UAEU Law Journal

Volume 2024
Number 99 *Year 39 Issue No. 99 September 2024*

Article 9

January 2024

مدى اعتبار الهجمات السيبرانية انتهاكاً للحظر المفروض على استخدام القوة أو التهديد بها في ضوء أحكام القانون الدولي للجوء للحرب

Assessing Cyberattacks as Violations of the Prohibition on the Use or Threat of Force in the Context of the International Law to Resort to War "jus ad bellum"

Omar Ahmed Al-Saeedi

Holder of Master's Degree in Public Law, College of Law, Al Ain University, United Arab Emirates

Omar1442@yahoo.com

Dr. Zeyad Mohammad Jafal

Associate Professor of Public International Law – Al Ain University – United Arab Emirates

zeyadjaffal2021@gmail.com

Abstract

Jurisprudence of international law, including the 2013 Tallinn Manual experts, have argued that cyberattacks may constitute an unlawful use of force under Article 2(4) of the UN Charter if it is of such severity as to result in severe human and material casualties similar to that caused by a kinetic attack.

However, it is unclear whether a cyberattack can be included in the scope of Article 2 (4) which is subject to multiple and conflicting interpretations governed by different considerations that can create confusion and

ambiguity regarding its exact meaning, making it difficult to establish an international legal framework governing armed attacks.

*** Received on 06/09/2022, and approved for publication on 21/12/2022**

Additionally, it is unclear whether a cyberattack could be considered an armed attack since the UN Charter does not define the term. The prevailing trend in international law, in the absence of a binding international instrument governing operations in cyberspace, considers that cyber-attacks often do not reach the threshold of “armed attack”, which is backed by recent state practices.

Keywords: international law, cyberattacks, threat or use of force, armed attacks, Tallinn Manual.

مدى اعتبار الهجمات السيبرانية انتهاكاً للحظر المفروض على استخدام القوة أو التهديد بها في ضوء أحكام القانون الدولي للجوء للحرب

عمر أحمد السعيدي

ماجستير قانون عام - كلية القانون– جامعة العين– الإمارات العربية المتحدة

Omar1442@yahoo.com

د. زياد محمد جفال

أستاذ مشارك - القانون الدولي العام - كلية القانون– جامعة العين– الإمارات العربية المتحدة

zeyadjaffal2021@gmail.com

ملخص البحث

مضى فقهاء القانون الدولي بمن فيهم خبراء دليل تالين لعام 2013 إلى أن الهجوم السيبراني قد يشكل استخداماً محظوراً للقوة بموجب المادة 2 (4) من ميثاق الأمم المتحدة إذا كان من الشدة بحيث تنتج عنه إصابات بشرية ومادية فادحة شبيهة بتلك التي يحدثها الهجوم الحركي، ومع ذلك فليس من الواضح ما إذا كان يمكن إدراج الهجوم السيبراني في نطاق المادة 2 (4) التي تواجه تفسيرات متعددة ومتضاربة تحكمها اعتبارات مختلفة يمكن أن تخلق التباسًا وغموضًا فيما يتعلق بمعناها الدقيق ، ومن ثم صعوبة وضع إطار قانوني دولي يحكم الهجمات المسلحة. إضافة إلى ذلك ليس من الواضح ما إذا كان الهجوم السيبراني يمكن أن يشكل هجومًا مسلحًا حيث لا يقدم ميثاق الأمم المتحدة أي تعريف لمعنى "الهجوم المسلح"، ومع أن بعض الهجمات السيبرانية القادرة على إلحاق ضرر مادي سوف تتحدى عتبة "الهجوم المسلح"، فإن الاتجاه الغالب في القانون الدولي، في ظل عدم وجود صك دولي ملزم يحكم العمليات في الفضاء السيبراني يرى أن الهجمات السيبرانية غالبًا لا تصل إلى عتبة "الهجوم المسلح" ، وهو ما أكدته الممارسات الحديثة للدول في هذا المجال.

***استُلم بتاريخ 2022/09/06، و أجيز للنشر بتاريخ 2022/12/21.**

الكلمات المفتاحية: القانون الدولي، الهجمات السيبرانية، اللجوء إلى استخدام القوة أو التهديد بها، الهجمات المسلحة، دليل تالين.

المقدمة

نتيجة للثورة الشاملة التي أحدثتها تكنولوجيا المعلومات والاتصالات في جميع نواحي الحياة، ظهر فضاء جديد- إلى جانب البر والبحر والجو والفضاء الخارجي- ألا وهو الفضاء السيبراني [1] الذي يُعرف بأنه "مجال عالمي داخل بيئة المعلومات يتكون من شبكة مترابطة من البنى التحتية لتكنولوجيا المعلومات، بما في ذلك الإنترنت، وشبكات الاتصالات، وأنظمة الكمبيوتر، والمعالجات، وأجهزة التحكم المضمنة". [2] إنه "الوسط الذي توجد به، وتعمل من خلاله شبكات الحواسيب السيبرانية، وتشمل أجهزة الكمبيوتر، وأنظمة الشبكات، والبرمجيات، وحوسبة المعلومات، ونقلها، وتخزينها، بالإضافة إلى مستخدميها من البشر والهيئات والمؤسسات". [3]

وقد عزز هذا الفضاء المفتوح أمام جميع الدول والمتجاوز لحدودها السياسية من انتشار الأنشطة السيبرانية غير السلمية مثل الهجمات السيبرانية والإرهاب السيبراني والقرصنة السيبرانية والتجسس السيبراني وغيرها.[4] وهو ما أدى إلى ظهور بُعد جديد في الصراعات الدولية سمي بـ "صراع الفضاء السيبراني".[5] وإلى

[1] يعرف الفضاء بأنه كل مكان أو حيز أو مجال يمكن من قيام الحياة فيه بمختلف تشعباتها وعلاقاتها. راجع: طالب حسن موسى وعمر محمود عمر، الإنترنت قانوناً، مجلة الشريعة والقانون، جامعة الإمارات العربية المتحدة، العدد 67، يوليو 2016، ص. 339.

[2] Wolff Heintschel von Heinegg, Legal Implications of Territorial Sovereignty in Cyberspace, 4th International Conference on Cyber Conflict, Faculty of Law Europa-Universität, Frankfurt (Oder), Germany, 2012, p-p :7-19. P. 9. Available at: https://www.ccdcoe.org/uploads/2012/01/1_1_von_Heinegg_LegalImplicationsOfTerritorialSovereigntyInCyberspace.pdf

[3] عادل عبد الصادق، الفضاء الإلكتروني والرأي العام: تغير المجتمع والأدوات والتأثير، المركز العربي لأبحاث الفضاء الإلكتروني: قضايا استراتيجية، العدد 2459، سنة 2013، ص 35.

[4] رغدة البهي، الردع السيبراني: المفهوم والإشكاليات والمتطلبات، مجلة العلوم السياسية والقانون، المركز الديمقراطي العربي للدراسات الاستراتيجية والسياسية والاقتصادية (برلين- ألمانيا) العدد الأول يناير 2017، ص 49.

[5] علاء الدين فرحات، الفضاء السيبراني: تشكيل ساحة المعركة في القرن الحادي والعشرين. مجلة العلوم القانونية والسياسية، المجلد 10، العدد 3، ديسمبر 2019، ص 89.

اعتبار الفضاء السيبراني ساحة حرب جديدة في القرن الحادي والعشرين.[6] فقد أصبح هذا الفضاء البعد الخامس للحرب بعد الأرض والمحيطات والجو والفضاء، ويمكن من خلاله استخدام القوة السيبرانية الكامنة فيه في الصراع بين الدول بشكل متواز أو غير متواز مع حرب عسكرية تقليدية، وهو ما يمثل خطراً عالمياً متصاعداً ينذر بتحوله إلى أكبر تهديد أمني دولي.[7] فبعدما كان للجيوش دورها المهم في الصراعات الدولية، أصبح الفضاء السيبراني ساحة قتال جديدة يصعب رؤيتها، وهو ما أدى إلى خلق واقع عالمي جديد "يسوده ما أصبح يطلق عليه "سباق التسلح السيبراني"،[8] المتمثل في سعي الدول إلى امتلاك وتطوير القدرات السيبرانية في سبيل تعظيم القوة والتفوق والهيمنة وتعزيز التنافس حول السيطرة والابتكار والتحكم في المعلومات من أجل زيادة النفوذ والتأثير ليس فقط على نطاق محلي، بل دولي أيضاً.[9] مما أدى إلى أن يصبح الاهتمام بالأمن السيبراني أحد تجليات الأمن القومي للدول.[10]

ولعل أبرز ما يعزز انتشار الأنشطة غير السلمية في الفضاء السيبراني، التي قد تقوم بها الدول أو الفاعلون من غير الدول أو الأفراد، وزيادة مخاطرها هو ارتباط العالم المتزايد بالفضاء السيبراني وزيادة خطر تعرض البنية التحتية الكونية للمعلومات لهجمات سيبرانية، واستخدام الفاعلين من غير الدول للفضاء السيبراني لتحقيق أهدافهم، وتأثير ذلك في سيادة الدولة إضافة إلى انسحاب الدولة من قطاعات استراتيجية لصالح القطاع الخاص.[11] وتتنوع الأضرار التي قد تحدثها هذه الأنشطة ما بين تدمير أنظمة إلكترونية لمنشآت حيوية عسكرية أو مدنية، وتعطيل أو إتلاف شبكات الدفاع العسكرية عن بعد، واختراق أو تعطيل أو تدمير شبكات القطاع الخاص

---

[6] See Cameron Ryan Scullen, Cyberspace: The 21st Century Battlefield, University of Miami National Security & Armed Conflict Law Review, Vol. 6, No.1, 233, 2015, p.236.

[7] عمر محمود أعمر، الحرب الإلكترونية في القانون الدولي الإنساني، دراسات، علوم الشريعة والقانون، المجلّد 46، عدد 3، 2019، ص 134.

[8] Frédérick Douzet & Aude Gery, Cyberspace is used, first and foremost, to wage wars: proliferation, security and stability in cyberspace, Journal of Cyber Policy, Vol. 6, No.1, Pp96-113, 2021, p.110.

[9] ريتشارد إيه كلارك، روبرت كيه كنيك، حرب الفضاء الإلكتروني الخطر القادم على الأمن القومي وسبل المواجهة، الطبعة الأولى، أبو ظبي: مركز الإمارات للدراسات والبحوث الاستراتيجية، 2012، ص 267.

[10] أميرة عبد العظيم محمد عبد الجواد، المخاطر السيبرانية وسبل مواجهتها في القانون الدولي العام. مجلة الشريعة والقانون، جامعة الأزهر، الجزء 3، العدد 45، سنة 2020، ص 9.

[11] عادل عبد الصادق، أسلحة الفضاء الإلكتروني في ضوء القانون الدولي، سلسلة أوراق، العدد 23، مكتبة الإسكندرية، مصر، 2016، ص 17-18، إيهاب خليفة، مجتمع ما بعد المعلومات: تأثير الثورة الصناعية على الأمن القومي. مصر: العربي للنشر والتوزيع، سنة 2017، ص 142.

والبنية التحتية للدول.[12] على سبيل المثال اختراق أنظمة الكمبيوتر للسيطرة على الحركة الجوية وخطوط أنابيب النفط ومحطات الطاقة النووية ومراقبة الحركة الجوية والبرية والبحرية والسدود؛ لذلك فإن الأثر المحتمل لمثل هذه العمليات سيكون على درجة عالية من الخطورة قد يؤدي إلى وقوع أحداث كارثية مثل التصادم بين الطائرات، وإطلاق المواد السامة من المصانع الكيماوية أو انقطاع تشغيل البنية التحتية والحيوية مثل شبكات إمدادات المياه والكهرباء، وقد يكون المدنيون هم الضحايا الرئيسيون لهذه العمليات.[13]

لهذه الأسباب وغيرها لا يزال النقاش متواصلاً حول الأمن والاستقرار في الفضاء السيبراني، وتشارك الدول في مبادرات متعددة مع الجهات الفاعلة الخاصة والمجتمع المدني لمحاولة احتواء التهديد الناجم عن الهجمات السيبرانية، وهو ما ستحاول هذه الدراسة- كأحد الأهداف التي تسعى إليها-بيانه.

نطاق الدراسة

النطاق الموضوعي لهذه الدراسة سيركز على دراسة الهجمات السيبرانية التي تشنها الدول في أوقات السلم، حيث إن هذا النوع من الهجمات التي يحدث في زمن الحرب تخضع- على الأغلب- لقواعد القانون الدولي الإنساني الذي يعدها وسائل وأساليب للقتال خلال النزاع المسلحة،[14] وبالحماية التي يوفرها هذا القانون ضد الآثار الناجمة عن استخدامها.[15] بينما الهجمات السيبرانية التي تشنها الدول وقت السلم فإن دراستها تدخل في إطار النظام القانوني الذي يوفره القانون الدولي للجوء إلى الحرب.

وفي هذا السياق يجدر التذكير بأن قانون الحرب ينقسم إلى مجالين أساسيين: قانون اللجوء إلى الحرب Jus ad bellum ، وقانون الحرب أو القانون الدولي الإنساني Jus in bello، وتحكم مبادئ قانون اللجوء إلى الحرب الانتقال من حالة

---

[12] أميرة عبد العظيم محمد عبد الجواد، مرجع سابق، ص 373-374.

[13] عمر محمود أعمر، المرجع السابق، ص 134- 135.

[14] يحظى هذا الاستنتاج بدعم قوي في الرأي الاستشاري لمحكمة العدل الدولية حول مشروعية التهديد بالأسلحة النووية أو استخدامها، حيث أشارت المحكمة إلى أن المبادئ والقواعد الثابتة للقانون الدولي الإنساني السارية في النزاعات المسلحة تنطبق "على كافة أشكال الحرب وعلى كافة أنواع الأسلحة، بما في ذلك ما سيكون في المستقبل".
See Legality of the Threat or Use of nuclear weapons, Advisory Opinion, 1996 ICJ Report. 22 (July 8) para 86.

[15] القانون الدولي الإنساني والعمليات السيبرانية خلال النزاعات المسلحة، ورقة موقف اللجنة الدولية للصليب الأحمر مقدمة إلى فريق العمل المفتوح العضوية المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي، وإلى فريق الخبراء الحكوميين المعني بالارتقاء بسلوك الدول المسؤول في ميدان الفضاء السيبراني في سياق الأمن الدولي، تشرين الثاني/ نوفمبر 2019، ص 3-4. متوفرة في الموقع الإلكتروني للجنة الدولية للصليب الأحمر.https://www.icrc.org

السلم إلى الحرب، وتتبين متى يجوز لدولة اللجوء إلى الاستخدام المشروع للقوة ضد دولة أخرى استناداً بالأساس إلى أحكام المادة 2(4) من ميثاق الأمم المتحدة التي تحظر اللجوء إلى استخدام القوة أو التهديد بها، والاستثناءات الواردة عليها.[16] من أجل بناء عالم يسوده السلام. بينما تستند قوانين الحرب - بمفهومها المعاصر القانون الدولي الإنساني- التي تنظم سلوك المحاربين وحماية السكان والأعيان المدنيين في زمن النزاعات المسلحة- إلى قوانين جنيف الإنسانية التي تحمي فئات معينة من ضحايا الحرب ، وقوانين لاهاي التي تنظم الوسائل والأساليب العامة للقتال.[17]

منهج الدراسة

ستستعين هذه الدراسة بالمنهج الاستقرائي من خلال استدلال تصاعدي من الجزء إلى الكل (أو من الخاص إلى العام). إذ ينطلق الباحثان من دراسة الظاهرة الجزئية (الهجمات السيبرانية) وردها إلى الظاهرة الكلية (استخدام القوة في العلاقات بين الدول) في عملية تتضمن إعادة تفسير القانون الدولي ورسم أوجه تشابه بين القوة الحركية (kinetic) والقوة السيبرانية بهدف التوصل إلى قانون أو قاعدة كلية تحكم الهجمات السيبرانية في ظل القانون الدولي للجوء للحرب.

إشكالية الدراسة

تتمثل إشكالية الدراسة في التساؤل الرئيسي الآتي: إلى أي مدى يمكن اعتبار الهجمات السيبرانية استخداماً للقوة أو التهديد بها وفقاً للمادة 2 (4) من ميثاق منظمة الأمم المتحدة، وهل يمكن أن تصل هذه الهجمات إلى عتبة الهجمات المسلحة، وهو الشرط الأساسي الذي يمكن للدول المتضررة اللجوء لاستخدام القوة المسلحة في الرد

---

[16] وضع الميثاق "استثناءات حصرية" من الحظر العام لاستخدام القوة. بموجب المادة 39 ووفقًا للمادتين 41 و42، يقرر مجلس الأمن التدابير التي يجب اتخاذها ... للحفاظ على السلم والأمن الدوليين أو إعادتهما ... الاستثناء الثاني من الحظر العام لاستخدام القوة موجود في المادة 51 من الميثاق التي تنظم حقوق الدولة في استخدام القوة في الدفاع الفردي أو الجماعي عن النفس. بجانب هذين الاستثناءين، هناك ما يسمى "استثناءات من خارج الميثاق" لاستخدام القوة الناتجة عن ممارسات الدولة أو المبادئ العرفية أو السوابق القضائية. ومن بين هذه الاستثناءات ما يسمى بإجراء "متحدون من أجل السلام" الذي اعتمدته الجمعية العامة كاستجابة سياسية لمواجهة عدم عمل المجلس المفترض وكذلك استخدام القوة لإعمال الحق في تقرير المصير الذي تم التعبير عنه في العديد من الصكوك، وأبرزها العهد الدولي الخاص بالحقوق المدنية والسياسية لعام 1966. انظر

See Michael N. Schmit, International Law and the Use of Force: The Jus Ad Bellum, The Quarterly Journal, Volume II, No.3, September 2003, p. 91-92.

[17] Chris af Jochnick & Roger Normand, The Legitimation of Violence: A Critical History of the Laws of War, Harvard International Law Journal, Vol. 35, No.1, 1994, 49. p. 52

على هذه الهجمات استناداً إلى حق الدفاع عن النفس الوارد في المادة (51) من الميثاق.

فرضيات الدراسة

تتمثل الفرضيات التي ستحاول هذه الدراسة معالجتها على النحو الآتي:

- إن الهجمات السيبرانية تخضع للحظر الوارد في المادة 2(4) من ميثاق منظمة الأمم المتحدة.
- إن الهجمات السيبرانية التي تؤدي إلى ضحايا بشرية وخسائر مادية جسيمة تعد استخداماً للقوة المسلحة بموجب قواعد القانون الدولي للجوء للحرب.
- إن قواعد القانون الدولي الحالية غير كافية للتعامل مع الهجمات السيبرانية.

أهمية الدراسة

تكمن أهمية هذه الدراسة في أنها تسلط الضوء على مدى قدرة القانون الدولي في التعامل مع التهديدات الجديدة التي تثيرها الهجمات السيبرانية على الساحة الدولية، ولا سيما مع تزايد أهمية الأمن السيبراني في القطاعات الحكومية والعسكرية والاقتصادية بعد أن أصبحت حماية الفضاء السيبراني عنصراً مهما لاستراتيجية الأمن القومي لجميع الدول.

كما نأمل أن تشكل هذه الدراسة إضافة علمية ذات قيمة ستساهم في بلورة فهم أفضل للجوانب الإشكالية التي تثيرها الهجمات السيبرانية والتطوير التدريجي لنظام قانوني يحكم هذه الهجمات في إطار القانون الدولي للحرب بهدف إحلال نظام عالمي يسوده الأمن والسلام.

خطة الدراسة

ستقسم الدراسة إلى أربعة مباحث: مبحث تمهيدي سيعرف بمفهوم الهجمات السيبرانية، وتمييزه عن غيره من المفاهيم المشابهة; ومبحث أول سيدرس بالتحليل مفهوم القوة في القانون الدولي للجوء للحرب استناداً للمادة 2(4) من ميثاق منظمة الأمم المتحدة، والمبحث الثاني هو تحليل مدى اعتبار الهجمات السيبرانية انتهاكاً للحظر المفروض على استخدام القوة أو التهديد بها بموجب هذه المادة، وما هي العتبة اللازمة للوصول بها إلى أن تكون بمثابة هجمات مسلحة، وتفحص الدراسة في مبحث ثالث موقف الفقه الدولي الحديث ولاسيما دليل تالين بشأن القانون الدولي المطبق على

الهجمات السيبرانية لعام 2013، وهو الجهد القانوني الجماعي الوحيد المعتبر حالياً الذي يقدم إضافة مهمة من الممكن أن تشكل أساساً في المستقبل لإبرام صك قانون دولي ملزم.

مبحث تمهيدي

التعريف بالهجمات السيبرانية

يعتقد بعضهم أن أول عملية معلنة للهجمات السيبرانية كانت في العام 1999 حينما استهدف سلاح الجو التابع لحلف الشمال الأطلسي (NATO) العديد من الأهداف في الأراضي اليوغسلافية، من بينها السفارة الصينية في العاصمة بلغراد، مما استدعى رد فعل مباشر من طرف الصين تمثل في شن هجوم سيبراني على مجموعة من المواقع السيبرانية التابعة للولايات المتحدة الأمريكية، وأهمها الموقع السيبراني للبيت الأبيض حيث استحوذت الصين على الآلاف من البيانات والوثائق الرقمية المصنفة بأنها ذات سرية عالية.[18]

وعادت العمليات السيبرانية إلى صدارة الاهتمام القانوني الدولي بعد الهجوم السيبراني الواسع النطاق على إستونيا في العام 2007.[19] ففي 27 أبريل من ذلك العام شنت روسيا هجمات سيبرانية متلاحقة نتج عنها توقف كامل لشبكات الاتصال السيبرانية والمواقع الرسمية للحكومة الإستونية في أعقاب اعترض الروس على قرار الحكومة الإستونية بنقل نصب تذكاري سوفياتي للحرب العالمية الثانية (تمثال الجندي البرونزي) من وسط العاصمة تالين إلى مقبرة عسكرية خارج المدينة، كما استهدفت الهجمات مصالح تجارية مثل أنظمة المعلومات المصرفية والصحف.[20]

كما وقعت حوادث سيبرانية أخرى تنطوي على عمليات سيبرانية عدائية ضد دول وكيانات اعتبارية بعد الهجمات السيبرانية على إستونيا، ومن الأمثلة البارزة الهجوم السيبراني الذي حدث ضد جورجيا أثناء نزاعها المسلح مع روسيا في عام

[18] Thomas W. Smith, The New Law of War: Legitimizing Hi-Tech and Infrastructural, International Studies Quarterly, Vol.46, 2002, P.366; See Klaus-Peter Saalbach, Cyber War, Methods and Practice, Version 9.0, University of Osnabruck-17 Jun 2014, p.28.

[19] Michael N. Schmitt, 'Cyber Operations and the Jus Ad Bellum Revisited, Villanova Law Review, Vol.56, 2011, p. 569.

[20] Ibid, p. 569-570.

2008.[21] ففي 7 أغسطس 2007 شنت القوات الجورجية هجومًا على القوات الانفصالية التي تعمل داخل أراضيها، ونتيجة لذلك ردت روسيا بشن هجوم عسكري على الأراضي الجورجية، وسبق الوجود المادي للقوات الروسية في جورجيا ورافقه لاحقًا هجمات سيبرانية معادية ضد عدد كبير من المواقع الحكومية الجورجية، وهذا جعلها من بين الحالات الأولى التي صاحب فيها نزاع سياسي وعسكري دولي هجوم سيبراني منظما. [22] هجوم سيبراني بارزا آخر حدث في العام 2010 ألا وهو استخدام فيروس الكمبيوتر المسمى (Stuxnet) ضد المنشأة النووية الإيرانية من خلال أسلوب ومنهج يقوم على شقين: الأول يستهدف أجهزة الطرد المركزية وخروجها عن السيطرة من جهة، أما الثاني فبالتحايل على أجهزة التحكم والإيحاء لها أن عمليات تشغيل المنشأة النووية تعمل بصورة طبيعية، إلا أنها في الواقع معطلة.[23] كما تعرضت منشآت النفط والغاز في المملكة العربية السعودية في أغسطس2017، لفيروس يسمى (Trisis)، وهو فيروس ذو قدرات كبيرة يقوم بتدمير أنظمة التحكم الصناعية (ICS) بالتحديد إيقاف أنظمة الطوارئ الخاصة بهذه الأنظمة، مما أدى إلى توقف وإغلاق المنشآت لمدة زمنية طويلة متسبباً بخسائر فادحة للمملكة.[24]

وأدى حدوث هذه الهجمات وغيرها إلى ظهور تحديات قانونية وعملية حول تصنيفها بشكل حاسم في إطار القانون الدولي للحرب.

لتحليل ماهية الهجمات السيبرانية بموجب أحكام القانون الدولي للجوء إلى الحرب، ويعد تعريف مفهوم "الهجوم السيبراني" أمرًا بالغ الأهمية (أولاً)، كما أن التمييز بينه وبين غيره من المفاهيم المشابهة يساهم بلا شك في التكييف القانوني لهذه الهجمات (ثانيا).

---

[21] Peter Z. Stockburger, Known unknowns: state cyber operations, cyber warfare, and the jus ad bellum. American University International Law Review, Vol. 31, No.2, 2016, p. 555-556.

[22] Ibid.

[23] أحمد عبيس نعمة الفتلاوي، الهجمات السيبرانية: مفهومها المسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر، مجلة المحقق الحلي للعلوم القانونية والسياسية، المجلد 8، العدد 4، 31 ديسمبر 2016، ص 626.

[24] Jamie Collier, Strategies of Cyber Crisis Management: Lessons from the Approaches of Estonia and The United Kingdom, In: Taddeo M., Glorioso L. (Eds) Ethics and Policies for Cyber Operations. Philosophical Studies Series 124, 2017, p. 191.

أولاً: تعريف الهجمات السيبرانية

لا يوجد تعريف شامل ومقبول لمصطلح الهجمات السيبرانية، وتتراوح هذه التعاريف بين من يعد السيبرانية cyber بمثابة أداة للهجوم وآخر يعدها هدفاً له ، وثالث يركز على الآثار الناتجة عنه.

من الباحثين الذين ركزوا على الأداة عرف Wingfield الهجمات السيبرانية بأنها "هجمات تتم بواسطة استخدام الكمبيوتر والشبكات أو الأنظمة ذات الصلة، وتهدف إلى تعطيل أو تدمير أنظمة الإنترنت أو الممتلكات أو الوظائف الحاسوبية الخاصة بالخصم".[25] واستنادًا إلى اعتبار السيبرانية هدفاً للهجوم، عَرَفَ المجلس القومي للبحوث بالولايات المتحدة الهجوم السيبراني بأنه: "إجراءات متعمدة لتغيير أو تعطيل أو خداع أو إضعاف أو تدمير أنظمة أو شبكات الكمبيوتر أو المعلومات و / أو البرامج الموجودة في هذه الأنظمة أو الشبكات أو التي تمر عبر هذه الأنظمة أو الشبكات". [26] وفي الاتجاه نفسه عرف مجموعة من الباحثين الهجوم السيبراني بأنه " "أي إجراء يتم اتخاذه لتقويض وظيفة شبكة الكمبيوتر لأغراض سياسية أو تتعلق بالأمن القومي".[27] فبدلاً من وصف أداة الهجوم التي تُركت غير محددة تستخدم هذه التعاريف السيبرانية للإشارة إلى هدف الهجوم، على سبيل المثال، الإجراءات المتخذة لتعطيل أو تدمير أجهزة الكمبيوتر وشبكات الكمبيوتر، ويبدو هذا التعريف غير مناسب وعفا عليه الزمن، ومن الذين استندوا إلى الآثار التي يمكن أن تترتب عنها عرف Roscini الهجمات السيبرانية بأنها "أي تصرف دفاعي أو هجومي متوقع منه أن يتسبب بالقتل أو إلحاق ضرر مادي أو دمار يهدف منه المهاجم".[28] وهو التعريف الذي يقرب الهجمات السيبرانية من أن تعد بمثابة هجمات مسلحة - طبقاً لقواعد القانون الدولي الإنساني- قد تشن ضد دولة ما بغض النظر عمن يقوم بها ،

[25] Thomas C. Wingfield, The Law of Information Conflict, National Security Law in Cyber Space (Falls Church, VA: Aegis Research, 2000) p.44.

[26] William A. Owens, Kenneth W. Dam & Herbert S. Lin eds., National Research Council's Committee on offensive Information Warfare, Technology, Policy Law and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities (Washington, DC; National Research Council, 2009). p. S-2.

[27] Oona A. Hathaway, Rebecca Crootof, Philip Levitz, Haley Nix, Aileen Nowlan, William Perdue And Julia Spiegel,The Law of Cyber-Attack. California Law Review, vol. 100, no. 4, 2012, pp. 817–885. P, 821.

[28] Marco Roscini, Worldwide Warfare – Jus Ad Bellum and The Use of Cyber Force. Max Planck Yearbook of United Nations Law, Vol. 14, 2010, p.81.

والأداة المستخدمة فيها، وسواء أكانت للدفاع عن النفس ضد هجمات حركية أم سيبرانية أو ذات طابع هجومي.

من جانب آخر لا يستخدم الباحثون غير الغربيين مصطلح الهجمات السيبرانية بل العمليات المعلوماتيةinformation operations، وهم يعرفونها بشكل مغاير،و في هذا الصدد يعد باحثان من الصين أن الهجوم السيبراني هو مفهوم أوسع مما يشار إليه تقليدياً بقولهما: " في العمليات المعلوماتية يتم دمج القدرات الرئيسية للحرب السيبرانية وعلم النفس وشبكات الكمبيوتر والخداع العسكري والعمليات الأمنية بالتنسيق مع الدعم الخاص والقدرات ذات الصلة، من أجل اختراق أو إيقاف أو تدمير أو اختطاف القرارات الإنسانية".[29] وهو التعريف الذي يتسق مع تعريف كل من حكومتي روسيا والصين لما تسمينها العمليات المعلوماتية، كما سنرى لاحقاً.

من جانب آخر تتباين التعاريف التي تعطيها حكومات الدول للهجمات السيبرانية التي يمكن التعرف عليها من خلال مفهوم حكومة كل من الولايات المتحدة الأمريكية من جهة وروسيا الاتحادية من جهة أخرى، و ليس من المستغرب أن تكون هاتان الدولتان قد توصلتا إلى مفاهيم مختلفة للغاية استناداً إلى سياسات واستراتيجيات كل طرف.

ولا تستخدم وزارة الدفاع الأميركية مصطلح الهجمات السيبرانية، بل "العمليات السيبرانية" Cyber operations التي عرفتها بأنها: "توظيف القدرات السيبرانية حيث يكون الغرض الأساسي هو تحقيق الأهداف أو الآثار العسكرية في الفضاء السيبراني أو من خلاله".[30] وقد عرفت الوزارة في استراتيجيتها السيبرانية لعام 2018، "الحادث السيبراني الكبير" بأنه " أي حدث (أو مجموعة أحداث متصلة) يحدث في شبكة كمبيوتر أو يتم إجراؤه من خلالها ومن المحتمل أن يؤدي إلى إلحاق ضرر واضح بمصالح الأمن القومي أو العلاقات الخارجية أو اقتصاد الولايات

[29] Yuchong Li and Qinghui Liu, A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments, Energy Reports 7 (2021) 8176–8186, p.8177. https://www.sciencedirect.com/science/article/pii/S2352484721007289

[30] U.S. Department of Defense. Dictionary of Military and Associated Terms . (Washington: U.S. Department of Defense, November 8, 2010) (As Amended Through February 15, 2012).

المتحدة أو ثقة الجمهور أو الحريات المدنية أو الصحة العامة والسلامة للشعب الأمريكي".[31]

وفي المقابل لا يستخدم الروس عمومًا مصطلحات cyber (kiber) أو الحرب الإلكترونية (kibervoyna)، إلا عند الإشارة إلى الكتابات الغربية أو الأجنبية الأخرى حول هذا الموضوع.[32] بدلاً من ذلك، مثل الصينيين، فإنهم يميلون إلى استخدام كلمة المعلوماتيةinformatizatio ، وعليه يصورون العمليات السيبرانية ضمن النطاق الأوسع لحرب المعلومات التي هي- حسب وجهة نظر العسكريين الروس- مفهوم شامل يشمل عمليات شبكات الكمبيوتر، والحرب الإلكترونية، والعمليات النفسية، وعمليات المعلومات.[33] وبعبارة أخرى يُنظر إلى السيبرانية على أنها أداة لتمكين الدول من السيطرة على الفضاء السيبراني الذي يعد مجال حرب مستقل حسب رأيهم.[34]

وهو ما أكدت عليه العقيدة العسكرية للاتحاد الروسي لعام 2010 من أنه تتمثل إحدى سمات النزاعات العسكرية الحديثة في: "التنفيذ المسبق لإجراءات حرب المعلومات من أجل تحقيق أهداف سياسية دون استخدام القوة العسكرية، وبالتالي، من أجل تشكيل رد إيجابي من المجتمع الدولي على استخدام القوة العسكرية."[35] وهذا يعني أنه يمكن استخدام أدوات حرب المعلومات قبل بدء العمليات العسكرية لتحقيق أهداف الدولة دون اللجوء إلى القوة أو إلى إرباك الخصم وإحباطه معنوياته حتى تكون الدولة قادرة على تبرير إجراءات للجمهور في حالة اللجوء إلى القوة المسلحة،

[31] See U.S Department of Defense, "Summary: Department of Defense Cyber Strategy 2018," released September 19, 2018, supra note. 3, p .3.

[32] Michael Connell and Sarah Vogler, Russia's Approach to Cyber Warfare, Center for Naval Analysis (CAN), Washington DC, September 2016. p. 2.

[33] Ibid.

[34] Ibid, p.3.

[35] "the prior implementation of measures of information warfare in order to achieve political objectives without the utilization of military force and, subsequently, in the interest of shaping a favourable response from the world community to the utilization of military force". See The Military Doctrine of the Russian Federation, approved by Russian Federation presidential edict on February 5, 2010 (translated). para. 13(d). Available at http://carnegieendowment.org/files/2010russia_military_doctrine.pdf .

وبذلك تصبح حرب المعلومات، وبالتالي الحرب السيبرانية، أداة شرعية للدولة في كل من أوقات السلم والحرب. [36]

وبذلك تنظر روسيا إلى حرب المعلومات- كما تسميها- بشكل مختلف عن نظيراتها الغربية، سواء من حيث التعريف أم التطبيق العملي، وهي تقر صراحة بأنها تدمج حرب المعلومات- كما تسميها- في استراتيجية كبرى قادرة على تحقيق أهداف سياسية.

على صعيد المنظمات الدولية عرف حلف شمال الأطلسي (الناتو) الهجوم السيبراني- كما يرد في القاعدة 30 من دليل تالين لعام 2013 حول "القانون الدولي الواجب التطبيق على الحرب السيبرانية" لعام 2013- الذي أعده مركز التميز للدفاع الإلكتروني التعاوني التابع للحلف (CCDCOE)- بأنه "عملية سيبرانية، سواء كانت هجومية أو دفاعية، من المتوقع بشكل معقول أن تتسبب في إصابة الأشخاص أو موتهم أو إلحاق ضرر أو تدمير في الممتلكات".[37] وهو التعريف الذي يعبر عن وجهة نظر الدول الأعضاء في الحلف ، ويستند إلى أحكام ومبادئ القانون الدولي الإنساني أكثر من القانون الدولي للحرب خاصة من خلال تركيزه على آثار الهجوم السيبراني على المدنيين والأعيان المدنية.

وفي هذا السياق عدَّ حلف شمال الأطلسي (NATO) في بيان قمة وارسو التي عقدت في الفترة من 8 إلى 9 يوليو 2016 أن الهجمات السيبرانية تمثل تحديًا واضحًا لأمن الحلف ، ويمكن أن تحدث أضراراً كبيرة بالمجتمعات الحديثة مثلها مثل الهجمات التقليدية.[38] وأعرب الحلف في بيانه عن دعمه للردع والدفاع الأوسع لحلف الناتو: سيستمر دمج الدفاع السيبراني في التخطيط التشغيلي وعمليات ومهام الحلف، وسنعمل معًا للمساهمة في نجاحها، كما سيضمن الحلف تنظيمًا أكثر فعالية للدفاع السيبراني وإدارة أفضل للموارد والمهارات والقدرات. [39]

[36] Ibid.
[37] Tallinn manual on the international law applicable to cyber warfare: prepared by the international group of experts at the invitation of the NATO Cooperative Cyber Defense Centre of Excellence / General Editor, Michael N. Schmitt. Cambridge: Cambridge University Press, 2013. Rule 30, p. 106.
[38] Warsaw Summit Communiqué, issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw 8-9 July 2016. Para.70.
[39] Ibid.

في المقابل اتبعت منظمة شنغهاي للتعاون - وهي مجموعة تعاون أمني تتألف من الصين وروسيا ومعظم جمهوريات آسيا الوسطى السوفيتية السابقة إضافة إلى مراقبين بما في ذلك إيران والهند وباكستان -نهجًا مختلفاً يعتمد على الوسائل والأهداف في التعامل مع الهجمات السيبرانية التي أسمتها حرب المعلوماتInformation war. فقد عرّفت المنظمة "حرب المعلومات" بأنها: "مواجهة بين دولتين أو أكثر في فضاء المعلومات بهدف إتلاف أنظمة المعلومات والعمليات والموارد، والهياكل ذات الأهمية الحاسمة وغيرها من الهياكل، وتقويض الأنظمة السياسية والاقتصادية والاجتماعية، والتلاعب النفسي بجماهير السكان لزعزعة استقرار المجتمع والدولة، وكذلك إجبار الدولة على اتخاذ قرارات لصالح الطرف الخصم"،[40] ويبدو أن منظمة شنغهاي للتعاون قد تبنت رؤية موسعة للهجمات السيبرانية التي تتضمن استخدام القدرات السيبرانية لتقويض الاستقرار السياسي للدول، وهو ما يتناغم مع الموقف الروسي والصيني السالف ذكرهما.

وتكشف مقارنة مفاهيم الهجمات السيبرانية لدول الناتو مع مفاهيم روسيا والصين عن الجدل حول ما إذا كانت الحرب السيبرانية تقتصر على الصراع العسكري فقط أو تشمل أبعاداً مدنية واقتصادية أيضًا.

إضافة إلى ما سبق يستلزم التوصل إلى تعريف مقبول لمفهوم الهجمات السيبرانية تمييزه عن غيره من المفاهيم المشابهة.

ثانيا: التمييز بين مفهوم الهجمات السيبرانية وغيره من المفاهيم المشابهة

إن التحدي القانوني المتمثل في معالجة العمليات السيبرانية في ضوء أحكام القانون الدولي معقد بسبب التنوع الكبير في هذه العمليات والجهات الفاعلة المحتمل أن تقوم بها؛ إذ يمكن أن يقوم متسلل hacker بإغلاق موقع إلكتروني حكومي على شبكة الكمبيوتر، قد تتطلب هذه العملية استجابة مختلفة عندما تتسبب عملية سيبرانية ينفذها وكلاء حكوميون في انفجار خط أنابيب غاز في بلد آخر. يمكن تحليل تحديد عملية سيبرانية على أنها استخدام للقوة العسكرية أو هجوم مسلح بموجب ميثاق الأمم المتحدة بينما يمكن تقييم عملية اختراق شبكة كمبيوتر على أنها تجسس سيبراني أو

[40] Agreement Between the Governments of the Member States of the Shanghai Cooperation Organization on Cooperation in the field of International Information Security, Yekaterinburg, 16 June 2009annex I, p. 9.

جرائم جنائية أخرى؛ [41] لذلك يعد تحديد الأنواع المختلفة للعمليات السيبرانية، مثل الحرب السيبرانية، والجريمة السيبرانية، والتجسس السيبراني والإرهاب السيبراني والقرصنة السيبرانية أمرًا مُهِمًّا في تحليل الاستجابة القانونية المناسبة، وهو ما سنوضحه تباعاً:

1. الحرب السيبرانية:

الحرب السيبرانية هي "مجموعة من الإجراءات التي تتخذها الدول للهجوم على نظم المعلومات المعادية بهدف التأثير والإضرار بها في الوقت نفسه للدفاع عن نظم المعلومات الخاصة بها".[42] إنها تشير إلى وسائل وأساليب القتال التي تتألف من عمليات في الفضاء الإلكتروني ترقى إلى مستوى النزاع المسلح، أو تجري في سياقه ضمن المعنى المقصود في القانون الدولي الإنساني.[43]

وإن كانت الحرب السيبرانية تتفق كثيراً مع الهجمات السيبرانية إلا أن ذلك لا يعني عدم وجود ما يميزها عن بعضهما بعضاً. فالحرب السيبرانية تعني مجموعة العمليات السيبرانية التي تحدث أثناء نزاع مسلح دائر أو التي تنتج آثاراً مادية تشبه وتعادل آثار الهجمات المسلحة التقليدية. [44] بينما الهجمات السيبرانية هي كل نشاط سيبراني ضارٍ بالدول الأخرى يقع في وقت السلم سواء نتجت عنه أضرار مادية جسيمة في الأرواح أو الممتلكات أو لم يؤد إلا للتشويش على أنظمة الكمبيوتر فيها ما دام كان ذلك لأغراض أمنية وعسكرية وإحداث إرباك في عمل الحكومة التابعة لتلك الدولة.[45]

وبالتالي فإن دراسة الحرب السيبرانية تخرج من دراسة القانون الدولي للحرب وتدخل في نطاق القانون الدولي الإنساني الذي يهتم بتنظيم وسائل وأساليب القتال خلال النزاعات المسلحة بما فيها الحرب السيبرانية.

---

[41] See David Weissbrodt, Cyber-Conflict, Cyber-Crime, and Cyber-Espionage, Minnesota Journal of International Law, Vol. 22, 2013, p.349.

[42] أحمد عبيس نعمة الفتلاوي، مرجع سابق، ص 612.

[43] عمر محمود أعمر، المرجع السابق، ص 134.

ميزت القاعدة القاعدة 41 من دليل تالين لعام 2013 بين "وسائل الحرب الإلكترونية" ، وهي الأسلحة السيبرانية والأنظمة الإلكترونية المرتبطة بها، و"أساليب الحرب الإلكترونية" ، وهي التكتيكات والتقنيات والإجراءات الإلكترونية التي يتم من خلالها تنفيذ الأعمال العدائية.

Tallinn Manual, P. 141.

[44] أحمد عبيس نعمة الفتلاوي وزهراء عماد محمد كلنتر، تكييف الهجمات السيبرانية في ضوء القانون الدولي، مجلة الكوفة للعلوم القانونية والسياسية، المجلد 13، العدد 44، ج. 1 ،31 يناير 2020، ص 53.

[45] نفس المرجع.

2. الجرائم السيبرانية:

الجريمة السيبرانية هي عبارة عن الفعل غير المشروع الذي يمس مصلحة أو حقاً ويتعلق بالمكونات المادية وغير المادية للوسائل السيبرانية، ويكون المشرع قد قدر حمايتها بنصوص التجريم والعقاب بأن عد الاعتداء عليها جريمة معاقب عليها بجزاء جنائي.[46]

ومع أن كلاً من الجرائم السيبرانية والهجمات السيبرانية تحدثان في البيئة نفسها ألا وهي الفضاء السيبراني، إلا أن ما يميز الجرائم السيبرانية هو كونها تصرفاً يصدر عن جهة لا تمثل الدولة أو إحدى مؤسساتها، سواء كان شخصاً عادياً أو اعتبارياً.[47] وغني عن القول إن هذا التصرف لا يرقى إلى مستوى الجريمة السيبرانية إلا إذا شكل جريمة وفقاً للقانون الجنائي الداخلي استناداً إلى مبدأ " لا جريمة ولا عقوبة إلا بنص".[48] كما يختلفان في الباعث من وراء كل منهما، حيث إن الباعث من الجرائم السيبرانية هو تحقيق مكاسب مالية من خلال التسلل إلى الشبكات الإلكترونية العامة والخاصة، بخلاف الهجمات السيبرانية التي يستهدف مرتكبوها أساساً الشبكات التي تتحكم بالبنى التحتية الأساسية في الدولة وتدميرها بقصد إرباكها وزعزعة النظام فيها لتحقيق أهداف أمنية أو عسكرية أو سياسية أو قومية،[49] ويضاف إلى ذلك أن الأضرار المحتملة لكل منهما تختلف بشكل كبيرعلى اعتبار أن الهجمات السيبرانية تهدف إلى إلحاق ضرر شامل بالأشخاص أو الممتلكات في دولة أخرى في حين ينحصر الضرر في الجريمة السيبرانية عموماً في مستخدمين معينين.[50] كما أن القواعد القانونية التي تقرأ من خلالها الهجمات السيبرانية هي قواعد القانون الدولي العام بينما الجرائم السيبرانية فهي قواعد القانون الجنائي الوطني. [51]

3. الإرهاب السيبراني:

لا يوجد إجماع بين الحكومات ومجتمع أمن المعلومات حول ما يمكن عدَّه عملًا من أعمال الإرهاب السيبراني لعدم وجود اتفاق دولي يحدد المقصود بالإرهاب ذاته

---

46 راشد محمد المري، الجرائم السيبرانية في ظل الفكر الجنائي المعاصر دراسة مقارنة، دار النهضة العربية، سنة 2018، ص 21.

47 رزق أحمد سمودي، حق الدفاع عن النفس نتيجة الهجمات الإلكترونية في ضوء قواعد القانون الدولي العام، مجلة جامعة الشارقة للعلوم القانونية، المجلد 15، العدد 2 ديسمبر 2018، ص345-346.

48 نفس المرجع.

49 أحمد عبيس نعمة الفتلاوي وزهراء عماد محمد كلنتر، المرجع السابق، ص 52.

50 رزق أحمد سمودي، المرجع السابق، ص 346.

51 نفس المرجع.

بشكله التقليدي، لكن استنادا إلى التعريف التقليدي للإرهاب يعرف فقه القانون الدولي الإرهاب السيبراني بأنه استخدام شبكات المعلومات والكمبيوتر من قبل التنظيمات الإرهابية من أجل نشر الخوف والرعب بين الأشخاص والدول والشعوب ومحاولة الضغط عليهم للرضوخ لأهداف تلك التنظيمات من ناحية، ومن أجل الحصول على التمويل المالي أو إبراز قوة التنظيم الإرهابي وفي عمليات التجنيد والتعبئة والدعاية وجمع المعلومات حول الأهداف العسكرية وكيفية التعامل مع الأسلحة وتدريب المجندين الجدد عن بعد.[52] ووفقًا للجنة الأمريكية لحماية البنية التحتية الحيوية، تشمل الأهداف المحتملة للإرهاب السيبراني الصناعة المصرفية والمنشآت العسكرية ومحطات الطاقة ومراكز التحكم في الحركة الجوية وأنظمة المياه وغيرها.[53]

إن الإرهاب السيبراني ما هو إلا شكل من أشكال العمليات السيبرانية التي يقوم به الفاعلون من غير الدول، ولاسيما الجماعات والتنظيمات الإرهابية كتنظيم القاعدة وتنظيم الدولة الإسلامية في العراق وبلاد الشام (داعش) بخلاف الهجمات السيبرانية التي يقوم بها، حسب مفهوم القانون الدولي للجوء للحرب الدول كما أنهما يختلفان في الهدف مع أن كليهما يستخدم الفضاء السيبراني وأدواته لإلحاق الضرر سواء بحكومات الدول أم القطاعات الحيوية الاقتصادية والمالية فيها، لكن في كثير من الأحيان يصعب التمييز بينهما وهما يتداخلان بدرجة كبيرة، فكما سنرى صنف المجتمع الدولي الهجمات السيبرانية على إستونيا وجورجيا بأنهما إرهاب سيبراني وليست هجمات سيبرانية.

ويتقاطع مفهوم "الإرهاب السيبراني" مع مفهوم "القرصنة السيبرانية" المرتبطان ارتباطًا وثيقًا في سياق الممارسات السيبرانية العدائية، فـ"المتسلل" هو "مواطن عادي يشارك في القرصنة بمبادرته الخاصة من بين أمور أخرى لأسباب أيديولوجية أو سياسية أو دينية أو وطنية. [54] وانطلاقاً من أن كلا من الإرهاب

[52] أميرة عبد العظيم ص 420-419، ناصر العلي، الجهود الدولية في مكافحة الإرهاب الإلكتروني، مجلة الباحث للدراسات الأكاديمية، المجلد 8، العدد 1، سنة 2021، ص 30، إسماعيل زروقة، الفضاء السيبراني والتحول في مفاهيم القوة والصراع، مجلة العلوم القانونية والسياسية، المجلد 10، العدد 1، أبريل 2019 ص 1020.

[53] Cyber – Terrorism: A Threat for The European Union and Its Response. Webinar 65/2018. Available at:
https://www.cepol.europa.eu/tags/cyberterrorism

[54] Daniel Garrie and Shane Reeves, An Unsatisfactory State of the Law: The Limited Options for a Corporation Dealing with Cyber Hostilities by State Actors, Cardozo Law Review, Vol. 37, No. 5, 2016, Cardozo Legal Studies Research Paper No. 495, p. 1832-1833.

والقرصنة في الفضاء السيبراني يمكن أن يتسببا في أضرار كبيرة للدولة، لكن ليس من المؤكد ما إذا كان بإمكانهما أن يشكلا هجومًا سيبرانيا.[55]

4. التجسس السيبراني:

يهدف التجسس السيبراني إلى جمع المعلومات الاستخبارية - الحكومية أو الخاصة - وينطوي عمومًا على سرقة الأسرار التجارية والملكية الفكرية والمعلومات الحكومية السرية.[56] وباعتبار أنه يقتصر فقط على جمع المعلومات الحساسة فإنه لا يتسبب في ضرر مادي، ويمكن أن يقوم به فرد أو جماعة بهدف تحقيق مكاسب مالية أو ميزة عسكرية استراتيجية؛[57] لذا فإنه بشكل عام لا يؤدي إلى "تطبيق القانون الدولي للحرب"، بل يتطلب استجابة قانونية جنائية محلية أو دولية مختلفة.[58] كما أن هناك شبه إجماع على أن أعمال التجسس الإلكتروني لا تشكل هجمات سيبرانية؛ لأن جمع المعلومات الاستخبارية لا يؤدي إلى تعطيل البيانات المخزنة أو إتلافها أو تغييرها،[59] وهذا يتوافق مع القانون الدولي الحالي الذي يقبل ممارسة التجسس طويلة الأمد من قبل وكالات الاستخبارات في جميع أنحاء العالم كوجه تقليدي للسياسة الخارجية لكل دولة ذات سيادة.[60]

ومما يجدر ذكره أن القانون الدولي لا يتناول التجسس في حد ذاته، وعليه فإن مسؤولية الدولة عن عمل تجسس سيبراني يقوم به جهاز من أجهزة الدولة في الفضاء السيبراني لا يتم التعامل معها كمسألة من مسائل القانون الدولي ما لم تنتهك جوانب معينة من التجسس محظورات قانونية دولية محددة كما في حالة التجسس السيبراني الذي يشمل الاتصالات الدبلوماسية.[61]

ويتبين من مقارنة الهجمات السيبرانية مع غيرها من العمليات غير السلمية التي تحدث في الفضاء السيبراني مع كثرة تعاريف هذه العمليات وتداخلها في أحيان كثيرة

---

[55] Ibid.
[56] Ibid, p. 1831.
[57] Rebecca Helene Sussman, The Reusable Bomb: Exploring How the Law of Armed Conflict Applies in Cyberspace, Boston University Journal of Science & Technology Law, Vol. 23, 481, Summer 2017, p. 486.
[58] Daniel Garrie and Shane Reeves, op.cit, p. 1831-1832
[59] Oona A. Hathaway et al., op.cit, p.836-837.
[60] Arie J. Schaap, Cyber warfare operations: development and use under international law, Air Force Law Review, vol. 64, winter 2009, 121, P. 140.
[61] Tallinn Manual, P. 36 and Rule 66.

أن الاستجابة القانونية للرد على هذه الهجمات قد تختلف استناداً إلى نوعها فبينما تخضع الحرب السيبرانية لأحكام القانون الدولي الإنساني نجد أن الجريمة السيبرانية والتجسس السيبراني والقرصنة السيبرانية لا تخضع- على الأغلب- لأحكام القانون الدولي وتتم معالجتها في إطار القوانين الجنائية الوطنية للدول، بينما الإرهاب السيبراني يخضع لكلا النظامين القانونين الدولي والوطني حسب الجهات التي تقوم به أو الآثار المترتبة عنه.

في ختام هذا المبحث وانسجاماً مع أهداف هذه الدراسة يرى الباحثان أنه من المنطقي تعريف الهجوم السيبراني استنادا إلى أن السيبرانية هي أداة الهجوم وليست هدفًا له؛ لأن قانون الحرب بشقيه يعتمد عموماً على مفاهيم تؤثر بشكل أكبر في نوع القوة التي يمكن أن تمارس ضد الهدف أكثر من طبيعة الهدف الذي تتم مهاجمته؛ لذلك يقترح الباحثان تعريف الهجوم السيبراني لأغراض هذه الدراسة على أنه: "أي عمل عدائي يقع في زمن السلم تقوم به الدول أو جهات تابعة لها ضد دول أخرى، ويتم باستخدام أدوات القوة التي يوفرها الفضاء السيبراني بهدف تدمير أو تعطيل أو التشويش على شبكات الكمبيوتر التي تتحكم أساساً بالبنية التحتية الحيوية، المدنية أو العسكرية، لتلك الدول لأغراض سياسية أو أمنية أو اقتصادية أو غيرها".

ومن جهة نظر الباحثين فإن هذا التعريف يقدم بديلاً أفضل للتعريفات السابقة للهجمات السيبرانية حيث إنه يتميز بالآتي:

1. إن الهجوم السيبراني عمل عدائي تقوم به الدول أو الجهات التابعة لها ضد دول أخرى.
2. يستخدم في الهجوم أدوات القوة التي يوفرها الفضاء السيبراني.
3. يترك هذا التعريف نوع الضرر الذي قد يتسبب به الهجوم السيبراني على تلك الدول مفتوحًا.
4. يقيد هذا التعريف الهجوم السيبراني من خلال هدفه السياسي أو الأمني القومي بما يميزه أشكال أخرى من العمليات التي تتم في الفضاء السيبراني مثل الجريمة السيبرانية والقرصنة السيبرانية.

المبحث الأول

مفهوم "القوة" استناداً إلى المادة 2(4) من ميثاق منظمة الأمم المتحدة

إن تحديد ما إذا كان الهجوم السيبراني ينتهك الحظر العام لاستخدام القوة أو التهديد بها في القانون الدولي يتطلب فهم كيفية تفسير مصطلح "القوة" الوارد في المادة 2 (4) من الميثاق التي تنص على أنه " يمتنع أعضاء الهيئة جميعاً في علاقاتهم الدولية عن التهديد باستعمال القوة أو استخدامها ضد سلامة الأراضي أو الاستقلال السياسي لأية دولة أو على أي وجه آخر لا يتفق ومقاصد "الأمم المتحدة".

جنباً إلى جنب مع الالتزام بحل النزاعات الدولية بالطرق السلمية يعد حظر استخدام القوة أو التهديد باستخدامها الوارد في المادة 2 (4) صميم نظام الأمن الجماعي لميثاق الأمم المتحدة، وحجر الزاوية في القانون الدولي العام، وهو لا يشكل فقط جزءًا من القانون الدولي التقليدي، ولكن أيضًا من القانون الدولي العرفي العام ذي الطبيعة الآمرة، وهو ما أكدت عليه محكمة العدل الدولية في قضية نيكاراغوا بقولها إنه: "يمكن العثور على تأكيد آخر لصلاحية مبدأ حظر استخدام القوة المنصوص عليه في الفقرة 4 من المادة 2 من ميثاق الأمم المتحدة كقانون دولي عرفي في حقيقة أنه كثيراً ما يشار إليه في البيانات من قبل ممثلي الدول ليس فقط باعتباره مبدأ من مبادئ القانون الدولي العرفي ولكن أيضًا مبدأ أساسياً أو جوهرياً لهذا القانون".[62]

من جهة أخرى فإن الحظر الورد في المادة 2(4) لا يقتصر فقط على استخدام القوة بل والتهديد بها كذلك، في هذا السياق يمكن تعريف التهديد باستخدام القوة بأنه " التهديد الصريح أو الضمني، شفاهاً أو عملاً باستخدام غير شرعي للقوات المسلحة ضد دولة أو عدة دول الذي يرتبط تحقيقه بإرادة الدولة التي قامت بعمل التهديد".[63] ، واستناداً إلى الرأي الاستشاري لمحكمة العدل الدولية بشأن الأسلحة النووية بينت المحكمة أن مفهومي "التهديد" و"استخدام" القوة بموجب المادة 2 (4) من الميثاق متلازمان؛ أي أنه إذا كان استخدام القوة بحد ذاته في حالة ما غير قانوني - لأي سبب

[62] See Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States of America), Merits, 1986 ICJ Rep. 14 (June 27), para. 190, P. 90. [“Nicaragua case”].

[63] أحمد عبيس نعمة الفتلاوي وزهراء عماد محمد كلنتر، مرجع سابق، ص 60-61.

من الأسباب - فإن التهديد باستخدام هذه القوة هو أيضا غير قانوني".[64] ولا يزال ما يشكل تهديد باستخدام القوة غامضًا نِسْبِيًّا، لكنه قد يشمل- على سبيل المثال لا الحصر- التهديدات اللفظية، والتحركات الأولية للقوات، والتحركات الأولية للصواريخ الباليستية، وحشد القوات على الحدود، والتشويش على أنظمة الإنذار المبكر والقيادة والتحكم.[65]

ومن جهة أخرى يتمم مبدأ حظر استخدام القوة أو التهديد بها الوارد في المادة 2(4) بمبدأ آخر أساسي ألا وهو عدم التدخل الوارد في القانون الدولي العرفي الذي يحظر على الدول التدخل في الشؤون الداخلية للدول الأخرى.[66] وهو ما أكدت عليه محكمة العدل الدولية في قضية نيكاراغوا بقولها " وتخلص المحكمة إلى أن الأفعال التي تشكل انتهاكًا للمبدأ العرفي لعدم التدخل ستشكل أيضًا إذا انطوت بشكل مباشر أو غير مباشر على استخدام القوة انتهاكًا لمبدأ عدم استخدام القوة في العلاقات الدولية".[67]

ميثاق الأمم المتحدة جاء صامتا بشأن الأشكال التي قد يتخذها استخدام القوة الوارد في سياق المادة 2(4)؛ لذا كانت هذه المادة والمعنى الدقيق لكلمة "قوة" مصدرًا لنقاش مثير للجدل منذ إقرار الميثاق، وفي هذا الإطار تلاحظ Bianchi أنه: "على الرغم من الالتزام الخطابي بالميثاق فإن تفسير أحكامه، ولا سيما المادة 2 (4) والمادة 51 أصبح مثيرًا للجدل إلى حد كبير، وبعبارة أخرى فإن الإجماع حول مركزية الإطار التنظيمي للميثاق لاستخدام القوة يتبخر عندما يتعلق الأمر بتفسير محتوى ونطاق تطبيق أحكامه الأساسية".[68]

ويبرز في هذا الإطار اتجاهان رئيسيان: الأول يتبنى مفهوماً واسعاً " للقوة "؛ ليشمل كل أشكال الإكراه Coercion بما فيها الإكراه الاقتصادي والسياسي، وليس

[64] Legality of the Threat or Use of nuclear weapons, para 47.
[65] See David Weissbrodt, op.cit, p.357.
[66] أحمد عبيس نعمة الفتلاوي وزهراء عماد محمد كلنتر، مرجع سابق، ص 58.
[67] Nicaragua case, para. 109, P. 99-100.
[68] Andrea Bianchi, The International Regulation of the Use of Force: The Politics of Interpretive Method, Leiden Journal of International Law, Vol. 11, 2009, 651-676, p. 659.

فقط العنف المسلح والثاني يتبنى مفهوماً ضيقاً يقصر مفهوم القوة فقط على العنف المسلح Armed violence.[69]

أولا: القوة باعتبارها شكلاً من أشكال الإكراه:

هذا الاتجاه تدافع عنه البلدان النامية وبلدان الكتلة الشرقية السابقة الذي يتبنى المفهوم الواسع للقوة من أنه قد يشمل أشكالًا أخرى من الإكراه، مثل الضغط السياسي والاقتصادي، ويميل أصحاب هذا الاتجاه إلى أن استعمال وسائل الضغط التي قد تمارس على الدول، إذا مورست بدرجة كبيرة فإنها تدخل في نطاق حظر استخدام القوة، وحجتهم في ذلك أن العبارات التي تضمنها الميثاق في المادة 2 (4) جاءت عامة ومطلقة بحيث لا تنصرف إلى القوة المسلحة وحدها، وإن القوة المحظور استخدامها هي تلك الموجهة ضد سلامة الأراضي أو الاستقلال السياسي لأي دولة التي تمارس على نحو لا يتفق ومقاصد الأمم المتحدة وأهدافها.[70] إن وجهة النظر هذه لا تنظر إلى الأداة المستخدمة ولكن الغرض منها وتأثيرها العام: إنها تحظر الإكراه، والقوة العسكرية الحركية ليست سوى أداة واحدة للإكراه.[71]

في هذا السياق خلال المناقشات المستفيضة لصياغة إعلان مبادئ القانون الدولي المتعلقة بالعلاقات الودية والتعاون بين الدول لعام 1966 أيدت العديد من الدول المستقلة حديثًا والنامية اَلتَّفْسِير الواسع لمصطلح "القوة".[72] فقد أوضحت العديد منها أنه لم تتح لهم الفرصة لتشكيل تفسير المادة 2 (4) خلال مؤتمر سان فرانسيسكو، وجادلت بأن أشكال الضغط الاقتصادي والسياسي كانت في بعض الأحيان أكثر

---

[69] Matthew C. Waxmant, Cyber-Attacks and the Use of Force: Back to The Future of Article 2(4), Yale Journal of International Law, Vol. 36, 2011, 421, p. 426-430.

[70] Ibid.

[71] Ibid.

[72] See, Second Report of the Special Committee on Principles of International Law Concerning Friendly Relations and Co-Operation Among States, UN Doc. A/6230, 27 June 1966, Para. 64['Second Report']; Third Report of The Special Committee on Principles of International Law Concerning Friendly Relations and Co-Operation Among States, UN Doc A/6799, 26 September 1967, See Para. 51 Ff for Summary of Debate.

يتضمن اقتراح الجزائر والكاميرون وغانا والهند وكينيا ومدغشقر ونيجيريا وسوريا والجمهورية العربية المتحدة ويوغوسلافيا ... أحكامًا تفيد بأن الضغط الاقتصادي والسياسي وغيره من أشكال الضغط ضد وحدة الأراضي أو الاستقلال السياسي لأي دولة يعد ضمن استخدامات القوة المحظورة.

خطورة من القوة المسلحة.[73] كما شدد العديد من ممثليها على الحاجة إلى تفسير مصطلح القوة في ضوء التطورات اللاحقة لصياغة الميثاق.[74]

وقد اعترفت العديد من الصكوك الدولية الصادرة عن هذه الدول أو بدعم منها بواجب الدول في الامتناع عن ممارسة الضغوط غير المبررة بما في ذلك الضغوط الاقتصادية أو غيرها من أشكال الضغط، مثل إعلانات باندونغ، وبلغراد، والقاهرة، وقراري الجمعية العامة للأمم المتحدة 2131 (xx) و2160(xxi) ، وميثاق منظمة الوحدة الأفريقية ، والمادة 51 من اتفاقية فيينا لقانون المعاهدات، وإعلان حظر الإكراه العسكري أو السياسي أو الاقتصادي الذي اعتمده مؤتمر فيينا لقانون المعاهدات.[75]

في السياق ذاته يعد هذا الاتجاه أيضاً أنه ليس فقط استخدام القوة بل إن التهديد باستخدامها هو شكل من أشكال الإكراه موضحاً أن الغرض من العبارة الواردة في المادة 2(4) من الميثاق ليس تضييق نطاق القوة المحظورة، بل إنه " تأكيد على أن التهديد باستخدام القوة أو التهديد بها غير مسموح به تحت أي ظرف من الظروف باستثناء ما يسمح به الميثاق".[76] وهو الموقف المستند إلى الرأي الاستشاري لمحكمة العدل الدولية بشأن الأسلحة النووية السالف ذكره.[77] كما أن الاتفاقيات الدولية تتعامل مع التهديد باستخدام القوة والاستخدام الفعلي لها على أن أنهما فعل غير مشروع متساوٍ في الخطورة وإن كانا متمايزين.[78]

ثانيا: القوة باعتبارها عنفاً مسلحاً Armed violence:

هذا المفهوم للقوة تدافع عنه الولايات المتحدة الأمريكية وحلفاؤها الغربيون، ويتبنى المفهوم الضيق للقوة الذي ينطبق فقط على الهجمات العسكرية أو العنف

[73] Fourth Report of The Special Committee on Principles of International Law Concerning Friendly Relations and Co-Operation Among States, Un Doc A/7326 (1968), para. 52.
[74] Second Report, op.cit, Para. 71.
[75] Ibid, Para. 73; Fifth Report of the Special Committee on Principles of International Law Concerning Friendly Relations and Co-Operation Among States, UN Doc A/7619 (1969). paras. 52 and 91.
[76] Julius Stone, Aggression and World Order: A critique of the United Nations theories of aggression, University of California Press, California, 1958.
[77] Legality of the Threat or Use of nuclear weapons, para 47.
[78] See Romana Sadurska, Threats of Force, The American Journal of International Law, Vol. 82, No. 2, 1988, Pp. 239–268. P.239.

المسلح، ويستند مفهوم القوة- حسب هذا الاتجاه- على نهج ميثاق منظمة الأمم المتحدة ، و"الغرض والهدف" من الميثاق، إذ يعتبر أن الهدف الصريح للأمم المتحدة هو الحفاظ على السلم والأمن الدوليين، وكذلك "إنقاذ الأجيال المقبلة من ويلات الحرب" كما يرد في ديباجة الميثاق.[79] وإن فكرة القوة كانت مقتصرة في عام 1945 على الأداة العسكرية، حيث يعزز تاريخ صياغة الميثاق هذا الاستنتاج. في هذا الصدد كتب مايكل شميث يقول:

"في مؤتمر سان فرانسيسكو قدم الوفد البرازيلي تعديلات لمقترحات دمبارتون أوكس Dumbarton Oaks من شأنها أن توسع نطاق المادة 2 (4) إلى الإكراه الاقتصادي. على الرغم من أن الاقتراح حصل على أغلبية الأصوات في اللجنة رفض المؤتمر اعتماده بتصويت 26-2. وبالتالي فإن التحليل القائم على كل من أعمال ميثاق الأمم المتحدة والنص يؤدي إلى تفسير يستبعد الإكراه الاقتصادي والسياسي، من المجال الإرشادي للمادة 2 (4)".[80]

ومن الذين دعموا المفهوم الضيق للقوة المقتصر على القوة المسلحة Sturchler الذي دلل على هذا الفهم للمادة 2 (4) الذي يستبعد أشكال التدخل غير القسرية من نطاق حظر استخدام القوة بمجموعة من العوامل أهمها: أولاً، اختيار واضعي الصياغة لاستخدام مصطلح "استخدام القوة" للتغلب على المشاكل المرتبطة بمصطلح "الحرب"، ثانيًا تشير الإشارات إلى "القوة" في مكان آخر في ميثاق الأمم المتحدة إلى "القوة المسلحة"؛ وثالثاً: رفض واضعو الميثاق صراحة اعتبار الإكراه الاقتصادي شكلاً من أشكال "القوة" التي تندرج تحت المادة 2(4).[81] معتبراً أنه "تم تصميم الصياغة الجديدة في ميثاق الأمم المتحدة لحل المشكلة المتمثلة في أن الحكومات يمكن أن تنكر وجود حالة حرب ببساطة من خلال عدم اسناد هذا المصطلح إلى أعمالها العسكرية."[82] وكذلك Randelzhofer and Dörr اللذان اعتبرا أنه إذا امتدت المادة 2 (4) لتشمل أشكالًا أخرى من القوة، مثل الإكراه الاقتصادي

[79] Albrecht Randelzhofer and Oliver Dörr, Article 2(4), In B Simma et al (eds), The Charter of the United Nations: A Commentary (2nd ed, Oxford University Press, Oxford, 2002), p.118.

[80] Michael N. Schmitt, Computer Network Attack and the use of force in International Law: Thoughts on a Normative Framework, The Columbia Journal of Transnational Law, Volume 37, 1999, 885-937, p. 905.

[81] Nikolas Stürchler, The Threat of Force in International Law (Cambridge: Cambridge University Press, 1st ed, 2007) p. 2.

[82] Ibid.

والسياسي، فلن يكون للدول أي وسيلة قانونية لممارسة الضغط على الدول التي تنتهك القانون الدولي، وأن المجتمع الدولي الذي لا تستطيع أجهزته ضمان الامتثال للقانون الدولي سيجد أن هذه النتيجة غير مقبولة.[83]

في رده على دعم فقيه القانون الدولي هانس كلسن في كتابه قانون الأمم الصادر في عام 1950، للمفهوم الواسع للقوة عد Brownlie أنه: "صحيح أن الأعمال التحضيرية للميثاق لا تشير إلى أن مفهوم القوة ينطبق على القوات المسلحة فقط، إلا أنه لا يوجد دليل على ما طرحه كلسن سواء في المناقشات التي جرت في مؤتمر سان فرانسيسكو أو في ممارسات الدول أو أعمال منظمة الأمم المتحدة."[84]

واستمرار في التشديد على موقفها تمسكت الدول الغربية بمفهومها الضيق " للقوة " خلال المناقشات المستفيضة لصياغة إعلان مبادئ القانون الدولي المتعلقة بالعلاقات الودية والتعاون بين الدول لعام 1966 مستندة إلى العديد من الحجج نذكر منها:[85]

1. إن رفض مؤتمر سان فرانسيسكو للمقترح البرازيلي المشار إليها سلفاً الهادف إلى توسيع نطاق الحظر المنصوص عليه في المادة 2 (4) من خلال إضافة عبارة "والتهديد بالتدابير الاقتصادية أو استخدامها" هو دليل قاطع على المعنى الذي ينبغي إعطاؤه لكلمة "القوة" الواردة في هذه المادة.
2. تم استخدام مصطلح "القوة" أيضًا دون أي قيد في المادة 44 من الميثاق، وليس هناك شك في أنه يشير حَصْرِيًّا إلى القوة المسلحة.
3. من شأن التفسير الواسع لمصطلح "القوة" الوارد في الفقرة 4 من المادة 2 (4) من الميثاق أن يغير العلاقة القائمة بين تلك المادة وأحكام الفصل السابع من الميثاق تمامًا، ومن شأنه أيضًا أن يعطي تفسيراً أوسع للحق الأصيل للدفاع الفردي أو الجماعي عن النفس المنصوص عليه في المادة 51 من الميثاق.
4. بغض النظر عن الاعتراضات القانونية الأساسية على إدراج الضغوط الاقتصادية والسياسية في تعريف القوة، لم يكن هناك تعريف مرضٍ قَانُونِيًّا لها.

[83] Albrecht Randelzhofer and Oliver Dörr, op.cit, p.118.
[84] Ian Brownlie, International Law and the use of force by States (Clarendon, 1963), p. 362.
[85] See Second Report, op.cit, Para. 75; Third Report, op.cit, Para. 56..

في المحصلة لم يتوصل المؤتمرون في مفاوضات إعلان مبادئ القانون الدولي المتعلقة بالعلاقات الودية والتعاون بين الدول لعام 1966 إلى اتفاق نهائي بشأن مسألة ما إذا كان حظر استخدام القوة يشمل حظر أشكال أخرى من الإكراه.[86]

ومن جانب آخر أحدث تعريف العدوان الوارد في المادة الأولى من قرار الجمعية العامة رقم 3314 (د-29) سنة 1974 تطوراً مهماً في الجدل حول مفهوم القوة، فقد عرف القرار العدوان بأنه "استخدام القوة المسلحة من قبل دولة ما ضد سيادة دولة أخرى أو سلامتها الإقليمية أو استقلالها السياسي، أو بأي طريقة أخرى تتعارض مع ميثاق الأمم المتحدة وفقاً لنص هذا التعريف".

إن إدخال مصطلح "مسلح" بعد مصطلح "القوة" في المادة الأولى من قرار الجمعية العامة بشأن تعريف العدوان هو أهم ما يميزها عن نص المادة 2 (4). وفي هذا السياق يعد أحد الباحثين أن استخدام مصطلح "مسلح" في هذه المادة يعزز الاتجاه القائل إن المادة 2 (4) من ميثاق الأمم المتحدة موجهة إلى القوة المسلحة فقط؛ لأنها تشكل جزءًا من إطار الأمن الجماعي للأمم المتحدة بموجب المادة 39 من الميثاق.[87] ويرى آخر إنه يمكن اعتبار ذلك بمثابة تطور تدريجي للقانون الدولي من خلال الاتفاق اللاحق بين الأطراف فيما يتعلق بتفسير المادة 2 (4)، حيث أنهى استخدام كلمة "مسلح" في مضمون القرار "النقاش حول العدوان الاقتصادي أو الأيديولوجي".[88]

لكن يبدو أن هذه الآراء تجانب الصواب وتعبر عن موقف معين ليس محل إجماع دولي، ففي بيانه الذي أدلى به خلال المفاوضات على قرار الجمعية العامة للأمم المتحدة بخصوص تعريف العدوان عد الاتحاد السوفييتي السابق: " أن فكرة استخدام القوة أوسع نطاق من الهجوم المسلح أو العدوان، وأن الحوادث الصغيرة المتنوعة التي لا تصل إلى درجة العدوان ربما لا تعتبر مطلقا استخداما للقوة".[89] كما

[86] George Winthrop Haight. “United Nations: Principles of International Law Concerning Friendly Relations and Co-Operation Among States, The International Lawyer, Vol. 1, No. 1, 1966, pp. 96–133.

[87] Tho Tom Ruys, The meaning of ‘force’ and the boundaries of the jus ad bellum: are ‘minimal’ uses of force excluded from un charter article 2(4)? The American Journal of International Law, vol. 108, no. 2, 2014, Pp159–210. p. 164.

[88] Thomas Bruha, The General Assembly’s definition of the act of aggression, In Claus Kres and Stefan Barriga (Eds), Commentary on the crime of aggression (Cambridge University Press, 2015) p. 159.

[89] Tho Tom Ruys, op.cit, p. 164.

ينص قرار تعريف العدوان الذي اتخذته جمعية الدول الأطراف في المحكمة الجنائية الدولية سنة 2010 بأن مصطلح: " استخدام القوة أوسع نطاق من العدوان" حسب المادة 8 مكرر من النظام الأساسي للمحكمة الجنائية الدولية.[90]

إن الصراع السياسي الذي كان سائدا بعد إنشاء منظمة الأمم المتحدة ودخولها ميثاقها حيز التنفيذ، ولاسيما في فترة الحرب الباردة بين المعسكرين الغربي بقيادة الولايات المتحدة الأمريكية وحلفائها الغربيين، والشرقي بقيادة الاتحاد السوفياتي وحلفائها من دول المعسكر الاشتراكي ودول العالم الثالث، ولا يخدم التفسير القانوني لمفهوم القوة في إطار ميثاق الأمم المتحدة، وعليه فمن الأجدر الوقوف على موقف الجهاز القضائي الرئيسي للأمم المتحدة ألا وهو محكمة العدل الدولية.

في هذا السياق يعد حكم محكمة العدل الدولية في قضية نيكاراغوا مرجعاً أساسياً لتفسير مفهوم القوة الوارد في المادة 2(4) من الميثاق.[91] فقد أكدت المحكمة في هذه القضية على شمولية المادة ، وعدم اقتصارها على استخدام القوة بالمعنى التقليدي، والمتمثل في استخدام قوات عسكرية نظامية خارج حدود الدولة، مؤكدة على أن المادة 2 (4) من الميثاق لا تمثل سوى جزءاً من القانون الدولي العرفي المتعلق باستخدام القوة، وموضحة أن "ميثاق الأمم المتحدة لا يغطي بأي حال من الأحوال كامل مجال تنظيم استخدام القوة في العلاقات الدولية؛ لأن القانون الدولي العرفي لا يزال موجودًا جنبًا إلى جنب مع قانون المعاهدات".[92] كما أكدت المحكمة على هذا النهج في رأيها الاستشاري الخاص بالأسلحة النووية، من أن أحكام ميثاق الأمم المتحدة بشأن استخدام القوة، ولاسيما المادتين 2 (4) و 51 التي تعكس جميعها القانون الدولي العرفي "تنطبق على أي استخدام للقوة بغض النظر عن الأسلحة المستخدمة".[93]

ومما يجدر ذكره أيضاً أن المحكمة قد أكدت في قضايا أخرى عرضت أمامها على الطبيعة الديناميكية لتفسير أحكام الميثاق معتبرة أنه "عندما تستخدم الأطراف مصطلحات عامة في معاهدة ما يكون الأطراف بالضرورة على دراية بأن معنى

[90] Ibid.
[91] Eimear Bourke, A War Without Bullets: Protecting Civilians in the Technology Trenches, Albany Law Journal of Science and Technology, Vol. 8, No. II, 2018, p.11.
[92] Nicaragua case Para 176.
[93] Legality of the Threat or Use of nuclear weapons, para 39. See Michael N. Schmitt, Cyberspace and International Law. the penumbral mist of uncertainty, Harvard Law Review Forum, Vol. 126, 2013. p.176.

المصطلحات من المرجح أن يتطور بمرور الوقت، وحيث تم الدخول في المعاهدة لفترة طويلة جِدًّا أو كانت ذات مدة مستمرة، يجب أن يُفترض، كقاعدة عامة، أن الأطراف قصدت أن يكون لهذه المصطلحات معنى متطور".[94] وإنه "يجب تفسير الصك الدولي وتطبيقه في إطار النظام القانوني السائد حينها".[95]

وفي هذا الصدد ورد في التعليق على ميثاق منظمة الأمم المتحدة أن المحكمة أقرت بأن: " أحكام الميثاق ديناميكية وليست ثابتة، وبالتالي فهي قادرة على التغيير بمرور الوقت من خلال ممارسة الدولة".[96] وإن "وجهة النظر السائدة اليوم هي أنه يجب تفسير الميثاق بطريقة ديناميكية هادفة وليس بطريقة جامدة ثابتة"[97] ، وهو ما يدعمه الباحثان حيث إن بعض أشكال الإكراه مثل فرض العقوبات الاقتصادية يمكن أن تكون له أضرار مدمرة، ليس على النظام السياسي الحاكم في تلك الدولة فقط بل على مواطنيها أيضا.

ومن جانب آخر وبالرجوع إلى اتفاقية فيينا لقانون المعاهدات لعام 1969 قررت المادة 31(1) أنه يجب تفسير المعاهدة بحسن نية طبقاً للمعنى العادي لألفاظ المعاهدة في الإطار الخاص بها وفي ضوء موضوعها والغرض منها، وفي هذا السياق يرى أحد الباحثين أن المعنى العادي" للقوة " هو العنف أو الضغط الموجه ضد دولة، وهو بالتالي واسع بما يكفي لتغطية ليس فقط القوة المسلحة التقليدية، ولكن أيضا أنواع أخرى من الإكراه.[98] وإن الميثاق يشير صراحة في مواده عندما يريد واضعوه إلى الإشارة إلى "القوة المسلحة"، وبما أن الأمر لم يكن كذلك في المادة 4 (2) فربما أراد واضعوه الرجوع إلى نطاق أوسع في تفسيره ليتماشى مع الهدف العام للميثاق هو" إنقاذ الأجيال من ويلات الحرب".[99] كما يرى آخر أن التفسير الضيق للمادة 2(4) لا يدعمه المفهوم الضمني للمادة 31 (3) (ب) من اتفاقية فيينا لقانون المعاهدات لعام 1969 التي تنص على أنه يجب تفسير المعاهدات بطريقة

[94] Dispute Regarding Navigational and Related Rights (Costa Rica V Nicaragua), Judgment Of 13 July 2009, ICJ Reports 2009, Para 66.

[95] Legal Consequences for States of the Continued Presence of South Africa in Namibia (South West Africa) Notwithstanding Security Council Resolution 276 (1970), Advisory Opinion, 21 June 1971, ICJ Reports 1971, Para 53.

[96] 'Reform' in Bruno Simma et al (eds), The Charter of The United Nations: A Commentary (Oxford University Press, 3rd ed, Vol I, 25, 2012, p. 31-32.

[97] Ibid.

[98] عمر محمود أعمر، مرجع سابق، ص 140-141.

[99] نفس المرجع.

تأخذ في الاعتبار: "أي تعامل لاحق في مجال تطبيق المعاهدة يتضمن اتفاق الأطراف على تفسيرها". ؛ إذ يدعم نص هذه الفقرة الزعم بأن المعاهدات ليست ثابتة، بل هي أدوات ديناميكية ، وهكذا ينبغي تفسيرها بحيث تأخذ في الاعتبار السياقات الجديدة والناشئة، وهو ما يعرف في فقه القانون الدولي بالتفسير التطوري evolutive interpretation للمعاهدات الدولية.[100]

وهذا يوفر أسبابًا لاستنتاج أن مصطلح "استخدام القوة" كان يُقصد به أن يخضع لتفسير تطوري من أجل تنظيم الظروف المتغيرة والاستخدامات الجديدة للقوة التي لم تكن متوقعة في عام 1945، وهذا الاستنتاج مدعوم من نهج محكمة العدل الدولية، ولقد صُمم ميثاق الأمم المتحدة كما يرى الباحثان بحيث يستمر لمدة طويلة، وأن يحكم الظروف الدولية المتغيرة.

المبحث الثاني

الهجمات السيبرانية باعتبارها استخداماً للقوة المسلحة أو التهديد بها

إن مفهوم القوة في إطار الحرب السيبرانية له مدلولاته المختلفة عن مفهومها التقليدي كما قصده واضعو ميثاق الأمم المتحدة، ولاسيما في ضوء استخدام الهجمات السيبرانية في ظروف وسياقات مختلفة؛ إذ يتم استخدام الهجمات السيبرانية كأداة لصراع منخفض الشدة محدود الأثر، ومثال ذلك ما تعرضت له الولايات المتحدة الأمريكية من قرصنة سيبرانية اتهمت بها روسيا خلال الانتخابات الرئاسية لعام 2016 التي فاز بها المرشح الجمهوري دونالد ترامب في مواجهة منافسته الديمقراطية هيلاري كلنتون.[101] كما يمكن أن تكون هذه الهجمات عنصراً فاعلاً في حال استخدامها في نزاع مسلح تقليدي مستمر من أجل الحصول على ميزة

[100] See Rudolf Bernhardt, Evolutive Treaty Interpretation, Especially of the European Convention on Human Rights, German Year Book of International law, Vol.42, 1999, p.15; Sondre Torp Helmersen, Evolutive Treaty Interpretation: Legality, Semantics and Distinctions, European Journal of Legal Studies, Volume 6, No. 1 (Spring/Summer 2013), p 127-148.

[101] Delbert Tran, The Law of Attribution: Rules for Attributing the Source of a Cyber-Attack, The Yale Journal of Law & Technology, Vol.20, 376, 2018, p. 378-379. https://openyls.law.yale.edu/bitstream/handle/20.500.13051/7830/DelbertTranTheLawofAttrib.pdf?sequence=2&isAllowed=y

عسكرية.[102] حيث يتم تحويل الصراع عبر الفضاء السيبراني ساحةً موازية أو مرافقة أو مرتبطة بحرب تقليدية دائرة على الأرض، ومثل ذلك ما تتعرض له أوكرانيا من هجمات سيبرانية خلال العدوان الروسي عليها في أواخر شهر فبراير من العام 2022.[103] أيضا قد تتراوح آثار الهجوم السيبراني من إزعاج بسيط (مثل هجوم DDoSالذي يعطل مواقع الإنترنت مؤقتًا) إلى التدمير المادي (مثل تغيير الأوامر المعطاة إلى مولد الطاقة الكهربائية مما يؤدي إلى حدوث انفجار)، وحتى الموت (مثل تعطيل خطوط الطوارئ بحيث لا يمكن الاتصال هاتفياً بالشرطة أو خدمات الإسعاف).[104]

السؤال الذي يطرح نفسه: ما هي العتبة التي قد يصل فيها الهجوم السيبراني إلى عتبة "الهجوم المسلح"؟

في ظل غياب اتفاق دولي يحكم الهجمات السيبرانية اقترح فقه القانون الدولي عدة معايير لفحص متى يمكن اعتبار هذه الهجمات بمثابة هجمات مسلحة.[105]

أولاً: النهج القائم على الوسيلة المستخدمة في التنفيذ:

تبنى أصحاب هذا النهج معيار الوسيلة المستخدمة في الهجوم، وبموجب هذه النظرية، لكي يشكل الهجوم السيبراني هجوماً مسلحاً يجب أن يحتوي على

---

[102] Herbert Lin, Cyber Conflict and International Humanitarian Law, International Review of the Red Cross, Vol. 94, No. 886, 2012, P.515.

[103] See Friedel Taube, Russia-Ukraine conflict: What role do cyberattack play? (28/2/2022)
https://www.dw.com/en/russia-ukraine-conflict-what-role-do-cyberattacks-play/a-60945572

[104] Michael Gervais, Cyber Attacks and The Laws of War, Berkeley Journal of International Law, Vol. 30, No. 2, 2012, p. 525.

[105] يشار إلى أن المادة 49 (1) من البروتوكول الإضافي الأول لاتفاقيات جنيف لعام 1949 الذي دون قواعد القانون الدولي العرفي للنزاعات المسلحة الدولية، قد عرفت "الهجمات" بأنها "أعمال العنف الهجومية والدفاعية صد الخصم". وقد أوضح تعليق اللجنة الدولية للصليب الأحمر على هذه المادة أن "الهجوم" يعني عمل قتالي "combat action" يشير إلى عنف مادي. ومن ثم فإن مصطلح "الهجمات" يستبعد وسائل الحرب غير المادية الأخرى (على سبيل المثال النفسية أو الاقتصادية أو السياسية).

See Yves Sandoz, Christophe Swinarski, Bruno Zimmermann eds, Commentary on the Additional Protocols of 8 June 1977 to The Geneva Conventions of 12 August 1949 (Geneva: International Committee of the Red Cross: Martinus Nijhoff Publishers, 1987). para.1880, p.603.

"الخصائص المادية المرتبطة تَقْلِيدِيًّا بالإكراه العسكري".[106] ؛ أي القوة الحركية (kinetic) التي تتميز بها الأسلحة التقليدية.[107] ويدلل Dinstein على صحة هذا النهج بأنه إذا كان من الممكن أن يتسبب هجوم سيبراني في تدمير شبكة للطاقة الكهربائية فإنه يشكل هجومًا مسلحًا، ويعزي ذلك إلى حقيقة أنه قبل تطوير القدرات السيبرانية، لم يكن من الممكن أن يكون هذا التدمير ممكنًا إلا باستخدام الطاقة الحركية.[108]

ويتفق معظم الباحثين على أن هذا النهج غير فعال حيث إن التمييز بين الأسلحة العسكرية التقليدية والأسلحة السيبرانية يعد تعسفياً للغاية ، ولا يعكس بشكل كافٍ الإمكانات المتأصلة للأسلحة السيبرانية غير الحركية التي قد تتسبب في نفس مستويات الضرر والموت التي تتسبب بها الأسلحة العسكرية التقليدية. [109]

ثانيا: النهج القائم على الهدف (المسؤولية الصارمة):

هذا النهج يعد أن الهجمات السيبرانية تعد هجمات مسلحة إذا ما استهدفت البنية التحتية الحيوية للدولة بغض النظر عما إذا كان هذا الهجوم قد تسبب في أي تدمير مادي أو خسائر بشرية.[110] في هذه الحالة يكون للدولة حق ممارسة تدابير دفاعية نشطة أو شن هجوم سيبراني مضاد دون تحمل المسؤولية.[111]

هناك من ينتقد هذا النهج بسبب عدم وجود تعريف مقبول عالميًا لما يشكل "البنية التحتية الحيوية". لكن يبدو أن معظم التعريفات تتفق على أن بعض الخدمات مثل الأمن والغذاء والمياه والنقل والمصارف والتمويل والصحة والطاقة والخدمات

[106] أحمد عبيس نعمة الفتلاوي وزهراء عماد محمد كلنتر، المرجع السابق، ص 59.
[107] نفس المرجع.
[108] Yoram Dinstein, Computer Network Attacks and Self-Defense, In M N Schmitt and B T O'donnell (Eds), Computer Network Attack and International Law (Naval War College, Newport, Ri, 1999) Pp 99-119, p.99
[109] Matthew Rinear, Comment: Armed with A Keyboard: Presidential Directive 20, Cyber-Warfare, And the International Laws of War, Capital University Law Review, Vol. 43, 697, Summer 2015, p. 701-702.
[110] Sean M. Condron, Getting It Right: Protecting American Critical Infrastructure in Cyberspace, Harvard journal of law & technology, Vol.20, 2007, 403, p. 415-416.
[111] Ibid.

الحكومية والعامة تشكل بنية تحتية حيوية للدولة.[112] انتقاد آخر يكمن في أن هذا النهج قد يجيز الدفاع عن النفس رداً على الهجمات السيبرانية الأقل جسامة التي قد تستهدف البنية التحتية الوطنية للدولة.[113]

ثانيا: النهج القائم على الآثار:

يعد البروفيسور مايكل شميت مدير فريق الخبراء المشرف على إعداد تالين لعام 2013 صاحب هذا النهج الذي يبدو أنه تأثر بنفس النهج الذي تفضله وزارة الدفاع الأميركية في قياس متى يمكن أن تصل الهجمات السيبرانية إلى عتبة الهجمات المسلحة.[114] وهو يجادل بأنه لكي يرقى الهجوم السيبراني إلى هجوم مسلح يجب أن يتسبب في حدوث أضرار مادية وخسائر بشرية جسيمة تضاهي تلك الناتجة عن هذا الأخير.[115] وقد عد شميث بأنه للتحقق من ذلك ينبغي قياس آثار الهجوم السيبراني بالرجوع إلى ستة معايير: الشدة severity، والفورية immediacy، والمباشرة directness، والغزو (التوغل) invasiveness، وقابلية القياس measurability، والشرعية الافتراضية presumptive legitimacy.[116]

---

[112] Nicholas Tsagourias, Cyber Attacks, Self-defense and the Problem of Attribution, Journal of Conflict and Security Law, vol. 17, no. 2, 2012, 229–244, p. 231.

[113] Ibid.

[114] Duncan B. Hollis: Why States Need an International Law for Information Operations, Lewis & Clark Law Review, Vol. 11, 2007, 1023-1042. P. 1040.

[115] Michael N. Schmitt, Computer Network Attack, op.cit, p. 913.

[116] Ibid, p. 914-15.

يقصد بهذه المعايير الستة الآتي:

1. الشدة: تبحث في نطاق وشدة الهجوم. يفحص التحليل بموجب هذا المعيار عدد القتلى وحجم المنطقة التي تعرضت للهجوم ومقدار الأضرار التي لحقت بالممتلكات، وكلما زاد الضرر زادت قوة الحجة للتعامل مع الهجوم السيبراني على أنه هجوم مسلح.

2. الفورية: تنظر في مدة الهجوم السيبراني إضافة إلى عوامل التوقيت الأخرى، ويفحص التحليل بموجب هذا المعيار مقدار الوقت الذي استمر فيه الهجوم السيبراني والمدة الزمنية التي شعرت فيها الدولة المستهدفة بالآثار، وكلما طالت مدة الهجوم وآثاره تعززت الحجة القائلة بأنه هجوم مسلح.

3. المباشرة: تنظر مباشرة في الضرر الناجم عن الهجوم، إذا كان الهجوم هو السبب المباشر للضرر، فإنه يعزز الحجة القائلة إن الهجوم السيبراني كان هجومًا مسلحًا. إذا كان الضرر ناتجًا كليًا أو جزئيًا عن هجمات موازية أخرى، تضعف هذه الحجة.

4. الغزو (التوغل): ينظر إلى مكان الهجوم. الهجوم الغازي هو الهجوم الذي يعبر فعليًا حدود الدولة، أو يعبر الحدود إلكترونيًا ويسبب ضررًا داخل دولة الضحية. كلما كان الهجوم السيبراني أكثر توغلاً، بدا وكأنه هجوم مسلح.

5. قابلية القياس: تحاول قابلية القياس تحديد مقدار الضرر الناجم عن الهجوم السيبراني. كلما زادت قدرة الدولة على تحديد مقدار الضرر الذي لحق بها، بدا الهجوم السيبراني أشبه بهجوم مسلح.

ويعتقد شميث أن معياره يتوافق مع مبادئ قانون اللجوء إلى الحرب؛ لأن"الإكراه المسلح لا يتم تعريفه من خلال استخدام الطاقة الحركية أو إطلاقها، بل من خلال طبيعة الآثار المباشرة الناتجة عنه، وتحديدًا الأضرار المادية والإصابات البشرية".[117] موضحاً أن العمليات السيبرانية التي تهدف إلى إجبار دولة اِقْتِصَادِيًّا على الانخراط في مسار عمل معين أو الامتناع عنه وكذلك تمويل العمليات السيبرانية لمجموعة متمردة لن ترقى إلى مستوى استخدام القوة.[118]

ويستند هذا النهج إلى الاجتهاد القضائي لمحكمة العدل الدولية: في قضية نيكاراغوا ميزت المحكمة بين أخطر أشكال استخدام القوة gravest forms تلك التي تشكل هجومًا أو عدوانًا مسلحًا، واستخدامات أخرى للقوة، عدتها المحكمة على أنها "أشكال أقل خطورة" less grave forms.[119] وأوضحت المحكمة أن الاختلاف بين "الهجمات المسلحة" والأشكال الأقل خطورة من استخدام القوة هو في الأساس مسألة "الحجم والآثار".[120] لكن المحكمة رفضت تحديد المقصود بـ "استخدام القوة" أو "الهجوم المسلح" صراحة، أو معالجة ما يمكن أن يشكل تدبيراً مضاداً مسموحًا به، إن وجد، عندما لا ترقى القوة إلى مستوى الهجوم المسلح.[121] وقد أعادت المحكمة التأكيد على هذا التمييز في قضية منصات النفط، موضحة أن: "أخطر أشكال استخدام القوة" هي فقط التي تعد "هجمات مسلحة".[122] وفي قضية الأنشطة المسلحة على أراضي الكونغو عدت المحكمة أن حجم ومدة التدخل العسكري غير المشروع من جانب أوغندا يجعل منه انتهاكًا خطيرًا لحظر استخدام القوة المنصوص عليه في

6. الشرعية الافتراضية: تركز على ممارسات الدول ومعايير السلوك المقبولة في المجتمع الدولي. قد يكتسب سلوك معين الشرعية بموجب القانون عندما يقبله المجتمع الدولي. كلما كان الهجوم السيبراني أقل شبهاً بالممارسات المقبولة للدول، زادت قوة الحجة القائلة بأنه استخدام غير قانوني للقوة أو هجوم مسلح.
See Thomas C. Wingfield, op.cit, P. 124-127.

117 Michael N. Schmitt, Computer Network Attack, op.cit, p. 913.

118 Michael N. Schmitt, The Law of Cyber Warfare: Quo Vadis, Stanford Law & Policy Review, Vol 25, 2014, 269. p.280

119 Nicaragua Case, para. 191. See J. A. Green, The International Court of Justice and Self-Defence in International Law (Oxford: Hart Publishing, 2009), At Pp. 31-36.

120 Nicaragua Case, para.195.

121 Reese Nguyen, Navigating jus ad bellum in the age of cyber warfare. California Law Review, Vol. 101, 2013. 1079, p.1115.

122 Oil Platforms (Islamic Republic of Iran V. United States of America), Judgment, I.C.J. Reports 2003, paras. 51, 64.

المادة 2 (4) من الميثاق.[123] ورفضت المحكمة في هذه القضية مطلب أوغندا بالدفاع عن النفس بموجب المادة 51، وخلصت إلى أن أوغندا لم تتعرض للهجوم من قبل قوات جمهورية الكونغو الديمقراطية.[124] وقضت بأن الهجمات عبر الحدود من قبل الجماعات المتمردة المناهضة لأوغندا من داخل أراضي جمهورية الكونغو الديمقراطية لم تكن مرتبطة بشكل كافٍ بحكومة جمهورية الكونغو الديمقراطية لتبرير استخدام أوغندا للقوة.[125]

من أهم الانتقادات التي وجهت للنهج القائم على الآثار هو أنه لا ينطبق إلا على الهجمات السيبرانية التي يكون لها آثار مشابهة لتلك التي تحدثها الأسلحة التقليدية خاصة تدمير الممتلكات وإزهاق الأرواح، حيث إن عددًا محدودا فقط من تلك الهجمات هي التي يمكنها أن تتسبب في حدوث ذلك.[126] كما أنه في كثير من الأحيان يصعب رسم الحدود الفاصلة بين الآثار المباشرة وغير المباشرة لبعض الهجمات السيبرانية، فالإغلاق المؤقت لخطوط الاتصال بالشرطة وخدمات الإسعاف قد يؤدي إلى حدوث أضرار مباشرة في الممتلكات والأرواح، وقد لا يؤدي إلى حدوث ذلك.[127]

لم تحظ المناهج الثلاثة السابقة بتأييد العديد من المحللين، ويجادل Hollis بأن اختيار أحد هذه المناهج ليس هو الحل، فبسبب حداثة أساليب الهجمات السيبرانية فإن كل نهج منها يثبت عدم فعاليته.[128]

لكن يبدو أن النهج القائم على الآثار هو الذي قوي على الصمود خاصة بعدما تم تبنيه من قبل خبراء دليل تالين مع بعض التعديل كما سنرى لاحقا، وهو، مع الانتقادات الموجهة له، لا يوفر فقط إطارًا لتحليل الهجمات السيبرانية التي لا تضاهي بدقة الهجمات المسلحة الحركية فحسب، بل إنه يشمل أيضا كل ما يحاول النهج القائم على الوسيلة التصدي له إضافة إلى ذلك يتفوق هذا النهج على نهج المسؤولية

[123] Armed Activities on the Territory of the Congo (Dem. Rep. Congo v. Uganda), 2005 I.C.J. 116 (Dec. 19) para 165.
[124] Ibid, paras. 141and 147.
[125] Ibid, paras.222-223.
[126] Daniel B. Silver, Computer Network Attack as A Use of Force Under Article 2(4), International Law Studies, Vol. 76, 2002, p. 92–93
[127] Michael Gervais, op.cit, p.539
[128] See Duncan B. Hollis, op.cit, P. 1040-1042.

الصارمة؛ لأن هذا الأخير قد يتسبب في انتهاك الدولة الضحية لقانون الحرب من خلال الرد بالدفاع عن النفس في مواجهة الهجمات السيبرانية الأقل جسامة.

ومع أننا لم نشهد حتى اليوم هجومًا سيبرانيا شديدًا يمكن أن يتسبب في إلحاق أضرار مادية وبشرية كبيرة، فهذا لا يعني أن الهجوم السيبراني أو سلسلة من هذه الهجمات لا يمكن أن ترقى، ولو نظرياً إلى مستوى ما يعد هجومًا مسلحًا بموجب القانون الدولي للحرب، [129] ومع ذلك لكي يكون للدولة الضحية الحق في استخدام القوة المسلحة للدفاع عن نفسها بشكل قانوني أمام هذه الهجمات يجب عليها أن تستوفي مجموعة من المتطلبات من أهمها أن تنسب مثل هذا الهجوم بشكل مباشر وقاطع إلى دولة أخرى أو الوكلاء الخاضعين للسيطرة المباشرة لتلك الدولة [130] إضافة إلى ضرورة احترام مبادئ وقواعد القانون الدولي الإنساني ولاسيما مبدأي الضرورة والتناسب،[131] وهي مسائل يصعب إثباتها وتثير العديد من الإشكاليات.

في خاتمة هذا المبحث لا بد من وقفة أخيرة تتمثل في السؤال الآتي: هل تستبعد الدول تماماً القانون الدولي للحرب الذي يجيز استخدام القوة المسلحة للرد على الهجمات السيبرانية، في هذا السياق يعد بعضهم أن التركيز على الفضاء السيبراني كساحة معركة يتعارض مع القانون الدولي الذي يحكم استخدام القوة بينما يفضل بعضهم الآخر استبعاد القانون الدولي من النقاش في هذا المجال تمامًا. [132] آخرون لا يستبعدون القانون الدولي، لكنهم يفسرونه بأي طريقة تجعله مستبعدًا في الواقع. [133] في هذا السياق أشار الرئيس الأمريكي باراك أوباما في مايو 2011 إلى أن القانون الدولي سيؤدي دورًا في تخطيط الأمن السيبراني في الولايات المتحدة مشيرًا، مع ذلك، إلى أنه سيكون القانون الدولي كما يفسره أولئك الذين يدافعون عن حق واسع غير مقيد للولايات المتحدة في اللجوء إلى القوة. [134] وهو ما تكرر في الاستراتيجية الدولية للفضاء السيبراني لعام 2011، حيث أعلن البيت الأبيض الآتي:

---

[129] Sean M. Condron, op.cit, p. 414
[130] Ibid. See Delbert Tran, op.cit, p. 381-383.
[131] حول مبدأي الضرورة والتناسب راجع
Michael N. Schmit, International Law and the Use of Force, op.cit, p. 92-93.
[132] See Mary Ellen O'Connell, Cyber Security without Cyber War, Journal of Conflict & Security Law, Vol. 17, 187, 2012, p. 198.
[133] Ibid.
[134] Ibid.

عندما يكون هناك ما يبرر ذلك سترد الولايات المتحدة على الأعمال العدائية في الفضاء السيبراني كما نرد على أي تهديد آخر لبلدنا، وتمتلك جميع الدول حَقًّا متأصلاً للدفاع عن النفس، ونحن ندرك أن بعض الأعمال العدائية التي تتم عبر الفضاء السيبراني يمكن أن تفرض إجراءات بموجب الالتزامات التي تعهدنا بها مع شركائنا في المعاهدات العسكرية نحتفظ بالحق في استخدام جميع الوسائل الضرورية - الدبلوماسية والمعلوماتية والعسكرية والاقتصادية - بالشكل المناسب والمتوافق مع القانون الدولي المعمول به من أجل الدفاع عن أمتنا وحلفائنا وشركائنا ومصالحنا، وبذلك سنستنفد جميع الخيارات قبل اللجوء لاستخدام القوة العسكرية، كلما أمكننا ذلك، وسوف نوازن بعناية بين تكاليف ومخاطر اتخاذ إجراء مقابل تكاليف عدم اتخاذ أي إجراء؛ وسنعمل بطريقة تعكس قيمنا وتعزز شرعيتنا، وتسعى للحصول على دعم دولي واسع كلما أمكن ذلك.[135]

والولايات المتحدة الأمريكية ليست وحدها في هذا التوجه، فقد ذهبت روسيا إلى أبعد من ذلك ةعدت أن الهجوم على صناعات الاتصالات السلكية واللاسلكية والطاقة الإلكترونية في روسيا- بحكم عواقبه الكارثية- سيتداخل تمامًا مع استخدام أسلحة الدمار الشامل، [136] وعليه تحتفظ روسيا بالحق في الرد على هجوم حرب المعلومات بالأسلحة النووية.[137]

هذا هو الواقع الدولي السائد حيث تفسر الدول القانون الدولي الذي يسمح باللجوء للحرب بما يتفق مع مصالحها ومصالح حلفائها؛ لذا ليس من المستبعد اللجوء لاستخدام القوة العسكرية للرد على هجمات سيبرانية خارج نطاق هذا القانون، لكن لا يزال الأمل قائما في إمكانية التوصل إلى إطار قانوني دولي يحكم الأعمال العدائية في الفضاء السيبراني أو من خلاله، ويساهم في كبح جماح مثل هذه التوجهات، التي إذا ما تحققت ستشكل خطراً حقيقياً على السلم والأمن الدوليين، ويبدو أن "دليل تالين بشأن القانون الدولي المطبق على الحرب السيبرانية" قد يكون مفيداً في هذا الإطار.

---

[135] Ibid. See International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World (May 2011), P.14. https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

[136] Scott J. Shackelford, From Nuclear War to Net War: Analogizing Cyber Attacks in International Law, Berkley Journal of International Law (BJIL), Vol. 25, No. 3, 2009, p. 215.

[137] Ibid.

المبحث الثالث

معايير دليل تالين لعام 2013 بشأن اعتبار الهجمات السيبرانية استخداما للقوة أو التهديد بها في القانون الدولي

أدت الهجمات السيبرانية ضد إستونيا العضو في حلف الناتو إلى إنشاء مركز التميز للدفاع الإلكتروني التعاوني التابع لحلف الناتو (CCDCOE) الموجود في تالين (عاصمة إستونيا) ووكالة إدارة الدفاع الإلكتروني (CDMA) واعترافًا بالحاجة إلى توضيح القانون الدولي المطبق على العمليات السيبرانية أنشأت CCDCOE مجموعة من الخبراء من الدول الأعضاء كُلفت بصياغة " دليل تالين بشأن القانون الدولي المطبق على الحرب السيبرانية" لعام 2013.[138] ويتكون هذا الدليل من 95 قاعدة قانونية إرشادية لممارسات أو سلوك الدول في سياق الحرب السيبرانية اعتمدتها بالإجماع مجموعة الخبراء الحكوميين، وترأسها البروفيسور مايكل شميث، والتي تهدف إلى عكس القانون الدولي العرفي مصحوبة بـ "تعليقات" تحدد أساسها القانوني وتسلط الضوء على أي اختلافات في الرأي بين الخبراء فيما يتعلق بتفسيرهم للقوة في السياق السيبراني، [139] وهو محاولة من قبل فقهاء القانون الدولي البارزين لتسهيل تنظيم العمليات السيبرانية بموجب القانون الدولي الحالي كجزء من تقليد طويل الأمد لعلماء وممارسين قانونيين يقومون بتكييف هذا القانون مع الظروف الجديدة بدلاً من تطوير نموذج قانوني جديد.

---

[138] Tallinn Manual, p.11.

تجدر الإشارة إلى أنه قد تم إصدار طبعة ثانية لدليل تالين في العام 2017 بعنوان " دليل تالين بشأن القانون الدولي المطبق على العمليات السيبرانية".

Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (Cambridge University Press,2017)

عرف دليل تالين 2.0 "العملية السيبرانية" على أنها "توظيف القدرات السيبرانية لتحقيق أهداف في الفضاء السيبراني أو من خلاله". ومصطلح "العملية السيبرانية" يبدو أضيق من مصطلح "النشاط السيبراني" الذي يعرفه الدليل بأنه "أي نشاط يتضمن استخدام البنية التحتية الإلكترونية أو يستخدم وسائل إلكترونية للتأثير على تشغيل هذه البنية التحتية". نقلاً عن

Dan Efrony and Yuval Shany, A Rule Book on The Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice, American Journal of International Law, vol. 112, 583, October 2018, n.1.

[139] Michael N. Schmitt, International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed, Harvard International Law Journal, Vol. 54, December 2012, p.15.

سنتناول في هذا المبحث المفاهيم والمعايير التي أوردها دليل تالين حول مدى اعتبار الهجمات السيبرانية استخداماً للقوة (المسلحة) أو التهديد بها في ضوء أحكام القانون الدولي للجوء للحرب.

أولا: حظر استخدام القوة أو التهديد بها:

تنص القاعدة 10 من دليل تالين الخاصة بتعريف: " حظر استخدام القوة أو التهديد بها" على أن "العملية السيبرانية التي تشكل تهديدًا أو استخدامًا للقوة ضد السلامة الإقليمية أو الاستقلال السياسي لأي دولة، أو التي تتعارض بأي طريقة أخرى مع أغراض الأمم المتحدة، تعتبر غير قانونية".[140] وتستند هذه القاعدة إلى كل من قانون المعاهدات والقانون الدولي العرفي كما أقرت بذلك محكمة العدل الدولية في قضية نيكاراغوا.[141]

ويوضح التعليق على هذه القاعدة أن- وبالإشارة إلى الأعمال التحضيرية لميثاق الأمم المتحدة- عبارة التهديد أو استخدام القوة "بأي طريقة أخرى تتعارض مع مقاصد الأمم المتحدة" تنص على افتراض عدم شرعية أي سلوك غير متسق مع ميثاق الأمم المتحدة وإن لم يكن موجهاً ضد السلامة الإقليمية أو الاستقلال السياسي لأي دولة.[142]

ومن القضايا المهمة التي يتناولها التعليق على هذه القاعدة أن الهجمات السيبرانية التي لا ترقى إلى حد استخدام القوة ليست بالضرورة مشروعة بموجب القانون الدولي، ومن خلال التأكيد على أن الحوادث السيبرانية التي لا ترقى إلى استخدام القوة قد لا تزال تشكل انتهاكًا لحظر التدخلالذي وإن لم ينص عليه ميثاق الأمم المتحدة صراحة إلا أنه يمكن استشفافه من مبدأ المساواة في السيادة بين الدول التي نصت عليه المادة 2(1) من الميثاق.[143] وتضمن هذه القاعدة بشكل فعال أنه حتى في حالة الشك لن يكون هناك مجال للإفلات من المسؤولية.

[140] Tallinn Manual, p.42-43.
[141] Nicaragua Case, paras. 188-190.
[142] Tallinn Manual, Rule 10, Para 2, P.43.
[143] Tallinn Manual, Rule 10, Para 6, P.44.

ثانيا: الهجمات السيبرانية باعتبارها استخداماً للقوة:

تنص القاعدة 11 " من الدليل على أنه "تشكل العملية السيبرانية استخدامًا للقوة عندما يكون حجمها وآثارها قابلة للمقارنة مع العمليات غير السيبرانية التي ترتقي إلى مستوى استخدام القوة".

وفي التعليق على هذه القاعدة رأى فريق الخبراء أن ميثاق الأمم المتحدة لا يقدم أي معايير يمكن من خلالها تحديد متى يكون الفعل بمثابة استخدام للقوة. وفي مناقشاته المتعلقة بالعتبة المناسبة لاستخدام القوة، واستند الفريق إلى حكم محكمة العدل الدولية في قضية نيكاراغوا المشار إليها مسبقا من أنه يجب مراعاة "الحجم والآثار" Scale and effects عند تحديد ما إذا كانت أعمال معينة ترقى إلى مستوى هجوم مسلح.[144] ووجد الفريق أن التركيز على حجم الهجوم وآثاره سيكون نهجاً مفيداً بنفس القدر عند التمييز بين تلك الأفعال التي تعد استخدامات للقوة وتلك التي لا تعتبر كذلك.[145]

و لأن ممارسات الدول غير واضحة فقد طور فريق الخبراء الدولي النهج القائم على الآثار الذي وضعه البروفيسور مايكل شميث، مع بعض التعديل، فقد أضاف هذا الفريق معيارين إضافيين لمعايير شميث هما معيار الطابع العسكري Military Characterالذي يركز على أن العلاقة بين العملية السيبرانية المعنية والعمليات العسكرية تزيد من احتمالية توصيفها على أنها استخدام للقوة، ومعيار مشاركة الدولة State Involvementالذي يركز على مدى مشاركة الدولة في عملية سيبرانية ضمن سلسلة متصلة من العمليات التي تقوم بها الدولة نفسها (على سبيل المثال، وأنشطة قواتها المسلحة أو وكالاتها الاستخباراتية) إلى تلك التي تكون مشاركتها فيها هامشية.[146] ليصبح هناك ثمانية معايير لتحديد ما إذا كانت العملية السيبرانية ترقى إلى استخدام القوة، وهي قائمة غير حصرية تشمل: الشدة، والفورية، والمباشرة، والانتهاك، والقابلية للقياس، والطابع العسكري، ومشاركة الدولة والشرعية الافتراضية.[147]

[144] Tallinn Manual, Rule 11, Para. 1, p.45.
[145] Ibid.
[146] Tallinn Manual, para.9, p. 48-52
[147] Ibid.

ويشير التعليق على هذه القاعدة إلى أنه من المرجح أن تنظر الدول في هذه العوامل وتوليها أهمية كبيرة، من بين أمور أخرى، عند تقرير ما إذا كان سيتم تصنيف أي عملية، بما في ذلك العملية السيبرانية، على أنها استخدام للقوة، وأكد الدليل أن هذه المعايير هي مجرد عوامل إرشادية للدول وليست معايير قانونية رسمية.[148]

وقد عدَّ خبراء دليل تالين في تعليقهم على العوامل السابقة أن الشدة severity هي أهم عامل في التحليل، وهو الذي يمكن من خلاله أن يتم وصف العملية السيبرانية بأنها استخدام للقوة، بقولهم "من المرجح جِدًّا أن يتم اعتبار العملية السيبرانية التي تؤدي إلى ضرر أو تدمير أو إصابة أو وفاة استخدامًا للقوة، ومن الواضح أن شدة الضرر هي أهم عامل في التحليل".[149]

ومن الأمور الأخرى التي وجدها الخبراء أنها ذات مغزى البيئة السياسية السائدة، وعلاقة العملية بالقوة العسكرية المحتملة، وهوية المهاجم، وسجل المهاجم فيما يتعلق بالعمليات السيبرانية، وطبيعة الهدف.[150]

ثالثا: الهجمات السيبرانية باعتبارها تهديدا باستخدام القوة:

بشأن تعريف التهديد باستخدام القوة في إطار الفضاء السيبراني تنص القاعدة 12 من دليل تالين على أنه: "تشكل العملية السيبرانية أو التهديد بالعملية السيبرانية تهديدًا غير قانوني باستخدام القوة عندما يكون التهديد، إذا تم تنفيذه، بمثابة استخدام غير قانوني للقوة".[151] وهذه القاعدة لها أساسها القانوني في المادة 2 (4) من ميثاق الأمم المتحدة على النحو الذي أوضحته محكمة العدل الدولية في فتواها بشأن الأسلحة النووية المشار إليه سابقاً.

إن النهج الذي تتبعه القاعدة 12 من دليل تالين فيما إذا كانت عملية سيبرانية معينة تشكل "تهديدًا" باستخدام القوة في انتهاك للمادة 2 (4) يعتمد على ما إذا كان " الاستخدام المعين للقوة سيكون موجهًا ضد سلامة الأراضي أو الاستقلال السياسي لأية دولة أو على أي وجه آخر لا يتفق ومقاصد الأمم المتحدة، أو ما إذا كان ، في حال كان القصد منها أن تكون وسيلة للدفاع، أن ينتهك بالضرورة مبادئ الضرورة

[148] Ibid, p. 48.
[149] Ibid, p. 50.
[150] Ibid, para. 10, p. 51-52.
[151] Ibid, p.52.

والتناسب".[152] وعند تطبيقه على العمليات السيبرانية فإن هذا يعني أن التهديد باستخدام القوة السيبرانية من شأنه أن ينتهك الحظر الوارد في المادة 2 (4) فقط إذا كانت القوة السيبرانية المهددة ترقى إلى استخدام غير مشروع للقوة في الظروف نفسها.[153]

وترى القاعدة 12 من الدليل- كما هو موضح في تعليقها- أن الاستحواذ العدواني من قبل دولة على القدرات السيبرانية ليس في حد ذاته تهديد- غير قانوني باستخدام القوة.[154] لكن تبقى العديد من الأمور المجهولة في سياق "التهديد"، وكان فريق الخبراء الحكومي الدولي "منقسماً بشأن ما إذا كانت الدولة التي تفتقر بوضوح إلى أي قدرة على متابعة أو تنفيذ تهديدها يمكن أن تنتهك" المادة 2 (4).[155] وبالمثل لا يمكن التوصل إلى توافق في الآراء بشأن دولة لديها القدرة على تنفيذ التهديد، ولكن من الواضح أنه ليس لديها النية للقيام بذلك". وبالمثل جادل أحد الباحثين بأن "إظهار القوة السيبرانية " يمكن أن يشكل "تهديدًا باستخدام القوة" بالمعنى المقصود في المادة 2 (4).[156]

رابعاً: الهجمات السيبرانية باعتبارها هجمات مسلحة:

فيما يتعلق ما إذا كان يمكن اعتبار الهجمات السيبرانية بأنها هجمات مسلحة أجابت القاعدة 13 من الدليل على ذلك، فقد جاء فيها أنه: " قد تمارس الدولة التي تكون هدفًا لعملية سيبرانية ترتقي إلى مستوى هجوم مسلح حقها الأصيل في الدفاع عن النفس يعتمد ما إذا كانت العملية السيبرانية تشكل هجوماً مسلحاً على حجمها وآثارها."[157]

ويتبين من ذلك أن العامل الحاسم فيما إذا كانت هجمات سيبرانية محددة ستشكل هجومًا مسلحًا بالمعنى المقصود في المادة 51 من ميثاق الأمم المتحدة هو "حجمها وآثارها".

[152] Peter Z. Stockburger, op.cit, p. 584, citing the advisory opinion of the Legality of Threat or Use of nuclear weapons, Advisory Opinion, 1996 I.C.J. 226, para. 48 (July 8).
[153] Ibid, p. 584- 585.
[154] Tallinn Manual, Rule 12, Paras 4-6. P. 53.
[155] Peter Z. Stockburger, op.cit, p. 584
[156] Ibid.
[157] Tallinn Manual, p.53.

ويلاحظ التعليق على القاعدة 13 أن فريق الخبراء الدولي انقسم حول ما إذا كان مفهوم الهجوم المسلح ينطوي بالضرورة على استخدام "أسلحة"، لكن الدليل لم يحسم هذه المسالة، وبدلاً من ذلك كان العامل الحاسم هو ما إذا كانت تأثيرات العملية السيبرانيةالتي تختلف عن الوسائل المستخدمة لتحقيق تلك التأثيرات مماثلة لتلك التي قد تنجم عن إجراء مؤهل لكونه هجومًا حَرَكِيًّا عَسْكَرِيًّا.[158] ورأى الفريق أن مصطلح "هجوم مسلح" لا يجب أن يُقارن بمصطلح "استخدام القوة" الوارد في القاعدة 11. الهجوم المسلح يفترض مسبقًا على الأقل استخدام القوة بمعنى المادة 2 (4)، ومع ذلك- وكما لاحظت محكمة العدل الدولية- لا يرتفع كل استخدام للقوة إلى مستوى الهجوم المسلح، إن الحجم والآثار المطلوبة لعمل ما لكي يصنف هجومًا مسلحًا تتجاوز بالضرورة تلك التي تصف هذا العمل بأنه استخدام للقوة فقط في حالة وصول استخدام القوة إلى عتبة هجوم مسلح يحق للدولة الرد باستخدام القوة دفاعًا عن النفس، [159] ويوضح هذا التعليق أن عبارة "الحجم والآثار" مستمدة من الحكم في قضية نيكاراغوا.

وقد اتفق فريق الخبراء على أن أي استخدام للقوة يؤدي إلى إصابة أو قتل الأشخاص أو الإضرار بالممتلكات أو تدميره يفي بمتطلبات الحجم والآثار، كما اتفقوا على أن أعمال التجسس السيبراني والقرصنة السيبرانية، وكذلك العمليات السيبرانية التي تنطوي على انقطاع قصير أو دوري للخدمات الإلكترونية غير الأساسية لا تعد هجمات مسلحة.[160]

وهكذا تؤكد القاعدة 13 أن الحق في استخدام القوة للدفاع عن النفس ينطبق على الهجمات السيبرانية المسلحة التي يكون حجمها وآثارها السلبية مماثلة للهجمات المسلحة الحركية التقليدية، وهو المبدأ الذي أقرته محكمة العدل الدولية في قضية نيكاراغوا.[161]

لكن يثير عنصر الآثار الذي استند إليه دليل تالين لاعتبار الهجمات السيبرانية بأنها هجوم مسلح بعض القضايا الإشكالية، فعلى عكس الهجمات المسلحة الحركية قد لا تؤدي الهجمات السيبرانية إلى حدوث آثار مادية (ضرر أو تدمير أو إصابة أو وفاة)، السؤال القانوني المهم هو ما إذا كانت الهجمات السيبرانية التي لا تؤدي إلى

[158] Ibid, Rule 13, Para, 4, p.55.
[159] Tallinn Manual, Para, 5, p.55.
[160] Ibid, Para, 6, p. 55.
[161] Nicaragua, Paras 191, 193-95, 211, 237. See Matthew C. Waxmant, op.cit, p.437.

أضرار مادية، ولكنها تسبب آثارًا ضارة واسعة النطاق ستشكل هجومًا مسلحًا لأغراض الدفاع عن النفس.

ومن المؤسف أن هذه المسألة ذات الأهمية العملية قد تركت دون إجابة من قبل فريق خبراء دليل تالين، ورأى بعض الخبراء أن الضرر الذي يلحق بالأشخاص أو الأضرار المادية للممتلكات أمر حاسم، بينما أكد آخرون أن حجم الآثار المترتبة عن الهجوم وليس الطبيعة الضارة أو المدمرة لهذه الآثار هو المهم.[162] ومن المؤسف أن دليل تالين لا يعلق كثيراً على صحة هذه المواقف المتباينة، وهكذا تركت القضية دون حل.

وفي هذا الصدد يرى الباحثان أن الطبيعة الضارة أو المدمرة لآثار الهجمات السيبرانية يمكن أن تتجسد بشكل أفضل إذا ما استهدفت هذه الهجمات البنية التحتية الحيوية للمجتمع، وليست أهدافا أقل أهمية، فعلى سبيل المثال إذا ما استهدفت هجمات سيبرانية المنشآت النووية التي تعمل على إنتاج القدرة الكهربائية، وكذلك المعامل البيولوجية التي تنتج العقاقير والأمصال الضرورية للحياة البشرية، وأيضاً المعامل الكيميائية، فإن استهداف مثل هذه المنشآت قد يسبب كوارث تعم العالم أجمع نتيجة التسربات الإشعاعية أو الفيروسات البيولوجية.

ومن جانب آخر يمكن توضيح التأثير السلبي لفشل دليل تالين في تقديم إجابة نهائية بشأن متى يمكن عد الهجمات السيبرانية بأنها هجمات مسلحة، من خلال الإشارة إلى الهجمات السيبرانية التي حدثت فعلاً. فقد وصف المجتمع الدولي الهجوم السيبراني على إستونيا بأنه جريمة سيبرانية أو إرهاب سيبراني، وليس هجوماً سيبرانياً، وذلك لآثاره المحدودة التي اقتصرت على حدوث اضطراب اقتصادي وانهيار نظام الاتصالات دون أي أضرار مادية أو خسائر بشرية.[163] كما أن حلف شمال الأطلسي التي تعد إستونيا عضواً فيه لم يرد على هذا الهجوم بهجوم مضاد سواء سيبراني أم مسلح، فقط قام الحلف بإنشاء مركز التميز للدفاع الإلكتروني التعاوني (CCDCOE)، وكذلك إستونيا التي لم تقم بأي رد ، ولكن أنشأت وحدة

[162] Tallinn Manual, para 9, p. 56.
[163] See Sean Watts, Low-Intensity Computer Network Attack and Self-Defense, International Law Studies, Vol. 87, 2010, p. 69- 70.

من المتطوعين من خبراء الإنترنت، على غرار الحرس الوطني الأمريكي، لمكافحة الهجمات السيبرانية.[164]

والشيء نفسه فقد كان الضرر الفعلي الذي أحدثته الهجمات السيبرانية ضد جورجيا عام 2008 ضئيلاً، فقداقتصرت آثار هذه الهجمات فقط على تعطيل البريد الإلكتروني وعدم توفر بعض المواقع المستهدفة للجمهور.[165] إضافة إلى ذلك لم يكن هناك دليل قاطع على أن الحكومة الروسية هي التي نفذت أو أجازت أيا من هذه الهجمات، مع عدم وجود دليل على أنها حاولت إيقافها أيضًا [166] على غرار مثال إستونيا، نظر المجتمع الدولي إلى الهجوم على جورجيا على أنه جريمة سيبرانية أو إرهاب سيبراني.[167] وهو ما دعمه دليل تالين الذي خلص إلى أنه: "من الصعب للغاية تطبيق قانون النزاعات المسلحة على الهجمات السيبرانية الجورجية - الحقائق الموضوعية غامضة للغاية بحيث لا تفي بالمعايير الضرورية لمشاركة الدولة وجسامة الآثار".[168]

وبينما لا يزال المجتمع الدولي غير مستقر بشأن فيما إذا كانت القدرات السيبرانية تعد أسلحة بشكل قانوني، وما إذا كانت الهجمات السيبرانية يمكن عدها أدوات مشروعة للنزاعات المسلحة، فإن الهجمات ضد إستونيا وجورجيا توضح أن هذا الشكل الجديد من الحرب يبدو فعالاً للغاية، ويعزز الحاجة إلى تطوير فهم أفضل لكيفية ارتباط القانون الدولي بالحرب السيبرانية.[169] ودون هذا الفهم، فإن هذا الشكل الناشئ من الحرب سيتسبب في تصعيد التوترات وتكثيف العمليات العسكرية خارج نطاق الفضاء السيبراني.[170]

وفي النهاية يجب فهم دليل تالين على أنه تعبير عن آراء مجموعة من الخبراء الدوليين فيما يتعلق بحالة القانون، ومع أن الدليل لا يقدم أفضل الممارسات ولا يمثل تطوراً تدريجياً للقانون الدولي إلا أنه قصد منه أن يكون إعادة صياغة موضوعية

[164] Mary Ellen O'Connell, op.cit, p. 193.
[165] Stephen W. Koms and Joshua E. Kastenberg, Georgia's Cyber Left Hook," Parameters (U.S. Army War College Quarterly) Vol. 38, no. 4, 2008, p.171.
[166] Arie J. Schaap, op.cit, p. 145-146.
[167] Ibid, p. 146.
[168] Stephen W. Koms and Joshua E. Kastenberg, op.cit, p.171.
[169] Arie J. Schaap, op.cit, p. 124.
[170] Ibid.

للقانون الدولي القائم المطبق فعلياً Lex lata ، وليس القانون الذي يجب أن يكون Lex ferenda، كما وصف ذلك الدليل نفسه.[171]

الخاتمة

ركزت هذه الدراسة على " مدى اعتبار الهجمات السيبرانية انتهاكاً للحظر المفروض على استخدام القوة أو التهديد بها في ضوء أحكام القانون الدولي للجوء للحرب" من خلال التطرق إلى جانب مفاهيمي حاول تعريف هذه الهجمات ، والتمييز بينها وبين المفاهيم المشابهة للعمليات التي تجري في الفضاء السيبراني، وكذلك محاولة الوقوف على التكييف القانوني لهذه الهجمات في ضوء أحكام القانون الدولي للجوء إلى الحرب ولاسيما المادة 2(4) من ميثاق منظمة الأمم المتحدة، ومتى يمكن عدها بمثابة هجمات مسلحة تَجُزُّ للدولة الضحية الحق في الدفاع عن نفسها.

فيما يلي أهم النتائج والتوصيات التي خلصت إليها الدراسة:

أولا: النتائج

1. ومع المحاولات العديدة التي قام بها الباحثون والهيئات الحكومية لتعريف المقصود بالهجوم السيبراني إلا أنه لا يوجد تعريف ثابت ومتفق عليه بسبب تنوع أشكال هذه الهجمات وصعوبة تمييزها عن العمليات الأخرى التي تحدث في الفضاء السيبراني، وفي هذا السياق اقترح الباحثان أن الهجمات السيبرانية تعني: " أي عمل عدائي يقع في زمن السلم تقوم به الدول أو جهات تابعة لها ضد دول أخرى، ويتم باستخدام أدوات القوة التي يوفرها الفضاء السيبراني بهدف تدمير أو تعطيل أو التشويش على شبكات الكمبيوتر التي تتحكم أساساً بالبنية التحتية الحيوية، المدنية أو العسكرية لتلك الدول لأغراض سياسية أو أمنية أو اقتصادية أو وغيرها".
2. مع وجود مبادئ واضحة وكافية في القانون الدولي اللجوء إلى الحرب التي قد تنطبق على الهجمات السيبرانية التي تحدث وقت السلم، لكن هناك عدد لا يحصى من التحفظات والصعوبات من طرف الدول حول كيفية تطبيقها، إذ لا يزال الخلاف والانقسام قائماً بين الدول، وكذلك فقهاء القانون الدولي، حول ما إذا كانت هذه الهجمات تخضع للحظر الوارد في المادة 2(4) من ميثاق منظمة الأمم المتحدة، وذلك نتيجة للاتجاهات الفكرية والسياسية والأهداف الاستراتيجية المختلفة مع أن التفسير الديناميكي للمادة 2(4) الذي نؤيده كافٍ لاعتبار الهجمات السيبرانية بأنها استخدام محظور للقوة في العلاقات الدولية لكن ردود أفعال الدول على الهجمات السيبرانية

[171] Tallinn Manual, p.5.

التي حدثت فعلاً- كما هو الحال في إستونيا وجورجيا وإيران، وأيضا النقاشات التي تجري في إطار منظمة الأمم المتحدة- لا تدعم هذا الرأي.

3. اتفق فريق خبراء دليل تالين على أن أي هجوم سيبراني- استناداً إلى حجمه وآثاره- يؤدي إلى إصابة أو قتل الأشخاص أو الإضرار بالممتلكات أو تدميرها يعد هجوماً مسلحاً، وأن أعمال التجسس السيبراني والقرصنة السيبرانية، وكذلك العمليات السيبرانية التي تنطوي على انقطاع قصير أو دوري للخدمات الإلكترونية غير الأساسية لا تعد كذلك. كما اتفقوا على أن الهجمات السيبرانية التي لا ترقى إلى حد استخدام القوة تعد غير مشروعة كونها تشكل انتهاكًا لمبدأ حظر التدخل.
4. قد يساهم دليل تالين، مع أنه لا يرقى إلى مرتبة القواعد القانونية الملزمة ويعبر عن وجهة نظر حلف شمال الأطلسي- في بدء تشكل عرف دولي متواتر ومستقر يحكم الهجمات السيبرانية، وهو ما يحتاج إلى القبول بهذا العرف من قبل الدول ذات العلاقة في المجتمع الدولي، كما أنه قد يكون أساساً مقبولاً لإبرام اتفاقية دولية في هذا المجال مع صعوبة المهمة؛ لأن هذه الاتفاقية يمكن أن تؤثر في هيكل الفضاء السيبراني نفسه، ومع ذلك- وإلى حين أن يحظى هذا الدليل بقبول أوسع- فمن المرجح أن تواصل الدول تصنيف الهجمات السيبرانية اعتمادًا على تفسيرها الخاص لمصطلح القوة كما ورد في المادة 2(4) من الميثاق إضافة إلى الضرورات التي تفرضها مصالحها الوطنية الحيوية ومصالح حلفائها.
5. تعامل العديد من الدول الهجمات السيبرانية على انها مسألة تخضع للقانون الجنائي الوطني، وتكيفها على هذا الأساس كونها جرائم سيبرانية أو تجسساً سيبرانياً، وذلك بدافع عدم اليقين بشأن ما إذا كانت هذه الهجمات تعد هجمات مسلحة ، وكذلك لصعوبة نسبها إلى الدول أو للجهات الفاعلة التابعة لها.
6. وترى العديد من الدول، ولاسيما التي لديها قدرات سيبرانية فائقة أن الرد الأنسب على الهجمات السيبرانية هو بشن هجمات سيبرانية مضادة أخرى؛ لذلك تنشأ العديد من الدول- في إطار قواتها المسلحة التقليدية- قوات أو فرق سيبرانية متخصصة سواء لشن هجمات سيبرانية أم للرد عليها.

التوصيات:

1. إن الاستنتاج القائل إن القواعد الحالية بشأن استخدام القوة كافية لكي يتم تطبيقها على الهجمات السيبرانية يعتمد في نهاية المطاف على فعالية نظام الأمن الجماعي الذي رسخه ميثاق الأمم المتحدة، فضلاً عن استعداد أعضاء مجلس الأمن وغيرهم للاستجابة للأشكال الجديدة لاستخدام القوة؛ لذا يجب أن يكون هناك إجماع واسع على

قواعد القانون الدولي الحالية بشأن استخدام القوة، فضلاً عن دعم أكبر للمؤسسات الدولية، ولا سيما مجلس الأمن التابع للأمم المتحدة، ولا يتطلب الأمر وضع قواعد جديدة أو إصلاح مجلس الأمن ، ولكنه يتطلب التوافق على تفسير أحكام الميثاق وكيفية تطبيقها، وقد يكون لدليل تالين مساهمة مهمة في هذا السياق.

2. في ظل عدم قدرة المجتمع الدولي على الاتفاق حول عد الهجمات السيبرانية بأنها استخدام للقوة (المسلحة) أو التهديد بها استناداً إلى أحكام المادة 2 (4) من ميثاق منظمة الأمم المتحدة، وعلى اعتبارها بمثابة عدوان مسلح طبقاً لتعريف العدوان الوارد في المادة الأولى من قرار الجمعية العامة رقم 3314 (د- 29) سنة 1974، مما يحرم الدول من حقها في الدفاع عن النفس بموجب المادة 51 من الميثاق، فما على الدول التي تتعرض لمثل هذه الهجمات سوى تقوية وتعزيز دفاعاتها السيبرانية إما بشكل فردي وغما جماعي من خلال التعاون فيما بينها عن طريق تبادل المعرفة والخبراء وغيرها.
3. محاولة بذل الجهد على المستوى الدولي للتوصل إلى إطار قانوني يحكم الفضاء السيبراني يساهم، مع صعوبة المهمة في اعتبار الهجمات السيبرانية عدواناً على الدول ويفرض عقوبات على الدولة المعتدية أما على شكل عقوبات اقتصادية أو سياسية أو حتى السماح باستخدام القوة المسلحة استناداً إلى الفصل السابع من ميثاق الأمم المتحدة، وفي هذا السياق يعد الدور الذي يمكن أن يلعبه مجلس الأمن التابع للأمم المتحدة، ولاسيما الدول الدائمة العضوية فيه جوهريا في هذا الصدد.
4. خيار آخر للتصدي للهجمات السيبرانية هو إمكانية معاقبة المسؤولين عن القيام بها أمام القضاء الجنائي الدولي ممثلاً بالمحكمة الجنائية الدولية، وفي هذا الإطار هناك حاجة إلى قيام المحكمة بتوسيع تعريفها لجرائم الحرب بموجب المادة 8 لتشمل الأسلحة الجديدة للفضاء السيبراني وفقًا للمادة 8 (2) (أ) (4) من نظام روما الأساسي، ويشكل "إلحاق تدمير واسع النطاق بالممتلكات والاستيلاء عليها دون أن تكون هناك ضرورة عسكرية تبرر ذلك وبالمخالفة للقانون وبطريقة عابثة"، جريمة حرب، وهو ما أحدثته الهجمات السيبرانية ضد إستونيا وجورجيا وغيرها.

وهذه كلها قضايا تطرح كثيراً من الإشكاليات التي يمكن للباحثين التصدي لها.

قائمة المراجع

المراجع باللغة العربية:

الكتب:

1. إيهاب خليفة، مجتمع ما بعد المعلومات: تأثير الثورة الصناعية على الأمن القومي. مصر: العربي للنشر والتوزيع، سنة 2017.
2. راشد محمد المري، الجرائم السيبرانية في ظل الفكر الجنائي المعاصر دراسة مقارنة، دار النهضة العربية، سنة 2018.
3. ريتشارد إيه كلارك، روبرت كيه كنيك، حرب الفضاء الإلكتروني الخطر القادم على الأمن القومي وسبل المواجهة، الطبعة الأولى، أبو ظبي: مركز الإمارات للدراسات والبحوث الاستراتيجية، سنة 2012.
4. عادل عبد الصادق، أسلحة الفضاء الإلكتروني في ضوء القانون الدولي، سلسلة أوراق، العدد 23، مكتبة الإسكندرية، مصر، 2016.

الدوريات:

1. أحمد عبيس نعمة الفتلاوي وزهراء عماد محمد كلنتر، تكييف الهجمات السيبرانية في ضوء القانون الدولي، مجلة الكوفة للعلوم القانونية والسياسية، المجلد 13، العدد 44، ج. 1 ،31 يناير 2020.
2. أحمد عبيس نعمة الفتلاوي، الهجمات السيبرانية: مفهومها المسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر، مجلة المحقق الحلي للعلوم القانونية والسياسية، المجلد 8، العدد 4، 31 ديسمبر 2016.
3. إسماعيل زروقة، الفضاء السيبراني والتحول في مفاهيم القوة والصراع، مجلة العلوم القانونية والسياسية، المجلد 10، العدد 1، ابريل 2019.
4. أميرة عبد العظيم محمد عبد الجواد، المخاطر السيبرانية وسبل مواجهتها في القانون الدولي العام. مجلة الشريعة والقانون، جامعة الأزهر، الجزء 3، العدد 45، سنة 2020.
5. رزق أحمد سمودي، حق الدفاع عن النفس نتيجة الهجمات الإلكترونية في ضوء قواعد القانون الدولي العام، مجلة جامعة الشارقة للعلوم القانونية، المجلد 15، العدد 2 ديسمبر 2018.

6. رغدة البهي، الردع السيبراني: المفهوم والإشكاليات والمتطلبات، مجلة العلوم السياسية والقانون، المركز الديمقراطي العربي للدراسات الاستراتيجية والسياسية والاقتصادية (برلين- المانيا) العدد الأول يناير 2017.
7. طالب حسن موسى وعمر محمود أعمر، الإنترنت قانونا، مجلة الشريعة والقانون، جامعة الإمارات العربية المتحدة، العدد 67، يوليو 2016.
8. عادل عبد الصادق، الفضاء الإلكتروني والرأي العام: تغير المجتمع والأدوات والتأثير، المركز العربي لأبحاث الفضاء الإلكتروني: قضايا استراتيجية، العدد 2459، سنة 2013.
9. علاء الدين فرحات، الفضاء السيبراني: تشكيل ساحة المعركة في القرن الحادي والعشرين. مجلة العلوم القانونية والسياسية، المجلد 10، العدد 3، ديسمبر 2019.
10. عمر محمود أعمر، الحرب الإلكترونية في القانون الدولي الإنساني، دراسات، علوم الشريعة والقانون، المجلّد 46، عدد 3، 2019.
11. القانون الدولي الإنساني والعمليات السيبرانية خلال النزاعات المسلحة، ورقة موقف اللجنة الدولية للصليب الأحمر مقدمة إلى فريق العمل المفتوح العضوية المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي، وإلى فريق الخبراء الحكوميين المعني بالارتقاء بسلوك الدول المسؤول في ميدان الفضاء السيبراني في سياق الأمن الدولي، تشرين الثاني/ نوفمبر 2019. متوفرة في الموقع الإلكتروني للجنة الدولية للصليب الأحمر. https://www.icrc.org
12. ناصر العلي، الجهود الدولية في مكافحة الإرهاب الإلكتروني، مجلة الباحث للدراسات الأكاديمية، المجلد 8، العدد 1، سنة 2021.
13.

المراجع العربية:

al-Marājiʻ bi-al-lughah al-ʻArabīyah:

al-Kutub:

1. Īhāb Khalīfah, mujtamaʻ mā baʻda al-maʻlūmāt: Taʼthīr al-thawrah al-Ṣināʻīyah ʻalá al-amn al-Qawmī. Miṣr: al-ʻArabī lil-Nashr wa-al-Tawzīʻ, sanat 2017.

2. Rāshid Muḥammad al-Murrī, al-jarā'im alsybrānyh fī ẓill al-Fikr al-jinā'ī al-mu'āṣir dirāsah muqāranah, Dār al-Nahḍah al-'Arabīyah, sanat 2018.
3. Rītshārd īha KLughahRobert kyh knyk, Ḥarb al-faḍā' al-iliktrūnī al-khaṭar al-qādim 'alá al-amn al-Qawmī wa-subul al-muwājahah, al-Ṭab'ah al-ūlá, Abū Ẓaby: Markaz al-Imārāt lil-Dirāsāt wa-al-Buḥūth al-Istirātījīyah, sanat 2012.
4. Ādil 'Abd al-Ṣādiq, asliḥat al-faḍā' al-iliktrūnī fī ḍaw' al-qānūn al-dawlī, Silsilat Awrāq, al-'adad 23, Maktabat al-Iskandarīyah, Miṣr, 2016.

al-Dawrīyāt:

1. Aḥmad 'bys Ni'mah al-Fatlāwī wzhrā' 'Imād Muḥammad klntr, takyīf alhjmāt alsybrānyh fī ḍaw' al-qānūn al-dawlī, Majallat al-Kūfah lil-'Ulūm al-qānūnīyah wa-al-siyāsīyah, al-mujallad 13, al-'adad 44, J. 1, 31 Yanāyir 2020.
2. Aḥmad 'bys Ni'mah al-Fatlāwī, alhjmāt alsybrānyh: mafhūmuhā al-Mas'ūlīyah al-Dawlīyah al-nāshi'ah 'anhā fī ḍaw' al-tanẓīm al-dawlī al-mu'āṣir, Majallat al-muḥaqqiq al-Ḥillī lil-'Ulūm al-qānūnīyah wa-al-siyāsīyah, al-mujallad 8, al-'adad 4, 31 Dīsimbir 2016.
3. Ismā'īl Razzūqah, al-faḍā' alsybrāny wa-al-taḥawwul fī Mafāhīm al-qūwah wa-al-ṣirā', Majallat al-'Ulūm al-qānūnīyah wa-al-siyāsīyah, al-mujallad 10, al-'adad 1, Abrīl 2019.
4. Amīrah 'Abd al-'Aẓīm Muḥammad 'Abd al-Jawwād, al-makhāṭir alsybrānyh wa-subul muwājahatihā fī al-qānūn al-dawlī al-'āmm. Majallat al-sharī'ah wa-al-qānūn, Jāmi'at al-Azhar, al-juz' 3, al-'adad 45, sanat 2020.
5. Rizq Aḥmad smwdy, Ḥaqq al-Difā' 'an al-nafs Natījat alhjmāt al-iliktrūnīyah fī ḍaw' Qawā'id al-qānūn al-dawlī al-

‘āmm, Majallat Jāmi‘at al-Shāriqah lil-‘Ulūm al-qānūnīyah, al-mujallad 15, al-‘adad 2 Dīsimbir 2018.
6. Raghdah al-Bahī, al-rad‘ alsybrāny : al-mafhūm wālāshkālyāt wa-al-mutaṭallabāt, Majallat al-‘Ulūm al-siyāsīyah wa-al-qānūn, al-Markaz al-dīmuqrāṭī al-‘Arabī lil-Dirāsāt al-Istirātījīyah wa-al-siyāsīyah wa-al-iqtiṣādīyah (brlyn-Almāniyā) al-‘adad al-Awwal Yanāyir 2017.
7. Ṭālib Ḥasan Mūsá wa-‘Umar Maḥmūd A‘mar, al-intirnit qānūnan, Majallat al-sharī‘ah wa-al-qānūn, Jāmi‘at al-Imārāt al-‘Arabīyah al-Muttaḥidah, al-‘adad 67, Yūliyū 2016.
8. Ādil ‘Abd al-Ṣādiq, al-faḍā’ al-iliktrūnī wa-al-ra’y al-‘āmm : Taghayyur al-mujtama‘ wa-al-adawāt wa-al-ta’thīr, al-Markaz al-‘Arabī li-Abḥāth al-faḍā’ al-iliktrūnī : Qaḍāyā istirātījīyah, al-‘adad 2459, sanat 2013.
9. Alā’ al-Dīn Faraḥāt, al-faḍā’ alsybrāny : tashkīl sāḥat al-ma‘rakah fī al-qarn al-ḥādī wa-al-‘ishrīn. Majallat al-‘Ulūm al-qānūnīyah wa-al-siyāsīyah, al-mujallad 10, al-‘adad 3, Dīsimbir 2019.
10. ‘UmarAl-Dīnd A‘mar, al-ḥarb al-iliktrūnīyah fī al-qānūn al-dawlī al-insānī, Dirāsāt, ‘ulūm al-sharī‘ah wa-al-qānūn, almjlld 46, ‘adad 3, 2019.
11. al-qānūn al-dawlī al-insānī wa-al-‘amalīyāt alsybrānyh khilāl al-nizā‘āt al-musallaḥah, Waraqah Mawqif al-Lajnah al-Dawlīyah lil-Ṣalīb al-Aḥmar muqaddimah ilá farīq al-‘amal al-maftūḥ al-‘uḍwīyah al-Ma‘nī bāltṭwrāt fī Maydān al-ma‘lūmāt wa-al-ittiṣālāt al-silkīyah wa-al-lāsilkīyah fī siyāq al-amn al-dawlī, wa-llá farīq al-khubarā’ al-ḥukūmīyīn al-Ma‘nī bālārtqā’ bslwk al-Duwal al-mas’ūl fī Maydān al-faḍā’ alsybrāny fī siyāq al-amn al-dawlī, Tishrīn al-Thānī /

Nūfimbir 2019. mtwfrh fī al-mawqi‘ al-iliktrūnī lil-Lajnah al-Dawlīyah lil-Ṣalīb al-Aḥmar. https : / / www. icrc. Org

12. Nāṣir al-‘Alī, al-Juhūd al-Dawlīyah fī Mukāfaḥat al-irhāb al-iliktrūnī, Majallat al-bāḥith lil-Dirāsāt al-Akādīmīyah, al-mujallad 8, al-‘adad 1, sanat 2021.

المراجع باللغة الإنجليزية

Books

1. Albrecht Randelzhofer and Oliver Dörr, 'Article 2(4)', In B Simma et al (eds), The Charter of the United Nations: A Commentary (2nd ed, Oxford University Press, Oxford, 2002).
2. Heather Harrison Dinniss, Cyber Warfare and The Laws of War. Cambridge; New-York: Cambridge University Press, 2014.
3. Ian Brownlie, International Law and the use of force by States (Clarendon, 1963).
4. J. A. Green, The International Court of Justice and Self-Defence in International Law (Oxford: Hart Publishing, 2009).
5. Julius Stone, Aggression and World Order: A critique of the United Nations theories of aggression (California; University of California Press, 1958).
6. Klaus-Peter Saalbach, Cyber War, Methods and Practice, Version 9, University of Osnabruck-17 Jun 2014. https://archive.law.upenn.edu/live/files/3477-saalbach-k-methods-and-practice-2014
7. Nikolas Stürchler, The Threat of Force in International Law (Cambridge: Cambridge University Press, 1st ed, 2007).

8. Tallinn manual on the international law applicable to cyber warfare: prepared by the international group of experts at the invitation of the NATO Cooperative Cyber Defense Centre of Excellence / General Editor, Michael N. Schmitt. (Cambridge: Cambridge University Press, 2013).
9. Thilo Rensmann, Reform, in Bruno Simma et al (eds), The Charter of The United Nations: A Commentary (Oxford University Press, 3rd ed, Vol I, 25, 2012).
10. Thomas Bruha, The General Assembly's definition of the act of aggression, In Claus Kreß and Stefan Barriga (Eds), *Commentary on the crime of aggression* (Cambridge University Press, 2015).
11. Thomas C. Wingfield, The Law of Information Conflict: National Security Law in Cyberspace, (Falls Church, VA: Aegis Research, 2000).
12. U.S Department of Defense, "Summary: Department of Defense Cyber Strategy 2018," released September 19, 2018. https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF
13. U.S. Department of Defense, Dictionary of Military and Associated Terms. (Washington: U.S. Department of Defense, November 8, 2010) (As Amended Through February 15, 2012).
14. William A. Owens, Kenneth W. Dam & Herbert S. Lin eds., National Research Council's Committee on offensive Information Warfare, Technology, Policy Law and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities (Washington, DC; National Research Council,

2009). Available at: https://www.steptoe.com/a/web/2306/3785.pdf

15. Yoram Dinstein, Computer Network Attacks and Self-Defense, Michael N. Schmitt & Brian T. O'Donnell (eds), Computer Network Attack and International Law (Naval War College, Newport, Ri, 1999) 99-119.
16. Yves Sandoz, Christophe Swinarski, Bruno Zimmermann eds, Commentary on the Additional Protocols of 8 June 1977 to The Geneva Conventions of 12 August 1949 (Geneva: International Committee of the Red Cross: Martinus Nijhoff Publishers, 1987). https://tile.loc.gov/storage-services/service/ll/llmlp/Commentary_GC_Protocols/Commentary_GC_Protocols.pdf

Law Reviews

1. Andrea Bianchi, The International Regulation of the Use of Force: The Politics of Interpretive Method, Leiden Journal of International Law, Vol. 11, 2009, 651-676.
2. Arie J. Schaap, Cyber warfare operations: development and use under international law, Air Force Law Review, vol. 64, winter 2009.
3. Cameron Ryan Scullen, Cyberspace: The 21st Century Battlefield, 6 University of Miami National Security & Armed Conflict Law Review, Vol. 6 (1), 2015.
4. Chris af Jochnick & Roger Normand, The Legitimation of Violence: A Critical History of the Laws of War, Harvard International Law Journal, Vol. 35, No.1, 1994, 49.

5. Daniel B. Silver, Computer Network Attack as A Use of Force Under Article 2(4), International Law Studies, Vol. 76, 73, 2002.
6. Daniel Garrie and Shane Reeves, An Unsatisfactory State of the Law: The Limited Options for a Corporation Dealing with Cyber Hostilities by State Actors, Cardozo Law Review, Vol. 37, No. 5, 2016, Cardozo Legal Studies Research Paper No. 495. Available at SSRN: https://ssrn.com/abstract=2799970
7. David Weissbrodt, Cyber-Conflict, Cyber-Crime, and Cyber-Espionage, Minnesota Journal of International Law, Vol. 22, 2013. 347.
8. Delbert Tran, The Law of Attribution: Rules for Attributing the Source of a Cyber-Attack, The Yale Journal of Law & Technology, Vol.20, 376, 2018.
9. Duncan B. Hollis: Why States Need an International Law for Information Operations, Lewis & Clark Law Review, Vol. 11, 2007. Available at: https://law.lclark.edu/live/files/9551-lcb114art7hollis.pdf
10. Eimear Bourke, A War Without Bullets: Protecting Civilians in the Technology Trenches, Albany Law Journal of Science and Technology, Vol. 8, No. II, 2018.
11. Frédérick Douzet & Aude Gery, Cyberspace is used, first and foremost, to wage wars: proliferation, security and stability in cyberspace, Journal of Cyber Policy, Vol. 6, No.1, Pp96-113, 2021. Available at: https://www.tandfonline.com/doi/pdf/10.1080/23738871.2021.1937253?needAccess=true

12. George Winthrop Haight, United Nations: Principles of International Law Concerning Friendly Relations and Co-Operation Among States, The International Lawyer, Vol. 1, No. 1, 1966.
13. Herbert Lin, Cyber Conflict and International Humanitarian Law, International Review of the Red Cross, Vol. 94, No. 886, 2012. Available at: https://international-review.icrc.org/sites/default/files/irrc-886-lin.pdf
14. Jamie Collier, Strategies of Cyber Crisis Management: Lessons from the Approaches of Estonia and The United Kingdom, In: Taddeo M., Glorioso L. (Eds) Ethics and Policies for Cyber Operations. Philosophical Studies Series 124, 2017. Available at: https://www.politics.ox.ac.uk/sites/default/files/2022-03/strategies-of-cyber-crisis-management.pdf
15. Marco Roscini, Worldwide Warfare – Jus Ad Bellum and the Use of Cyber Force, Max Planck Yearbook of United Nations Law, Vol. 14, 2010. Available at: https://www.mpil.de/files/pdf3/03_roscini_14.pdf
16. Mary Ellen O'Connell, Cyber Security without Cyber War, Journal of Conflict **&** Security Law, Vol. 17, 187, 2012. Available at: https://archive.law.upenn.edu/live/files/8989-maryellenoconnellcybersecpdf
17. Matthew C. Waxmant, Cyber-Attacks and the Use of Force: Back to The Future of Article 2(4), Yale Journal of International Law, Vol. 36, 2011, 421. Available at: https://cpb-us-w2.wpmucdn.com/campuspress.yale.edu/dist/8/1581/files/

2016/09/36-2-waxman-cyber-attacks-and-the-use-of-force-2hg9mio.pdf

18. Matthew Rinear, Comment: Armed with A Keyboard: Presidential Directive 20, Cyber-Warfare, And the International Laws of War, Capital University Law Review, Vol. 43, 697, Summer 2015.
19. Michael Connell and Sarah Vogler, Russia's Approach to Cyber Warfare, Center for Naval Analysis (CAN), Washington DC, September 2016. P. 2. Available at: https://apps.dtic.mil/sti/pdfs/AD1019062.pdf
20. Michael Gervais, Cyber Attacks and The Laws of War, Berkeley Journal of International Law, Vol. 30, No. 2, 2012.
21. Michael N. Schmit, International Law and the Use of Force: The Jus Ad Bellum, The Quarterly Journal, Volume II, No.3, September 2003.
22. Michael N. Schmitt, Computer Network Attack and the use of force in International Law: Thoughts on a Normative Framework, The Columbia Journal of Transnational Law, Volume 37, 1999, 885-937.
23. Michael N. Schmitt, Cyber Operations and the Jus Ad Bellum Revisited, Villanova Law Review, Vol.56, 2011.
24. Michael N. Schmitt, Cyberspace and International Law. the penumbral mist of uncertainty, Harvard Law Review Forum, Vol. 126, 2013.
25. Michael N. Schmitt, International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed, Harvard International Law Journal, Vol. 54, December 2012.
26. Michael N. Schmitt, The Law of Cyber Warfare: Quo Vadis, Stanford Law & Policy Review, Vol 25, 2014, 269.

27. Nicholas Tsagourias, Cyber Attacks, Self-defense and the Problem of Attribution, Journal of Conflict and Security Law, Vol. 17, No. 2, 2012, 229–244.
28. Oona A. Hathaway, Rebecca Crootof, Philip Levitz, Haley Nix, Aileen Nowlan, William Perdue And Julia Spiegel, The Law Of Cyber-Attack, California Law Review. V0l. 100, No. 4, Aug 2012.
29. Peter Z. Stockburger, Known unknowns: state cyber operations, cyber warfare, and the jus ad bellum. American University International Law Review, Vol. 31, No.2, 2016.
30. Rebecca Helene Sussman, The Reusable Bomb: Exploring How the Law of Armed Conflict Applies in Cyberspace, Boston University Journal of Science & Technology Law, Vol. 23, 481, Summer 2017.
31. Reese Nguyen, Navigating jus ad bellum in the age of cyber warfare. California Law Review, Vol. 101, 2013. 1079.
32. Romana Sadurska, Threats of Force, The American Journal of International Law, Vol. 82, No. 2, 1988, Pp. 239–268.
33. Rudolf Bernhardt, Evolutive Treaty Interpretation, Especially of the European Convention on Human Rights, German Year Book of International law, Vol.42, 1999.
34. Scott J. Shackelford, From Nuclear War to Net War: Analogizing Cyber Attacks in International Law, Berkley Journal of International Law, Vol. 25, No. 3, 2009. Available at SSRN: https://ssrn.com/abstract=1396375

35. Sean M. Condron, Getting It Right: Protecting American Critical Infrastructure in Cyberspace, Harvard journal of law & technology, Vol.20, 2007.
36. Sean Watts, Low-Intensity Computer Network Attack and Self-Defense, International Law Studies, Vol. 87, 2010.
37. Sondre Torp Helmersen, Evolutive Treaty Interpretation: Legality, Semantics and Distinctions, European Journal of Legal Studies, Volume 6, No. 1 (Spring/Summer 2013).
38. Stephen W. Koms and Joshua E. Kastenberg, Georgia's Cyber Left Hook," Parameters (U.S. Army War College Quarterly) Vol. 38, no. 4 2008.
39. Tho Tom Ruys, The meaning of 'force' and the boundaries of the *jus ad bellum*: are 'minimal' uses of force excluded from un charter article 2(4)? The American Journal of International Law, Vol. 108, No. 2, 2014, Pp 159–210.
40. Thomas W. Smith, The New Law of War: Legitimizing Hi-Tech and Infrastructural, International Studies Quarterly, Vol.46, 2002. https://archive.law.upenn.edu/live/files/3477-saalbach-k-methods-and-practice-2014
41. Yuchong Li and Qinghui Liu, A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments, Energy Reports 7 (2021) 8176–8186. https://www.sciencedirect.com/science/article/pii/S2352484721007289

Conferences

1. Cyber – Terrorism: A Threat for The European Union and Its Response. Webinar 65/2018, https://www.cepol.europa.eu/tags/cyberterrorism
2. Wolff Heintschel von Heinegg, Legal Implications of Territorial Sovereignty in Cyberspace, 4th International Conference on Cyber Conflict, Faculty of Law Europa-Universität, Frankfurt (Oder), Germany, 2012, p. 9. Available at; https://www.ccdcoe.org/uploads/2012/01/1_1_von_Heinegg_LegalImplicationsOfTerritorialSovereigntyInCyberspace.pdf

The ICJ's Jurisprudence

1. Armed activities on the territory of the Congo (Dem. Rep. Congo V. Uganda), 2005 ICJ Report 168.
2. Dispute Regarding Navigational and Related Rights (Costa Rica V Nicaragua), Judgment Of 13 July 2009, 2009 ICJ Reports.
3. Legal Consequences for States of the Continued Presence of South Africa in Namibia (South West Africa) Notwithstanding Security Council Resolution 276 (1970), Advisory Opinion, 21 June 1971, 1971 ICJ Reports.
4. Legality of the Threat or Use of nuclear weapons, Advisory Opinion, 1996 ICJ Report 22 (July 8).
5. Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States of America), Merits, 1986 ICJ Report. 14 (June 27). [Nicaragua Case]

6. Oil Platforms (Islamic Republic of Iran V. United States of America), Judgment, 2003 ICJ Reports.

Legal Instruments.

1. Agreement Between the Governments of the Member States of the Shanghai Cooperation Organization on Cooperation in the field of International Information Security, Yekaterinburg, 16 June 2009annex I.
2. Fifth Report of the Special Committee on Principles of International Law Concerning Friendly Relations and Co-Operation Among States, UN Doc A/7619 (1969).
3. Fourth Report of The Special Committee on Principles of International Law Concerning Friendly Relations and Co-Operation Among States, Un Doc A/7326 (1968).
4. https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=185
5. Second Report of the Special Committee on Principles of International Law Concerning Friendly Relations and Co-Operation Among States, UN Doc. A/6230, 27 June 1966. ['Second Report'].
6. The Military Doctrine of the Russian Federation, approved by Russian Federation presidential edict on February 5, 2010 (translated). para. 13(d) Available at http://carnegieendowment.org/files/2010russia_military_doctrine.pdf .
7. Third Report of The Special Committee on Principles of International Law Concerning Friendly Relations and Co-

Operation Among States, UN Doc A/6799, 26 September 1967. ['Third Report'].

8. Warsaw Summit Communiqué, issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw 8-9 July 2016.

Websites

Friedel Taube, Russia-Ukraine conflict: What role do cyberattack play? (28/2/2022) https://www.dw.com/en/russia-ukraine-conflict-what-role-do-cyberattacks-play/a-60945572