لرد هجوم مسلح "وشيك" ساحق لا يترك أية خيارات أو وسائل أخرى لإيقافه ولا لاحظة للتداول. إذ تستند مشروعية ممارسة حق الدفاع الشرعي الوقائي على مراعاة النطاق الزمنى الصارم لهجوم أو تهديد مسلح "وشيك" في مرحلته النهائية قبل انطلاقه أو وصوله إلى هدفه فعلياً. بيد أن، السرعة الخاطفة للهجوم الإلكتروني؛ قد جعلت من إمكانية الرد عليه وقائيا خلال الفترة الزمنية الصارمة لمعيار كارولين مسألة شبه مستحيلة. والتي من المفترض أن تكون اللحظات الأخيرة التي يكون فيها المهاجم على "وشك" النقر فوق الزر الإلكتروني لإطلاق الهجوم الإلكتروني. وحتى إذا قام المهاجم بإطلاق الهجوم الإلكتروني، من المحال أيضا أن يتم الرد عليه وقائيا، لأن الفارق الزمنى ما بين الضغط على الزر ووصول الهجوم لهدفه لا يتعدى بضع ثواني محدودة بسبب سرعته الرهينة. وبالتالي، لن يكون هناك أية متسع من الوقت أمام الدولة الضحية لإيقافه[10].

---

[9] ينظر:

- Nilsson, C., ibid, p.34.
- Murphy, S.D.(2005), "The Doctrine of Preemptive Self-Defense", ***Villanova Law Review,*** Vol. 50, No.3, pp. 711.713.

[10] ينظر:

- Svarc, D.(2006), "Redefining Imminence: The Use of Force against Threats and Armed Attacks in the Twenty-First Century", ***ILSA Journal of International Law***, Vol.13, No. 1, pp. 182-183.
- Hayward, R.J.(2017), "Evaluating The (Imminence) of A cyber Attack For Purposes Of Anticipatory Self-Defense", ***Columbia Law Review.*** Vol. 117, No.2, p.414.
- Shahriar, S.R. (2020), "The Issue of Imminence: Can the Threat of a Cyber- Attack Invoke the Right to Anticipatory Self-Defence Under International Law?", ***UCL Journal of Law and Jurisprudence***, Vol.9, pp. 73.75.

ومن المفارقات الدالة في هذا الصدد، هو موقف أستراليا، إذ برغم تأييدها التام للتذرع بحق الدفاع الشرعي الوقائي ردا على الهجمات الإلكترونية المسلحة الوشيكة، وذلك حسبما جاء في استراتيجية أستراليا الدولية للانخراط الإلكتروني:

قد تتذرع الدولة بحقها في الدفاع الشرعي الوقائي ردا على هجوم مسلح عندما يتضح لديها أن المهاجم بصدد شن هجوم مسلح، في الظروف التي ستفقد فيها الدولة الضحية فرصتها الأخيرة للدفاع عن نفسها بفاعلية إذا لم تتصرف. ويعكس هذا التصرف طبيعة التهديدات المعاصرة.... إذ لا يعقل أيضا ألا تتخذ الدولة الضحية إجراء قبل لحظة انطلاق هجوم إلكتروني مسلح يمكن أن يتم شنه في جزء من الثانية مسببا حدوث خسائر جسيمة للأفراد والبنية التحتية الحيوية للدولة

ومع ذلك، فحسبما جاء في الاستراتيجية أيضا، يواجه هذا الحق الكثير من التحديات التي تبدو عصية عن الحل، كسرعة الهجمات الإلكترونية فضلا عن طبيعتها التي تتسم بخاصية إخفاء الهوية[11].

إذ من التحديات الكبيرة التي يفرضها النطاق الزمنى الصارم في ظل السرعة الخاطفة للهجوم الإلكتروني، هو استحالة تقييم أو تقدير أضرار الهجوم المسلح الإلكتروني الوشيك بشكل دقيق. وبالتالي، صعوبة تقييم كيفية الرد عليه بشكل وقائي خلال تلك الفترة الزمنية. وبدون إجراء هذا التقدير الدقيق، لاسيما وأن الرد سيكون على هجوم وشيك وليس قائم، سيشكل الرد إخلالاً جسيما بمتطلب التناسب[12].

واتساقاً مع ما سبق، يمكن القول أيضا، أن الطبيعة السرية لتنفيذ الهجمات الإلكترونية، والسمة غير المرئية للهجمات الإلكترونية والفضاء الإلكتروني؛ أمور من شانها أن تعذر الرد وقائياً على هجوم وشيك خلال الفترة الزمنية الصارمة للوشيك. إذ لا تترك هذه الخصائص أية أدلة أو شواهد قوية للاستدلال على هجوم إلكتروني وشيك في مرحلته النهائية، أو على وشك أن ينطلق فورا بشكل لا رجعه فيه. وهذا على النقيض تماماً، من السياق التقليدي للهجمات المسلحة، الذى تتوافر فيه الكثير من الأدلة والشواهد المادية القوية الدالة بشكل لا لبس فيه على اقتراب هجوم مسلح أو نوايا بشن هجوم مسلح بشكل لا رجعة فيه،

[11] Australia's International Cyber Engagement Strategy, "2019 International Law Supplement", Annex A: Supplement to Australia's Position on the Application of International Law to State Conduct in Cyberspace,https://www.dfat.gov.au/publications/international-relations/international-cyber-engagement strategy/aices/chapters/2019_international_law_supplement.html.

[12] Hoisington, M, ibid, pp. 451.452.

مثل التعبئة المكثفة للقوات العسكرية على الحدود (كأبرز هذه الشواهد) وقد يرافقها تهديدات صريحة وتصريحات عدائية، أو زيادة نشاطات المراقبة والاستطلاع، أو التسلل السرى لعملاء المخابرات[13].

وعليه، لا يشكل النطاق الزمنى الصارم لمفهوم الوشيك حائلا أو تحدياً كبيراً أمام ممارسة حق الدفاع الشرعي رداً على هجوم إلكتروني مسلح وشيك، بل يُعذر في حقيقية الأمر من إمكانية ممارسة الحق من أساسه، بل ربما يدفعه هذا التحدي إلى ممارسة مرنه أو واسعة مختلفة تماما

ثانيا: إشكالية تكييف عتبة جسامة الهجوم الإلكتروني المسلح الوشيك، والتأكد من النوايا لارتكاب هجوم إلكتروني مسلح

في سياق الجدل الفقهي بشأن إمكانية الاحتجاج بحق الدفاع الشرعي عن النفس ردا على هجوم إلكتروني مسلح وفقا للمادة 51 من الميثاق. أثير خلافاً كبيراً، بشأن مدى إمكانية إدراج الهجمات الإلكترونية ضمن نطاق حظر المادة 2(4). أو تصنيفها كقوة بالمعنى المقصود للمادة. وبالتبعية أيضا، مدى إمكانية تصنيف الهجوم الإلكتروني كهجوم مسلح منشئ لحق دفاع شرعي عملا بالمادة 51. إذ يمكن القول في هذا الصدد، أن تصنيف الهجمات الإلكترونية كقوة وفقا للمادة 2(4) أو كهجوم مسلح وفقا للمادة 51؛ يواجه بتحدي رئيسي وهو، تعارض الأسلحة الإلكترونية أو الهجمات الإلكترونية مع التفسير الضيق أو الدراج لمعنى القوة المقصود حظرها وفقا للمادة 2(4)، ألا وهى "القوة المسلحة التقليدية الحركية أو المادية Kinetic/Physical Armed Forces". وللتغلب على هذا التحدي، قدم الفقهاء ثلاثة اقترابات بشأن إمكانية تكييف الهجوم الإلكتروني كاستخدام للقوة عملا بالمادة 2(4) أو كهجوم مسلح عملا بالمادة 51.

(أ): اقتراب الأداة Instrument-based Approach

يستند هذا الاقتراب على السلاح المستخدم كمحدد رئيسي. والمقصود هنا السلاح العسكري الحركي التقليدي. وبالتالي، يرفض مؤيدو هذا الاقتراب تصنيف الهجوم أو السلاح الإلكتروني كقوة وفقا للمادة 2(4) لأنها لا تتصف بتلك الصفة العسكرية الحركية التقليدية. ويرى انصار هذا الاقتراب، أن نص

[13] Horace, B. and Robertson, J.(2002), "Self-Defense against Computer Network Attack under International Law", ***International Law Studies***, Vol.76, p. 138.

الميثاق يدعم هذا الاقتراب خاصة المادة 41 التي حصرت التدابير التي لا تنطوي على استخدام القوة المسلحة كالقطع الجزئي أو الكامل لوسائل الاتصال[14]. كما يرى أنصاره أيضا، أن تكريس هذا الاقتراب في سياق الممارسة الدولية يحول دون توسع مفهوم استخدام القوة بشكل مفرط وغامض[15].

ولم يحظى هذا الاقتراب بالتأييد القوى على المستويين الفقهي والدولي. إذ أن تشبث أنصاره بالتفسير التقليدي لمفهوم القوة يخالف من جهة عدم اعتداد الممارسة الدولية بهذا التفسير الضيق الذى يحصر مفهوم القوة في القوة العسكرية الحركية فقط. ويتناقض، من جهة أخرى، مع حقيقية ما قد تحدثه الهجمات الإلكترونية من تأثيرات أو خسائر مادية أو بشرية. فالهجمات الإلكترونية الواسعة التي شهدها المجتمع الدولي، لاسيما الهجمات الإلكترونية "ستاكسنت" على المفاعلات الإيرانية النووية في 2010، قد أثبتت قدرة تلك الأسلحة غير الحركية على إحداث تأثيرات وأضرار مادية مشابهة لتلك الناجمة عن استخدام الأسلحة الحركية التقليدية[16].

(ب): اقتراب الهدف Target-based Approach

يفترض هذا الاقتراب أن أي هجوم إلكتروني على بنية تحتية حيوية أو هامة يعد استخدام غير مشروع للقوة بالمعنى المقصود للمادة 2(4). وواجه هذا الاقتراب انتقادات عديدة لعدة أسباب أهمها، عدم تركيز هذا الاقتراب على الجسامة وتركيزه عوضا عن ذلك على هدف الهجوم الإلكتروني وهو البنية التحتية. وعلى هذا النحو، يطلق هذا الاقتراب العنان للدول لتكييف أي هجوم إلكتروني يستهدف بنيتها التحتية الحيوية كهجوم مسلح حتى ولو لم تبلغ الأضرار الناجمة عنه حد الجسامة. وواجه هذا الاقتراب انتقادات شديدة أيضا إلى حد وصفه بغير الموضوعي على الإطلاق بسبب عدم وضع أنصاره لمعايير أو تعريفات أو تصنيفات محددة منضبطة لما يعد بنية تحتية حيوية أو حساسة. وخطورة ذلك الأمر، هو

[14] Peagler, J.(2014), "The Stuxnet Attack: A New Form of Warfare and the Inapplicability of Current International Law", ***Arizona Journal of International & Comparative Law***, Vol. 31, No. 2, p.410.
[15] Lahmann, H.(2020), ***Unilateral Remedies to Cyber Operations: Self-Defence, Countermeasures, Necessity, and the Question of Attribution***, New York: Cambridge University Press, p.24.
[16] Holmberg, E.J.(2015), ***Armed Attacks In Cybersapce: Do They Exist and Can They Trigger The Right to Self-Defence?***, Thesis dissertation, Faculty of Law, Stockholm University, pp. 30. 31.

إطلاق العنان للدول في تحديد ما تراه من منظورها بنية تحتية حيوية، مما قد يترتب على ذلك إساءة واضحة في استخدام القوة المسلحة وتصعيد غير مبرر في العلاقات بين الدول[17].

(ج): اقتراب التأثيرات Effects-based Approach

يستند هذا الاقتراب على التأثيرات العامة للهجوم الإلكتروني كمحدد رئيسي بغض النظر عن المستهدف من هذا الهجوم، ومناظرة Analog تلك التأثيرات أو التبعات بالتأثيرات الناجمة عن هجوم مسلح تقليدي لتكييف الهجوم الإلكتروني كاستخدام غير مشروع للقوة وفقا للمادة 2(4) أو كهجوم مسلح عملا بالمادة 51. على سبيل المثال، هجوم إلكتروني استهدف أنظمة التحكم الإلكترونية لسد مائي مما تسبب في تدمير هذا السد وحدوث فيضانات أودت أيضا بحياة عشرات الأشخاص، على هذا الأساس يعد هذا الهجوم الإلكتروني استخدام غير مشروع للقوة أو هجوم مسلح لأنه تبعاته أو أضراره الجسمية كانت ستكون متطابقة تماما لو ضرب هذا السد بسلاح حركي تقليدي-ربما الهجمات الإلكترونية في بعض الأحيان تكون تأثيراتها المادية الجسمية أكثر ضراوة- وفى مثال آخر، هجوم إلكتروني استهدف النظام المالي الإلكتروني للدولة مما تسبب في حدوث خسائر اقتصادية أو فوضى في سوق البورصة. ورغم التأثيرات العامة الواضحة لهذا الهجوم لكن لا يعد استخدام غير مشروع للقوة بالمعنى المقصود للمادة 2(4) لأن تلك التأثيرات الناجمة غير مناظرة ومن الصعب مناظرتها أيضا بالتأثيرات الناجمة لهجوم مسلح تقليدي لغياب الحد الأدنى من الجسامة أو الخطورة أي تدمير منشآت أو وفاة أفراد[18].

والواقع أن الدفاع عن نهج "مقاربة التأثيرات العسكرية" بدلا من التقييد بالنهج الآداتى الحركي التقليدي ليس بالأمر الجديد، فقد أكد عليه الفقه القضائي الدولي في مناسبتين تم الإشارة إليهما آنفا: الأول- نظر محكمة العدل الدولية في قضية النشاطات العسكرية وشبه العسكرية لنيكاراجوا، حينما أقرت بأن تدريب وتسليح الفصائل العسكرية المنخرطة في عمليات ضد دولة أخرى يعد بمثابة استخدام غير

---

[17] ينظر:

- Schmitt, M.N and O'Donell, B.T.(2002), "Computer Network Attack and International Law", ***International Law Studies***, Vol.76, p. 137.
- Radziwill, Y.(2015), ***Cyber-Attacks and the Exploitable Imperfections of International Law***, Brill/Nijhoff, p.138.

[18] ينظر:

- Radziwill, Y, ibid, OP. Cit, p.138.
- Hathaway, O.A.(2014), "The Drawbacks and Dangers of Active Defense", ***NATO CCD COE Publications***, Tallinn, pp. 43.44.

مشروع للقوة وانتهاكاً للمادة 2(4). الثانية في رايها الاستشاري بشأن مشروعية استخدام السلاح النووي أو التهديد به حينما خلصت صراحة أن مصطلح القوة قد جاء في المادة 2(4) منفردا ولم يشير إلى نوع سلاح محدد وأن الاعتبار الأساسي في تحديد القوة غير المشروعة عملا بالمادة 2(4) يكون بناء على التأثيرات الناشئة عنها وليس طبيعة أو نوع السلاح المستخدم. وبذلك، فضلت المحكمة اتباع نهج أوسع لمعنى القوة المقصود حظرها في المادة 2(4) بدلا من قصر هذا الحظر على استخدام القوة المسلحة التقليدية الحركية التفجيرية، لمواكبة التداعيات الخطيرة للأسلحة الدمار الشامل "النووية-الكيميائية، والبيولوجية، التي لا تنطوي بالضرورة على "تأثيرات انفجارية" لكن تأثيراتها وأضرارها الناشئة عنها تفوق في الكثير من الأحيان التأثيرات الناشئة عن السلاح الحركي أو التقليدي. وعليه، فبالقياس على الهجمات الإلكترونية، التي تمثل ضربة جديدة للتفسير الضيق للمادة 2(4)، يمكن تصنيفها بسهولة ضمن نطاق حظر القوة للمادة 2(4)، بناء على مقاربة تأثيراتها العسكرية الناشئة عنها[19].

ويبدو جلياً من واقع تتبع الفقه والممارسة الدولية أن اقتراب التأثيرات الاقتراب الأكثر قبولاً. فبحسب خبراء دليل تالين (1) الذين اعتمدوا معيار "الجسامة Gravity" باعتباره المحدد الرئيسي لتحديد عتبة الهجوم المسلح الإلكتروني، يعد الهجوم الإلكتروني الذى يتسبب في حدوث أضرار جسيمة للمصالح الوطنية الحرجة للدول كتدمير منشآت مدنية وعسكرية حيوية، كذلك الهجوم الإلكتروني الذي يتسبب في وفاة وإصابة عدة كبير من مواطني الدولة، هو فقط الهجوم الذى يرتقى إلى عتبة الهجوم المسلح المنشئ لحق دفاع شرعي[20].

وكانت الولايات المتحدة من أول الدول التي تبنت الاقتراب إذ تعتبر الولايات المتحدة أن التذرع بحق الدفاع الشرعي قد يكون ردا على هجوم إلكتروني مباشر أو "وشيك" يصل إلى عتبة الهجوم المسلح. أو

---

[19] ينظر:
- Delerue, F.(2020), ***Cyber Operations and International Law***, Cambridge University Press, pp. 284.287.
- Michael N. Schmitt, M.N.(2015), "The Use of Cyber Force and International Law", in: Weller, M, ed, ibid, p.1114.
- Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion of 8 July 1996, I.C.J. Reports 1996, Paras. 38.39.

[20] Tallinn Manual 1.0. (2013), ***Tallinn Manual on The International Law Applicable to Cyber Warfare***, Cambridge University Press, Rule 11, Paras. 6-9.

يتشابه في نطاقه وتأثيراته مع الهجوم المسلح التقليدي وذلك من حيث تسببه في قتل أو إصابات جسيمة أو تدمير مادي هائل للمنشآت[21].

لكن على الرغم من ذلك، لاتزال مسألة تكييف عتبة جسامة الهجوم الإلكتروني "الوشيك" إشكالية كبرى. إذ يمكن القول، أن تكييف عتبة جسامة الهجوم المسلح الوشيك في النطاق التقليدي، أو مع الأسلحة الحركية-السهل توقع أضرارها الناشئة الجسيمة- أمر سهل نسبيا لاسيما كلما أزادت الشواهد المادية على انطلاق هذا الهجوم كقيام الدولة المعتدية بعمل حشد عسكري ضخم على حدود الدولة الضحية، مما يبرر مشروعية حق الدفاع الوقائي كضرورة لرد هجوم مسلح وشيك. لكن في مقابل ذلك، تفرض الطبيعة الخاصة للهجمات الإلكترونية، إلى جانب غياب شواهد ومؤشرات مادية قوية على هجوم إلكتروني وشيك؛ تفرض تحدى هائل بشأن تكييف عتبة جسامة الهجوم الإلكتروني كهجوم مسلح، وأيضا بشأن التأكد من نوايا المهاجم في شن هجوم إلكتروني مسلح. إذ في ظل هذه الطبيعة الخاصة للهجمات الإلكترونية، كونها بالأساس مجموعة برامج افتراضية متنوعة التأثيرات والأغراض، من الصعب تحديد أو توقع جسامة أضراها الناشئة إلا بعد وقوعه بالفعل، والوقوف على درجة معقولة من اليقين حول نية مرتكب الهجوم بشن هجوم إلكتروني مسلح. حتى وإن استهدف المهاجم منشئة نووية أو عسكرية حساسة، إذ ليس بالضرورة أن تكون نية المهاجم تدمير هذه المنشأة، بل قد يكون دافعه الحقيقي هو التجسس عليها. وهذا الأمر من الصعب التيقن منه في ظل خاصية التعددية التي تتسم بها الهجمات الإلكترونية[22].

---

[21] Carrielyn D. Guymon (Ed), Digest of United States Practice in International Law 2012, Office of the Legal Adviser United States Department of State, 2012, https://2009-2017.state.gov/documents/organization/211955.pdf.

[22] :

- Carr, J.(2012), ***Inside Cyber Warfare***, O'Reilly Media, Inc., p.70.
- Kesan, J.P and Hayes, C.M. (2012), "Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace", ***Harvard Journal of Law & Technology***, Vol.25, No.2, p.528.
- Rafighdoust, H.(2018), ***The Right of Self-Defence Against Cyber Attacks by States and Non-State Actors***, PhD Thesis, Universitat Autònoma de Barcelona, p. 285.

ففي سياق ذلك، اتفق غالبية خبراء تالين (2) أن مسألة "النية[23]" لا ينبغي أن يعتد بها في مسالة تصنيف عملية إلكترونية كهجوم مسلح، بل ما يجب أن يعتد به فقط في هذا الشأن هو جسامة الحجم والتأثيرات الناشئة عن الهجوم الإلكتروني[24].

ثالثا: تحدى الإسناد

يشكل تحدى الإسناد على نحو عام المعضلة الرئيسة أمام إمكانية تأصيل ممارسة لحق دفاع شرعي ردا على الهجمات الإلكترونية المسلحة. ويتمحور تحدى إسناد الهجوم الإلكتروني في إشكاليتين رئيستين: الأولى- خصوصية الفضاء الإلكتروني والهجمات الإلكتروني. إذ على خلاف النطاق المادي التقليدي للصراعات المسلحة حيث يكون مصدر ومرتكب الهجوم المسلح-حتى ولو فاعل من غير الدول-واضح ومعلوم نسبيا. تواجه مسألة التحديد الدقيق والسريع لمصدر ومرتكب الهجوم الإلكتروني صعوبة بالغة لاسيما التحديد الدقيق لهوية مرتكب الهجوم الإلكتروني، وذلك بسبب النطاق الافتراضي غير المحدود، غير المرئي، وغير المادي للفضاء الإلكتروني. ففي سياق هذا النطاق الافتراضي من الصعب، بل من المستحيل في بعض الأوقات، معرفة منفذ الهجوم الإلكتروني الذى يختبئ وراء أجهزة حاسوب، كذلك المعرفة الدقيقة لمصدر هذا الهجوم في ظل نطاق افتراضي غير محدود شديد التعقيد والترابط ومتبدل باستمرار. وفرضت خصوصية الهجمات الإلكترونية بدورها تحديات هائلة بشأن عبء إسناد الهجمات الإلكترونية. ففي ظل السرعة الرهيبة للهجمات الإلكترونية وسهولة شنها وتوجيهها وتشابه أغراضها وسرعة اختفائها أو زوال أية أثار لها؛ من الصعب توفير دلائل قوية على مصدرها ومرتكبها والنية وراء ارتكابها. يضاف إلى ذلك، أن النطاق غير المادي الخاص للفضاء الإلكتروني والهجمات الإلكترونية، قد

---

[23] من الجدير بالذكر، أن بعض الدول خاصة الولايات المتحدة، قد عرضت موقفها صراحة بشان استنادها إلى معيار النية العدائية لاسيما حال استهداف منشئة أمريكية حيوية في سياق ممارسة حقها لحق الدفاع الشرعي الوقائي. فبحسب وثيقة الاستراتيجية الأمريكية للفضاء الإلكتروني 2011، تحتفظ الولايات المتحدة بحقها في الرد الوقائي ضد أية أعمال أو نوايا أو تهديدات عدائية لبلادنا في الفضاء الإلكتروني. وعليه، يبدو بوضوح من موقف الولايات المتحدة أن التركيز سينصب على الرد دون اعتبار لعتبة الجسامة الضرورية لتبرير مشروعية استخدام القوة وتحديد كيفية الرد أو تقييم درجة ونوعية استخدام القوة. ينظر:

- US International Strategy for Cyberspace, "Prosperity, Security and Openness in a Networked World" May 2011, http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

[24] Tallinn Manual 2.0.(2017), ***Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations,*** Cambridge University Press, Rule 71, Para 14.

عذر من إمكانية توافر أدلة قوية-على عكس الأدلة المادية في النطاق التقليدي- يمكن من خلالها تحديد مصدر ومنفذ الهجوم الإلكتروني بسهولة[25].

والثانية- تقنيات تمويه وإخفاء وتوجيه الهجوم الإلكتروني. إذ في ظل هذه التقنيات من الصعب للغاية تحديد مصدر الهجوم بدقة وبسرعة، ويكاد يكون من المستحيل التوصل إلى هوية أو مرتكب الهجوم الإلكتروني لاسيما وأن أغلب مرتكبي الهجمات الإلكترونية أفراد يعملون لحساب دول. فمن خلال تلك التقنيات، يستطيع مرتكبي الهجمات الإلكترونية إخفاء سجل نشاطهم على الأنترنت أو العناوين الرقمية IP Addresses، لأجهزة الحاسوب الخاصة بهم. بل والأخطر من ذلك، تمكن تلك التقنيات المرتكبين من عمل محاكاة أو انتحال عن بعد لعناوين رقيمة أخرى أو لشبكات إلكترونية حكومية بحيث يجعلون البيانات الرقيمة لأجهزة الحاسوب الخاصة بهم هي نفسها العناوين التي تم انتحالها. يضاف إلى ذلك، أن مرتكبي الهجمات الإلكترونية قد يقومون بشن هجمات عبر أجهزة حاسوب مسروقة في أماكن مختلفة بعيدة تماما عن موطنهم[26].

ومن التقنيات والتكتيكات الأخرى المعروفة، تكتيك الهجمات الإلكترونية متعددة المراحل Multi-stage .Cyber-attacks أو التوجيه المتعدد والذى يعتمد على استخدام خوادم وكيلة Proxies متعددة ترحل عبرها البيانات المشفرة إلى عقد إلكترونية موزعة في الألاف من أجهزة الحاسوب المتفرقة في مناطق عدة حول العالم بحيث تقوم كل عقدة إلكترونية بفك أجزاء من التشفير بحيث تتجمع البيانات الضارة في النهاية في عقدة محددة ويتم توجيهها إلى الهدف المقصود. واستخدمت تلك التقنية في الهجوم الإلكتروني على شركة "سوني Sony" في 2014. الذى تسبب في تعطل الألاف من أجهزة كمبيوتر سوني، وسرقة معلومات الملكية ومعلومات الموظفين الشخصية. حيث لم يخترق منفذي الهجوم سوني

---

[25] John S. Davis, J.S *et al*., (2017), ***Stateless Attribution: Toward International Accountability in Cyberspace***, Santa Monica, Rand, pp. 9-10.

[26] ينظر:

- Candiani, L.(2018), ***The responsibility of actors for cyber-attacks and the problem of attribution. Who can be held responsible from the perspective of International Law's norms on States' responsibility?,*** Master Thesis, Faculty of Law, Tilburg University, The Netherlands, p.44.
- Tran, D.(2018), "The Law of Attribution: Rules for Attributing the Source of a Cyber-Attack", ***The Yale Journal of Law & Technology,*** Vol. 20, p.389.
- Margulies, P.(2013), "Sovereignty and Cyber Attacks: Technology's Challenge to the Law of State Responsibility"**, *Melbourne Journal of International Law,*** Vol.14, pp. 8.9.

مباشرة، بل قاموا بترحيل الهجوم عبر عقد وأجهزة حاسوب متعددة ومواقع مختلفة. فالتتبع الرجعى للهجوم قد كشف عن مصادر متعددة للهجوم كتايلاند وإيطاليا وبولندا وسنغافورة وبوليفيا وقبرص، وخوادم وكيلة متعددة أيضا بما في ذلك خمسة عناوين للبريد الإلكتروني مجهولة في فرنسا[27].

ومن الملاحظ في هذا التكنيك البالغ التعقيد؛ أن تحديد مصدر ومرتكب أو التتبع التقني[28] لتلك الهجمات أمر يكاد يكون مستحيلا ومرهق للغاية. وكلما كان مرتكبي الهجوم على درجة عالية من الاحتراف، كلما قل نجاح التتبع الرجعى لتحديد أصل هذا الهجوم. خاصة وإن كان العقل المدبر لهذا الهجوم دولة تمتلك من الإمكانات والخطط التي تمكنها من تنفيذ الهجوم دون ترك أثار تقنية واضحة[29].

وتتجلى معضلة الإسناد في أوضح صورها في سياق ممارسة هذا الحق ردا على هجوم إلكتروني مسلح وشيك. وذلك بسبب الوقت المحدود للغاية لمعرفة مصدر ومنفذ هذا الهجوم الإلكتروني الوشيك بشكل دقيق، والرد عليه وقائياً خلال تلك الفترة الزمنية المحدودة قبل وصوله لهدفه. وهذا بطبيعة الحال ضربا من المستحيل في ظل الطبيعة الخاطفة للهجمات الإلكترونية، وتحديات الإسناد الإلكترونية، وصعوبة توافر أدلة قوية في الفضاء الإلكتروني يمكن من خلالها الاستدلال على هجوم إلكتروني وشيك، أو توقعه، أو تحديد مصدره بدقة وبشكل سريع. وفى ذات السياق، يمكن القول، إن تذرع الدولة الضحية باستخدام حقها الوقائي ولو من منطلق الاحتجاج بالضرورة ردا على هجوم وشيك أو هجمات تمهيدية معلومة المصدر لكن غير محدد هوية منفذها بدقة، ناهيك عن صعوبة تكييف جسامة تلك الهجمات

---

[27] Kittichaisaree, K.(2017), "Public International Law of Cyberspace, Law, Governance and Technology Series", **Springer International Publishing, Switzerland**, Vol.32, pp. 32-34.

[28] بخصوص تلك المسألة يجب التنويه أن مسالة التطور الكبير فيما يسمى أساليب وأدوات التحليل الجنائي الإلكتروني Cyber Forensic، لا يجب النظر إليها من جهة واحدة لتخفيف عبء الإسناد. ففي مقابل هذا التقدم هناك تقدم موازي للأدوات والأساليب القادرة على مواجهة ومقاومة هذا التقدم، تعكف عليه الفواعل والكيانات والدول التي باتت تستخدم الفضاء الإلكتروني كساحة جديدة لإدارة صراعاتها ومهاجمة خصومها ككوريا الشمالية وروسيا. وعليه، سيبقى التحدي التقني والقانوني للإسناد على أشدة في ظل هذا التقدم الموازي. وعليه أيضا، ستتطلب عملية الإسناد المزيد من الدعم السياسي والمخباراتى والإعلامي. فضلا عن ذلك، يتم تنفيذ الهجمات الإلكترونية بشكل متكرر من خلال أنظمة كمبيوتر وسيطة لإخفاء الهوية الحقيقية للمهاجم. وعلى الرغم من أن برامج التتبع قادرة على اختراق التنكر الوسيط والعودة إلى مصدرها الإلكتروني، ومع ذلك فإن معدل نجاحها ليس مثاليًا. للمزيد ينظر:

- Tsagouria, N.(2012), "Cyber Attacks, Self-Defense and The Problem of Attribution", ***Journal of Conflict and Security Law***, p.234.

[29] ينظر:

- Candiani, L, ibid, p.44.
- Grimal, F and Sundaram, J.(2017), "Cyber warfare and autonomous self-defence", ***Journal on the Use of Force and International Law***, pp. 3.4.

الوشيك، سيفضى حتما إلى سوء استخدام القوة والتدخل غير المشروع في الأنظمة الإلكترونية لدول أخرى. ويزداد الأمر تعقيدا عندما تكون تلك الهجمات الوشيك قادمة من دول عابرة متعددة، إذ سيكون التذرع بالرد الوقائي-ولو من منطلق الاحتجاج بالضرورة- أمر في غاية الصعوبة، وغير معقول في ذات الوقت. وأخيراً، يمكن القول أن الإسناد عموما في سياق الفضاء الإلكتروني لن يكون دقيقا وحاسماً في أغلب الوقت، فحتى مع توافر أحدث برامج التتبع لن يكون تحديد المصدر الحقيقي للهجوم الإلكتروني يقيني تماما في الكثير من الأحوال[30].

إذن نخلص مما تقدم أن التحديات الثلاثة السابقة لا سيما تحدى النطاق الزمنى الصارم لمفهوم الوشيك، والذى بدوره يؤثر في/ ويتداخل من التحدين الآخرين، يجعل من إمكانية ممارسة حق دفاع شرعي وقائي ردا على هجوم إلكتروني مسلح وشيك أمر شبه مستحيل. وعليه، برزت اجتهادات فقهية أبرزها اقتراب نافذة الفرصة، سعت إلى تأصيل ممارسة لحق دفاع وقائي ردا على الهجوم الإلكتروني الوشيك تستند على ضرورة منح النطاق الزمنى الصارم للوشيك هامش من المرونة.

المبحث الثالث: الهجوم الإلكتروني الوشيك واقتراب نافذة الفرصة الأخيرة الممكنة*last feasible window of opportunity*

أولا: النطاق الزمنى المرن لمفهوم الوشيك وحق الدفاع الشرعي الاستباقى في مواجهة أنماط وأشكال الحروب الحديثة

مع ما تتميز أنماط وأدوات وأشكال الحروب الحديثة من خصائص غير متوافرة في الحروب التقليدية لاسيما سرعتها الخاطفة، أضحت تلك الحروب تشكل تحديا كبيراً أمام ممارسة حق دفاع شرعي وقائي ردا عليها، وخاصة في ظل النطاق الزمنى الصارم لمفهوم الوشيك أو معيار كارولين. إذ أن الاستمرار بالتمسك بتلك العتبة الزمنية الصارمة لكارولين في زمن الحروب الخاطفة، سيحرم الدول من

---

[30] ينظر:

-Horace, B and Robertson, J, ibid, pp. 138.139.

- Dinniss, H.H.(2012), ***Cyber Warfare and The Laws of War***, Cambridge: Cambridge University Press, p.65.

حقها في حماية أمنها ومصالحها، بل وجودها في بعض الأحيان. ويجادل مايكل شميت في هذا الصدد، بأن القراءة الضيقة لمفهوم الوشيك التي سادت في القرنين التاسع عشر والعشرين لا تتناسب مع تطورات ووسائل الحرب في القرن الواحد والعشرين. فالدول قد بات لديها من الأسلحة التدميرية التي تمكنها من توجيه ضربة مدمرة لخصومها على الفور. ومن ثم، فتلك المقاربة التقييدية للوشيك تتعارض كليا مع حق الدفاع عن النفس ذاته. وعليه، دافع الكثير من الفقهاء بحتمية التخفيف من العتبة الزمنية الصارمة لكارولين وجعلها أكثر مرونة لتأصيل ممارسة لحق دفاع شرعي "استباقي" لمواجهة أشكال الحروب الحديثة دون غيرها فقط، ووفقا أيضا لضوابط صارمة أهمها توافر معلومات مؤكدة بهجوم وشيك قد يحدث قريباً، وذلك للحيلولة دون حرمان الدولة المستهدفة من الهجوم فرصة الدفاع عن نفسها قبل فوات الأوان[31].

واتساقا مع ذلك، يرى بعض الفقهاء أن مفهوم الوشيك مجرد مفهوم نسبى في حقيقية الأمر، حيث تُبرر مشروعية استخدام القوة بشكل استباقي أو أسرع إذ اقتضت الضرورة أو ظهرت أدلة راسخة على التخطيط لهجوم مسلح، إذ أن عدم السرعة في الرد عليه سيعق قدرة الدولة الضحية عن صده. ليس هذا فحسب، بل من الضرورة وتحديدا في مواجهة الإرهابيين استخدام القوة ضدهم بشكل استباقي حتى قبل تفكيرهم أو عزمهم التخطيط لهجوم إرهابي مسلح لاستئصال خطر تهديداتهم المستقبلية المتوقعة. وعليه، لا يجب أن يقترن مفهوم الوشيك بنطاق زمني صارم وهى اللحظات قبل هجوم على وشك الانطلاق، بل من الممكن توسيع نطاقه الزمنى شرط توافر أدلة على التخطيط لهجمات في المستقبل[32].

وفى ذات السياق، يدافع ويبرر Antonio Cassese، حق الدفاع الشرعي الاستباقى على أسس أخلاقية وسياسية لكن بشرط تقديم الدولة المعنية للمجتمع الدولي أو الأمم المتحدة أدلة مقنعة على التخطيط لهجوم وشيك، مع إظهار أن الضربات الاستباقية العسكرية قد تم اتخاذها بشكل متناسب مع التهديد[33].

ومثلت أزمة انتشار السلاح النووي بعد انتهاء الحرب الباردة المنعطف الرئيسي بحتمية الدفاع عن نهج زمني مرن لمفهوم الوشيك. إذ لم تثير خطورة الأسلحة النووية أو تأثيراتها المدمرة الانتباه بقدر ما

---

[31] DeWeese, G.S.(2015), "Anticipatory and Preemptive Self-Defense in Cyberspace: The Challenge of Imminence", **NATO CCD COE Publications**, Tallinn, p.87.

[32] Carr, J, ibid, p.51.

[33] Cassese, A.(2005), ***International Law*****,** New York: Oxford University Press, p.362.

أثارته السرعة الكبيرة لمن بيده هذا السلاح على تدمير مدى وقرى كاملة خلال بضعة دقائق. ومن ثم يرى المدافعين، أن مجرد التهديد فقط باستخدام السلاح النووي، وليس تصويبه بشكل ساحق كتمهيد لهجوم نووي وشيك، أمر لا بد أن يؤخذ على محمل الجد لأنه حال استخدامه فعليا ستمحو الدولة المستهدفة تماما. وفيما يبدو أيضا أن محكمة العدل الدولية في رأيها الاستشاري بشأن مشروعية استخدام الأسلحة النووية أو التهديد بها قد أدركت خطورة هذا الأمر تماما، إذ رأت أن استخدام الأسلحة النووية في إطار ممارسة حق الدفاع الشرعي الوقائي قد يكون مسموح بها في حالات الظروف القصوى للدفاع عن النفس التي يكون بقاء الدولة على المحك[34].

ويرى Rachel A. Weise، وهو واحد من أبرز المدافعين عن النهج المرن تجاه التهديدات النووية فقط، بأن تخفيف وطأة العتبة الزمنية الصارمة لكارولين ضرورة حتمية للحماية الوجودية للدول من التهديدات النووية. فبمجرد أن تمتلك أو تطور دولة سلاحاً نووياً، تنعدم الفرص أمام الدولة المستهدفة بالتهديد النووي من تفعيل حقها بالدفاع الشرعي الوقائي عن نفسها بسبب القوة التدميرية الرهيبة للسلاح النووي. ومن ثم، يحق للدولة المستهدفة، في حال تيقنها بامتلاك أو تطوير الدولة المهددة للسلاح النووي، أو توافر لديها معلومات مؤكدة على نيتها باستخدامه، تدمير المنشآت النووية للدولة الخصم أو المهددة كإجراء استباقي لحماية وجودها قبل فوات الأوان[35]. وفى هذا الصدد أيضا، خلصت لجنة الشئون الخارجية بمجلس العموم البريطاني أن مفهوم الوشيك بحاجة إلى إعادة تقييم في ضوء تنامى تهديدات أسلحة الدمار الشامل. لكن هذا لا يحول دون تطبيق حذر للغاية من قبل الحكومة البريطانية وأن يقتصر الرد الاستباقى المبنى على نطاق زمني مرن على التهديدات الكارثية المؤكدة ومراعاة التناسب في الرد على هذا التهديد الكارثي حتى يتقبل المجتمع الدولي مشروعية حق الدفاع الشرعي الاستباقى والحد من سوء استخدامه[36].

---

[34] Leys, N.(2020), "Autonomous Weapon System, International Crises and Anticipatory Self-Defense", ***The Yale Journal of International Law***, Vol.45, No.2, pp. 392.393.

[35] Weise, R.A.(2012), "How Nuclear Weapons Change the Doctrine of Self-Defense**",** ***International Law and Politics***, Vol. 44, p.1335.

[36] House of Commons, Foreign Affairs Committee, Foreign Policy Aspects of the War Against Terrorism, 2003–04, https://publications.parliament.uk/pa/cm200203/cmselect/cmfaff/196/19604.htm.

وساهمت بروز ظاهرة الإرهاب الدولي المسلح في إعطاء زخما كبيرا للنهج المرن للوشيك. فإزاء تنامى خطورة الهجمات المسلحة الخاطفة للجماعات الإرهابية، نادت أصوات بضرورة منح هامش من العمل العسكري الاستباقى القائم على المرونة الزمنية "كملاذ أخير" بشرط توافر أدلة قوية على التخطيط لشن المزيد من الهجمات الإرهابية الوشيكة أو المتوقعة[37]. ففي سياق ذلك، أقترح هارولد كوه Harold Koh، ما يسمى اقتراب الوشيك المرن أو المطول Elongated Imminence وهو أقرب لاقتراب "نافذة الفرصة الأخيرة المحتمل last possible window". ويستند هذا الاقتراب على تبرير الدفاع الوقائي بناء على أنماط ثابتة من أنشطة سابقة. فعلى سبيل المثال، لا يجب الانتظار حتى يقوم إرهابيين بتفجير طائرة، بل سيكون كافياً اكتشاف تصميم أو امتلاك هؤلاء الإرهابيين لسترات انتحارية لمواجهتهم. وبالتالي فهذا الاقتراب يدحض المعيار الضيق لفكرة الوشيك[38].

ومن واقع الممارسة الدولية في مواجهة الإرهاب المسلح، نجد أن الدول قد أضحت لا تلتزم بالتفسير الضيق لمفهوم الوشيك. إذ استنادا إلى معلومات استخبارية موثوقة، أصبحت تلجأ إلى استخدام القوة بشكل استباقي ضد تهديد متوقع خلال فترة قصيرة، قبل تجسده إلى تهديد وشيك فعلى. وأقرب مثال على ذلك، هو تبرير الولايات المتحدة لتدخلها العسكري في أفغانستان بغرض إحباط هجمات إرهابية في المستقبل من قبل تنظيم القاعدة. والذى دعمته المملكة المتحدة باعتباره كان ضروريا لتجنب المزيد من تهديدات القاعدة المستمرة[39].

ومن واقع ممارسة الولايات المتحدة لحقها في الدفاع الشرعي عن النفس ضد فلول تنظيم القاعدة في اليمن وباكستان والصومال عبر الطائرات من دون طيار، والذي تبرره الولايات المتحدة قانونيا على أنه عمليات عسكرية منفصلة في سياق نزاع مسلح مستمر. أضحى هناك تنامى واضح-حتى من قبل الفقهاء المتشبثين بالقراءة الضيقة لمفهوم الوشيك- لتقبل المزيد من المرونة فيما يتعلق بالإطار الزمنى لمفهوم الوشيك، أي السماح باستخدام القوة المسلحة-في حالات محددة- قبل وقوع الهجوم بالفعل، لردع

[37] Bethlehem, D.(2012), "Principles Relevant to the Scope of a State's Right of Self-Defense against an Imminent of Actual Armed Attack by Nonstate Actors", ***The American Journal of International Law***, Vol.106, p.3.
[38] Hayward, R.J, ibid, pp. 415.416.
[39] Shahriar, S.R, ibid, pp. 73-74.

الأعمال الإرهابية، وللحيلولة دون تمكن الدول المارقة من تطوير برامج أسلحة دمار شامل. علاوة على ذلك، فممارسة الولايات المتحدة، قد أثبتت أن التطورات التكنولوجية المتسارعة قادرة على تحريك المفهوم الضيق للوشيك وفقا لعقيدة كارولين إلى نطاق أوسع أو أكثر مرونة. فقدرة الأقمار الصناعية والطائرات بدون طيار على التحليق لأيام أو أسابيع فوق الأهداف والحصول على صور تفصيلية لمنشآت أسلحة الدمار الشامل، على سبيل المثال، قد حسن بشكل كبير قدرة الدول على قياس قدرة ونوايا الخصم بشكل صحيح. وينطبق نفس الأمر أيضا على الهجمات الإلكترونية، وبالتالي، يرى الكثيرين بان التطورات التكنولوجية الأخذة في التقدم بشكل متسارع ستقطع الطريق أمام أي حجج معارضة للنهج الزمنى المرن في سياق الهجمات الإلكترونية[40].

ثانيا- اقتراب نافذة الفرصة الأخيرة

يعد اقتراب أو اختبار نافذة الفرصة الأخيرة الممكنة أبرز الاجتهادات على الإطلاق التي تسعى إلى تأسيس ممارسة موضوعية مشروعة لحق دفاع شرعي وقائي أو استباقي ردا على الهجوم الإلكتروني المسلح الوشيك. ففي سياق النطاق الزمنى المرن الذى يستند عليه الاقتراب، يجادل أنصاره بإمكانية الاحتجاج بحق الدفاع الشرعي الاستباقى إذا تمكنت الدولة الضحية من تحديد الهجوم الإلكتروني المسلح "الوشيك" خلال مرحلة تطوره أو التخطيط له، وليس خلال المرحلة النهائية التي يكون فيها الهجوم على وشك الانطلاق.

وتم تطوير هذا الاقتراب على يد مايكل شميت Michael N. Schmitt، ووضع له ثلاثة ضوابط رئيسية:

- أن يكون هناك هجوم الإلكتروني في مرحلته التمهيدية، أو جزء من مخطط واسع لشن هجوم إلكتروني مسلح.
- أن يؤشر هذا الهجوم الإلكتروني التمهيدي أو المخطط برمته على أنه خطوة لا رجعة فيها لشن هجوم إلكتروني مسلح على المدى القريب.

[40] Deeks, A.S.(2015), "Taming the Doctrine of Pre-Emption", in: Weller, M, ed, ibid, pp.675.677.

- وأخيرا، أن تقوم الدولة المستهدفة بالتصدي لهذا الهجوم عند آخر فرصة ممكنة متاحة لديها عندما لا يكون لديها أية خيارات أخرى أمام هجوم مسلح لا مفر منه[41].

ويعد خبراء دليل تالين (2) من أبرز المؤيدين لهذا الاقتراب. إذ بسبب استحالة الرد وقائيا على هجوم إلكتروني وشيك بسبب سرعته الخاطفة، رفض خبراء تالين النطاق الزمنى الصارم لكارولين. وارتأوا بدلا من ذلك، بإمكانية أن تقوم الدول باستخدام القوة بشكل استباقي ضد هجوم إلكتروني مسلح في مرحلته التمهيدية عند آخر فرصة ممكنة مع مراعاة متطلب التناسب بحذر شديد جدا، شريطة التيقن تماما وبحذر شديد جدا بأن تلك المرحلة التمهيدية تؤشر بانطلاق هذا الهجوم بشكل لا عودة فيه No Return. إذ على سبيل المثال، يسبق بعض الهجمات الإلكترونية المسلحة، عمليات إلكترونية تهدف إلى جمع معلومات عن المكان المستهدف. وبالتالي، يمكن اعتبار عملية جمع المعلومات تلك مرحلة تمهيدية لهجوم إلكتروني مسلح وشيك. وفى مثال آخر، تحتاج بعض الأنماط من الهجمات الإلكترونية المسلحة إلى وقت أطول لكي تظهر تأثيراتها المدمر. ومع ذلك، تظهر تلك الأنماط من الهجمات الإلكترونية بعض من المؤشرات الخفيفة التي يمكن اعتبارها مرحلة تمهيدية، كتغير أنظمة السرعة لمحرك مفاعل نووي على سبيل المثال، قبل إحداثها لتأثيراتها المدمرة[42].

وفى مثال آخر، على افتراض تمكن دولة عبر أجهزتها المخابراتية من الحصول على معلومات وأدلة مؤكدة بشأن مخطط لدولة أخرى تعتزم فيه شن هجوم إلكتروني مسلح على أنظمة التحكم الإلكترونية لسد مائي قد يفضى إلى تدمير السد وحدوث فيضانات عارمة، وتزامن مع ذلك اكتشاف الدولة بالفعل لبرامج خبيثة قد أصابت أنظمة السد الإلكترونية. في هذه الحالة، يمكن اعتبار ما سبق مرحلة تمهيدية لهجوم مسلح وشيك، يبرر للدولة استخدام القوة بشكل استباقي كفرصة أخيرة ممكنة ضد مصدر الهجوم في الدولة المخططة[43].

---

[41] Schmitt, M.N, "Computer Network Attack and the Use of Force in International Law: Thoughts on A Normative Framework", https://apps.dtic.mil/dtic/tr/fulltext/u2/a471993.pdf.

[42] ينظر:

- Tallinn Manual 2.0, Rule 73, Paras, 1.2.3.4.5.6.7.8.9.
- Delerue, F, ibid, pp. 496.470.

[43] Gokce, Y.(2015), "Active Cyber Defense as a Preemptive Self-Defense Measure", in: Tatar, U, Gokce, Y and Gheorghe, A.V, eds, ***Strategic Cyber Defense: A Multidisciplinary Perspective*,** Amsterdam: IOS Press BV, p.125.

واستنادا إلى الأمثلة السابقة، يجادل البعض بموضوعية تذرع الدولة الضحية بحقها الاستباقى عملا باقتراب نافذة الفرصة، وذلك على اعتبار تعرضها لسلسلة من الهجمات الإلكترونية يمكن اعتبارها بمثابة شواهد "تراكمية" أو حملة ممهدة لهجوم إلكتروني أو حركي مسلح وشيك، لاسيما وإن اقترنت تلك الهجمات بدلائل أخرى سياسية أو استخباراتية، أو تسببت تلك الهجمات الممهدة بحدوث بعض الأضرار البسيطة. شريطة المعرفة الدقيقة لمصدر هذه الهجمات وهو الأمر الذى يتحقق في حال امتلاك الدولة الضحية لأجهزة مراقبة وتتبع إلكترونية متطورة للغاية[44].

ثالثا- تحديات تأسيس ممارسة لحق دفاع شرعي استباقي ردا على الهجوم الوشيك عملا باختبار نافذة الفرصة الأخيرة

مما لا شك فيه أن اقتراب نافذة الفرصة يمثل نقلة نوعية وضرورية بشأن التخلص من وطأة النطاق الزمنى الصارم لمعيار كارولين. ومع ذلك، لا يعنى ذلك إمكانية تأصيل ممارسة عملية ومشروعة سهلة لحق دفاع شرعي استباقي ردا على الهجوم الإلكتروني المسلح الوشيك. إذ بالنظر إلى الطبيعة الخاصة للهجمات الإلكترونية والفضاء الإلكترونية، تواجه مسالة إثبات المراحل التمهيدية للهجوم الإلكتروني المسلح الوشيك، بالإضافة إلى تحديي الإسناد وتكييف جسامة الهجوم الإلكترونية الوشيك؛ تواجه صعوبات جمة بالغة التعقيد تحول دون إمكانية الرد الاستباقى ضد هذا الهجوم عملا بالاقتراب[45].

ولا جدال بأن التطورات التكنولوجية المتسارعة سواء على مستوى تقنيات التحليل الإلكتروني التقني، أو أدوات المراقبة والاستطلاع كالأقمار الصناعية والطائرات من دون طيار. بالتوازي مع التطورات المتلاحقة لآلية جمع المعلومات الاستخبارية؛ تساهم على نحو كبير في كشف الهجمات والمخططات الإلكترونية الوشيكة، ونوايا ومخططات الخصوم. ومع ذلك، بالنظر إلى الطبيعة الخاصة للهجمات الإلكترونية خاصة تلك التي يمكن تنشيطها عن بعد كمرحلة أولية لهجوم مسلح وشيك، فمن العسير اكتشافها في الكثير من الأحيان. وتحتاج إلى تقنيات تكنولوجية بالغة التطور لا تتوافر لدى الكثير. وفى حال اكتشاف الدولة المستهدفة لتلك الهجمات، تظهر إشكالية أخرى وهى كيف تتيقن بانها خطوة لا

[44] Banks, W.(2013), "The Role of Counterterrorism Law in Shaping ad Bellum Norms for Cyber Warfare", ***International Law Studies***, Vol.89, pp. 174-175.
[45] Shahriar, S.R, ibid, pp. 75.76.

رجعة فيها لهجوم إلكتروني مسلح وشيك، ومتى تعرف تحديدا آخر نافذة فرصة ممكنة للتذرع بحقها في الدفاع الشرعي الاستباقى ضد هذا الهجوم الوشيك[46].

أما فيما يتعلق بإشكالية الإسناد وفقا للاقتراب، فيمكن القول إن اكتشاف الدولة الضحية عبر أحدث تقنيات التتبع الإلكتروني لمراحل تمهيدية لهجمات إلكترونية وشيكة من مصدر أو دولة معينة، لا يعنى بالضرورة ضلوع هذا المصدر في هذا الهجوم خاصة في ظل تقنيات إعادة التوجيه والتمويه والتنشيط عن بعد. كما أن المعلومات الاستخبارية لن تكون يقينية تماما لمعرفة المخطط الحقيقي أو النية الحقيقية وراء هذه الهجمات في ظل سهولة وسرية التخطيط للهجمات الإلكترونية. وعليه، فمسألة الإسناد ستكون دائما مسار شكوك. أما فيما يتعلق بإشكالية جسامة الهجوم الوشيك، والتأكد من نوايا شن هجوم مسلح، فيمكن القول أن اكتشاف الدولة الضحية للمراحل التمهيدية لهجوم وشيك أو لبرامج ضارة تمهيدية لهجوم مسلح وشيك، لا يعنى ذلك تكييف سهل لعتبة جسامة الهجوم المسلح الوشيك، أو التأكد بشكل يقيني من نوايا الخصم بشن هجوم مسلح. وذلك بسبب خاصية التنوع المتعدد الأغراض لنفس تقنيات الهجمات الإلكترونية. إذ على سبيل المثال، سيكون من الصعب للغاية التمييز بين اختراق العدو لمنشأة عسكرية حيوية بهدف جمع معلومات عن تلك المنشأة، وما بين اختراقها بغرض الإعداد لهجوم مسلح وشيك ضد هذه المنشاة، حيث يتم استخدام نفس البرامج والتقنيات الإلكترونية في كلتا العمليتين. وعليه، من الصعب اعتبار هذا الاختراق هجوم مسلح وشيك، أو مرحلة تمهيدية لهجوم مسلح وشيك، أو التأكد تماما من نوايا الخصم بشن هجوم مسلح، أو أهدافه الحقيقية من وراء هذا الاختراق. رغم النوايا الخبثة لهذا الاختراق باستهدافه منشأة عسكرية حيوية. فعلى سبيل المثال، عندما قامت روسيا بشن هجمات إلكترونية على شبكات الكهرباء الأوكرانية تسببت في قطع الكهرباء عن الأف الأوكرانيين، رصدت بعض أجهزة المراقبة اختراقات إلكترونية تمهيدية لتلك الهجمات. ومع ذلك، لم تتمكن السلطات الأوكرانية من التيقن من أهداف تلك الاختراقات، والنوايا الحقيقية من ورائها، حتى يتسنى لها اتخاذ إجراء استباقي ضد روسيا عملا بالاقتراب[47].

---

[46] ينظر:

- Narayanan, A *et al.,(*2020), ***Deterring Attacks against the Power Grid: Two Approaches for the U.S. Department of Defense***, Santa Monica, Rand, pp. 45.55.
- DeWeese, G.S, ibid, p.90.

[47] ينظر:

الخاتمة والتوصيات

يعد حق الدفاع الشرعي الوقائي ردا على هجوم مسلح وشيك ممارسة عرفية مشروعة مقبولة على نطاق واسع على المستويين الفقهي والدولي. وتنسحب مشروعية هذا الحق ردا على الهجوم الإلكتروني الوشيك المسلح الذى قد يفوق في خطورة وتبعاته الكارثية الهجوم المسلح التقليدي. ومع ذلك، تواجه هذه الممارسة ثلاثة تحديات رئيسية: تحدى النطاق الزمنى الصارم لمفهوم الوشيك، تحدى تكييف جسامة الهجوم الإلكتروني الوشيك، وتحدى الإسناد.

وبصدد التغلب على هذه التحديات وخاصة تحدى النطاق الزمنى، طور الفقهاء ما يسمى اقتراب نافذة الفرصة الأخيرة، الذى يراه الباحث خطوة هامة وضرورية على صعيد التخفيف من وطأة العتبة الزمنية الصارمة لمعيار كارولين التي تشكل أكبر عائقاً أمام ممارسة الدول لحقها الطبيعي والمشروع في الدفاع عن النفس ردا على هجوم إلكتروني مسلح وشيك وأنماط الحروب الخاطفة على نحو عام. ومع ذلك، بالنظر إلى خصوصيات وتعقيدات الهجمات الإلكتروني والفضاء الإلكتروني؛ لا تزال إمكانية ممارسة حق دفاع شرعي "استباقي" عملاً بالاقتراب تواجه صعوبات جمة وبالغة التعقيد.

وعليه، نستطيع القول أن تأصيل ممارسة مشروعة عملية لحق دفاع شرعي "وقائي" أو "استباقي" للدول ردا على الهجمات الإلكترونية المسلحة الوشيكة، لا يزال يواجه بتحديات كبيرة لاسيما تحدى الإسناد. ومن ثم، ففي حسبان الباحث، إن تطور ممارسة دولية لحق دفاع وقائي ردا على الهجمات الإلكترونية المسلحة مسألة متروكه لما ستسفر عنه الممارسة العملية، والتي قد تصل في بعض الأحيان لا سيما من قبل الدول الكبرى إلى الاحتجاج بالضرورة لرد الهجوم الإلكتروني الوشيك، متجاوزة جميع التحديات لا سيما تحدى الإسناد، وقد تكون محقه في ذلك-رغم العواقب الوخيمة لتلك الممارسة- خاصة إذا كان المستهدف منشآه عسكرية حساسة أو منشأة نووية.

- kehler, R, Lin, H and Michael Sulmeyer. (2017), "Rules of Engagement for Cyberspace Operations: A View from the USA", ***Journal of Cybersecurity***, Vol.3, No.1, p. 72.
- Der Meer, S.V.(2020), "How States Could Respond to Non-State Cyber-Attackers", ***Policy Brief***, Clingendael – the Netherlands Institute of International Relations, p.4.

ومن ثم، لتفادي ممارسة دولية منحرفة أو خطيرة، يوصى الباحث بالتالي:

1. ضرورة تبنى المجتمع الدولي المفهوم المرن أو الواسع "للوشيك" وحق الدفاع الاستباقى ردا على أنماط الحروب الحديثة الخاطفة فقط، ووضع تعريف وضوابط صارمة له، لعل أهمها تقديم دلائل وقرائن على درجة عالية من الموثوقية بشأن المرحلة التمهيدية للهجوم الوشيك الذى لا رجعة فيه.
2. التخفيف من وطأة عبء الإسناد عبر تكريس مبدأ العناية الواجبة في الفضاء الإلكتروني.
3. ضرورة اضطلاع الأمم المتحدة بوضع تعريف قانونياً محدداً للهجوم الإلكتروني المسلح. وبصدد الهجوم الإلكتروني المسلح الوشيك، قد تتضمن الصيغة القانونية نصوص محددة تعتبر أية هجوم إلكتروني على منشآت عسكرية حساسة بمثابة هجوم مسلح وشيك حتى ولو لم يسفر عنه تدمير هذه المنشأة، وذلك لردع المزيد من الهجمات الإلكترونية على تلك المنشآت بغض النظر عن أغراضها والنية وراء ارتكابها. وإتاحة المصوغ الشرعي للدول للرد على هذه الهجمات وقائياً.
4. تشجيع الدول على اللجوء إلى وسائل المساعدة الذاتية الأخرى كالتدابير المضادة، بحيث يتم اللجوء إلى حق الدفاع الشرعي الوقائي في حالات الضرورة القصوى فقط.
5. وأخيراً، يوصى الباحث أيضا أن تقوم الدول بتحسين وتطوير أجهزة الكشف المبكر والردع الإلكتروني لتقويض الهجمات الإلكترونية والدفاع عن أنظمتها الإلكترونية العامة والخاصة ضد أية هجمات إلكترونية خبيثة، وهذا الأمر في حد ذاته يقلل على نحو كبير من فرص لجوء الدول إلى استخدام القوة سواء العسكرية أو الإلكترونية للدفاع عن نفسها ضد هجوم إلكتروني مسلح.

المراجع

شامية، أحمد زهير، والجاسم، طارق (2014)، "الدفاع الشرعي الوقائي ومدى مشروعيته في العلاقات الدولية"، مجلة جامعة البعث، المجلد 36- العدد 6.

Barak, D.R.(2018), *Underground Warfare*, Oxford University Press

Banks, W.(2013), "The Role of Counterterrorism Law in Shaping ad Bellum Norms for Cyber Warfare", *International Law Studies*, Vol.89

Bethlehem, D.(2012), "Principles Relevant to the Scope of a State's Right of Self-Defense against an Imminent of Actual Armed Attack by Nonstate Actors", *The American Journal of International Law*, Vol.106

Cassese, A.(2005), *International Law*, New York: Oxford University Press

Candiani, L.(2018), *The responsibility of actors for cyber-attacks and the problem of attribution. Who can be held responsible from the perspective of International Law's norms on States' responsibility?,* Master Thesis, Faculty of Law, Tilburg University, The Netherlands

Der Meer, S.V.(2020), "How States Could Respond to Non-State Cyber-Attackers", *Policy Brief*, Clingendael – the Netherlands Institute of International Relations

Dinniss, H.H.(2012), *Cyber Warfare and The Laws of War*, Cambridge: Cambridge University Press

Dunlap, C.J.(2013), "Anticipatory Self-Defense and The Israeli-Iranian Crisis: Some Remarks", *ILSA Journal of International & Comparative Law*, Vol.19, No.2

Guiora, A.N.(2008), "Anticipatory Self-Defence and International Law- A Re-Evaluation", *Journal of Conflict & Security Law*, Vol. 13 No. 1.

Grimal, F and Sundaram, J.(2017), "Cyber warfare and autonomous self-defence*", Journal on the Use of Force and International Law*.

Hayward, R.J.(2017), "Evaluating The (Imminence) of A cyber Attack For Purposes Of Anticipatory Self-Defense", *Columbia Law Review*. Vol. 117, No.2.

John S. Davis, J.S *et al*., (2017), *Stateless Attribution: Toward International Accountability in Cyberspace*, Santa Monica, Rand.

kehler, R, Lin, H and Michael Sulmeyer. (2017), "Rules of Engagement for Cyberspace Operations: A View from the USA", *Journal of Cybersecurity*, Vol.3, No.1.

Lubell, N.(2015) "The Problem of Imminence in an Uncertain World", in: Weller, M, ed, *The Oxford Handbook of The Use of Force in International Law*, Oxford University Press

Leys, N.(2020), "Autonomous Weapon System, International Crises and Anticipatory Self-Defense", *The Yale Journal of International Law*, Vol.45, No.2

Margulies, P.(2013), "Sovereignty and Cyber Attacks: Technology's Challenge to the Law of State Responsibility", *Melbourne Journal of International Law,* Vol.14.

Mastrolembo, R.(2019), "Imminence and States' rights to Anticipatory self-Defence: Responding to Contemporary Security Threats and Divergence in Legal Diplomacy", *Canberra Law Review*, Vol.16, No.1.

Narayanan, A *et al.,(*2020), *Deterring Attacks against the Power Grid: Two Approaches for the U.S. Department of Defense*, Santa Monica, Rand

Rafighdoust, H.(2018), *The Right of Self-Defence Against Cyber Attacks by States and Non-State Actors*, PhD Thesis, Universitat Autònoma de Barcelona

Shahriar, S.R. (2020), "The Issue of Imminence: Can the Threat of a Cyber-Attack Invoke the Right to Anticipatory Self-Defence Under International Law?", *UCL Journal of Law and Jurisprudence*, Vol.9

Tran, D.(2018), "The Law of Attribution: Rules for Attributing the Source of a Cyber-Attack", *The Yale Journal of Law & Technology,* Vol. 20.