ISSN: 2663-5798 || Arab Journal for Scientific Publishing

الإصدار التاسع – العدد التاسع والثمانون
تاريخ الإصدار: 2 – آذار – 2026م
www.ajsp.net

"دور مجلس الأمن الدولي في مواجهة الهجمات السيبرانية بمقتضى الفصل السابع"

إعداد الباحثة:

ماريا جان التولاني

DOI Number: https://doi.org/10.36571/ajsp/8920

الإصدار التاسع – العدد التاسع والثمانون
تاريخ الإصدار: 2 – آذار – 2026م
www.ajsp.net
ISSN: 2663-5798 || Arab Journal for Scientific Publishing

الملخص

شهد المجتمع الدولي في السنوات الأخيرة بروز الهجمات السيبرانية كأحد أخطر التحديات الأمنية غير التقليدية، لما تملكه من قدرة على تجاوز الحدود الجغرافية وإحداث أضرار بشرية ومادية جسيمة تماثل تلك الناجمة عن النزاعات المسلحة التقليدية. ويطرح هذا الواقع إشكالية قانونية جوهرية تتمثل في مدى اختصاص مجلس الأمن الدولي، بمقتضى الفصل السابع من ميثاق الأمم المتحدة، في مواجهة هذه العمليات، باعتبارها تهديدًا أو خرقًا للسلم والأمن الدوليين، بل وحتى ارتقائها إلى مستوى العدوان.

يُعالج هذا البحث نطاق السلطات التقديرية الممنوحة لمجلس الأمن الدولي، لاسيما في ضوء تطوّر مفهوم السلم والأمن الدوليين واتساع دائرته ليشمل تهديدات من طبيعة اقتصادية، إنسانية وبيئية. كما يتناول مدى إمكانية تكييف الهجمات السيبرانية كأعمال عدوانيةوما إذا كانت الوسائل الإلكترونية يمكن اعتبارها "أسلحة" بالمعنى القانوني، وبالتالي تبرير استخدام التدابير القسرية بما فيها القوة المسلحة. كما يناقش البحث مشروعية الرد على الهجمات السيبرانية سواء استنادًا إلى إذن صريح من مجلس الأمن أو إلى موافقة ضمنية أو لاحقة، مع الإشارة إلى التحديات التقنية والقانونية التي تعترض عملية الإسناد وإثبات المسؤولية، فضلًا عن القيود العملية المرتبطة بغياب قوات سيبرانية تابعة للأمم المتحدة.

وقد استندت الدراسة إلى تحليل نصوص ميثاق الأمم المتحدة وقرارات الجمعية العامة ومجلس الأمن ذات الصلة، إضافةً إلى الاجتهادات القضائية الدولية وآراء الفقه القانوني، مع اعتماد منهج تحليلي مقارن يربط بين القواعد التقليدية للقانون الدولي ومقتضيات الفضاء السيبراني.

الكلمات المفتاحية: الهجمات السيبرانية– الفضاء السيبراني– مجلس الأمن الدولي– الفصل السابع– العدوان– السلم والأمن الدوليين

المقدمة

في السابع عشر من شهر أيلول من العام 2024، تعرّضت الجمهورية اللبنانية الى انفجارات هزّت العاصمة بيروت وعدد من المناطق الأخرى نتيجة لانفجار أجهزة بيجر يستخدمها عناصر من حزب الله. وفي غضون دقائق، امتلأت المستشفيات بآلاف الجرحى المُلطّخين بالدماء وبعدد كبير من الضحايا، وكأن ما كان خيالًا علميًا في الأفلام السينمائية بات واقعًا على الأراض اللبنانية. ونتيجةً لذلك، تمّ اعتبار هذا الهجوم بأنه الأول من نوعه في تاريخ النزاعات وفتح فصلاً جديداً من العمليات السيبرانية الخطيرة. فهذه الأخيرة، ورغم اختلاف أنواعها وأهدافها ومخاطرها ورغم الافتقار الى تعريف مُتّفق عليه لها، إلّا أنّها عبارة عن *"مجموعة الأعمال العدائيَّة المُوجَّهة ضدَّ مُعطيات الدولة الإلكترونيَّة المُخزَّنة أو المُعالجة أو المُتبادلة من حاسوب إلى آخر بهدف كَشْفِها أو نَسْخِها أو تعديلها أو إتْلافِها أو عرقلة تدفُّقها (كالهجوم على أنظمة المُراقبة الجويَّة، وأنابيب نقل الغاز والبترول، والمفاعلات النوويَّة)"*[1]. وتتميّز هذه الهجمات الغير تقليدية بأنّها عمليات تقنية مُتطورة تعكس قمة التطوُّر الذي وصلت إليه ثورة المعلومات، فهي غير مرئية تحصُل عبر الفضاء الإلكتروني، تخترق الحدود الجغرافية وتنتهك السيادة الوطنية بسهولة، كونها سريعة الانتشار والحصول بشكل يجعل من الصعب اكتشافها قبل تحقيق الهدف المراد منها. وبما أنّ مخاطر هذه الهجمات قد تتعدى المخاطر التي تُخلّفها الهجمات التقليدية من قتل ودمار؛ فهي قادرة على زعزعة النظام الدولي ووضعه في خطر جسيم. وبما أنّ مجلس الأمن الدولي، المسؤول بموجب ميثاق الأمم المتحدة عن الحفاظ على

[1] طارق المجذوب، السَّايبر ساحة "خَفِية" لحربٍ "ناعِمة" قادمة، مجلة الدفاع الوطني، المؤسسة العسكرية، لبنان، 2014/07، العدد 89.

الأمن والسلم الدوليين، لم يتّخذ حتى تاريخه أي قرار يتعلّق بسبل مواجهة الهجمات السيبرانية الخطيرة وما اذا كان من شأنها المساس بالسلم والأمن الدوليين، كان لا بُدّ من التساؤل حول صلاحية مجلس الأمن الدولي في استخدام السلطات الممنوحة له بمقتضى الفصل السابع لمواجهة العمليات السيبرانية والمخاطر الناجمة عنها، خصوصًا وأنّ هذا الفصل منح مجلس الأمن الدولي صلاحيات تقديرية واسعة، لاسيما لجهة حقه بالسماح للدول باستخدام تدابير قسرية وغير قسرية في حالات معينة.

وللإجابة على هذا السؤال، لا بد من معالجة العديد من التساؤلات وأبرزها:

متى يحق لمجلس الأمن الدولي التدخل لمواجهة العمليات السيبرانية الدولية؟ إلى أي مدى تقع الأسئلة المتعلقة بالتهديدات الرقمية والأمن السيبراني ضمن ولاية المجلس؟ هل يمكن أن تشكل الاستخدامات الحديثة لتكنولوجيا المعلومات تهديدا أو خرقا للسلم والأمن الدوليين أو عدوانا؟ ما هي التدابير التي يمكن اتخاذها في هذا الإطار؟ أي بعبارة أخرى، متى يحق لمجلس الأمن استخدام الفصل السابع في حالة الهجمات السيبرانية؟ وهل السلطات الممنوحة لمجلس الامن الدولي عام 1945، بمقتضى الفصل السابع، كفيلة بوضع حد لهذا النوع من التهديد أو الإنتهاك؟ هل يُمكن التوسُّع في تفسير قرارات مجلس الأمن الدولي واستخدام القوة للرد على الهجمات السيبرانية رغم افتقارها لإشارة صريحة لذلك؟

تكتسب هذه الدراسة أهميتها من كونها تسهم في توضيح الإطار القانوني الدولي وحدود ولاية مجلس الأمن بموجب الفصل السابع في مواجهة الهجمات السيبرانية، في ظل غياب قرارات صريحة للمجلس تُكيّف هجومًا سيبرانيًا بوصفه تهديدًا للسلم أو عدوانًا. كما تبرز أهميتها العملية بالنظر إلى تصاعد المخاطر السيبرانية على البنى التحتية الحيوية وما تثيره من إشكاليات الإسناد والمساءلة، بما ينعكس على خيارات الإنفاذ الدولي وآليات الردع.

على ضوء كل ذلك، تبرز ضرورة دراسة مشروعية الرد بمقتضى الفصل السابع من ميثاق الأمم المتحدة **(المطلب الأول)** وموافقة مجلس الأمن الضمنية أو اللاحقة للرد على الهجمات السيبرانية **(المطلب الثاني)**.

المطلب الأول: مشروعية الرد بمقتضى الفصل السابع من ميثاق الأمم المتحدة

يوفر الفصل السابع من ميثاق الأمم المتحدة الإطار الذي يجوز فيه لمجلس الأمن الدولي الإنفاذ. إذ يسمح لهذا الأخير أن يُقرّر "ما إذا كان قد وقع تهديد للسلم أو إخلال به أو كان ما وقع عملاً من أعمال العدوان"، وأن يقدم توصيات أو أن يلجأ إلى القيام بعمل غير عسكري أو عسكري "لحفظ السلم والأمن الدوليين"[2]. ممّا يعني أنّه ليتمكّن مجلس الأمن الدولي من استخدام صلاحياته هذه، لا بُدّ من توفُّر عدد من الشروط وعلى رأسها حصول تهديد أو خرق للسلم العالمي أو وقوع عمل عدواني. ولكن ونظرًا لأنّ هذه الصلاحيات الواسعة قد تمّ تكريسها عام 1945، أي قبل عقود من ظهور الفضاء السيبراني، كان لا بد من معرفة ما إذا كان من حق مجلس الأمن الدولي استخدامها لمواجهة مخاطر هجمات غير تقليدية وذلك من خلال دراسة مدى خطورة الهجمات السيبرانية على الأمن والسلم الدوليين **(الفرع الأول)**، وما إذا كان من شأنها الإرتقاء إلى مستوى العدوان (مدى شمول العدوان للهجمات السيبرانية) **(الفرع الثاني)**.

[2] ميثاق الأمم المتحدة لعام 1945، المواد 39 و42، متاح على: https://www.un.org/ar/about-us/un-charter/full-text.

الفرع الأول: مدى خطورة الهجمات السيبرانية على السلم والأمن الدوليين

إن الإستعمال المتزايد للهجمات السيبرانية وتنوّع أهدافها واتّساع أضرارها يسمح بالتأكيد بأن أمن وسلام المجتمع الدولي الذي بُني عام 1945 بات مُهدّدا. ولكن لتأكيد مدى خطورة الهجمات السيبرانية على الأمن والسلم العالمي لا بُدّ من إلقاء الضوء على تطوُّر مفهوم السلم والأمن الدوليين **(أولًا)** ومن ثم دراسة الهجمات السيبرانية كتهديد أو انتهاك للسلم والأمن الدوليين **(ثانيًا)**.

أولًا: تطوُّر مفهوم السلم والأمن الدوليين

تُشكّل المحافظة على السلم والأمن الدوليين الهدف الأساسي والعامود الفقري الذي تقوم عليه منظمة الأمم المتحدة. ولأجل ذلك، مُنِح مجلس الأمن الدولي صلاحية اعطاء الدول الحق باتّخاذ تدابير، ومن بينها تلك التي تنضوي على استخدام القوة، عند وجود تهديد أو انتهاك للسلم والأمن الدوليين[3]. إلّا أنّ ميثاق الأمم المتحدة افتقر الى تعريف للمقصود بالسلم والأمن الدوليين والحالات التي تُشكّل تهديدًا أو اخلالًا بهما. كما لا يُوجد أي نص دولي، مكتوب أو عرفي، يُوضّح هذه المفاهيم. ويبدو أنّ هذا الغموض كان مُتعمّدًا أولًا بهدف تمكين المجلس من مُواجهة التطوُّرات والتهديدات الجديدة، التي من شأنها تعريض السلم والأمن الدوليين للخطر[4] وثانيًا لترك الحرية لمجلس الأمن في هذا المجال لاعتبارات سياسية[5]. وقد حاولت المحكمة الجنائية الدولية الخاصة بيوغوسلافيا تحديد المقصود بهذين المفهومَين، حين اعتبرت أنه يجب تقييم مدى وقوع تهديد للسلم والأمن الدوليين على ضوء مقاصد الأمم المتحدة المنصوص عنها في المادة الأولى من الميثاق[6]. إلّا أنّ هذا الإقتراح لا يُقدِّم تحديدًا دقيقًا للتهديدات، كون المقاصد المنصوص عنها في المادة الأولى جاءت عامّة وفضفاضة كتنمية العلاقات الودية وتحقيق التعاون الدولي في حل المشاكل الدولية وغيرها من المقاصد.

وقد تطوّر مفهوم السلم والأمن الدوليين بشكل كبير، منذ انشاء منظمة الأمم المتحدة عام 1945، لاسيما في الفترة التي تلت إنتهاء الحرب الباردة. اذ بعد أن كان تهديد السلم والأمن ينحصر بالحروب والنزاعات أو التهديد بقيامها أي الحالات التي تنضوي على استخدام القوة العسكرية، أصبحت مصادر التهديد مُتنوّعة. إذ بات من الممكن أن يكون مصدر التهديدات ذات طبيعة اقتصادية، انسانية، اجتماعية، بيئية وغيرها[7]. وقد بدأت الدول بالتعبير صراحةً عن هذا الميل للتوسُّع في تفسير مفهوم السلم، منذ عام 1992، في الجلسة التي عقدها مجلس الأمن الدولي على مستوى رؤساء الدول والحكومات[8]. كما أكّد الأمناء العامين للأمم المتحدة على وجود تقارب مُتزايد في الآراء والمواقف الدولية حول عدم امكانية الإلتزام بتعريفٍ ضيّقٍ للأمن الجماعي، ذلك أنّ الانتهاكات الواسعة لحقوق الإنسان وانتشار الأوبئة والأمراض والمخدرات، وظهور الإرهاب الدولي والكوارث البيئية والكثير غيرها هي كلها أمور تشكل انتهاكًا لأمن الإنسانية[9].

---

[3] عبد الكريم علوان، الوسيط في القانون الدولي، الكتاب الرابع المنظمات الدولية ، دار الثقافة، الأردن، 2012، ص 105.
[4] حسام هنداوي، حدود سلطات مجلس الأمن في ضوء قواعد النظام العالمي الجديد، الطبعة الأولى، دار النهضة العربية، مصر، 1994، ص. 65.
[5] للمزيد راجع: عميمر نعيمة، دمقرطة منظمة الأمم المتحدة، المؤسسة الجامعية للدراسات والنشر والتوزيع، بيروت، 2007، ص. 54.
[6] المحكمة الجنائية الدولية ليوغسلافيا السابقة، قضية المدعي العام وتاديتش، رقم IT-94-1-A، غرفة الإستئناف، تاريخ 1999/07/15، متاح على: www.icty.org، تاريخ وساعة الزيارة: 2022/01/13، 16:00 ب.ظ.
[7] محمد صوفيان، السلم والأمن الدوليين: دراسة على ضوء أحكام ميثاق الأمم المتحدة، مجلة الواحات للبحوث والدراسات، المجلد 11، العدد 1، 2018، ص. 184.
[8] للمزيد راجع: محمد هنداوي، سلطات مجلس الأمن في ضوء قواعد النظام العالمي الجديد، مرجع سابق، ص. 79.
[9] مصطفى قرزان، مبدأ مسؤولية الحماية وتطبيقاته في ظل مبادىء وأحكام القانون الدولي العام، رسالة لنيل شهادة الدكتورة في الحقوق، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد بتلمسان، الجزائر، 2015، ص. 178.

وفي الممارسة الدولية، تنوّعت المعايير التي اعتمدها مجلس الأمن الدولي للاقرار بوجود تهديد للسلم والأمن الدوليين، ولم تكن معايير أو حالات مُوحّدة، فكان حجم الكارثة الانسانية في رواندا سببا لتهديد السلم، وشكل انهيار الدولة الألبانية تهديدًا لسلم وأمن المنطقة. وفي قرارات أخرى، اعتبر مجلس الأمن أنّ تهديد السلم والأمن الدوليين ناتج عن خطورة الوضع الذي خلفته النزاعات وعن الإرهاب[10]. فهل صدرت أي قرارات عن مجلس الأمن تحت باب الفصل السابع تعتبر أي من العمليات السيبرانية انتهاكًا للأمن الدولي أو هل هناك من توجُّه نحو ذلك؟

ثانيًا: الهجمات السيبرانية كتهديد أو انتهاك للسلم والأمن الدوليين

صحيح أنّ الهجمات الالكترونية الدولية لا تعتمد على الأسلحة التقليدية وليست مرئية بطبيعتها، إلّا أن من شأنها أن تتسبّب في نزاعات مسلّحة دولية وغير دولية، وأن تنتهك بشكل فاضح حقوق الإنسان، وأن تُؤثر على الأمن الإقتصادي والإجتماعي والسياسي والأمني والمالي والصحي والنووي، وأن تُلحق أضرارًا مادية وبشرية خطيرة. فاستهداف النظام الالكتروني العائد للسدود أو للقطارات أو للمطارات من شأنه تحقيق كوارث بشرية وأضرار مادية مهولة. ممّا يُؤكّد على أنّه لا يمكن استثناء الهجمات ذات الطبيعة السيبرانية من الأسباب المهددة أو المنتهكة للسلم والأمن الدوليين. لا بل مع ازدياد هذا النوع من العمليات والتطوّر التكنولوجي المُتسارع في هذا المجال، قد نكون أمام الخطر الأهم والأكبر على الأمن والسلم الدوليين، لاسيما وأنّ النصوص الدولية لم تربط التهديد والاخلال بالسلم الدولي بالوسيلة المستخدمة، وانّما بالآثار المترتبة على الأعمال الدولية. فقرار مجلس الأمن الدولي بالسماح باستخدام القوة لوضع حد لكارثةٍ إنسانيةٍ لا يتأثر بما اذا كانت هذه الكارثة وقعت نتيجة هجوم عسكري تقليدي أو نتيجة هجوم الكتروني. وخير دليل على ذلك، القرار رقم 1540 الصادر عن مجلس الأمن الدولي عام 2004 نتيجةً لانتشار الأسلحة النووية والكيميائية والبيولوجية، الذي حثّ بموجبه على ضرورة اتخاذ تدابير فعّالة ضد أي تهديد للسلم والأمن الدوليين[11]. اذ رغم الاختلاف في طبيعة هذا النوع من الأسلحة عن تلك التقليدية، اعتبر مجلس الأمن ان من شأن استخدامها زعزعة الاستقرار الدولي والتسبُّب بالمآسي الانسانية، لاسيما وأنّه يستحيل حماية المدنيين من آثارها[12]، والأمر يشبه الى حد بعيد الآثار التي يمكن أن تنتج عن الهجمات السيبرانية. فإذا أخذنا على سبيل المثال هجوم ستوكسنت لعام 2010 والهجمات الإلكترونية اللاحقة التي استهدفت منشأة نطنز والعديد من المنشآت النووية الإيرانية الأخرى، والتي أدّت إلى إحداث فوضى وإخراج أجهزة الطرد المركزي عن نطاق السيطرة، ألا يبدو واضحًا أنه كان بامكان هذه الهجمات أن تتسبّب بتفجير

[10] مجلس الأمن الدولي، الحالة المتعلقة برواندا، قرار رقم 929، تاريخ 1994/06/22، S/RES/929 (1994)، متاح على: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N94/260/25/PDF/N9426025.pdf?OpenElement؛ مجلس الأمن الدولي، الحالة في ألبانيا، قرار رقم 1101، تاريخ 1997/03/28، S/RES/1101 (1997)، متاح على: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N97/084/35/PDF/N9708435.pdf?OpenElement؛ مجلس الأمن الدولي، الحالة في العراق، قرار رقم 1511، تاريخ 2003/10/16، S/RES/1511 (2003)، متاح على: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N03/563/89/PDF/N0356389.pdf?OpenElement، تاريخ وساعة الزيارة: 2001/12/16، 11:50 ق. ظ.

[11] أكّد قرار مجلس الأمن الدولي رقم 1540 على أنّ" انتشار الأسلحة النووية والكيميائية والبيولوجية ووسائل إيصالها، يشكل تهديدا للسلم والأمن الدوليين"، مجلس الأمن الدولي، قرار رقم 1540، تاريخ 2004/04/28، S/RES/1540 (2004)، متاح على: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N04/328/41/PDF/N0432841.pdf?OpenElement، تاريخ وساعة الزيارة: 2021/12/16، 12:00 ظ.

[12] للمزيد راجع: وسيلة قنوفي، توسيع مفهوم السلم والأمن الدوليين في القانون الدولي، مجلة الآداب والعلوم الإجتماعية، جامعة محمد لمين دباغين سطيف، العدد 21، الجزائر، 2015، ص. 72.

المنشآت النووية وأن تؤدي إلى قتل وجرح وتشوية آلاف المدنيين وهدم ممتلكاتهم وتخريب البيئة وتلويثها لعقود طويلة وأن تشكل بطبيعة الحال تهديدا و انتهاكا مُباشرًا ليس فقط لأمن الدولة الإيرانية وإنّما للأمن الدولي على حد سواء؟

كما من الضروري الإشارة إلى إنّ تهديد السلم لا يفترض، بالضرورة، وقوع فعل غير مشروع مُسبق، كما لا يرتبط حصرًا بالتصرّفات التي تصل إلى عتبة القوة أو إلى مستوى الإعتداء المسلح؛ وبالتالي يتمتع مجلس الأمن الدولي بسلطة تقديرية في هذا المجال[13]. ممّا يعني أنّه يحق لهذا الأخير السماح باتخاذ التدابير المناسبة، بما في ذلك استخدام القوة العسكرية، ضدّ التهديدات والعمليات السيبرانية حتى ولو لم يُصَر إلى الاتفاق على عدم مشروعيتها، خصوصًا في ظل الاختلافات القانونية والسياسية التي لا تزال قائمة حول ماهية العمليات السيبرانية، شرط أن تشكل هذه التهديدات أو التصرفات تهديدا أو خرقًا للسلم [14]. فمجلس الأمن يُدرك تماما بأنه لاصدار قرارات في هذا السياق، وللسماح لأي دولة باللجوء للتدابير القسرية أو غير القسرية، يجب أن تُشكّل تهديدا للسلم أو خرق له وهو القيد الأساسي في هذه الحالة[15].

وفيما خص الهجمات السيبرانية، وبالرغم من أنّ مجلس الأمن الدولي لم يُصدر أي قرار يُصنّف بموجبه هجومًا إلكترونيًا كتهديد للسلم أو كخرق له، الا أنّه عقد في شهر حزيران السابق جلسة رسمية تحت عنوان "صون السلام والأمن الدوليين: التصدي للتهديدات المتطورة في الفضاء السيبراني"[16]، وما ذلك إلّا اعتراف بمدى خطورة العمليات التي تحصل في الفضاء السيبراني وتأثيرها على السلم والأمن الدوليين. وفي الجلسة عينها، كان الأمين العام للأمم المتحدة واضحًا وحاسمًا حين اعتبر صراحةً، أن للعمليات السيبرانية تكاليف أخطر من تلك المالية، فهي كفيلة بتهديد سلامة البلدان وأمنها واستقراراها المُشترك. فالأنشطة الضارة التي تقوض المؤسسات العامة والعمليات الانتخابية والنزاهة عبر الإنترنت تؤدي إلى تآكل الثقة وتأجيج التوترات، بل وتزرع بذور العنف والصراع[17]. وسبق لروسيا، وهي إحدى الأعضاء الخمس الدائمي العضوية في مجلس الأمن الدولي، أن أكّدت في اجتماع سابق للمجلس أنّ السؤال الأهم والذي لا يزال من دون إجابة هو أي حالات من الاستخدام الخبيث لتكنولوجيا المعلومات والاتصالات يمكن أن تعتبر من ضمن "التهديدات المباشرة للسلام والأمن الدوليين[18]. كما دعت الجمعية العامة للأمم المتحدة، في مناسبات عديدة، الدول الأعضاء إلى الاسترشاد بتوصيات فريق الخبراء المعني بالتطورات في مجال المعلومات والاتصالات في سياق الأمن الدولي عند استخدامها للوسائل السيبرانية[19]. اذ أكّد هذا الفريق على أن الهجمات السيبرانية التي تستهدف البنية التحتية الحيوية تشكل خطرًا حقيقيًا وجسيمًا، وأنّ العديد من الدول أعربت عن قلقها من احتمال نشوب صراعات مزعزعة للاستقرار وقادرة على إلحاق أضرار بمواطنيها وممتلكاتها واقتصادها، لاسيما في ظل وجود صعوبة في تحديد مصدر هذا النوع من الهجمات. وقد أعاد دليل تالين التأكيد على ما ورد في الفصل السابع من ميثاق الأمم المتحدة، لاسيما لناحية حق مجلس الأمن بتقدير ما اذا كان من شأن هجوم سيبراني أن يُشكل تهديدًا أو خرقًا للسلم الدولي، وأنّ الرد عليها يُمكن أن

[13] للمزيد راجع: إبراهيم شلبي، التنظيم الدولي، مكتبة الآداب، 1998، ص. 162 -321.
[14] ميثاق الأمم المتحدة، الفصل السابع، مرجع سابق.
[15] محمد الغنيمي، الاحكام العامة في قانون الامم، منشأة المعارف، مصر، 2005، ص. 8.
[16] مجلس الأمن يناقش التهديدات المتطورة في الفضاء السيبراني والأمين العام يدعو إلى اتخاذ تدابير وقائية، 2024/10/20، متاح على: https://news.un.org/ar/story/2024/06/1131931#:~:text، تاريخ وساعة الزيارة: 2024/08/09، 11:30 ق.ظ.
[17] المرجع السابق.
[18] Allison Pytlak, The UN Security Council Discusses Cyber Threats to International Security, 15/04/2024, available at: https://www.stimson.org/2024/un-security-council-cyber-threats-to-international-security/, accessed: 15/07/2024, 11:00 am.
[19] الجمعية العامة للأمم المتحدة، فريق الخبراء الحكوميين المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي، تاريخ 2015/07/22، UN Doc A/70/174 .

يكون بالاستناد الى القرارت الصادرة عن مجلس الأمن[20]. ولم تتوانَ العديد من الدول عن التأكيد على أن الهجمات السيبرانية قد تشكل تهديدا أو خرقا للسلم والأمن الدوليين ومن بينها فرنسا[21]، أوستراليا[22] وقطر[23]. كل ذلك يسمح بالقول أنه بات هناك اجماع دولي على أن العمليات التي تحصل في الفضاء السيبراني تشكل تهديدًا للسلم والأمن الدوليين كما هي الحال بالنسبة للعمليات العسكرية التقليدية، كما لأنّ ذلك يعني أن من حق مجلس الأمن الدولي استخدام سلطاته المُكرّسة في الفصل السابع لمواجهة الهجمات السيبرانية.

الفرع الثاني: مدى امكانية ارتقاء الهجمات السيبرانية الى مستوى العدوان

إنّ حصول عمل عدواني يُعطي مجلس الأمن الدولي صلاحية التصرُّف بمقتضى الفصل السابع من ميثاق الأمم المتحدة، وذلك بغض النظر عن نوع أو طبيعة العمليات الحاصلة. ولكنّ الهجمات السيبرانية التي تختلف بصورة جذرية عن تلك التقليدية، فتحت الباب واسعًا أمام الجدل حول مدى امكانية ادراج العمليات السيبرانية ضمن خانة العدوان المنصوص عنه في الفصل السابع المذكور أعلاه. إلّا أنه وبعد ثبوت الأضرار البشرية والمادية التي يمكن أن تُسببها الهجمات السيبرانية، بات من من الضروري إلقاء الضوء على الهجمات السيبرانية كعمل سيبراني عدواني **(أولًا)** ومن ثم تحديد ما إذا كان من حق مجلس الأمن الدولي السماح للدول باستخدام وسائل مماثلة للرد من خلال دراسة مدى مشروعية الرد بوسائل سيبرانية **(ثانيًا)**.

أولا: الهجمات السيبرانية كعمل سيبراني عدواني

يُعرّف قرار الجمعية العامة للأمم المتحدة رقم 3314، والذي صدر في 14 كانون الأول من عام 1974، العُدوان بأنّه *"استخدام القوة المُسلّحة من قبل دولة ما ضد سيادة دولة أخرى او سلامتها الإقليمية أو استقلالها السياسي، أو بأية صورة أخرى تتنافى مع ميثاق الأمم المتحدة، وفقًا لنص هذا التعريف"*[24]. وبناء على ذلك، أكد العديد من الفقهاء على أنّ تعريف العدوان يسمح باستبعاد العمليات الالكترونية، ونفوا أي امكانية لتحوّل الهجمات السيبرانية إلى عمل عدواني، ذلك أنه لوقوع فعل العدوان لا بُد من تحقُّق عناصره وعلى رأسها استخدام القوة المسلحة[25]، أي استخدام سلاح[26]. من هُنا، استند هؤلاء على نوع السلاح بحد ذاته، وأخذوا بمعيار الوسيلة دون النتيجة، مُعتَبرين أن العدوان لا يتحقّق الا اذا تم استخدام الأسلحة التقليدية[27]، ذلك أنّ المادة 51 من ميثاق الأمم المتحدة اعتمدت عبارة الإعتداء المسلح ولم تترك أي مجال للتفسيرات الواسعة، خصوصًا انه في عام 1945 لم يكن هناك سوى الأسلحة التقليدية العسكرية[28]. يُضاف إلى كل

[20] القاعدة 76 من دليل تالين، للمزيد راجع: François Delerue, Analyse du Manuel de Tallinn 2.0 sur le droit international applicable aux cyber-opérations, Étude prospective et stratégique, 2017, p.68.
[21] للمزيد راجع: International Law and Cyberspace, Report of the Study Group co-organised by the University of Bologna, University of Milan and University of Westminster,02/2021, p. 46.
[22] المرجع السابق، ص. 30.
[23] دولة قطر تؤكد أن الهجمات السيبرانية تهدد الأمن والسلم والاستقرار، 2024/05/22، متاح على: https://mofa.gov.qa، تاريخ وساعة الزيارة: 2024/03/02.
[24] الجمعية العامة للأمم المتحدة، القرار رقم 3314، تاريخ 1974/12/14، الدورة 29، المادة 1، A/RES/3314؛ أنطونيو كاسيزي، القانون الجنائي الدولي، الطبعة الأولى، ترجمة مكتبة صادر ناشرون، مكتبة صادر ناشرون، لبنان، 2015، ص. 265.
[25] للمزيد راجع: ختال هاجر، الوضع القانوني للحرب السيبرانية على ضوء قواعد القانون الدولي، التواصل في الإقتصاد والإدارة والقانون، الجزائر، المجلد 25، العدد 3، 2019، ص. 165.
[26] Mario Bettati, Droit Humanitaire, Dalloz, France, 2012, p. 128.
[27] عماد ابراهيم، التدابير المضادة ومدى مشروعيتها في مواجهة الهجمات السيبرانية المعادية في القانون الدولي العام، مجلة البحوث القانونية والاقتصادية، كلية الحقوق، جامعة المنوفية، مصر، المجلد 54، العدد 3، 2021، ص. 202.
[28] عمر أعمر، الحرب الإلكترونية في القانون الدولي الإنساني، علوم الشريعة والقانون، الجامعة الأردنية، الأردن، المجلد 46، العدد 3، 2019، ص. 136.

ذلك أنّ المادة 3 من القرار رقم 3314 المذكور أعلاه تضمّنت لائحة ببعض الممارسات التي تُشكّل أعمالًا عدوانية كقصف القوات المسلّحة للمدن، أو غزو القوات المسلحة للاقليم البري أو البحري أو الجوي للدولة، القصف والقاء القنابل والحصار. تُبيّن هذه الامثلة، بحسب البعض، أن العمل العدواني لا يتم الا من قبل قوات مُسلّحة ويستلزم أعمالًا مادية كالقصف والغزو وحصار المرافىء وغيرها. كل ذلك أدّى الى استبعاد أي امكانية في أن تُشكّل الهجمات غير التقليدية، كتلك ذات الطابع الالكتروني، عملًا عدوانيا، نظرًا لاشتراط أن يكون مصدر العدوان القوات المسلحة وضرورة تحقّق الطابع المادي للفعل وللآثار.

إلا أنّ هذه التفسيرات غير دقيقة ولا تتماشى مع التطوّرات المُتسارعة في ميدان الأسلحة. صحيح أنّ استخدام القوة المسلحة ضد الدولة المستهدفة هو العنصر الأول من عناصر العدوان، الا أن هذا العنصر لا يسمح باستبعاد الهجمات السيبرانية من إطار الأعمال العدوانية. إذ تمّ تبنّي تعريفات واسعة للسلاح، كما في دراسة اللجنة الدولية للصليب الأحمر حول القانون الدولي الإنساني العرفي، التي اعتبرت بأن الأسلحة هي وسيلة لارتكاب أعمال عنف ضد العناصر البشرية والمادية للعدوان[29]. وبدوره اعتبر دليل القانون الدولي المُطبّق في النزاعات المُسلحة الجوّية والصّاروخية، أنّ الوسائل المُستخدمة في النزاعات تشمل الأنظمة غير المادية أو غير الحركية، أجهزة الكمبيوتر وكافّة المعدات والشبكات المُرتبطة بها، كما في حالة النزاعات الإلكترونية والهجمات السيبرانية[30]. إنّ السّمة الرئيسية للسلاح، بحسب الدليل، هي القدرة على التسبُّب في إصابة أو وفاة الأشخاص أو إتلاف أو تدمير الأشياء[31]. وقد أيّد العديد من الفقهاء هذا الاتّجاه، حين اعتبروا أنّ الأسلحة تتضمّن أي سلاح أو ذخيرة أو غيرها من الأجهزة أو الآليات، التي تهدف إلى تدمير أو تعطيل أو إصابة الأفراد أو المعدّات أو المُمتلكات العائدة للعدو[32]. والقاسم المُشترك بين كل هذه التعاريف هو الآثار العنيفة التي تنتج عن استخدامه. فالسلاح يُعتبر كذلك نسبةً لآثاره، وليس لنوعه أو لطريقة عمله أو الغرض من استخدامه[33]. وتأكيدًا على ذلك اعتبرت محكمة العدل الدولية في الفتوى الصادرة عام 1996 والمُتعلقة بمشروعية التهديد بالأسلحة النووية أو استخدامها، أنّ الهجمات الكيمائية من الوسائل غير المشروعة في النزاعات، رغم أنّها لا تتوافق في طبيعتها مع الأسلحة التقليدية[34]. وقد وضّحت المحكمة في القضية عينها، أنّ المادة 51 من ميثاق الأمم المتحدة، كما المواد 4/2 و42 من ميثاق الأمم المتحدة، تنطبق على أي استخدام للقوة، بغض النظر عن الأسلحة المُستخدمة. وما يُؤكّد صحة هذا الإتّجاه، قرار مجلس الأمن الدولي الذي أعطى الحق في الدفاع عن النفس، ردًا على هجمات 11 أيلول 2001 التي استهدفت الولايات المتحدة الأميركية، رغم أنّ الأسلحة المُستخدمة كانت عبارة عن طائرات مدنية تمّ اختطافها[35]. والأهم، أنّ اللجنة

[29] Customary International Humanitarian Law, Cambridge Doswald-Beck, Jean-Marie Henckaerts and Loui University Press, USA, volume 1, 2005, Rule 6, p. 23.

[30] عمر أعمر، الحرب الإلكترونية في القانون الدولي الإنساني، مرجع سابق، ص. 139.

[31] سلافة الشعلان، تكييف استخدام الحرب الإلكترونية في النزاعات المسلحة وفقاً للقانون الدولي الإنساني، مجلة الكوفة للعلوم القانونية والسياسية، جامعة الكوفة، العراق، المجلد 9، العدد 26، 2016، ص. 22.

[32] للمزيد راجع: مصطفى نعوس، حق الدولة في استخدام القوة في الفضاء الإلكتروني للدفاع عن النفس، مجلة الحقوق، جامعة الكويت، العدد1، 2014، ص. 575.

[33] نبيله هروال، الجوانب الإجرائية لجرائم الانترنت في مرحلة جمع الإستدلالات، دراسة مقارنة، دار الفكر الجامعي، مصر، 2013، ص. 24.

[34] محكمة العدل الدولية، فتوى بشأن مشروعية التهديد بالأسلحة النووية أو استخدامها، تاريخ 1996/07/08، موجز الأحكام والفتاوى والأوامر، الأمم المتحدة، 1996، فقرة 57.

[35] مجلس الأمن الدولي، القرار رقم 1368، تاريخ 2001/09/12، S/RES/1368 (2001)؛ مجلس الأمن الدولي، القرار رقم 1373، تاريخ 2001/09/28، S/RES/1373 (2001).

الدولية للصليب الأحمر لم تتوانَ عن تصنيف الوسائل السيبرانية على أنها أسلحة، وذكرتها من ضمن لائحة الأسلحة، في إعلانها الخاص بالأسلحة المقدّم للأمم المتحدة عام 2017[36].

وبدورها باتت الدول تُؤكّد، بصورة صريحة، على أنّ الوسائل الإلكترونية تُشكّل أسلحة. إذ أثناء المؤتمر الدولي للصليب الأحمر لعام 2003، طالبت الدول الأطراف في اتفاقيات جنيف بأن تخضع جميع الأسلحة الجديدة ووسائل وأساليب الحرب الحديثة *"لاستعراض دقيق ومُتعدّد التّخصصات"* من أجل ضمان عدم تخطّي تطوُّر التكنولوجيا الحماية القانونية المكفولة[37]. كما نبّهت روسيا إلى أنّ الآثار المُدمّرة للأسلحة الإلكترونية يُمكن أن تُشبِه تلك الناتجة عن أسلحة الدَمار الشامل[38]. وبدورها، أكّدت المملكة المتحدة على أنّ الوسائل المُستخدَمة في الفضاء الإلكتروني تُعتَبر سلاحًا عسكريًا، يتم استعماله من قبل الدول وغير الدول[39]. كذلك، لم تتوانَ الولايات المتحدة الأميركية عن اعتبار الوسائل السيبرانية أسلحة[40]، حتى أنّه يُنظر إليها أحيانًا على أنها *"أسلحة مثالية"*، بسبب خصائصها (مجهولية المصدر، السرعة، السرية). أما شرط المساس بالسيادة والاستقلال السياسي المنصوص عنه في القرار 3314 المذكور أعلاه فيمكن أن يتحقق، ذلك أن مفعول هذا النوع من الهجمات الغير تقليدية يتخطّى الحدود الوطنية ويخرق السيادة. كل ذلك يسمح بالقول أن الوسائل السيبرانية تُشكّل سلاحًا جديدًا كغيرها من الأسلحة، التي تُستخدَم لشن الأعمال العدوانية.

أمّا بالنسبة لمن يؤكدون على أن الهجمات السيبرانية غير واردة ضمن لائحة العمليات التي تُعتبر عدوانا والتي تمّ تعدادها في القرار 3314 ، فان هذا الاستنتاج غير سليم. فالتّعداد الوارد في الفقرة الثالثة من القرار رقم 3314، والذي ذكر بعض الأعمال التي تشكّل عُدوانًا، قد ورد على سبيل المثال وليس الحصر، وتُرِك المجال مفتوحًا لحالات أخرى قد تُشكل عُدوانًا. كما تمّ إعطاء مجلس الأمن الدولي الحق بإدراج أفعالاً أخرى ضمن لائحة الأعمال العدوانية. يُضاف إلى ذلك، أنّه اذا ما اطّلعنا على لائحة الأعمال التي تُشكل عدوانًا والواردة في القرار المذكور أعلاه، نجد أنّ من شأن الهجمات الإلكترونية أن تُؤدّي نفس الغرض الذي تؤدّيه العمليات الواردة في التّعداد؛ فإذا كان من شأن القصف والغزوات تقويض سيادة الدولة، فإنّ الهجمات الإلكترونية قادرة على تحقيق الهدف عينه، من خلال السيطرة على شبكة المعلوماتية والتحكُّم بها أو تعطيلها. فلو أخذنا هجوم ستوكسنت على سبيل المثال، نجد أنّه تمّ تقويض برنامج إيران النووي، من خلال تدمير أكثر من ألف جهاز طرد مركزي في مجمع نطنز بعملية الكترونية، مثلما كان من الممكن أن يتم تدميرهم بغارة جوية. فالدول استبدلت الوسائل فقط لتحقيق نفس النتائج.

أخيرًا وفيما خصّ الادّعاء بأنّ الهجوم العدواني يجب أن يُرتكَب من قبل القوات المسلحة، فلا شيء يمنع بأن تقوم هذه القوات بشنّ الهجمات السيبرانية، خصوصًا أن العديد من الدول، كفرنسا، الولايات المتحدة الأميركية، إيران، حلف شمال الأطلسي والعديد غيرها، لم تتردّد في تشكيل وحدات خاصّة ضمن القوات المسلحة تُعنى بالشؤون السيبرانية. هذه الوحدات تعكس تَوجُّه الدُّول نحو استخدام الوسائل

[36] C.I.C.R., "Déclaration du C.I.C.R. aux Nations unies sur les armes, 2017", 10/10/2017, disponible sur: https://www.icrc.org/fr/document/declaration-du-cicr-aux-nations-unies-sur-les-armes-201, consulté le 12/10/2021, 14:00 pm.

[37] للمزيد راجع: لوران جيزيل، ما هي القيود التي يفرضها قانون الحرب على الهجمات السيبرانية، 2013/06/28، ص. 1، متاح على: https://www.icrc.org/ar/doc/resources/documents/faq/130628-cyber-warfare-q-and-a-eng.htm، تاريخ وساعة الزيارة: 2021/10/13، 13:20 ب. ظ.

[38] للمزيد راجع: Loïc Simonet, "L'usage de la force dans le cyberespace et le droit international", Annuaire Français de Droit International, France, 2012, p. 12.

[39] Marco Roscini, Cyber Operations and the Use of Force, Oxford University Press, UK, 2014, p. 233-254.

[40] Joint Chiefs of Staff, Joint Vision 2020-America's Military: Preparing for Tomorrow, 23/06/2000, available at: https://apps.dtic.mil/sti/citations/ADA526044, accessed: 13/04/2024, 10:30 am.

الإلكترونية كسلاح لتحقيق أهدافها. وقد أعلنت دول عديدة، ومن بينها تلك العضو في منظمة الأمن والتعاون في أوروبا، عن أن الهجمات السيبرانية التي تستهدف البنية التحتية الحيوية للدول وتلك التجارية باتت من حيث طبيعتها تساوي أعمال العدوان التقليدية.

ثانيًا: مشروعية الرد بوسائل سيبرانية

بعد أن تبيّن أن من شأن الهجمات السيبرانية أن تشكل تهديدًا وخرقا للسلم والأمن الدوليين وحتى أن ترتقي الى مستوى العدوان، بات من الثابت أن من حق مجلس الأمن الدولي اتّخاذ ما يراه مُناسبًا من تدابير. فإذا تبيّن له أن التدابير الغير قسرية، المنصوص عليها في المادة 41، لايمكن أن تفي بالغاية المرجوة أو ثبت أنها لم تفِ بها، "جاز له أن يتخذ بطريق القوات الجوية والبحرية والبرية من الأعمال ما يلزم لحفظ السلم والأمن الدولي أو لإعادته إلى نصابه"[41]. وبالتالي يمكن لمجلس الأمن، عند وقوع عمليات سيبرانية مهددة أو منتهكة للسلم والأمن الدوليين، أن يسمح باتّخاذ تدابير قسرية عن طريق القوات الجوية والبحرية والبرية، اذا تبين أن لا مجال لاعادة السلم بواسطة التدابير الأخرى. إلّا أنّ ما ورد في نص المادة 42 من ميثاق الأمم المتحدة، يُثير التساؤل حول ما اذا كان الرد عبر الفضاء الالكتروني وبواسطة الوسائل السيبرانية مُمكنًا، وما اذا كان من حق القوات التي تعمل في ميدان الفضاء الالكتروني الرد على عمليات سيبرانية تهدد السلم الدولي، أم أنّ ذلك حكرًا على " القوات الجوية والبحرية والبرية"، كما ورد في نص المادة المذكورة اعلاه.

في الواقع، إنّ قراءة المادة 42 على ضوء الفصل السابع من ميثاق الأمم المتحدة، تُبيّن أنّ الغاية من هذه المادة لم يكن تقييد الوسائل المُتوفّرة لمجلس الأمن لاعادة السلم الدولي الى نصابه وحصرها بميادين محددة، وإنّما توسيعها، بشكل يشمل كافة القوات والمجالات المتاحة أي البر أو الجو أو البحر. فالمادة 42 هدفت الى التأكيد على أنه يمكن الاعتماد على أي قوى تسمح بالمحافظة على السلم والأمن الدوليين، ولو كان الفضاء السيبراني موجودًا عام 1945، لم يكن واضعو الميثاق لِيتردّدوا عن الاضاءة على القوات العاملة في الاطار السيبراني. علمًا أنه لا حاجة لذكر ذلك على وجه التحديد، فالفضاء السيبراني جزء من اقليم الدول، والبنى التحتية السيبرانية موجودة في الأقاليم الثلاث، البرية البحرية والجوية، كما أنّه ليس بالضرورة انشاء قوات سيبرانية خاصة، وانما قد تقوم القوات المسلحة أو غير المسلحة، التي تعمل في البر أو البحر أو الجو، باستخدام الوسائل السيبرانية للرد على عمليات من النوع عينه. وقد ذهب خبراء دليل تالين في الاتجاه عينه، حين أكّدوا على أنه يحق لمجلس الأمن أن يسمح باللجوء الى تدابير سيبرانية غير قسرية، كقطع وسائل الاتصال، أو حتى الى اجراءات سيبرانية تصل الى مستوى القوة، اذا ما ما تبيّن له وجود تهديد أو انتهاك للسلم الدولي[42]. صحيح أنّ مجلس الأمن امتنع، حتى الآن، عن اللجوء الى خيار تقييد الاتصالات وقطعها لامكانية خرقها لحقوق الإنسان، إلّا أنّه لا يمكن انكار أنّ العمليات الإلكترونية قد تُوفّر، من الناحية المبدئية، طريقة لاستهداف الجهات والقوات المسؤولة عن خرق السلم الدولي وردعها، أو لوقف الاتصالات المحرّضة على ذلك، دون تعريض المدنيين للخطر[43].

ولكن، واذا كان اكتشاف المصادر أو العمليات التي تهدد السلم والأمن الدوليين أو التي ارتقت الى مستوى الأعمال العدوانية في الحالات التقليدية ليس بالمهمة الجد صعبة، الا أن الأمر قد يختلف في حالة العمليات التي تحصل أو يتم التحضير لها في الفضاء السيبراني. ففي بعض الأحيان، تقوم الدولة بزرع برنامج ضار كفيروس في نظام الدولة المُستهدفة قادر على تدمير النظام الالكتروني العائد لمحطة

[41] ميثاق الأمم المتحدة لعام 1945، المادة 52، مرجع سابق.
[42] François Delerue, Analyse du Manuel de Tallinn 2.0 sur le droit international applicable aux cyber opérations, op. cit., règle 76, p.68.
[43] للمزيد راجع: Michael Schmitt, "Computer Network Attack: The Normative Software", Yearbook of International Humanitarian Law, vol. 4, 2001, p.70.

نووية ولكنها تبقيه نائمًا. فهل اكتشاف هكذا فيروس لم يُفعّل يكفي لتصنيفه من قبل مجلس الأمن بأنه تهديد أو خرق للسلم والأمن الدوليين أو عدوانًا؟ والمشكلة الأكبر كيف سيحدد مجلس الأمن الجهة المسؤولة عن هذا البرنامج خصوصًا وأن عمليتي الاثبات والاسناد من أكثر المعضلات التي تفرضها هجمات الفضاء الالكتروني. ولكن وافتراضًا أنه تم اثبات مسؤولية احدى الدول، الا يُمكن لهذه الأخيرة أن تدّعي بأن الهدف من البرنامج المزروع جمع المعلومات فقط وليس تحقيق أضرار؟ مما يعني أن تعقيدات الهجمات الالكترونية وتطورها المتسارع سيشكل دون أدنى شك عائقًا أمام مُمارسة مجلس الأمن الدولي لمهمته الأساسية. يُضاف إلى كل ذلك أنّ الأمم المتحدة لا تمتلك قوات خاصة بها، وبالتالي ليس لديها القدرة على شن عمليات سيبرانية، فسيتعين عليها الاعتماد على الدول لتفعيل أي قرارات متعلقة بالفضاء السيبراني[44]، مما يعني أن ذلك رهن بإرادة الدول.

المطلب الثاني: موافقة مجلس الأمن الضمنية أو اللاحقة للرد على الهجمات السيبرانية

يمتلك مجلس الأمن سلطة تقديرية في اعتبار أي هجوم سيبراني تهديد أو خرق للسلم والأمن الدوليين أو عدوان، واصدار قرار يسمح باستخدام القوة لوضع حد له. ولكن وبما أنّ مجلس الأمن الدولي لم يُصدر حتى تاريخه أي قرار يسمح للدول التي تعرّضت لهجمات سيبرانية باستخدام القوة للرد، وبما أنّ الدول دائمة العضوية في المجلس قد تتردد في السماح بذلك بصورة صريحة لأسباب تقنية وسياسية وغيرها، كان لا بُدّ من البحث حول مدى مشروعية الرد القسري المستند الى إذن مجلس الأمن الضمني أو اللاحق **(لفرع الاول)** و العوائق أمام تكريس موافقة مجلس الأمن الضمنية أو اللاحقة **(الفرع الثاني)**.

الفرع الأول: مشروعية الرد القسري المستند الى إذن مجلس الأمن الضمني أو اللاحق

لتبيان مدى مشروعية اللجوء الى القوة للرد على هجوم سيبراني، في ظل غياب موافقة مجلس الأمن الصريحة والسابقة، لا بُدّ من القاء الضوء على حالة الاستناد الى موافقة مجلس الأمن الضمنية للرد قسرًا **(أولا)** والرد بالاستناد الى موافقة مجلس الأمن اللاحقة **(ثانيا)**.

أولًا: الاستناد الى موافقة مجلس الأمن الضمنية للرد قسرًا

تلجأ الدول في أحيانٍ كثيرة الى استخدام القوة استنادًا الى قرار صادر عن مجلس الأمن، رغم أنّه لا يتضمّن اذنًا صريحًا باللجوء الى التدابير القسرية، وبالتالي يستندون الى تفسيرات مُوسّعة أو ما يُطلَق عليه بالموافقة الضمنية. ولتأكيد مشروعية التصرفات القسرية التي تتّخذ بالاستناد الى الاذن الضمني، يستند أصحاب هذا الاتجاه الى عدد من السوابق الدولية. فعام 1991، دخلت قوات عسكرية تنتمي الى عدّة دول ومن بينها فرنسا، الولايات المتحدة الأميركية، ايطاليا وهولندا الى الأراضي العراقية، بهدف تأمين منطقة آمنة تسمح بعودة الأكراد العراقيين، المختبئين في الجبال من نظام الرئيس العراقي صدام حسين. وقد أسندت بعض الدول المُتدخلة تصرّفها إلى القرار رقم 688 الصادر عن مجلس الأمن[45]، الذي اعتبر أنّ قمع المدنيين يشكل تهديدًا للسلم والأمن الدوليين[46]. ولكن الاستناد الى هذا القرار، واستنتاج وجود موافقة ضمنية بالتدخل العسكري كان في غير محله. فالقرار رقم 688 افتقر الى أي اشارة إلى الفصل السابع من ميثاق

---

[44] ميثاق الأمم المتحدة لعام 1945، مرجع سابق، المادة 43، الفقرة 1: " يتعهد جميع أعضاء "الأمم المتحدة" في سبيل المساهمة في حفظ السلم والأمن الدولي، أن يضعوا تحت تصرف مجلس الأمن بناء على طلبه وطبقاً لاتفاق أو اتفاقات خاصة ما يلزم من القوات المسلحة والمساعدات والتسهيلات الضرورية لحفظ السلم والأمن الدولي ومن ذلك حق المرور"، إلّا أنّ هذه المادة لم تُترجم على أرض الواقع، ولم يتم تشكيل أي قوات تحت تصرُّف مجلس الأمن الدولي.

[45] مجلس الأمن الدولي، الحالة بين العراق والكويت، قرار رقم 688، تاريخ 1991/04/05، S/RES/688(1991).

[46] ومن بين هذه الدول، هولندا التي أعربت أنّ هذا القرار يشكل أساسا قانونيا للتدخل العسكري في العراق، للمزيد راجع: Netherlands State Practice, Netherlands Yearbook of International Law, 1992, p.362.

الأمم المتحدة، كما لم يتضمّن أي اذن للدول باتّخاذ "التدابير اللازمة"، وهي العبارة التي اعتاد مجلس الأمن ذكرها، حين يعطي الإذن للدول باللجوء الى القوة، حتى أنّ الفقرة الأخيرة من هذا القرار أعادت التأكيد على أنّ مجلس الأمن قرر ابقاء المسألة قيد النظر[47]، فكل ما أجازه للدول المشاركة في جهود الإغاثة الإنسانية[48]. وما يؤكد ذلك عدم تطرُّق المناقشات، التي سبقت اعتماد القرار المذكور أعلاه، إلى اي اقتراح للتدخل العسكري. يُضاف إلى كل ذلك، أنّ الدول التي شاركت في العملية لم تتوافق جميعها على هذه الحجة القانونية، وانما اعتبر بعضها أنّ تدخُّلهم يكتسب مشروعيته من القاعدة العرفية التي تكرّس حق التدخل الانساني[49]. إنّ هذا الإختلاف في الحجج المقدّمة لتبرير التدخل العسكري في العراق ما هو إلّا انعكاس لعدم قناعة الدول بوجود اذن ضمني يُستنتج من القرار رقم 688[50].

ويمكن الوصول الى الخلاصة عينها فيما خص تدخل حلف شمال الأطلسي في يوغوسلافيا عام 1999، والذي يُقدمه البعض على أنّه تكريس لحق استخدام القوة بالاستناد الى موافقة مجلس الأمن الضمنية. اذ استندت العديد من الدول المتدخلة الى القرارين رقم 1199 و1203 الصادرين عن مجلس الأمن لتشريع عملياتهم العسكرية[51]. إلّا أنّه وكما في حالة التدخل في العراق، لم تُكرِّس العمليات العسكرية ضد يوغوسلافيا شرعية التدخل بالاستناد الى الفصل السابع من ميثاق الأمم المتحدة، من دون اذن صريح من مجلس الأمن. صحيح أنّ هذا الأخير ذكر الفصل السابع عدة مرّات في قراراته، إلّا أنّه لم يسمح باتخاذ أي تدابير قسرية ضد يوغوسلافيا. وكما في الحالة السابقة، إنّ تعدد حجج الدول التي شاركت في العملية، بين من استند إلى موافقة مجلس الأمن الضمنية، وبين من استند إلى الحق بالتدخل لأسباب انسانية، ومعارضة عدد كبير من الدول الأخرى، يُؤكّد أنّه لا يوجد توجّه نحو تكريس حق اللجوء الى القوة بالاستناد الى موافقة مجلس الأمن الضمنية[52]. والأمر عينه يمكن استنتاجه من حالات أخرى كحالة التدخل الأميركي في أفغانستان وغيرها[53].

ممّا يسمح بالقول، أنه حتى في حالة الهجمات السيبرانية التي تشكّل تهديدًا أو انتهاكًا للسلم والأمن الدوليين، لا يُمكن الرد باستخدام القوة الّا اذا قرّر مجلس الأمن ذلك بقرار صريح.

---

47 مجلس الأمن الدولي، الحالة بين العراق والكويت، قرار رقم 688، مرجع سابق، فقرة 8.

48 المرجع نفسه، فقرة 6.

49 وهو ما عبّرت عنه المملكة المتحدة، للمزيد راجع: Christine Gray, "From Unity to Polarization: International Law and the Use of Force against Iraq", European Journal of International Law, vol. 13, no. 1, 2002, p. 9-10.

50 وهو ما عبّر عنه صراحةً وزير الخارجية البيلجيكي آنذاك، حين قال أنّه عند غياب اذن قانوني يجب خلقه، أي حين لا يوجد اذن واضح يسمح بالتدخل يمكن استنتاجه من قرارات مجلس الأمن، للمزيد راجع: Alain Daems, "L'absence de base juridique de l'opération Provide Comfort et la pratique belge en matière d'intervention armée « à but humanitaire »", Revue Belge de Droit International, vol. 1, 1992, p.266.

51 مجلس الأمن الدولي، قرار رقم 1199، الحالة المتعلقة بكوسوفو، تاريخ 1998/09/23، S/RES/1199 (1998)، متاح على: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N98/279/94/PDF/N9827994.pdf?OpenElement، تاريخ وساعة الزيارة: 2021/12/27، 14:40 ب.ظ.؛ مجلس الأمن الدولي، قرار رقم 1203، الحالة المتعلقة بكوسوفو، تاريخ 1998/10/24، S/RES/1203 (1998)، متاح على: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N98/321/19/PDF/N9832119.pdf?OpenElement، تالايخ وساعة الزيارة: 2021/12/27، 15:00 ب.ظ.

52 للمزيد راجع: Gerard Cahin, "Le rôle des organes politiques des Nations Unies", in Enzo Cannizzaro & Paolo Palchetti (eds), Customary International Law on the Use of Force, A Methodological Approach, Leinden/Boston, Martinus Nijhoff, 2005, p.170.

53 حصل هذا التدخل بالاستناد الى الدفاع المشروع، وليس الى حق التدخل الانساني، للمزيد راجع: مجلس الأمن الدولي، تهديدات السلم والأمن الدوليين التي تسببها أعمال إرهابية، قرار رقم 1368، تاريخ 2001/09/12، مرجع سابق.

ثانيًا: الرد بناءً على موافقة مجلس الأمن اللاحقة

مقابل من أكّدوا مشروعية الرد القسري المُستند الى موافقة مجلس الأمن الضمنية، هناك فئة أخرى اعتبرت أن الرد القسري يمكن أن يكتسب مشروعيته بمفعول رجعي، أي نتيجة لقرارٍ لاحقٍ من مجلس الأمن الدولي يُؤيّد هذا الرد أو على الأقل لا يُدينه. وهو ما يمكن أن يُساهم في حل المُعضلة، حين يكون الرد القسري الفوري الحل الوحيد أمام الدولة التي تتعرّض لهجمات إلكترونية من شأنها تهديد الأمن الدولي، أي في الحالة التي لا يمكنها انتظار صدور قرار عن مجلس الأمن. فهل كرّست الممارسات والمواقف الدولية هذا التوجُّه؟

في الواقع، من أجل دعم حججهم استند مؤيدو هذا التوجُّه الى عدد من الحالات، ومن بينها التدخل العسكري في سيراليون، عام 1998، بهدف اعادة الحكومة المُنتخبة شرعيًا الى السلطة، بعد أن تمّ اسقاطها بانقلاب[54]. وقد تمّ اعتبار أنّ هذه العملية مشروعة، نظرًا لاصدار مجلس الأمن قرارات لاحقة أثنت على جهود الجماعة الإقتصادية لدول غرب أفريقيا والمراقبين العسكريين التابعين لها[55]، أي القوات التي قامت بالعملية العسكرية، وتضمّنت تشكيل بعثة دولية للمراقبة لتعمل بالتعاون مع هؤلاء المراقبين العسكريين[56] ، وهو ما تمّ تفسيره على أنّه تأييد للعملية السابقة. الّا أنّ ذلك لا يتوافق مع مضمون قرارات مجلس الأمن ومع تصريحات رئيسه وحتى مع الحجج التي تمّ تقديمها من قبل بعض الدول المشاركة في العملية. اذ نفى البعض منها الطابع القسري للعملية، كما تبيّن أنها حصلت على موافقة مسبقة من السلطات المحلية للتدخل. أمّا من استند الى القرار رقم 1181 لاضفاء الشرعية على العملية، فذلك غير ممكن، اذ لم يتم تأييد العملية في أي فقرة من القرار[57]، وكان الهدف منه التأكيد على ضرورة معالجة الأزمة بطريقة سلمية، من خلال قوات حفظ السلم. كما انتقدت عدة دول هذه العملية، مؤكّدة على أن أي استخدام للقوة لا يكون مشروعًا، الا اذا حصل بالاستناد الى موافقة صريحة وواضحة من مجلس الأمن[58]. والأمر عينه يتبيّن من حالة التدخل في جورجيا، التي اعتبر البعض أنّها ساهمت في ولادة قاعدة تكرّس مشروعية استخدام القوة بمفعول رجعي، أي بقرار لاحق من مجلس الأمن[59]. الّا أنّ ذلك لا يتّفق مع مضمون قرار مجلس الأمن الذي أيّد إنشاء بعثة الأمم المتحدة للمراقبة وأدان التدخلات الغير مشروعة[60]. حتّى أنّ العديد من الدول التي شاركت أصرّت على أنّ هذه العملية لا تنضوي على طابع قسري، لعلمها بالحاجة الى قرار مسبق من مجلس الأمن لاستخدام القوة[61]. أخيرًا، لا بد من الإشارة إلى أنّ من يُعوّل على أنّ التدخل الدولي الذي استهدف ليبيا عام 2011 اكتسب مشروعيته نتيجة لقرار لاحق لمجلس الأمن، يتبيّن أنه كما في الحالات السابقة لا يمكن اثبات أي توجّه لتكريس هذا التوسُّع في تفسير الفصل السابع[62].

---

[54] للمزيد راجع: وليد الجرجري، دور الأمم المتحدة في إرساء الديمقراطية: دراسة تحليلية تطبيقية في إطار القانون الدولي العام، الطبعة الأولى، دار الأكاديميون للنشر والتوزيع، 2020، ص. 150.

[55] مجلس الأمن الدولي، الحالة في سيراليون، قرار رقم 1162، تاريخ 1998/04/17، S/RES/1162(1998)، فقرة 2.

[56] مجلس الأمن الدولي، الحالة في سيراليون، قرار رقم 1181، تاريخ 1998/07/13، S/RES/1181(1998)، فقرة 6.

[57] المرجع السابق، فقرة 5.

[58] للمزيد راجع: Erika De Wett, The Chapter VII Powers of the United Nations Security Council, Hart Publishing, UK, 2004, p.304.

[59] للمزيد راجع: Ugo Villani, « Les rapports entre l'ONU et les organisations régionales dans le domaine du maintien de la paix », Collected Courses of the Hague Academy of International Law, tome 1, 2001, 190, p. 413.

[60] مجلس الأمن الدولي، الحالة في جورجي، قرار رقم 858، تاريخ 1993/08/24، S/RES/858(1993)، الفقرة 2.

[61] Rapport établi par le Secrétaire général en application de la résolution 849 de 1993 du Conseil de sécurité, S/26250, 05/08/1993.

[62] مجلس الأمن الدولي، الحالة في ليبيا، قرار رقم 2009، تاريخ 2011/09/16، S/RES/2009(2011).

على ضوء ما تقدّم، يمكن القول أنّ الممارسات والمواقف الدولية لم تكرّس حق الدول باللجوء الى التدابير القسرية دون وجود موافقة مسبقة واضحة من مجلس الأمن الدولي، وهو ما يسري في حالة الدول التي تتعرّض لهجمات سيبرانية طالما لم يتم تكريس خلاف ذلك، وهو أمر مُستبعد ذلك أنّ التوسُّع في تفسير الفصل السابع يتعارض مع ميثاق الأمم المتحدة ومع قواعد ونصوص القانون الدولي.

الفرع الثاني: العوائق أمام تكريس موافقة مجلس الأمن الضمنية أو اللاحقة

تتعدّد العقبات التي تقف عائقًا أمام تكريس حق اللجوء الى القوة بالاستناد إلى موافقة مجلس الأمن الضمنية أو اللاحقة، لذلك لا بد من دراسة تعارض الموافقة الضمنية أو اللاحقة مع النظام القانوني الدولي **(أولا)** وتمسُّك الدول بالموافقة الصريحة السابقة **(ثانيا)**.

أولًا: تعارُض الموافقة الضمنية أو اللاحقة مع النظام القانوني الدولي

إنّ مراجعة سريعة لقواعد القانون الدولي، تُبيّن أنّ التوسُّع في تفسير هذه القواعد والنصوص، لاسيما تلك المُكرّسة في ميثاق الأمم المتحدة، لا يكون سليمًا إلّا اذا تماشى مع أهداف هذا الميثاق ومع ممارسات ومواقف الدول. ممّا يعني أنّ أي توسُّع في تفسير المادة 39 من ميثاق الأمم المتحدة سيتعارض حكمًا مع الهدف من الفصل السابع، ألا وهو المحافظة على الأمن الدولي. اذ إنّ الرد القسري، بالاستناد الى موافقة ضمنية أو لاحقة من مجلس الأمن، يتعارض أولًا مع المادة 27 من ميثاق الأمم المتحدة، التي تنص على أنّ قرارات مجلس الأمن تصدر بموافقة تسعة من أعضائه، يكون من بينها الأعضاء الدائمين[63]. ممّا يعني أنه حين توافق الدول على قرار معين وتصوّت ايجابًا عليه، تكون قد عبّرت عن موقفها الصريح، سواء من خلال التصويت أو من خلال المناقشات التي تسبق اعتماد القرار. فاذا وجدت أنّ من شأن استخدام القوة ازالة التهديد للأمن والسلم الدوليين أو وضع حد لانتهاكهما، يجب أن ينص القرار الصادر عنها صراحةً على ذلك[64]. فالمعيار هو القرار السابق للتصرف القسري وليس اللاحق له. يُضاف الى ذلك، أنّه حين يسمح مجلس الأمن باللجوء الى التدابير القسرية، يحتفظ لنفسه بحق مراقبة هذه التدابير، من خلال تقارير تُقدَّم له. فلو افترضنا أنّه يمكن للتدابير القسرية أن تكتسب مشروعيتها بقرار لاحق على حصولها، فكيف يُمكن لمجلس الأمن الدولي أن يُراقب هذه التدابير ويتأكّد من صحّتها؟ ولو افترضنا أنّ الدول استندت إلى موافقة ضمنية من مجلس الأمن واستخدمت القوة، فكيف ستقدّم تقارير عن أعمال لم يتم السماح بها أساسًا؟

يضاف ألى كل ذلك، إنّ الموافقة الضمنية أو اللاحقة لاستخدام القوة، بمقتضى الفصل السابع، تتعارض مع جوهر القانون الدولي، وتؤدي الى تحوّل الدولة المعتدية في بعض الأحيان إلى معتدى عليها والعكس صحيح. فلو افترضنا أنّ إحدى الدول تعرّضت لهجوم سيبراني وصل الى درجة الاعتداء المسلّح، وردّت بالاستناد إلى حق الدفاع المشروع، فماذا سيحصل لو تم القبول بفرضية اضفاء المشروعية على الهجمات السيبرانية بمقتضى قرار لاحق صادر عن مجلس الأمن الدولي؟ عندها تتحول الدولة التي ردّت على الهجوم الى معتدية، والمعتدية إلى مُعتدى عليها. هذه الحالات تضع النظام القانوني الدولي في حالة من الفوضى، وتسمح للدول بالتلاعب بالنصوص القانونية الدولية لمصلحتها، وتؤدي نتيجةً لذلك الى المساس بالأمن والسلم الدوليين[65].

---

[63] ميثاق الأمم المتحدة لعام 1945، مرجع سابق، المادة 27.

[64] للمزيد راجع: Linos-Alexandre Sicilianos, « L'autorisation par le Conseil de sécurité de recourir à la force: une tentative d'évaluation », Revue Générale de droit International Public, vol. 106, 2002, p.45.

[65] للمزيد راجع: Louis Henkin, "International Law and the Behaviour of Nations", Collected Courses, tome 114, 1965, p.261.

من هنا يُمكن القول، أنّ استخدام القوة السيبرانية أو التقليدية، من أجل الرد على هجمات إلكترونية تُشكّل تهديدًا للسلم الدولي، لا يكون مشروعًا إلّا إذا استند إلى قرار صريح من مجلس الأمن الدولي، وفقًا للفصل السابع من ميثاق الأمم المتحدة.

ثانيًا: تمسّك الدول بالموافقة الصريحة والسابقة

تمّت مناقشة امكانية الرد القسري بالاستناد الى موافقة ضمنية أو لاحقة من مجلس الأمن في مناسبات دوليةٍ عديدة. اذ تعاني الدول التي تتعرّض لعمليات من شأنها تهديد السلم الدولي أحيانًا كثيرة من تردُّد مجلس الأمن في اتخاذ القرارات الناجعة والسريعة، لاسيما وأنّ الحق في اصدار القرارات مبني في أغلب الأحيان على اعتبارات سياسية وليس قانونية. وقد بيّنت المناقشات التي سبقت اعتماد القرار رقم 2625 أنّه في معرض الحديث عن المادة 53 من ميثاق الأمم المتحدة، أبدت الدول تمسُّكها بضرورة أن يكون استخدام القوة من قبل أي منظمة أو وكالة، مَسبوقًا بقرار سابق وصريح من مجلس الأمن[66]. وتمّ التأكيد على أنّ اللجوء الى التدابير القسرية لا يكون مشروعًا اذا حصل خارج إطار الدفاع المشروع أو في ظل غياب موافقة صريحة من مجلس الأمن الدولي. ولم تُبدِ أي دولة اعتراضها على هذا التوجُّه. أمّا في المناقشات التي سبقت اعتماد تعريف للعدوان بموجب القرار رقم 3314، اعتبرت الولايات المتحدة الأميركية أنّ المادة 53 من ميثاق الأمم المتحدة لم تُحدّد ما اذا كانت موافقة مجلس الأمن الدولي يجب أن تكون سابقة أو لاحقة لتصرُّف المنظمات أو الوكالات، وما اذا كان يجب أن تكون صريحة أو ضمنية. ولم يلقَ الموقف الأميركي هذا تأييدًا إلّا من قبل مُمثّل إيطاليا، في حين لاقى اعتراضًا من قبل أغلب الدول المُشارِكة[67]. ولم تتوانَ الدول في الوثيقة الختامية للقمة العالمية لعام 2005 عن التأكيد على تمسُّكها بصلاحية مجلس الأمن الدولي المُكرّسة في ميثاق الأمم المتحدة، كونها ضمانة للمحافظة على السلم والأمن الدوليين، وان أي استخدام للقوة لا يستند الى نصوص هذا الميثاق يكون غير مشروعا[68].

إذًا، تمّ منح مجلس الأمن الدولي سلطة تحديد الإجراءات التي يراها مناسبة عند حصول تهديد أو خرق للسلم والأمن الدوليين أو في حالة العدوان. وصحيح أنّ هذه الصلاحية مُنِحت له قبل ظهور الفضاء السيبراني، إلّا أنّ ذلك لا يمنع من استخدامها حيال الهجمات السيبرانية. فقد تبيّن أنّ من حق مجلس الأمن الدولي، بالاستناد الى الفصل السابع، اصدار قرار يسمح باللجوء الى التدابير الضرورية ومن بينها تلك القسرية ردّا على هجمات إلكترونية تُهدد أو تنتهك السلم والأمن الدوليين. ولكن لا بد من أن يكون القرار واضحًا وصادر بصورة سابقة للتدبير.

الخلاصة

رغم اختلاف الدول حول كيفية تنظيم الفضاء السيبراني والهجمات التي تحصل من خلاله، بين داعٍ لاتفاقية دولية جديدة وبين رافض لذلك ومُتمسّك بقواعدِ القانون الدولي التقليدية، الا أنّ معظم الدول أكّدت خضوع الهجمات الالكترونية للقانون الدولي العام. وبما أنّه تبيّن أنّ من شأن الهجمات السيبرانية تهديد وانتهاك السلم والأمن الدوليين وحتى الإرتقاء إلى مستوى الأعمال العدوانية، فذلك يعني أنه يتوجب على مجلس الأمن– المُوكّل بالمحافظة على الأمن والسلم الدوليين– اتخاذ التدابير اللازمة بما فيها تلك التي تنضوي على استخدام

[66] للمزيد راجع: Olivier Corten, Le droit contre la guerre, op. cit., p. 638.
[67] مداخلة ممثل الولايات المتحدة آنذاك، للمزيد راجع: Special Committee on the Question of Defining Aggression, 3rd session, Summary records of the 52nd to 66th meetings, held at the Palais des Nations, Geneva, from 13 to 29/07/1970, vol. 1, available at: https://digitallibrary.un.org/record/802027?ln=en, accessed: 04/01/2022, 15:40 pm.
[68] Document finale du Sommet mondial de 2005, 20/09/2005, parag. 79-80, disponible sur: https://www.un.org/french/summit2005/documents.html, consulté le 16/11/2023, 15:10 pm.

القوة، لوضع حد لأي هجمات الكترونية تصل الى هذا المستوى. وقد منَح ميثاق الأمم المتحدة لهذا المجلس سلطة تُخوّله السماح للدول، للمنظات الاقليمية أو لقوات الأمم المتحدة، باتخاذ تدابير عسكرية وغير عسكرية في سبيل المحافظة على السلم والأمن الدوليين ووقف أي انتهاك أو تهديد لهما. ويتمتع مجلس الأمن بمقتضى الفصل السابع بسلطة تقديرية لتحديد التدابير الواجب اتخاذها، خلافا للدول والمنظمات التي لا تكتسب تصرفاتها، لاسيما العسكرية، المشروعية الا اذا حصلت تطبيقا لقرار صادر عن مجلس الأمن الدولي أو استنادًا الى حق الدفاع المشروع. وقرار المجلس يجب أن يكون واضحًا لا لبس فيه، اذ لا يمكن الاعتداد بالموافقة الضمنية أو اللاحقة لاضفاء المشروعية على ردود غير مشروعة لمواجهة الهجمات الإلكترونية.

إلّا أنه لا بُدّ من الاشارة، إلى أنه بالرغم من السلطات التقديرية الواسعة الممنوحة لمجلس الأمن والتي تُمكّنه من استخدام الفصل السابع سواء أكان الخطر أو العدوان ناتجًا عن عمليات تقليدية أو غير تقليدية، إلا أن مهمته في مجال مواجهة الهجمات السيبرانية لن تكون بالأمر اليسير. فطبيعة هذه الهجمات الغير مرئية التي تستخدم الفيروسات والديدان الالكترونية وسهولة شنّها وسرعتها المهولة التي تسمح لها بتحقيق أهدافها في غضون ثوانٍ دون ترك أي أدلة حول هوية المهاجم ومصدر العملية، يجعلان من عملية الرد والمواجهة في غاية الصعوبة، لاسيما وأن الوسائل التقليدية للرد قد تكون غير مفيدة وغير كافية. فكيف بامكان مجلس الأمن المحافظة على الأمن الدولي من التهديدات السيبرانية اذا كان من الصعب والمستحيل في أحيان كثيرة تحديد الجهة أو الجهات المسؤولة عنها، واثبات ارتباطها بها، دون أن ننسى أن الدول الأكثر تطورًا على صعيد تكنولوجيا المعلومات والأكثر خبرةً في هذا المجال هي نفسها عضو في مجلس الأمن الدولي، ولن تكون على استعداد للتخلي عن هذا السلاح المُتطوّر الذي يُوفّر لها امكانيات غير مسبوقة على المستويين الوطني والدولي، كما أنّ التنافس الخطير بين القطبين الصيني الروسي من جهة والأميريكي الأوروبي من جهة أخرى سيدفع كل جهة الى استغلال الفضاء السيبراني لتحقيق غاياتهم.

على ضوء ما تقدّم، وحفاظًا على السلم والأمن الدوليين من التهديدات السيبرانية، لا بد من تقديم المقترحات التالية:

–على مجلس الأمن الدولي عقد اجتماعات طارئة ومكثفة لتحديد معايير السلوك التي يجب على الدول التقيد بها عند استخدام تكنولوجيا المعلومات، والحدود التي يجب عدم تخطّيها والتي من شأنها أن تُشكل تهديدًا للسلم والأمن الدوليين، وتحديد سبل المواجهة التي تتلائم وطبيعة هجمات الفضاء السيبراني.

– على مجلس الأمن الدولي تفادي الردود العسكرية التقليدية أو السيبرانية التي تصل الى مستوى القوة، لأنّ من شأن ذلك أن يؤدي الى تفاقُم الخلافات وتزايد الأضرار المادية والبشرية، وصولًا إلى انتشار الفوضى وانتهاك السلم والأمن الدوليين.

– العمل على إبرام معاهدات ثنائية وإقليمية ودولية، أو اتفاقيات أو تعهدات غير رسمية كونها قادرة على الحد من خطورة الهجمات الإلكترونية وتأمين تبادل المعلومات. اذ من دون تفعيل التعاون الدولي والإقليمي في هذا المجال، ستستمر الدول بالتصرُّف دون قيد قانوني وستتحول ممارساتها، بمرور الوقت، إلى أمر مألوف وستُهدد الأمن والسلم الدوليين.

– العمل بأقصى سرعة على تحديد *"خطوط حمراء"* يُحظَّر تخطّيها عند شن الهجمات الإلكترونية، كحظراستهداف المستشفيات، شبكات الكهرباء، السدود، آبار النفط وغيرها. كما يجب أن يُصار إلى تحديد سبل المساءلة عند تجاوز هذه الخطوط.

– البدء بالتخطيط لإنشاء منظمة عالمية مُتخصصة بالشؤون السيبرانية تتمتع بالاستقلالية عن الأمم المتحدة، حيث لا تُمنَح فيها أي دولة امتيازات أو أفضلية؛ أو انشاء وكالة دولية خاصة بقضايا الأمن السيبراني تتولى مُهمة التحقيق والمساءلة وفرض العقوبات. كما يُمكن، وفي حال تعذُّر تحقيق أي من هذين الاقتراحين، تدعيم احدى وكالات الأمم المتحدة المُتخصّصة بالامكانيات والصلاحيات اللازمة للحد من المخاطر الإلكترونية والتمهيد لإتفاقيات في هذا المجال.

–على الدول اعتماد الوسائل التقنية التي تسمح لها بتفادي تعرُّضها لهجمات ذات طبيعة سيبرانية وحماية مصالحها، ومنها: جدران الحماية أو الجدران النارية Firewall، البرامج المضادة للبرمجيات الخبيثة وأنظمة كشف التسلُّل IDS. وبالإضافة إلى هذه التقنيات، هناك تدابير احتياطية بسيطة ذات مفعول كبير يمكن أن يتم اعتمادها، كعمليات فصل وتقسيم الشبكات، التشديد على بيانات الدخول وغيرها من التدابير.

"The Role of the United Nations Security Council in Addressing Cyberattacks under Chapter VII"

Abstract

In recent years, the international community has witnessed the rise of cyberattacks as one of the most serious non-traditional security challenges, given their ability to transcend geographical boundaries and cause severe human and material damage comparable to that resulting from traditional armed conflicts. This reality raises a fundamental legal question regarding the extent of the United Nations Security Council's jurisdiction, under Chapter VII of the UN Charter, to address such operations, considering them as threats or breaches of international peace and security, and even elevating them to the level of aggression.

This research examines the scope of the Security Council's discretionary powers, particularly in light of the evolving concept of international peace and security and its expansion to encompass threats of an economic, humanitarian, and environmental nature. It also explores the extent to which cyberattacks may be characterized as acts of aggression, and whether electronic means can be regarded as "weapons" in the legal sense, thereby justifying the use of coercive measures, including armed force. The study further discusses the legality of responding to cyberattacks, whether based on an explicit authorization from the Security Council or on implicit or subsequent approval, while highlighting the technical and legal challenges of attribution and the establishment of responsibility, as well as the practical limitations stemming from the absence of UN cyber forces.

The study is based on an analysis of the provisions of the UN Charter, relevant resolutions of the General Assembly and the Security Council, international judicial precedents, and scholarly opinions, employing a comparative analytical methodology that links traditional rules of international law with the requirements of cyberspace.

Keywords: Cyberattacks- Cyberspace- United Nations Security Council- Chapter VII- Aggression- International Peace and Security.