Journal of Anbar University for Law and Political Sciences
مجلة جامعة الانبار للعلوم القانونية والسياسية
P. ISSN: 2706-5804 E.ISSN: 2075-2024
Volume 13- Issue 2- December 2023 المجلد ١٣- العدد ٢ – كانون الاول ٢٠٢٣

# Cyber operations and the law of resorting to force

[1] Prof. Dr. Qasim Ahmad Qasim [2] helen abdulghany ramadhan.
College of Law/ University of Duhok

**Abstract:**

The state is seen as a key subject by international law, which governs relationships between its subjects by outlining their rights and obligation. The continual advancements and innovations that take place in the international community have presented a number of difficulties for the application of international law throughout history. The prohibition on the use of force is the most crucial principle. Recent developments in cyber operations rank among the most significant of these difficulties. The security of states and subsequently global peace and security are seriously threatened by these operations. This is a logical outcome of states' growing reliance on cyberspace. Despite this risk, there are currently no international agreements or norms that govern countries' use of cyber operations, which gives rise to the issue of how much and how to apply the traditional rules of international law to these operations since most of them emerged in a time that was not consistent with the development of cyber operations. There weren't any cyber operations, rather, their existence in the future was more like science fiction, Therefore, it is crucial to study them so that we can learn how to apply them, look for flaws in the current laws, and come up with fixes for them. In order to demonstrate the application of the law of resorting to the use of force, we will divide this research into two sections. In the first, we look at the rule prohibiting the use of force on cyber operations, and in the second we will discuss the practice of self-defense against cyber operations.

**1: Email:**
haidiabdulghany@yahoo.com

**2: Email**:
qasim.ahmed@uod.ac

DOI
10.37651/aujlps.2023.142788.1065

Submitted: 29/9/2023
Accepted: 10/10/2023
Published: 05/12/2023

**Keywords**:
cyber operations
effects
data
Critical Infrastructure
armed attack.

# العمليات السيبرانية وقانون اللجوء إلى القوة

[١] أ.د قاسم أحمد قاسم [٢] هيلين عبدالغني رمضان
كلية القانون/ جامعة دهوك

**الملخص:**

ينظم القانون الدولي العلاقات بين أشخاصه من خلال بيان حقوقهم وواجباتهم ويعتبر الدولة شخصاً رئيسياً فيه، وواجه تطبيق القانون الدولي على مر العصور تحديات مختلفة نظراً للتطورات المستمرة والابتكارات التي تظهر في المجتمع الدولي ومن أهم هذه القواعد هو حظر استخدام القوة، وتعتبر العمليات السيبرانية والتي ظهرت منذ زمن ليس ببعيد من أهم هذه التحديات، وتشكل هذه العمليات خطورة كبيرة على أمن الدول وبالتالي السلم والأمن الدوليين وهذه نتيجة طبيعية للاعتماد المتزايد من جانب الدول على الفضاء السيبراني. وبالرغم من هذه الخطورة لا يوجد حتى الآن اتفاقية دولية أو أعراف دولية تنظم لجوء الدول للعمليات السيبرانية مما تؤدي إلى ظهور مشكلة مدى وكيفية تطبيق القواعد التقليدية للقانون الدولي على العمليات السيبرانية وذلك لأنها ظهرت في فترة زمنية لم تكن العمليات السيبرانية موجودة، من هنا تظهر أهمية دراستها حيث يمكننا معرفة كيفية تطبيقها والبحث عن أوجه القصور الموجودة في القواعد الحالية وإيجاد الحلول لها، ومن أجل بيان تطبيق قانون اللجوء لاستخدام القوة سنقسم هذا البحث إلى مبحثين نبحث في الأول تطبيق قاعدة حظر استخدام القوة على العمليات السيبرانية، أما الثاني فسنبحث فيه عن ممارسة حق الدفاع عن النفس ضد العمليات السيبرانية.

**الكلمات المفتاحية:**

**العمليات السيبرانية، الآثار، البيانات، البنية التحتية الحيوية، الهجوم المسلح.**

## المقدمة

### أولاً: موضوع الدراسة

بعد توسع المجتمعات البشرية وازدياد حاجاتها حاول الإنسان البحث عن وسائل الاتصال والتكنولوجيا وتطويرها لخدمة مصالحهم وتسهيل حياتهم، وبالفعل شهد المجتمع البشري في مطلع القرن الحادي والعشرين تطوراً كبيرا في وسائل الاتصال والتكنولوجيا، وأصبحت هذه الوسائل جزءاً لا يتجزأ من حياة الأفراد العادية بالإضافة إلى القطاع العام والخاص الذي يعتمد بصورة كبيرة عليه نظراً لما يوفره الاعتماد هذا من السهولة والسرعة والتنظيم في غاية الدقة في أداء مهامها. ولكن وشبيهاً بكثير من الابتكارات البشرية كان لهذا التطور جوانب سلبية منها ظهور مجال آخر يتسم بخصائص فريدة ومغرية للجهات المتعددة وعلى مختلف المستويات من الأفراد والدول والمنظمات والجماعات لاستخدامها ضد الغير في سبيل تحقيق مصالحها، أو بمعنى آخر ظهر مجال آخر للتهديد وهو مجال الفضاء السيبراني أو ما يسمى بالفضاء الرقمي وبالتالي ظهور مجال جديد بالإضافة للمجالات التقليدية الأخرى (البرية، البحرية، الجوية، الفضاء الخارجي)، ومنذ ظهورها اهتم الأكاديميون والدول بدراسة العمليات السيبرانية في ظل قانون لجوء الدول لاستخدام القوة[١] ومدى شرعيتها من عدمه.

### ثانياً: أهمية الدراسة

يعد تناول موضوع العمليات السيبرانية بحد ذاته في غاية الأهمية، ويرجع ذلك لكون العمليات السيبرانية أصبحت في اليوم أمراً لا مفر منه وذلك بسب الاعتماد المتزايد على الفضاء السيبراني من قبل الجهات المختلفة نظراً لصعوبة القيام بالمهام بدونه والسهولة والسرعة التي يوفرها هذا الفضاء في تنفيذ المهام هذه.

فضلاً عن أن دراسة العمليات السيبرانية في نطاق قانون اللجوء إلى القوة له أهمية خاصة، فمن المعلوم بأن قانون اللجوء إلى القوة يشكل أحد الأركان الأساسية للنظام القانوني الدولي، وذلك كونها نتيجة طبيعية وانعكاساً لأهم الأهداف التي تقوم عليه منظمة الأمم المتحدة ألا وهي حفظ السلم والأمن الدوليين كما أنه من أهم مبادئها هو حظر استخدام القوة، وما يبرز

(١) يطلق عليها أيضاً قانون مسوغات الحرب أو "قانون اللجوء إلى الحرب (قانون اللجوء إلى القوة) - jus ad bellum" أو "قانون منع الحرب- jus contra bellum"، ويشير إلى الظروف التي يمكن للدول فيها اللجوء إلى الحرب أو إلى استخدام القوة المسلحة. ويعتبر حظر استخدام القوة بين الدول والاستثناءات المنصوص عليه في ميثاق الأمم المتحدة لعام ١٩٤٥، هي المكونات الأساسية لهذا القانون، ينظر:- "اللجنة الدولية للصليب الأحمر، القانون الدولي الإنساني: إجابات على أسئلتكم:، (٢٠١٤): ص ٨؛ "اللجنة الدولية للصليب الأحمر، القانون الدولي الإنساني: إجابات على أسئلتكم"، (٢٠٠٧): ص ١٤.

أهمية الدراسة هو أن كل من ميثاق الأمم المتحدة، وقرار تعريف العدوان استخدمت مصطلح (استخدام القوة المسلحة)، و(هجوم مسلح)، وهي مصطلحات لا تنسجم مع التصورات السيبرانية مما يضعها ظاهرياً خارج نطاق القانون الدولي، فالأمر يحتاج الى تفسيرات فقهية تستوعب هذا التطور الهائل وقواعد واتفاقات دولية تواكب المتغيرات الدولية.

**ثالثاً: مشكلة الدراسة**

بخلاف العمليات التقليدية التي تحصل في ميدان مادي، تقع العمليات السيبرانية في ميدان غير ملموس تختلف عن المجالات الأخرى كما أنها عمليات مستحدثة ظهرت بعد وضع قانون اللجوء إلى القوة، ومن هذا المنطلق يتجسد جوهر مشكلة الدراسة فيما يأتي: ما هو مدى قابلية تطبيق قانون اللجوء إلى القوة على العمليات السيبرانية، ومدى كفايتها للتحديات التي تطرحها الطبيعة الخاصة لهذه العمليات وبشكل خاص في ظل وجود هذه القواعد القانونية في زمن سابق لظهور تلك العمليات التي كانت مجرد خيال علمي، وما هو مدى استجابة هذه القواعد للتطبيق على العمليات السيبرانية في زمن كانت القوة المسلحة تنطوي على استخدام الأسلحة الحركية وميدان مادي.

**رابعاً: فرضية الدراسة**

تقوم دراستنا على الفرضية التالية: يتسم الفضاء السيبراني وهي الفضاء الذي ينفذ فيه العمليات السيبرانية بخصائص مختلفة عن المجالات التقليدية الأخرى (البرية، البحرية، الجوية، الفضاء الخارجي) وبالتالي وبالرغم من أنه يمكن تطبيق القواعد القانونية الدولية السارية عليه إلا أن هناك بعض الحالات والمشاكل التي لا يمكن مواجهتها بالقواعد الحالية كما هي مما يؤدي بالضرورة إلى وضع قواعد جديدة يتفق مع خصائصها المميزة.

**خامساً: نطاق الدراسة**

إن العمليات السيبرانية قد تنفذها جهات متعددة كالأفراد والجماعات المسلحة والإرهابيين والقطاع الخاص والمنظمات الدولية والدول ولكن دراستنا تقتصر على تلك العمليات السيبرانية التي تجري بين الدول فقط ويتم اسنادها لها طبقاً لقواعد الإسناد في القانون الدولي، وبالتالي تخرج من نطاقنا العمليات السيبرانية التي تجريها الجهات الأخرى.

**سادساً: منهجية الدراسة**

إن طبيعة هذا الموضوع تستدعي اتباع المنهج الوصفي مع المنهج التحليلي، فسنستخدم المنهج الوصفي لغرض وصف هذه العمليات وآثارها والمشاكل التي تجري في الفضاء السيبراني ومن ثم نستعين بالمنهج التحليلي من أجل تحليل القواعد القانونية وآراء الفقهاء وأحكام القضاء الدولي للوصول إلى معرفة كيفية تطبيقها على العمليات السيبرانية من خلال بيان المشاكل التي تواجه كيفية تطبيق هذا ووضع الحلول المناسبة لها.

**سابعاً: هيكلية الدراسة**

من أجل معالجة مشكلة الدراسة واثبات صحة الفرضيات من عدمها فقد ارتأينا توزيع الدراسة على مبحثين تسبقها مقدمة، جاء المبحث الأول بعنوان تطبيق قاعدة حظر استخدام القوة على العمليات السيبرانية، وتم تقسيمه إلى مطلبين الأول نخصصه لبيان مدى شمول العمليات السيبرانية بحظر استخدام القوة، وثانيهما لبيان الحد الأدنى لاعتبار العمليات السيبرانية استخداماً للقوة، أما المبحث الثاني فقد تم تخصيصه لبحث ممارسة حق الدفاع عن النفس ضد العمليات السيبرانية، وتم تقسيمه أيضا على مطلبين يعرض الأول منهما الشروط المتعلقة بفعل العدوان، وثانيهما خصص لشروط المتعلقة بفعل الدفاع. وقد ختمنا الدراسة بخاتمة عرضنا فيها أهم الاستنتاجات والمقترحات.

## I. المبحث الأول

## تطبيق قاعدة حظر استخدام القوة على العمليات السيبرانية

من المعلوم بأن ميثاق الأمم المتحدة قد وضع في فترة زمنية لم تكون العمليات السيبرانية موجودة، بل حتى لم يكون بالإمكان التخيل بوجودها في المستقبل، وكان الهدف الأساسي من تأسيس المنظمة هو حفظ السلم والأمن الدوليين[١]، ولذلك يعتبر الحظر الوارد على استخدام القوة في الميثاق من أهم المبادئ الذي تقوم عليها المنظمة، إذ تنص المادة (٢/ ٤) منه على أنه "تعمل الهيئة وأعضاؤها في سعيها وراء المقاصد المذكورة في المادة الأولى وفقاً للمبادئ الآتية:...٤- 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.."، لذلك ومنذ ظهور العمليات السيبرانية ظهرت التساؤلات حول مدى امكانية شمول العمليات السيبرانية بهذا الحظر، فهل يمكن أن تصل العملية السيبرانية لعتبة استخدام القوة طبقا للقانون الدولي أم لا، للإجابة على هذا سؤال سنقسم هذا المبحث لمطلبين، في المطلب الأول نبين امكانية شمول العمليات السيبرانية بالحظر الوارد في المادة (٢/ ٤) من ميثاق الأمم المتحدة، أما في المطلب الثاني سنناقش فيه الحد الادنى اللازمة لاعتبار العمليات السيبرانية استخداماً للقوة.

### I.أ. المطلب الأول

### مدى شمول العمليات السيبرانية بحظر استخدام القوة

طبقاً للمادة (٢/ ٤) من ميثاق الأمم المتحدة تحظر على الدول اللجوء لاستخدام القوة في علاقاتهم أو التهديد بها، ولتطبيق هذه المادة في السياق السيبراني تم اثارة سؤال حول مدى امكانية اعتبار العمليات السيبرانية قوة وبالتالي يحظر استخدامها من قبل الدول.

(١) إذ تنص المادة (١)، من الميثاق على أنه "مقاصد الأمم المتحدة هي: ١- حفظ السلم والأمن الدولي...."

وبلا شك يتطلب تحديد ما إذا كانت العمليات السيبرانية تنتهك الحظر الوارد على استخدام القوة طبقاً للمادة (٢/ ٤) من ميثاق الأمم المتحدة أم لا يتوقف على تفسير مصطلح (القوة) الواردة في المادة المذكورة، وذلك لأن القوة مصطلح واسع ويشمل بجانب القوة المسلحة جميع الأنواع الأخرى من القوة كالقوة الاقتصادية والسياسية والايدولوجية وغيرها، فهل القوة المقصود تحريمها في المادة (٢/ ٤) يشمل جميع صور القوة أو فقط القوة المسلحة دون غيرها؟ للإجابة على هذا التساؤل ظهر اتجاهين:-

**الاتجاه الواسع:** يرى هذا الاتجاه أن مصطلح القوة في المادة (٢/ ٤) يشمل القوة المسلحة وغير المسلحة، وبالتالي يشمل الاكراه والقوة الاقتصادية والسياسية وغيرها[١]، ومنهم مثلاً يذهب هانز كلسن أن عبارة القوة الواردة في المادة (٢/ ٤) من الميثاق تشمل أيضا الإجراءات الاقتصادية التي تنطوي على الضغط والقسر الدوليين مستنداً في ذلك إلى نص المادة (٤١ و٤٢) من ميثاق الأمم المتحدة، وهما النصان اللذان يتحدثان عن التدابير العسكرية وغير العسكرية التي يجوز لمجلس الأمن أخذها ويمكن أن يتحقق بها القسر الدولي، مما ينبغي معه القول أن الميثاق يعتبر معنى القوة ممكن التحقيق عن طريق التدابير الاقتصادية العسكرية المبينة في النصين المتقدمين[٢]، كما أنه في بعض الأحوال قد يكون استخدام الضغط الاقتصادي أو السياسي أو الاستراتيجي مهدداً للاستقلال السياسي للدول يعادل في خطورته استخدام القوة المسلحة[٣].

**الاتجاه الضيق:** يذهب هذا الاتجاه إلى أن المقصود بالقوة هو القوة المسلحة فقط دون الأنواع الأخرى من القوة [٤]، ويستند هذا الاتجاه فيما ذهبوا إليه إلى عدة حجج هي[٥]:

**الحجة الأولى:** أنه ولغرض التفسير يجب علينا الرجوع الى القواعد المتعلقة بالتفسير الواردة في اتفاقية فيينا لقانون المعاهدات لعام (١٩٦٩)، وبالرجوع إلى الاتفاقية المذكورة نجد أنها تنص على أنه "تفسر المعاهدة بحسن النية ووفقًا للمعنى الذي يعطي لألفاظها ضمن السياق

(١) د. السيد مصطفى أحمد أبو الخير، *المبادئ العامة في القانون الدولي المعاصر*، ط ١، (القاهرة: ايتراك للطباعة والنشر والتوزيع، ٢٠٠٦)، ص ٢٥٧.

(2) Hans Kelsen, Principles of International Law, 2nd Edition, 1967, p 84.

(٣) نقلاً عن: د. صالح جواد الكاظم، *دراسة في المنظمات الدولية*، (بغداد: مطبعة الارشاد، ١٩٧٥)، ص ١٥٢.

(٤) ينظر: د. حسن الجلبي، *مبادئ الأمم المتحدة وخصائصها التنظيمية*، (القاهرة: معهد البحوث والدراسات العربية، ١٩٧٠)، ص ٤٠- ٤٣؛ د. سمعان بطرس فرج الله، "تعريف العدوان"، بحث *منشور في المجلة المصرية للقانون الدولي*، المجلد الرابع والعشرون، (١٩٦٨): ص ٢٢٠.

(٥) ينظر: د. سامي جاد عبدالرحمن واصل، *ارهاب الدولة في اطار قواعد القانون الدولي العام*، (الاسكندرية: دار الجامعة الجديدة للنشر والتوزيع، ٢٠٠٨)، ص ١٩٣.

الخاص بموضوعها والغرض منها"[١]، وفيما يتعلق بالسياق الذي ظهرت فيه كلمة القوة في الميثاق فنجد أنها استخدمت في أكثر من موضع تسبقها صفة مسلحة وذلك في ديباجة الميثاق و في المادتين (٤١ و ٤٦ و٥١)[٢]، وكذلك وبالاستناد إلى موضوع وهدف الميثاق، فإن (القوة) يجب أن تقرأ بشكل ضيق، لأن الهدف الصريح من انشاء منظمة الأمم المتحدة هو الحفاظ على السلم والأمن الدوليين، وإنقاذ الأجيال المقبلة من ويلات الحرب، وهذا يشير إلى أن فكرة القوة عند وضع الميثاق كانت مقتصرة على القوة المسلحة دون غيرها[٣].

**الحجة الثانية:** هذا التأويل يتفق مع حقيقة ما تقضى به الأعمال التحضيرية لوضع الميثاق[٤]، لأنه قدمت برازيل اقتراحاً إلى لجنة صياغة هذه المادة لتوسيع نطاق المادة (٢/ ٤) ليشمل الضغوط الاقتصادية إلا أنه تم رفض الاقتراح المذكور في النهاية، وأشار واضعو المسودة إلى أن تحديد ما إذا كانت دولة ما قد استخدمت القوة في انتهاك للمادة (٢/ ٤) يركز فقط على الأدوات العسكرية، كما أثيرت نفس المسألة مرة أخرى عند صياغة اعلان بشأن مبادئ القانون الدولي المتعلقة بالعلاقات الودية والتعاون بين الدول وفقاً لميثاق الأمم المتحدة لعام (١٩٧٠)، حيث اثارت التساؤل حول ما إذا كانت (القوة) تشمل جميع أشكال الضغط، بما في ذلك تلك التي ذات الطابع السياسي أو الاقتصادي والتي لها تأثير يهدد السلامة الإقليمية أو الاستقلال السياسي لأي دولة، ولكن تم الرد بالنفي عليها[٥].

**الحجة الثالثة:** تشير الوثائق الصادرة من الأمم المتحدة واللاحقة للميثاق إلى القوة المسلحة فقط ومنها مثلاً إعلان مبادئ القانون الدولي المتصلة بالعلاقات الودية والتعاون بين الدول وفقا لميثاق الأمم المتحدة لعاك (١٩٧٠) مع هذا التفسير، مشيراً إلى حظر استخدام القوة في

---

(١) المادة (٣١ /١)، من اتفاقية فيينا لقانون المعاهدات لعام (١٩٦٩).

(٢) ورد في ديباجة الميثاق بأنه "..وأن نكفل بقبولنا مبادئ معيّنة ورسم الخطط اللازمة لها ألاّ تستخدم القوة المسلحة في غير المصلحة المشترك..."، أما المادة (٤١)، فتنص على "لمجلس الأمن أن يقرر ما يجب اتخاذه من التدابير التي لا تتطلب استخدام القوات المسلحة..."، في حين ورد في المادة (٤٦)، "الخطط اللازمة لاستخدام القوة المسلحة.."، وتنص المادة (٥١)، فتنص على أنه "... في الدفاع عن أنفسهم إذا اعتدت قوة مسلحة...".

(٣) ديباجة ميثاق الأمم المتحدة.

(٤) وفقًا للمادة (٣٢)، من اتفاقية فيينا لقانون المعاهدات (١٩٦٩)، تعتبر الأعمال التحضيرية وسيلة تكميلية لتفسير المعاهدة.

(٥) ينظر: د. قاسم أحمد قاسم، "حق الدفاع عن النفس في القانون الدولي المعاصر (دراسة تحليلية مقارنة)"، مقارنة)"، (اطروحة دكتوراه مقدم إلى كلية القانون- جامعة صلاح الدين، ٢٠٠٨)، ص ١٠٠؛ د محمود حسين الشرقاوي، مصدر سابق، ص ١٩٨؛

Marco Roscini, Cyber Operations and the Use of Force in International Law, Oxford University Press, 2014, p 45; Michael N. Schmitt (GEN. ED.), Tallinn manual on the international law applicable to cyber warfare, prepared by the International Group of Experts at the invitation of the NATO CCDCOE, Cambridge University Press. Cambridge, 2013, commentary to Rule 11, Para 2.

سياق القوة المسلحة، ويشير فقط إلى المسائل الاقتصادية والسياسية فيما يتعلق بواجب عدم التدخل في الشؤون الداخلية، وكذلك قرار الجمعية العامة بشأن تعريف العدوان رقم (٣٣١٤) عام (١٩٧٤) الذي عرف العدوان في المادة الأولى منه بأنه "استخدام القوة المسلحة..." وكذلك إعلان الجمعية العامة (٢٢/ ٤٢) في (١٨ نوفمبر ١٩٨٧) بشأن تحسين فعالية مبدأ الامتناع عن التهديد بالقوة أو استخدامها في العلاقات الدولية[١].

وهذا هو موقف فريق المعد لـ(دليل تالين ١)[٢] أيضاً حيث أقروا بأن مفهوم القوة يفهم تقليدياً بأنها القوة المسلحة[٣]، وبناء على ما تقدم تبين لنا أن الراجح هو الاتجاه الضيق وبالتالي يشمل الحظر الوارد في المادة (٢/ ٤) القوة المسلحة فقط دون غيرها، وهنا يثار تساؤل حول مدى امكانية اعتبار العمليات السيبرانية استخداماً للقوة المسلحة أم لا؟ للإجابة على هذا السؤال ظهرت ثلاثة اتجاهات فقهية وكما يلي: -

**الاتجاه الأول: الاتجاه القائم على الأداة**

يركز النهج القائم على الأداة على الوسائل المستخدمة للقيام بعمل ما، أي الأسلحة، بمعنى التركيز على الأدوات المحددة بخصائصها الفيزيائية وبالتالي لكي يعد عمل ما بأنه استخدام قوة مسلحة يجب أن يكون القيام به عن طريق أسلحة ذات خصائص فيزيائية، وذلك لأنه طبقاً لهذا الاتجاه ما يميز القوة المسلحة عن الاكراه الاقتصادي أو السياسي هو الاستخدام

(1) Marco Roscini, Op. Cit. p 46; Haataja, Samuli, Cyber Attacks and International Law on the Use of Force: an Informational Approach, Thesis (PhD Doctorate), Griffith Law School , 2016, P 83.

(٢) بعد الأحداث التي وقعت في إستونيا في عام ٢٠٠٧ قامت "CCDCOE" بدعوة فريق من الخبراء الدوليين بدراسة قابلية تطبيق المبادئ القانونية على العمليات السيبرانية وجمعها في دليل بعنوان "دليل تالين"، وهي وثيقة غير ملزمة قانوناً، إلا أنها بدون شك مبادرة رائدة في إرساء قواعد القانون الدولي المطبقة على العمليات السيبرانية، وصدرت حتى الآن اصدارين من هذا الدليل ويتم العمل حالياً على مشروع النسخة الثالثة من دليل تالين ينظر: د. محمد عادل محمد عسكر، "وضع العمليات السيبرانية في القانون الدولي مع التطبيق على ممارسة التجسس في وقت السلم (دراسة على ضوء دليل تالين بشأن القانون الدولي المطبق على العمليات السيبرانية ٢٠١٣- ٢٠١٧)"، *بحث منشور في مجلة البحوث القانونية والاقتصادية تصدرها كلية الحقوق بجامعة بني سويف*، المجلد ٣٣، العدد ١، ص ٣١١- ٣١٢، ص ٤٨٣، د. زينب رياض جبر، *التجسس الرقمي في ضوء قواعد القانون الدولي العام*، ط ١، (القاهرة: المركز العربي للدراسات والبحوث العلمية للنشر والتوزيع، ٢٠٢٣)، ص ١٨٩؛

The CCDCOE Invites Experts to Contribute to the Tallinn Manual 3.0: https://ccdcoe.org/news/2021/the-ccdcoe-invites-experts-to-contribute-to-the-tallinn-manual-3-0/ تاريخ الزيارة (٢٠٢٣/ ٤/ ٩)

(3)Michael N. Schmitt (GEN. ED.), Tallinn manual on the international law applicable to cyber warfare, Op. Cit. commentary to Rule 11, para 9 (F).

القسري للأسلحة، وقد تم استخدامه تقليديًا للتمييز بين القوة المسلحة التي يشملها الحظر الوارد على استعمال القوة وبين الأنواع الأخرى من القوة التي لا يشملها كالإكراه الاقتصادي أو السياسي[١].

وبالرغم من أن المادة (٤١) من الميثاق تدعم هذا الرأي، حيث تنص على أنه "لمجلس الأمن أن يقرر ما يجب اتخاذه من التدابير التي لا تتطلب استخدام القوات المسلحة لتنفيذ قراراته، وله أن يطلب إلى أعضاء الأمم المتحدة تطبيق هذه التدابير، ويجوز أن يكون من بينها وقف الصلات الاقتصادية والمواصلات الحديدية والبحرية والجوية والبريدية والبرقية واللاسلكية وغيرها من وسائل المواصلات وقفا جزئياً أو كليا وقطع العلاقات الدبلوماسية"، إلا أنه رفض معظم الباحثين الأخذ بها نظراً لأن العمليات السيبرانية يمكن أن تسبب ضرراً كارثياً دون استخدام الأسلحة التقليدية، والأخذ بهذا النهج يستبعد اعتبار العمليات السيبرانية استخداماً للقوة المسلحة نظراً لعدم استخدام الأسلحة الحركية فيه، فإن كان النهج القائم على الأدوات أكثر دقة في الماضي، ولكن مع تطوير تقنيات ووسائل حرب جديدة لا تشبه الأسلحة التقليدية فقد الكثير من بروزها ومزاياها ويعتبر نهجاً تقليدياً عفا عليها الزمن وبالأخص بعد إصدار محكمة العدل الدولية بشأن مشروعية التهديد بالأسلحة النووية أو استخدامها السابقة ذكرها[٢].

**الاتجاه الثاني: الاتجاه القائم على الهدف**

يركز هذا النهج على الهدف من العمليات السيبرانية ويعتبرها استخداماً للقوة المسلحة عندما تستهدف أنظمة البنية التحتية الوطنية الحيوية، ويبررون قولهم هذا بأنها يتناسب مع الطبيعة المدمرة الفورية للعمليات السيبرانية، فبمجرد أن يستهدف المهاجم السيبراني البنية التحتية الحيوية يمكن القول بأن هناك مستوى كافٍ من الضرر لتبرير اعتبار الفعل كالقوة المسلحة، وبالتالي تبرير الدفاع عن النفس، ويذهب هذا الاتجاه أنه حتى مجرد التجسس على

(1)Oliver Dörr, Use of Force, Prohibition of. IN The Max Planck Encyclopedia of Public International Law, Rüdiger Wolfrum (ed.), Oxford University Press, vol. VIII, 2012, p 611; Marco Roscini, Op. Cit. P 46.

(2)ona A. Hathaway and others, The Law of Cyber-Attack, California Law Review, vol. 100:817, 2012, P 846; Duncan Hollis, Why States Need an International Law for Information Operations, Lewis and Clark Law Review, Vol. 11, 2007, P 1041; Matthew C Waxman, Self-Defensive Force against Cyber Attacks: Legal-Strategic and Political Dimensions, International Law Studies, Vol 89, 2013, p 111; Marco Roscini, World Wide Warfare – Jus ad bellum and the Use of Cyber Force, Max Planck Yearbook of United Nations Law, Vol 14, 2010, p 106.

معلومات عسكرية حساسة يمكن أن يعد أيضاً استخداماً للقوة المسلحة، ويبررون الدفاع عن النفس ضدها[١].

ويؤخذ على هذا الرأي بأنه نهج شامل للغاية من حيث أنه سيكون سبباً لاعتبار تلك العمليات السيبرانية التي تسبب فقط إزعاجاً أو تهدف فقط إلى جمع المعلومات استخداماً للقوة طالما أنها تستهدف أنظمة البنية التحتية الحيوية بغض النظر عن شدتها أو خصائصها، بالإضافة إلى عدم وجود تعريف مقبول بشكل عام للبنية التحتية الحيوية[٢]، إضافة إلى ذلك قد تكون آثار العمليات السيبرانية عشوائية، وبالتالي قد لا تستهدف العملية السيبرانية عمداً البنية التحتية الحيوية التي تم تعطلها كأثر جانبي للعملية[٣]، وفي الحقيقة وإن كان لا يمكن الأخذ بهذا الاتجاه في حد ذاته لتحديد العملية السيبرانية على أنها استخدام للقوة، إلا أنها لا تزال ذات صلة، حيث يمكن النظر في طبيعة البنية التحتية المستهدفة عند تقييم آثار العمليات السيبرانية كما سنأتي إليه لاحقاً.

**الاتجاه الثالث: الاتجاه القائم إلى النتائج**

وفقاً لها الاتجاه يتم تقييم العملية السيبرانية بناءً على آثاره، فالتركيز هو على آثار العملية السيبرانية هل تتشابه آثار استخدام القوة المسلحة أم لا، وبمعنى آخر وطبقاً لهذا الرأي ما يهم ليس نوع السلاح المستخدم ولكن النتيجة النهائية عندما تصيب الهدف[٤].

(1)Walter Gary Sharp, Sr., Cyberspace and the Use of Force, Aegis Research Corporation, Virginia, 1999,P 129; Christopher C. Joyner and Catherine Lotrionte, Information warfare as international coercion: Elements of a legal framework. IN The Use of Force in International Law (The International Law of Peace and Security), Nicholas Tsagourias and Tarcisio Gazzini (eds.), Routledge, London and New York, 2016, 825.

(2) Marco Roscini, Cyber Operations and the Use of Force in International Law, Op.Cit. P 47.

(3) Michael Gervais, Cyber Attacks and the Laws of War, Berkeley Journal of International Law, Vol. 30 2012, p 538.

(٤) ينظر:- د. محمود حسين الشرقاوي، مصدر سابق، ص ٢٠٣؛

Yoram Dinstein, Computer Network Attacks and Self-Defense, International Law Studies, Vol. 76, 2002, p 103, Marco Roscini, Cyber Operations and the Use of Force in International Law, Op.Cit. P 47; François Delerue, Cyber Operations and International Law, Cambridge University Press, Cambridge, 2020, P 289.

وتبرر هذا الاتجاه ما أقرته فتوى محكمة العدل الدولية بشأن مشروعية التهديد بالأسلحة النووية أو استخدامها [١] والتي ذهبت بأن المواد: (٢/ ٤) و (٥١) و (٤٢) من ميثاق الأمم المتحدة لا تُشير إلى أسلحة محددة، إذ وردت فيه أنه "وليس في تلك الأحكام ما يشير إلى أسلحة معينة. وانما هي تنطبق على أي استعمال للقوة. بصرف النظر عن الأسلحة المستخدمة. والميثاق لا يحظر صراحة، ولا هو يبيح استخدام أية أسلحة معينة بما فيها الأسلحة النووية. والسلاح الذي هو بحد ذاته محرم سواء بموجب معاهدة أو عرف، لا يغدو مشروعاً بسبب كونه يستخدم لغرض مشروع بموجب الميثاق"[٢]، وهذا ما أكد معظم الفقهاء والدول كذلك.

حيث أكد الفقهاء بأنه يجب التركيز على الآثار واعتبار الأدوات التي يتم تنفيذ العمليات السيبرانية بها أسلحة حديثة مثل الأسلحة التقليدية، فمثلاً ذهب (Dinstein) بأن "الإنترنت. . . يجب أن يُنظر إليه على أنه وسيلة جديدة للحرب بعبارة أخرى، سلاح: ليس أقل ولا أكثر من أسلحة أخرى"[٣]، وبنفس الاتجاه ذهب البعض بأن الديدان والفيروسات ورموز الروبوتات والبرامج الضارة الأخرى يتم التعامل معها الآن على أنها مجرد نظام أسلحة آخر أرخص وأسرع من الصاروخ[٤].

(١) أبلغ الأمين العام للأمم المتحدة قلم المحكمة العدل الدولية رسمياً بقرار اتخذته الجمعية العامة بموجب قرارها "٧٥/٤٩" في ١٥ كانون الأول- ديسمبر ١٩٩٤الذي قررت فيه عملاً بالفقرة ١ من المادة ٩٦ من ميثاق الأمم المتحدة أن تطلب من المحكمة العدل الدولية إصدار فتواها على وجه السرعة بشأن مسألة (هل التهديد بالأسلحة النووية أو استخدامها في أي ظرف من الظروف يكون مسموحاً به بموجب القانون الدولي؟)، وفي ٨ تموز- يوليو ١٩٩٦ أصدرت المحكمة العدل الدولية فتواها بشان المسألة التي وجهتها إليها الجمعية العامة، ينظر: الجمعية العامة للأمم المتحدة، نزع السلاح العام الكامل- فتوى محكمة العدل الدولية بشأن مشروعية التهديد بالأسلحة النووية أو استخدامها، وثيقة رقم A/51/218 الصادرة بتاريخ ١٥ اكتوبر ١٩٩٦، ص ١.

(٢) ينظر: الأمم المتحدة، موجز الأحكام والفتاوى والأوامر الصادرة عن محكمة العدل الدولية ١٩٩٢-١٩٩٦، نيويورك، وثيقة رقم ST/LEG/SER.F/1/Add.1 الصادرة في ١٩٩٨، ص ١١٦- ١١٧؛
Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, I. C.J. Reports 1996, p. 226, para 37- 39.

(3)Yoram Dinstein, Cyber War and International Law: Concluding Remarks at the 2012 Naval War College International Law Conference, International Law Studies, Vol. 89, 2013, p 280.

( (4 James Lewis, To Protect the U.S. Against Cyberwar, Best Defense Is a Good Offense, 29 March 2010, available on website:
https://www.usnews.com/opinion/articles/2010/03/29/to-protect-the-us-against-cyberwar-best-defense-is-a-good-offense
تاريخ الزيارة (٢٠٢٣/ ١/ ٢٦)

وأثار (الدكتور محمد سعادي) عدة أسئلة متعلقة بالموضوع فيرى بأنه "ألا يصح لنا أن نوصف الهجومات بالفيروسات المعلوماتية على مصالح الدول الأخرى باعتباره سلاح العصر الرقمي، بأنه عدوان مسلح ولا ينقص استعمال الفيروسات المعلوماتية من صفة العدوانية قياسا بالفيروسات الجرثومية المستعملة كسلاح بيولوجي ضد الدول؟ فما الفرق بين ضرب الدول بالفيروسات الجرثومية واعتبارها حربا بيولوجيا وضرب الدول بالفيروسات الالكترونية واعتبارها حربا فيروسية تمس مصالح الدول في الصميم إذا علمنا بأن الدول ومصالحها الكلية اليوم لا تسير إلا بالحواسيب والإعلام الآلي في أدق الأمور وأوسعها وهي مرتبطة بها ارتباطا تابعيا؟"[١].

ويؤيد فريق الخبراء الدولي في (تالين ١) هذا الاتجاه، حيث تنص (القاعدة ١١) منها على أنه "تشكل العملية السيبرانية استخدامًا للقوة عندما يكون نطاقها وآثارها قابلة للمقارنة مع العمليات غير السيبرانية التي تصل لمستوى استخدام القوة".

بالإضافة إلى الفقهاء، غالبية الدول أكدت على أن ما يهم ليس السلاح المستخدم في العملية لاعتباره استخداماً للقوة المسلحة بل الأثر المترتب عليه هو ما يهم وأشاروا إلى خطورة الآثار الناتجة عن العمليات السيبرانية، مثلاً أشارت وزارة الدفاع الامريكية في دراسة اجرتها إلى انه "يبدو من المرجح ان المجتمع الدولي سيكون مهتما بعواقب الهجوم على شبكة الكمبيوتر أكثر من آليته"[٢].

وترتيباً على ما تقدم فإن غالبية الدول أقرت بتطبيق قاعدة حظر استخدام القوة في الفضاء السيبراني، فمثلاً نجد أن اليابان تؤكد بأنه وفي ظل ظروف معينة، قد تشكل العملية السيبرانية استخدامًا للقوة المحظورة بموجب المادة (٢/ ٤) من ميثاق الأمم المتحدة[٣]، وباكستان كذلك اشارت إلى أن مبدأ عدم استخدام القوة على النحو المنصوص عليه في ميثاق الأمم المتحدة سارية في الفضاء السيبراني كما هو في العالم المادي[٤]، وبولندا بدورها أكدت على حظر استخدام القوة المنصوص عليه في المادة (٢/ ٤) من ميثاق الأمم المتحدة والقانون الدولي العرفي، وأكدت كذلك على أنه وفقاً لفتوى محكمة العدل الدولية بشان مشروعية التهديد

(١) د. محمد سعادي، *أثر التكنلوجيا المستحدثة على القانون الدولي العام*، ط ١، (الإسكندرية: دار الجامعة الجديدة للنشر، ٢٠١٤)، ص ٢٠٠.

(2) United States Department of Defense, An Assessment of International Legal Issues in Information Operations, May 1999, p 18.

(3)Ministry of Foreign Affairs of Japan, Basic Position of the Government of Japan on International Law Applicable to Cyber Operations, 28 May 2021, P 6.

(4)Pakistan Mission to the UN, Pakistan's Position on the Application of International Law in Cyberspace (3 March 2023), Para 6.

بالأسلحة النووية أو استخدامها، يمكن اعتبار فعل ما استخدامًا للقوة بغض النظر عن الوسائل المستخدمة. إذ ما يهم هو آثار الفعل، ونتيجة لذلك، لا يمكن استبعاد أنه بإمكان آثار عملية سيبرانية أن تصل في بعض الحالات لعتبة استخدام القوة المحظورة[١]، والسويد أيضاً ذكرت بأن حظر استخدام القوة هو قاعدة أساسية في القانون الدولي العرفي، ويسري أيضًا فيما يتعلق بالعمليات السيبرانية، مستشيراً بذلك ما ذهبت إليه محكمة العدل الدولية بأن الأحكام المتعلقة باستخدام القوة لا تعتمد على اختيار الوسائل، بل تنطبق على أي استخدام للقوة بغض النظر عن الأسلحة المستخدمة، وبالتالي يمكن اعتبار العمليات السيبرانية استخداماً للقوة إذا كانت قابلة للمقارنة مع حجم وتأثيرات الاستخدام التقليدي للقوة[٢].

وكذلك أكدت (**فريق** الخبراء الحكوميين التابع للأمم المتحدة المعني بأمن المعلومات- UNGGE) على أن الدول ملزمة بالمبادئ الواردة في ميثاق الأمم المتحدة وغيرها من قواعد القانون الدولي في أفعالها في الفضاء السيبراني ومنها الامتناع عن استخدام القوة في علاقاتها الدولية ضد السلامة الإقليمية وأو الاستقلال السياسي لأية دولة أو بأية طريقة تتعارض مع مقاصد الأمم المتحدة[٣].

كما أكدت (المنظمة الاستشارية القانونية الآسيوية- الإفريقية - AALCO) على أنه اعتبرت محكمة العدل الدولية أن المادتين (٤/ ١) و (٥١) من ميثاق الأمم المتحدة فيما يتعلق بحظر استخدام القوة والدفاع عن النفس على التوالي، تنطبقان على أي استخدام للقوة بغض النظر عن الأسلحة المستخدمة، مع تأكيدها على أن مسألة تحديد متى يمكن لعملية سيبرانية أن ترقى إلى استخدام القوة المحظورة يكون بمقارنة نطاقها وتأثيراتها مع العمليات التقليدية التي ترتفع إلى مستوى استخدام القوة وبأن مهمة تطبيق هذه القاعدة في الفضاء السيبراني ليست مهمة مباشرة بل يتطلب المزيد من المداولات بين الدول للتوصل إلى أي توافق في الآراء [٤]، كما ورد في "المبادي الأساسية التوافقية للقانون الدولي المطبقة في الفضاء السيبراني" التي قدمها الأمين العام للمنظمة بانه ينبغي أن تحترم الدول أن القانون الدولي، ولا سيما ميثاق الأمم المتحدة، مطبق على أفعالها وهذا يشمل عدم استخدام القوة[٥].

---

(1) Ministry of Foreign Affairs of Poland, The Republic of Poland's Position on the Application of International Law in Cyberspace, 29 December 2022, p 5.

(2)Government Offices of Sweden, Position Paper on the Application of International Law in Cyberspace, July 2022, P 3.

(٣) الجمعية العامة للأمم المتحدة، تقرير فريق الخبراء الحكوميين المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي، ١٤ يوليو ٢٠٢١، وثيقة رقم A/76/135، ص ١٩.

(٤) المنظمة الاستشارية القانونية الآسيوية - الإفريقية، القانون الدولي في الفضاء السيبراني، وثيقة رقم AALCO/59/HONG KONG/2021/SD/S17، ٢٠٢١، ص ٢٧- ٢٨.

(٥) المنظمة الاستشارية القانونية الآسيوية - الإفريقية، القانون الدولي في الفضاء السيبراني، وثيقة رقم AALCO/58/DAR ES SALAAM/2019/SD/S17، ٢٠١٩، ص ٢٨.

ونتيجة لما تقدم نذهب أن تحديد المقصود بالقوة المسلحة بالنظر إلى آثارها يسمح للمجتمع الدولي بتكييف ميثاق الأمم المتحدة مع التكنولوجيا المتطورة واعتبار العمليات السيبرانية التي تنتج تأثيرات مشابهة للأسلحة التقليدية استخداماً للقوة المسلحة، ولكن التركيز على الآثار فقط يثير الكثير من التساؤلات في السياق السيبراني، وذلك لأن آثار العمليات السيبرانية متنوعة، ونتيجة لهذا التنوع في الآثار ظهرت تساؤلات حول كيفية تطبيق الاتجاه القائم على الآثار على العمليات السيبرانية، أو بمعنى آخر ما هو الحد الأدنى من الآثار التي يجب أن تتوفر لاعتبار العملية السيبرانية استخداماً للقوة المسلحة؟ وهذا هو محل موضوعنا في المطلب التالي.

## I.ب. المطلب الثاني

## الحد الأدنى لاعتبار العمليات السيبرانية استخداماً للقوة

ينتج عن العمليات السيبرانية آثار مختلفة، حيث تكون مجرد التجسس أو اتلاف البيانات وقد يتسبب في تعطيل وظائف البنية التحتية الحيوية في الدولة، بل أكثر من ذلك فقد تصل آثارها إلى فقدان الأرواح والممتلكات، ولذلك يثار تساؤل حول الآثار التي يجب أن يترتب على عملية سيبرانية حتى يصل لعتبة استخدام القوة المسلحة؟ فالقاعدة في دليل تالين قد حددت المعيار التي يمكن من خلالها تحديد ما إذا كانت العمليات السيبرانية تصل إلى حد استخدام القوة أم لا وذلك عن طريق المقارنة بين آثار العمليات السيبرانية وآثار العمليات التقليدية إلا أنها لم تحدد الحد الأدنى من الأضرار المطلوبة لذلك[١].

للإجابة على هذا السؤال، يتفق غالبية الفقهاء والدول على الأخذ بمعيار الشدة لكي تصف العملية السيبرانية التي تشنها دولة ما ضد دولة أخرى بأنها استخدام للقوة أو هجوم مسلح ، ويقصد بمعيار الشدة العملية التي تؤدي إلى اصابة جسدية أو تدمير للممتلكات[٢]، وذهب إلى هذا الاتجاه أغلب الفقهاء، فمثلاً وفقًا لـ(Lin ) تكون حالات الغموض أقل عندما تتسبب العملية السيبرانية في أضرار مادية للممتلكات وخسائر في الأرواح بطرق يمكن مقارنتها بالهجمات الحركية والحرب التقليدية[٣]، كما ذهب (Silver) بأن من المرجح أن

(١) د. محمود حسين الشرقاوي، مصدر سابق، ص ٢١١.

(٢) معيار الشدة من إحدى المعايير الذي اقترحه (Schmitt) في مقالته المنشورة في عام ١٩٩٩، في هذه المقالة قدم (Schmitt) ستة معايير يمكن من خلالها تمييز كل من الاكراه الاقتصادي والسياسي عن استخدام القوة وهذه المعايير هي (١) الشدة (٢) الفورية (٣) المباشرة (٤) الغزو (٥) قابلية القياس (٦) الشرعية الافتراضية، وتم إعادة استخدام هذه المعايير وتطويرها من قبل مجموعة الخبراء الدولية المشاركة في عملية إعداد دليل تالين برئاسة (Schmitt) نفسه في النسختين الأولى والثانية، بحيث تم اضافة معياريين آخرين وهما: الطابع العسكري ومشاركة الدولة، ينظر:-

Michael N. Schmitt, Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework. Columbia Journal of Transnational Law, Vol. 37, 1999, p 914- 915; Michael N. Schmitt (GEN. ED.), Tallinn manual on the international law applicable to cyber warfare, Op. Cit., commentary to Rule 11, Paras 8–11.

(3) Herbert S. Lin, Offensive Cyber Operations and the Use of Force, Journal Of National Security Law & Policy, Vol. 4:63, p 73.

يشكل العملية السيبرانية استخدامًا للقوة إذا كانت آثاره إصابة جسدية أو أضرار بالممتلكات[١]، وبنفس الاتجاه يؤكد (Dinniss) على أن العملية السيبرانية التي يترتب عليها عواقب مادية أي تدمير الممتلكات المادية أو الإصابة أو فقدان الأرواح، فإنه سيعتبر خرقاً لقاعدة حظر استخدام القوة بموجب المادة (٢/ ٤)[٢]، وكذلك (Joyner and Lotrionte) يذهبان بأن هناك قناعة تامة بأن الأنشطة السيبرانية التي تؤدي إلى وفيات أو تدمير مادي تخرق الحظر الوارد على استخدام القوة وذلك على عكس الحالات التي لا يترتب عليها وجود ضرر مادي ملموس كالتي تؤدي إلى تعطيل أو حذف البيانات[٣].

كما أكدت غالبية الدول على أن وجود الآثار المادية نتيجة لعملية سيبرانية يترتب عليه اعتبارها استخداماً للقوة وكذلك هجوم مسلح عندما تكون ذات خطورة كافية، فمثلاً يذهب فرنسا بأنه يتم تصنيف العملية السيبرانية على أنه هجوم مسلح إذا تسبب في خسائر كبيرة في الأرواح أو أضرار مادية أو اقتصادية جسيمة. سيكون هذا هو حالة عملية في الفضاء السيبراني تسببت في فشل البنية التحتية الحيوية مع عواقب وخيمة من شأنها أن تشل قطاعات كاملة من نشاط البلد، وتسبب كوارث تكنولوجية أو بيئية تودي بحياة العديد من الضحايا[٤]، وكذلك ترى المملكة المتحدة أنه من الواضح أن العمليات السيبرانية التي تؤدي إلى الموت والدمار تعتبر هجوم مسلح وبالتالي ينشأ حق الدفاع عن النفس المعترف به في المادة (٥١) من ميثاق الأمم المتحدة[٥].

والولايات المتحدة الأمريكية كذلك ذهبت أنه ومن المرجح أن يُنظر إلى العمليات السيبرانية التي تؤدي إلى وفاة أو إصابة أو تدمير كبير على أنها استخدام للقوة/ هجوم مسلح، فإذا كانت العواقب المترتبة على العملية السيبرانية مشابهة لتلك التي يؤدي إليه إلقاء قنبلة أو

(1) Daniel B. Silver, Computer Network Attack as a Use of Force under Article 2(4) of the United Nations Charter, International Law Studies Series US Naval War College, Vol. 76, 2002, p 85.

(2)Heather Harrison Dinniss, Cyber Warfare and the Laws of War, Cambridge University Press, Cambridge, 2012. p 74.

(3)Christopher C. Joyner and Catherine Lotrionte, Op. Cit. p 850.

(4) French Ministry of Armed forces, International law applied to operations in cyberespace, Paper shared by France with the Open-ended working group established by resolution 75/240, 2019, p 5.

( (5Government of United Kingdom- Attorney General's Office and The Rt Hon Sir Jeremy Wright KC MP, Speech by The Attorney General Jeremy Wright about Cyber and International Law in the 21st Century, 23 May 2018, available on website:
https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century

تاريخ الزيارة (٢٠٢٢/ ١١/ ١٧)

إطلاق صاروخ، يجب اعتبارها استخداماً للقوة/ الهجوم المسلح[١]، وكذلك أكدت إيران أن العمليات السيبرانية التي تؤدي إلى أضرار مادية بالممتلكات و/ أو الأشخاص تشكل استخداماً للقوة[٢]، واستونيا أيضاً ذهبت إلى أن العملية السيبرانية التي تستهدف البنية التحتية الحيوية وتؤدي إلى أضرار جسيمة أو إصابة أو وفاة أو تهديد بمثل هذه العملية يعتبر مثالاً على استخدام القوة وكذلك هجوماً مسلحاً[٣].

ولكن إذا كانت العملية السيبرانية التي تؤدي إلى اصابة جسدية أو الحاق الضرر بالممتلكات من المتفق عليه أنه يعتبر استخداماً للقوة، إلا أن هناك حالتين يصعب الإجابة عليها وهما:-

**الحالة الأولى: العمليات السيبرانية التي تستهدف تعطيل البنية التحتية الحيوية[٤] دون إحداث آثار مادية**

إن غالبية البنية التحتية الحيوية في الوقت الحالي يتم تشغيلها والتحكم بها بالاعتماد على الفضاء السيبراني وبالتالي أصبحت بالإمكان تعطيلها ووقفها عن التشغيل من خلال العمليات السيبرانية دون وجود أضرار بشرية أو مادية، ولا يمكن الانكار بأن تعطيلها يشكل خطراً

(1)UNGA, Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States, Op. Cit. p 137.

(2) Declaration of General Staff of the Armed Forces of the Islamic Republic of Iran Regarding International Law Applicable to the Cyberspace, 18 August 2020, Article IV.

(3)UNGA, Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States, Op. Cit. p 26 and 30.

(٤) أقرت كل من (UNGA, UNGGE, UNOEWG) بحرية كل دولة في تحديد البنية التحتية الحيوية لها أي التي تعتبرها بالغة الأهمية، وذلك بما يتفق مع أولوياتها الوطنية والطرق التي تتبعها في تصنيف البنية التحتية الحيوية، مع ذكرها لبعض الأمثلة التي قد تعتبرها غالبية الدول من البنية التحتية الحيوية وهم البنية التحتية التي تستخدم في توليد الطاقة، النقل، الخدمات المصرفية والمالية، تزويد المياه، الصحة العامة، توزيع الأغذية، والاتصالات، ينظر:

الجمعية العامة للأمم المتحدة، تقرير فريق الخبراء الحكوميين المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي، ١٤ يوليو ٢٠٢١، وثيقة رقم A/76/135، ص ١٤؛ الجمعية العامة للأمم المتحدة، قرار رقم (٥٨/ ١٩٩) اتخذته الجمعية العامة في (٢٣ كانون الأول/ ديسمبر ٢٠٠٣) بشأن إرساء ثقافة عالمية لأمن الفضاء الحاسوبي وحماية الهياكل الأساسية الحيوية للمعلومات، وثيقة رقم A/RES/58/199، ص ١-٢؛

UNGA, UNOEWG on developments in the field of information and telecommunications in the context of international security (Final Substantive Report), A/AC.290/2021/CRP.2, 10 March 2021, PARA 18, P 4.

كبيراً حتى وإن لم يتسبب ذلك في حصول آثار مادية، وهذا ما أكدته التقارير الصادرة من (UNGGE وUNOEWG) إذ وردت فيها وبإجماع الدول بأن العمليات السيبرانية التي تعيق تشغيل أو استخدام البنية التحتية الحيوية يمكن أن يشكل تهديداً لأمن وسيادة الدولة ، فضلاً عن التنمية الاقتصادية وسبل العيش، وفي نهاية المطاف سلامة ورفاهية الأفراد[١]، كما خصصت قاعدة تنص على أنه "ينبغي للدولة ألا تنفذ، أو تدعم عن علم أي نشاط من أنشطة تكنولوجيات المعلومات والاتصالات يتعارض مع التزاماتها بموجب القانون الدولي ويضر عمدا بالبنية التحتية الحيوية المستخدمة في تقديم الخدمات إلى الجمهور أو يعطل، بأي شكل آخر استخدام تلك البنية التحتية الحيوية وتشغيلها"، وأكدت على أن العمليات السيبرانية التي يقصد بها "الإضرار بالبنية التحتية الحيوية المستخدمة في تقديم الخدمات إلى الجمهور أو يعطل، بأي شكل آخر، استخدام تلك البنية التحتية الحيوية وتشغيلها، يمكن أن تكون له آثار محلية وإقليمية وعالمية متتالية. ويهدد هذا النشاط بشدة بإلحاق ضرر بالسكان، ويمكن أن يكون تصعيديا، وقد يفضي إلى نشوب نزاع"، بالإضافة إلى تأكيدها على "الأهمية القصوى للبنية التحتية الحيوية بوصفها ثروة وطنية، نظراً إلى أن هذه البنية التحتية تشكل العمود الفقري للوظائف والخدمات والأنشطة الحيوية للمجتمع. وإذا ما لحقها تعطل فإن التكلفة البشرية والآثار على اقتصاد الدولة وتنميتها وأدائها السياسي والاجتماعي وأمنها الوطني قد تكون باهظة"[٢].

وكذلك شددت كل من فيتنام و كينيا وايرلندا والولايات المتحدة الأمريكية في اجتماع لمجلس الأمن على ضرورة حماية البنية التحتية الحيوية للدول من التهديدات السيبرانية وعدم استهدافها، حيث اصبحت الخطر واضح عليها بعدما اصبحت الخدمات الحيوية من الغذاء والماء إلى الرعاية الصحية أهدافاً للعمليات السيبرانية[٣].

وبناء على ما تقدم هناك خطورة شديدة يترتب على توقف البنية التحتية الحيوية عن العمل حتى بدون حصول آثار مادية، وبالرغم من ذلك وبسبب التركيز على وجود أضرار

(1) ibid, P 4.

(٢) الجمعية العامة للأمم المتحدة، "تقرير فريق الخبراء الحكوميين المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي"، ١٤ يوليو، (٢٠٢١): وثيقة رقم A/76/135.، ص ١٣-١٤.

(3)Explosive Growth of Digital Technologies Creating New Potential for Conflict, Disarmament Chief Tells Security Council in First-Ever Debate on Cyberthreats, 29 June 2021, Available on the website:
https://press.un.org/en/2021/sc14563.doc.htm

تاريخ الزيارة (١٠ /٣ /٢٠٢٣)

مادية لا يوجد حتى الآن اتفاق بالإجماع حول مدى اعتبار هذه العمليات استخداماً للقوة، وسنبين فيما يلي موقف كل من الفقه والدول بهذا الشأن.

**موقف الفقه:**

يذهب جانب من الفقه على أنه لا يعتبر هذه العمليات استخداماً للقوة، ومنهم (Schmitt) الذي يرى بأنه لا يتفق مع وجهة النظر هذه، ويرجع ذلك بالقول إلى أنه غير متأكد من أن الدول ستساوي بسهولة الآثار غير الحركية مع التأثيرات الحركية، ويرى أنه يمكن فقط لممارسات الدول أن تنشئ مثل هذا المعيار[١]، ويذهب البعض في نفس هذا الاتجاه إذ يشترطون لاعتبار عملية سيبرانية ما استخداماً للقوة أن يكون هناك ضحايا مادية وليس مجرد تعطيل، فمثلا تعطيل محطة نووية فقط لا يعتبر استخداماً للقوة بل يشترط أن يكون هناك خطر بحدوث آثار مادية كذوبان قلب المفاعل النووية، وكذلك تعطيل وانقطاع البنى التحتية للكهرباء يشترط لاعتباره استخداماً القوة أن يكون هناك ضحايا[٢]، كما يرى البعض بأن العمليات السيبرانية التي تستهدف المؤسسات الاقتصادية مثل البورصة ويعطل الأسواق المالية دون وجود آثار مادية تعد ممارسة لإكراه اقتصادي وليس استخداماً للقوة[٣].

في حين وباتجاه مخالف هناك من يؤيد من الفقهاء اعتبارها استخداماً للقوة بل أبعد من ذلك منهم من يرى اعتباره هجوماً مسلحاً وبالتالي ومن باب أولى استخداماً للقوة، فذهب (Morth) بأن العملية السيبرانية التي ستستهدف البنية التحتية المالية للبلد كالبنوك مثلاً مما يؤدي إلى استنزاف أصولها، من شأنه أن يتسبب في حالة من الذعر الشديد لأن سكان البلاد لن يكون لديهم فرصة للاستعداد لخسارة قاعدتهم المالية، ويعتبر استخداماً للقوة المسلحة وليس مجرد اكراه اقتصادي طالما أن الغرض من استخدام القوة هو تدمير السوق بمنع المشترين

(1) Michael N. Schmitt, The Use of Force in Cyberspace: A Reply to Dr Ziolkowski. IN Proceedings of the 4th International Conference on Cyber Conflict, Christian Czosseck and others (eds), NATO CCD COE Publication, TALLINN, 2012, p 315.

(2)Torsten Stein and Thilo Marauhn, Völkerrechtliche Aspekte von Informationsoperationen, Zeitschrift für ausländisches öffentliches Recht und Völkerrecht, Vol. 60, 2000, p 8.

(٣) نقلاً عن:

Marco Roscini, Cyber Operations and the Use of Force in International Law, Op. Cit. p 62.

والبائعين من الاتصال ببعضهم البعض أو محو سجلات المعاملات بعكس الاكراه الاقتصادي التي تكون عادة عن طريق تقليل تقديم سلعة مهمة[١].

ويؤكد (Ziolkowski) بأن تعطيل هائل ومتوسط وطويل الأمد لأنظمة البنية التحتية الحيوية لدولة ما إذا كانت آثاره تعادل التدمير المادي للأنظمة المعنية يعتبر استخداماً للقوة[٢]، ويذهب البعض إلى أنه يجب أن يأخذ في الاعتبار الطابع الخاص والأهمية المحددة للبنى التحتية، وبالتالي فإن التعطيل الفوري للبنية التحتية الحيوية ذات الآثار المثبطة (التي لا يمكن إصلاحها بالسرعة الكافية) على قدرة الدولة على التصرف أو على الظروف المعيشية الأولية للسكان يمكن من حيث المبدأ أن تحدث الأثر الهدام الضروري الذي من شأنه اعتباره هجوماً مسلحاً[٣].

وكذلك (Brown and poellet) يذهبان بأن العملية السيبرانية ضد البنية التحتية الحيوية ومنها مثلاً شبكة طاقة الكهرباء والتي يتسبب في توقفها وعلى الرغم من عدم حدوث أي أثر مادي، إلا أن اعتماد المجتمعات الحديثة على الكهرباء للرعاية الصحية والاتصالات وتقديم الخدمات الأساسية يوضح أن هذا سيكون مؤهلًا لتأثير شبيه بالأسلحة الحركية وبالتالي سيشكل هجوماً مسلحاً إذا كان التوقف لفترة طويلة من الزمن[٤].

وذهب البعض الآخر بأنه ولأن المجتمع الحديث يعتمد على وجود بنية تحتية واسعة النطاق وتشغيلها بشكل صحيح، والتي تخضع بشكل متزايد لسيطرة تكنولوجيا المعلومات. يمكن اعتبار العمليات السيبرانية التي تتداخل بشكل كبير مع وظائف تلك البنية التحتية بشكل معقول على أنها استخدامات للقوة، سواء تسببت في أضرار مادية أم لا، ويؤكدون على أن العمليات السيبرانية على تكنولوجيا المعلومات التي يتحكم في عمل البنية التحتية لدولة ما والتي تكون لها تأثير كبير على عمل البنية التحتية هذا سواء تسببت في الآثار المادية أو لا ستكون هجوماً مسلحاً، فمثلاً العملية السيبرانية التي يتسبب في تعطيل بورصات للأوراق

(1)Todd A. Morth, Considering Our Position: Viewing Information Warfare as a Use of Force Prohibited by Article 2(4) of the U.N. Charter, Case Western Reserve Journal of International Law, Vol. 3: issue. 2, 1998, p 596.

(2)Katharina Ziolkowski, Confidence Building Measures for Cyberspace– Legal Implications, NATO CCD COE, Tallinn, 2013. P 75.

(٣) نقلاً عن:

Albrecht Randelzhofer and Georg Nolte, Article 51. IN The Charter of the United Nations: A Commentary, Bruno Simma and others (ed), Volume II, 3rd Edition, Oxford University Press, 2012, PARA 43.

(4)Gary Brown and Keira Poellet, The Customary International Law of Cyberspace, Strategic Studies Quarterly, Vol. 6 No. 3, 2012, p 137

المالية مؤقتًا ويجعل التداول مستحيلًا لفترة قصيرة لا يعتبر استخداما للقوة أو هجوماً مسلحاً ولكن إذا كان العملية السيبرانية هذا يحدث بشكل متكرر ومستمر، بحيث يتعطل التداول لفترة طويلة من الزمن، لأيام أو أسابيع، سيشكل بالتأكيد استخدامًا للقوة أو حتى هجومًا مسلحًا، حتى لو لم تكن هناك مبان دمرت[١]، وبنفس الاتجاه يذهب (Nils) إلى القول بأن العمليات السيبرانية التي لا تؤدي إلى الموت أو التدمير بالممتلكات من الممكن أن ترقى إلى مستوى هجوم مسلح إذا كانت تهدف إلى شل قدرة البنى التحتية الحيوية في الدولة[٢].

أما فريق الخبراء المعد لـ(دليل تالين ١) فقد أكدوا على أن طبيعة الهدف في هذه الحالة يأخذ بنظر الاعتبار كعنصر لاعتبار العملية استخداماً للقوة[٣]، كما ذهب بعض منهم في (تعليق رقم ٩ القاعدة ١٣) إلى أن العملية السيبرانية التي تستهدف البنية التحتية الحيوية في الدولة والتي يتسبب في إحداث آثار خطيرة وكارثية وإن لم تكن مادية، يمكن وصفها بأنها هجوم مسلح.

ويرى (Roscini) بأنه وعلى الرغم من أنها ليست العامل الحاسم الوحيد كما يذهب إليه مؤيدو النهج القائم على الهدف، إلا أن طبيعة الهدف عنصر مهم يجب مراعاته عند قياس آثاره مع العمليات التقليدية باعتباره ذات أهمية مما يؤثر تعطيله على الوظائف الأساسية للدولة ونظامها العام الداخلي، ولا يجب الاعتماد على طبيعة الهدف فقط في هذه الحالة، حيث هناك عوامل أخرى يجب مراعاتها مثل خطورة التعطيل ومدته ومدى اعتماد الدولة الضحية عليها، ويبرر رأيه بالحجج التالية[٤]:

١- إن تفسير مصطلح (القوة) وفقاً لتطور الأسلحة والمنطق الكامن وراء النص لا يمنع من توسيع نطاق الحظر من أجل إدراج هذه الحالة تحت حظر استخدام القوة، وهذا ما ذهب إليه محكمة العدل الدولية عندما قرر بأنه "حيثما استخدمت الأطراف مصطلحات عامة في معاهدة ... يجب أن يُفترض ، كقاعدة عامة ، أنها قصدت أن يكون لهذه المصطلحات معنى متطور"، وبناء على ذلك ينبغي أن يؤخذ في الاعتبار الاعتماد المتزايد للدول على أنظمة وشبكات الكمبيوتر لتقديم خدمات حيوية للمجتمع لأن التركيز فقط على العواقب المادية

(1)William A. Owens and others (eds.), Technology- Policy- Law and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities, National Academies Press, Washington, 2009, p 253- 255.
(2)Melzer Nils, Cyberwarfare and International Law, United Nations Institute for Disarmament Research, Geneva, 2011, p 16.
(3)Michael N. Schmitt (GEN. ED.), Tallinn manual on the international law applicable to cyber warfare, Op. Cit. commentary to Rule 11, para 10.
(4)Marco Roscini, Cyber Operations and the Use of Force in International Law, Op. Cit. p 59- 63.

المدمرة للأفراد والممتلكات هو أمر مختزل في السياق السيبراني، حيث يعتمد المجتمع الحديث على وجود بنية تحتية واسعة النطاق وأداءها بشكل صحيح يتم التحكم فيها بشكل متزايد بواسطة تكنولوجيا المعلومات.

٢- هناك بعض التعاريف للأسلحة تشمل حالة التعطيل دون حدوث الآثار المادية، فمثلاً يعرف البعض الأسلحة التقليدية بأنها "عبارة عن أجهزة مصممة لقتل الأشخاص أو إصابتهم أو تعطيلهم أو إعاقتهم مؤقتًا أو تدميرهم أو إلحاق الضرر بهم. أو تعطل الممتلكات أو العتاد مؤقتًا" وكذلك تشير الإستراتيجية العسكرية الوطنية للولايات المتحدة الأمريكية لعام ٢٠٠٤ إلى (أسلحة التأثير الشامل) والتي تعتمد بشكل أكبر على التأثير التخريبي بدلاً من التأثيرات الحركية المدمرة وتعطي مثالًا للعمليات السيبرانية على أنظمة المعلومات التجارية الأمريكية أو ضد شبكات النقل، والحقيقة هذا منطقي إذا اعتبر المرء أنه بسبب اعتماد المجتمعات الحديثة على أجهزة الكمبيوتر وأنظمة الكمبيوتر والشبكات، فإن التقنيات السيبرانية قد مكنت الدول من إنتاج نتائج مماثلة لتلك الخاصة بالأسلحة الحركية ولكن دون الحاجة إلى ضرر مادي.

٣- القول بأن العمليات السيبرانية التي تستهدف تعطيل المؤسسات الاقتصادية يعتبر إكراه اقتصادي وليس قوة مسلحة غير صحيح لسببين: أولهما أن الإكراه الاقتصادي ليس له هدف محدد في حين ان العملية السيبرانية سيشن ضد بنية تحتية حيوية محددة، ثانيا أن الاكراه الاقتصادي مثل حظر النفط يستخدم الاقتصاد كوسيلة للضغط على الدولة الضحية إجبارها على اتخاذ قرارات معينة أما العملية السيبرانية فيعطل السوق المالية أو يشل النظام المصرفي للدولة، لذلك إذا تم قصف البورصة أو المؤسسات المالية الأخرى بشكل حركي وتعطلت الأسواق نتيجة لذلك فمن المؤكد أن هذا سيعتبر استخداماً للقوة المسلحة وليس إكراهاً اقتصادياً على الرغم من أن العواقب الاقتصادية للهجوم ربما تفوق الأضرار المادية للمباني. وبالتالي لا يوجد سبب لعدم تطبيق نفس النتيجة عندما يتم إغلاق البورصة بدلاً من قصفها، لفترة طويلة من الزمن بواسطة العمليات السيبرانية، ويمكن القول أن هذه الحالة يتشابه مع الهجوم الحركي أكثر مما يتشابه مع حظر النفط بشرط أن يكون الآثار الناجمة عن الإغلاق شديدًا وذات خطورة.

٤- القلق حول تصاعد خطر النزاعات الدولية بسبب اعتبار هذه العمليات السيبرانية استخداماً للقوة ليست في محله، وذلك لأنه لا يكفي مجرد استخدام القوة المسلحة لتفعيل حق الدفاع عن النفس للدولة الضحية بل يشترط أن يكون على درجة من الخطورة بما يكفي بحيث يرتقي لمستوى الهجوم المسلح. أما التي تقل عن هذا المستوى فيحق للدولة فقط اتخاذ التدابير المضادة دون اللجوء لاستخدام القوة المسلحة. وهذا نتيجة مرحب به بالنظر إلى

التأثير السلبي الشديد الذي ينتج عن العمليات السيبرانية التي تستهدف تعطيل البنية التحتية الحيوية على النظام العام للدول في العصر الرقمي.

وبعد هذه الحجج يؤكد (Roscini) على أن العمليات السيبرانية التي تتجاوز مجرد الإزعاج وتعطل بشكل كبير أداء البنية التحتية الحيوية يمكن ادراجها ضمن نطاق المادة (٢/ ٤)، ففي هذه الحالات فقط يمكن معادلة آثار التعطيل بآثار الدمار الذي تسببه القوة المسلحة التقليدية، فالعملية السيبرانية التي يدوم اسبوعاً وبالتالي تؤدي إلى إغلاق الشبكة الوطنية، وبالتالي ترك ملايين الأشخاص بدون كهرباء، وشل السوق المالية ونظام النقل، ومنع الاتصالات الحكومية، من المرجح أن يعتبر استخداماً للقوة، وبعكس ذلك فالعملية السيبرانية التي تؤدي إلى إغلاق شبكة جامعية لا يعد استخدامًا للقوة، حتى لو تسبب في تعطيل طويل الأمد وشديد لأن البنية التحتية التي يؤثر عليها ليست بالغة الأهمية. لذلك وعلى الرغم من أن العمليات السيبرانية (DDoS) التي استهدفت عام (٢٠٠٧) البنية التحتية الحيوية (المصرفية والاتصالات) على إستونيا إلا أنها لا تعتبر استخداماً للقوة وذلك لأنها لم تسبب أي ضرر مادي أو اضطراب خطير.

**موقف الدول:**

بالإضافة إلى الفقهاء هناك دول عديدة تتجه نحو اعتبار هذه العمليات السيبرانية استخداماً للقوة بل حتى هجوماً مسلحاً، فمثلاً أكدت النرويج على أن العمليات السيبرانية التي تسبب اضطرابًا شديدًا في أداء الدولة كالتي تستهدف ضد شبكة الطاقة الحكومية أو الخاصة أو النظام المالي والمصرفي للدولة، أو العمليات التي تسبب آثاراً اقتصادية واسعة النطاق وزعزعة الاستقرار، قد يصل إلى حد استخدام القوة في انتهاك للمادة (٢/ ٤) وعلاوة على ذلك أكدت على أنه تعتبر العملية السيبرانية التي تلحق أضراراً جسيمة بالبنية التحتية أو الوظائف الحيوية للدولة أو تعطلها على أنها ترقى إلى مستوى هجوم مسلح بموجب القانون الدولي[١].

وكذلك ذهبت هولندا بأنه لا يمكن في هذا الوقت استبعاد أن تكون العملية السيبرانية ذات الأثر المالي أو الاقتصادي الخطير جدًا مؤهلة لاستخدام القوة[٢]، وعلاوة إلى ذلك وردت في التقرير الصادر من المجلس الاستشاري للشئون الدولية بالتعاون مع اللجنة الاستشارية

(1)UNGA, Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States, Op. Cit. p 70.
(2)Ministry of Foreign Affairs, Letter of 5 July 2019 from the Netherlands Minister of Foreign Affairs to the President of the House of Representatives on the International Legal Order in Cyberspace, and Appendix: International Law in Cyberspace, p 4.

المعنية بقضايا القانون الدولي في هولندا بأنه يعتبر العملية السيبرانية التي تمس بالوظائف الأساسية للدولة هجوماً مسلحاً بالمعنى المقصود في المادة (٥١) من ميثاق الأمم المتحدة إذا كان يمكن أن يؤدي إلى تعطيل خطير لعمل الدولة أو عواقب طويلة الأمد على استقرار الدولة. في مثل هذه الحالات، يجب أن يكون هناك اضطراب في الدولة، وليس مجرد عائق أو تأخير في الأداء الطبيعي للمهام حتى يمكن اعتباره هجومًا مسلحاً، وبالتالي لا يعتبر مجرد تعطيل المعاملات المصرفية بمثابة هجوم مسلح. ومع ذلك فإن العملية السيبرانية التي تستهدف النظام المالي بأكمله أو يمنع الحكومة من تنفيذ المهام الأساسية، على سبيل المثال هجوم على شبكة الاتصالات والقيادة العسكرية بأكملها يجعل من المستحيل نشر القوات المسلحة، يمكن أن يعتبر هجوماً مسلحاً[١].

وفرنسا أيضاً ترى بأنها لا تستبعد إمكانية وصف عملية سيبرانية بدون آثار مادية بأنها استخدام للقوة بل أبعد من ذلك ترى بأن العملية السيبرانية التي يتسبب في تعطيل البنية التحتية الحيوية مع عواقب وخيمة من شأنها أن تشل قطاعات كاملة من نشاط الدولة هجوماً مسلحاً[٢]، كما يتجه أمريكا لهذا الاتجاه، إذ جاء في إحدى التقارير الصادرة من وزارة الدفاع الأمريكية بأنها تحتفظ بالحق في استخدام جميع الوسائل اللازمة للدفاع ضد الأعمال العدائية في الفضاء السيبراني، وتشمل الأعمال العدائية الهجمات السيبرانية الموجهة ليس فقط ضد الحكومة الأمريكية أو الجيش الأمريكي بل وضد الاقتصاد الأمريكي أيضاً[٣]، كما ذهبت سنغافورة بأنه من وجهة نظرها وفي ظروف محدودة معينة من الممكن أن تصل عملية سيبرانية إلى مستوى هجوم مسلح حتى لو لم يتسبب بالضرورة في الوفاة أو الإصابة أو الضرر المادي أو التدمير وأحد الأمثلة على ذلك هو عملية سيبرانية مستهدفة تتسبب في انقطاع مستمر وطويل الأمد للبنية التحتية الحيوية[٤].

(1) Advisory Council on International Affairs/Advisory Committee on Issues of Public International Law, Cyber Warfare, no 77, AIV/No 22 CAVV, December 2001, p 21.

(2)French Ministry of Armed forces, Op. Cit. p 3 and 6.

( (3 United States Department of Defense, Cyberspace Policy Report. A Report to Congress Pursuant to the National Defense Authorization Act for Fiscal Year 2011, Section 934, November, 2011, p 4.

(4)UNGA, Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States, Op. Cit. p 84.

ومن النماذج التطبيقية التي تعتبر استخداماً للقوة هو حالة ستوكسنت [١] عام (٢٠١٠)، حيث يذهب الغالبية إلى ذلك نظراً لحدوث آثار مادية واتلاف اكثر من ألف جهاز في محطة نطنز النووية الإيرانية، أما الحالات الأخرى جميعها لا يعتبرها الغالبية استخداماً للقوة كالعمليات السيبرانية ضد استونيا [٢] عام (٢٠٠٧) وذلك لأنه وكما اشرنا إليه سابقاً وبالرغم من أنها تسبب في تعطيل البنية التحتية الحيوية إلا أنها لم تؤثر بشكل خطير عليها[٣].

**خلاصة القول**

من خلال ما سبق تبينت لنا بأن الذين يعتبرون هذه العمليات استخداماً للقوة يقيدون ذلك بتوافر شرطين وهما: أولهما أن تستهدف العملية بنية تحتية حيوية في غاية الأهمية بحيث يترتب على تعطيلها عرقلة الوظائف الأساسية للدولة وأمنها القومي، وثانيهما أن يكون التعطيل واسع النطاق بحيث يتعدى كونها مجرد تعطيل مؤقت لأنه وبتوافر هذين الشرطين فقط يمكننا أن نقارن آثار العمليات السيبرانية مع آثار الأسلحة التقليدية[٤].

ونحن نرجح هذا الرأي، وذلك لأنه وفي المجتمع المعاصر لا يستبعد أن يترتب على تعطيل البنى التحتية الحيوية للدولة آثار خطرة ومدمرة دون وجود آثار مادية، فالنظر إلى وجود الآثار المادية أم لا لاعتبار عملية سيبرانية استخداماً للقوة لا يفسر التطور الذي حصل بالمجتمعات المعاصرة، وهنا نشير بالإضافة إلى ما تقدم نقطتين وهما: -

١- نرى بأن تركيز الفقهاء على الآثار المادية هو بسبب الأساس القانوني الذي عليه يبررون اعتبار العمليات السيبرانية استخداماً للقوة وهو فتوى محكمة العدل الدولية بشأن

---

(١) في عام ٢٠١٠ تسببت فيروس "Stuxnet" في أضرار جسيمة لحوالي ١٠٠٠ جهاز طرد مركزي في منشأة نطنز النووية في إيران في يونيو ٢٠١٠ وتم تبديلهما حسب الوكالة الدولية للطاقة الذرية، وبالرغم من انكار ذلك من قبل الجهات الحكومية في إيران حيث ادعت بأن أثر الفيروس كان محدود جداً، ينظر:
David Albright and others, Did Stuxnet Take out 1,000 Centrifuges at the Natanz Enrichment Plant?, Institute for Science and International Security's REPORT, **December 22, 2010**, p 1_ 2.

(٢) في عام ٢٠٠٧، نفذت جماعات موالية لروسيا عمليات سيبرانية ضد استونيا، ذ تعرضت لعمليات رفض الخدمة الموزعة "DDoS" لمدة ثلاثة أسابيع، استهدفت مواقع الويب والخدمات الإلكترونية الحكومية والسياسية والمالية في إستونيا، ويعتبر هذا الحدث على نطاق واسع أول عملية سيبرانية هجومية في العالم، ينظر:
Stephen Herzog, Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses, Journal of Strategic Security, Vol. 4, No. 2, p 50.

(3)François Delerue, Op. Cit. p 342; Michael N. Schmitt (GEN. ED.), Tallinn manual on the international law applicable to cyber warfare, Op. Cit. commentary to Rule 10, para 9.

(٤) د. محمود حسين الشرقاوي، مصدر سابق، ص ٢٢٧،

مشروعية التهديد بالأسلحة النووية أو استخدامها، ولكن هنا يجب ملاحظة أن هناك نقطة تمييز جوهرية بين كل من العمليات السيبرانية من جانب وبين الأسلحة التقليدية والنووية من جانب آخر، وهو بأن للنوع الثاني من الأسلحة تأثير واحد فقط عند استخدامها ضد هدف من حيث التدمير المادي والإصابة وفقدان الأرواح، أما العمليات السيبرانية فلها عدة آثار مختلفة وبإمكانها وكما رأينا أن يترتب عليها اضطرابات خطرة في الدولة و تعرض أمنها القومي وحياة مواطنيها للخطر وعرقلة وظائفها الأساسية وبالتالي حصول اضطرابات خطرة في الدولة و تعرض أمنها القومي وحياة مواطنيها للخطر بدون وجود أية آثار مادية.

٢- طالما لا يشترط وجود خطورة كافية لاعتبار فعل ما استخدام للقوة بخلاف ما هو الحال في الهجوم المسلح، قد يكون التركيز على الآثار المادية فقط في بعض الحالات له نتائج غير منطقية، فمثلاً ليس من المنطقي أن نعتبر عملية سيبرانية ما استخداماً للقوة لأنه نتجت عنها تدمير محطة كهرباء تدير قرية صغيرة جداً في حين لا نعتبر العملية السيبرانية التي استهدفت تعطيل محطة كهرباء تدير مدينة كاملة لمجرد أنه في الفرضية الثانية لا يوجد تدمير مادي، فهل من المعقول أن لا نعتبر ذلك استخداماً للقوة بمجرد عدم تعرض بناية المصرف للتدمير في حين نعتبر في الفرضية الأولى كذلك؟ طالما يترتب في الحالتين عدم صلاحية البنية التحتية للغرض الذي من أجلها يتم استخدامها بل وإضافة إلى ذلك في الحالة الثانية نطاقها أوسع.

٣- اعتبار هذه العمليات استخداماً للقوة لا يعتبر تعارضاً مع القول بأن المقصود بالقوة المحظورة هو القوة المسلحة فقط دون غيرها، فكما أشار إليه (Roscini) أصبح التوجه حالياً إلى اعتبار الأسلحة تلك الوسائل التي تنتج عنها مجرد التعطيل وليس فقط الآثار المادية، وهذا هو التوجه السليم في ضوء التطورات التي طرأت على صناعة الأسلحة فإذا كانت في الماضي لا يتصور تعطيل البنية التحتية الحيوية دون تدميرها مادياً نظراً للإمكانيات المتوفرة أنذاك لصناعة الأسلحة أصبحت الآن هذا وارداً بحكم الابتكارات التي وجدها البشر.

**الحالة الثانية: العمليات السيبرانية التي تستهدف البيانات دون إحداث آثار مادية**

هناك عدة مؤلفين أشاروا إلى صعوبة هذه الحالة، فمثلاً وفقاً لـ(Dinniss) الطبيعة غير المادية لآثار العمليات السيبرانية تتسبب في عدم اليقين في تطبيق المتطلبات القانونية للقوة وقوانين الحرب، وتشير إلى أنه في بعض الحالات لا يوجد شيء ملموس يؤثر عليه

العملية كالبيانات[١]، وكذلك يؤكد (Shackelford) أن الصعوبات تنشأ فيما يتعلق بالعمليات السيبرانية التي تستهدف البيانات فقط وتغييرها بدون أية آثار مادية بالمعنى التقليدي[٢]. وبالمثل، يتساءل (Boothby) عما إذا كان عدم تأثير العمليات التي تستهدف البيانات فقط دون حدوث أية تأثيرات أخرى للمنشأة أو الخدمة التي يوفرها نظام الكمبيوتر المستهدف يعتبر استخداماً للقوة[٣]، وللإجابة حول مدى اعتبار هذه العمليات السيبرانية استخداماً للقوة سنبين كل من موقف الفقه والدول وكما يلي.

**موقف الفقه:**

يذهب (Ziolkowski) بأن مجرد إتلاف البيانات حتى ذات الأهمية الكبيرة، على سبيل المثال، البيانات المصنفة أو ذات القيمة الاقتصادية الكبيرة لا يعتبر استخداماً للقوة[٤]، في حين يذهب (Schmitt) بأن مجرد تدمير البيانات أو إتلافها لا يكفي لاعتباره بمثابة هجوم مسلح بل يشترط أن يكون البيانات المستهدفة قابلة للتحويل على الفور إلى أشياء ملموسة، مثل البيانات المصرفية[٥]، ويؤكد (Roscini) بأن وجهة نظر (Schmitt) هذا يطبق على استخدام القوة أيضاً من باب أولى وليس على هجوم مسلح فقط[٦].

ويؤكد البعض على وجوب اعتبار البيانات من ممتلكات الدولة في العصر الحالي، فيذهب (Barkham) إلى القول بأن العمليات السيبرانية التي تؤثر على البيانات فقط دون الأضرار المادية من الصعب شمولها بالمادة (٢/ ٤)، لأنه لا يشمل تعريف الممتلكات البيانات، ويشبه تأثير تدمير البيانات بقصف المصنع، لذلك يدعى بأنه بالنظر إلى أن التقدم التكنولوجي قد زاد من الأهمية الاستراتيجية للبيانات هناك حجة واضحة لمساواة البيانات

(1) Heather Harrison Dinniss, Op. Cit. p 67- 68.
(2) Scott J. Shackelford, From Nuclear War to Net War: Analogizing Cyber Attacks in International Law, Berkeley Journal of International Law, Vol. 27: 1, 2009, p 230.
(3)William H. Boothby, Methods and Means of Cyber Warfare, International Law Studies Series US Naval War College, Vol. 89, 2013, p 389.
(4)Katharina Ziolkowski, Confidence Building Measures for Cyberspace– Legal Implications, NATO CCD COE, Tallinn, 2013. P 75.
(5) Michael N. Schmitt, Cyber Operations in International Law: The Use of Force-Collective Security- Self-Defense, and Armed Conflicts. IN Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy, The National Academies Press, Washington, 2010, p 164.
(6) Marco Roscini, Cyber Operations and the Use of Force in International Law, Op. Cit. p 55.

بالممتلكات، وبالتالي توسيع تعريف الممتلكات ليشمل البيانات أيضاً[١]، كما أكد (Delerue) على أن من الواضح في الوقت الحاضر أنه يجب معاملة البيانات والبرامج على أنها ملكية للدولة بموجب القانون الدولي قياساً على القانون الداخلي، إذ يعترف معظم القوانين الداخلية بملكية البيانات في القوانين المتعلقة بحقوق النشر والملكية الفكرية، وبالمثل يبدو أن بيانات الكمبيوتر محمية على المستوى الدولي إذ تجرم اتفاقية بودابست لعام (٢٠٠١) بشأن الجرائم السيبرانية الجرائم ضد سرية وسلامة وتوافر البيانات والأنظمة الحاسوبية[٢]، كما أكد اعضاء منظمة التجارة العالمية في اتفاقية الجوانب المتصلة بالتجارة من حقوق الملكية الفكرية (تريبس) لسنة (١٩٩٤) على حماية برامج الكمبيوتر وكذلك البيانات[٣]، كما أنه يؤكد بأن العمليات السيبرانية التي تنتج تأثيرات غير مادية فقط قادرة على إحداث تأثيرات واسعة النطاق، وبالتالي يبدو من غير المنطقي عدم تصنيف العمليات السيبرانية على أنها استخدام للقوة إذا كانت لها عواقب تهدد بقاء الدولة المستهدفة[٤].

**موقف الدول:**

أما حول موقف الدول، فقد اعتبرت عدة دول العمليات السيبرانية التي تنتج آثاراً غير مادية فقط في بعض الظروف قد ترقى إلى مستوى استخدام للقوة وكذلك الهجوم المسلح دون الإشارة إلى اتلاف البيانات صراحة، فنجد مثلا فرنسا لا تستبعد إمكانية وصف عملية سيبرانية بدون آثار مادية على أنها استخدام للقوة حتى في حالة عدم وجود ضرر مادي[٥].

بالإضافة إلى ما تقدم أشارت منظمة (AALCO) وتحت بند بعنوان (سيادة البيانات وتدفق البيانات عبر الحدود وأمن البيانات) إلى أنه "نحن نعيش اليوم في عصر رقمي حيث

(1)Jason Barkham, Information Warfare and International Law on the Use of Force, New York University Journal of International Law and Politics, Vol. 34/ 57, 2001, p 88.

(٢) تنص المادة (٤)، من الاتفاقية بعنوان التدخل في البيانات على أنه "١. تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير لتجريم الأفعال التالية في قانونها الوطني، إذا ما ارتكبت عمداً: إتلاف بيانات حاسوبية، حذفها، إفسادها، تعديلها أو تدميرها ٢. يجوز لدولة طرف أن تحتفظ بحقها في أن تستلزم أن تتسبب الأفعال المشار إليها في الفقرة ١، في ضرر جسيم".

(٣) تنص المادة (١٠)، من الاتفاقية على أنه "١- تتمتع برامج الحاسب الآلي (الكمبيوتر)، سواء أكانت بلغة المصدر أو بلغة الآلة، بالحماية باعتبارها أعمالاً أدبية بموجب معاهدة برن (١٩٧١) ٢- تتمتع بالحماية البيانات المجمعة أو المواد الأخرى، سواء أكانت في شكل مقروء آلياً أو أي شكل آخر، إذا كانت تشكل خلقاً فكرياً نتيجة انتقاء أو ترتيب محتوياتها..."

(4)François Delerue, Op. Cit. p 297 and 409.

(5) François Delerue, Op. Cit. p 333; French Ministry of Armed forces, Op. Cit. p 3.

أصبحت البيانات أكثر قيمة من أي وقت مضى"، إضافة إلى إشارتها إلى اتفاقيات التجارة العالمية والاقليمية والتي تؤكد على حماية البيانات(١).

يستخلص مما تقدم بان عدم اقتصار مصطلح (الملكية) على الأشياء الملموسة يحظى بالقبول في القانون الداخلي كما أن القانون الدولي يعترف بالحماية المتوافرة للبيانات، لذلك وطالما أن الآثار المباشرة للعمليات السيبرانية تكون على البيانات في الغالب فهذا يعني بأن البيانات هي في الأصل التي تتأثر بهذه العمليات، بمعنى آخر الأضرار المادية غالباً ما تكون من الاثار غير المباشرة بينما الضرر غير المادي هو الأصل، وبالتالي من الضروري الإقرار بملكية الدولة للبيانات في العصر الرقمي الذي أصبحت البيانات فيه ذات أهمية بالغة، ذلك العصر الذي تعتمد غالبية الدول على التكنولوجيا لحفظ بياناتها، فإذا كان في الماضي تحتفظ الدول بالبيانات المتعلقة بالضرائب أو غيرها في سجلات ورقية والتي لم يكن من المتوقع اتلافها إلا بوجود آثار مادية أصبحت في يومنا وبعد نقلها من سجلات ورقية إلى أجهزة كمبيوتر بالإمكان اتلافها دون حدوث أية أثر مادي.

## II. المبحث الثاني
## ممارسة حق الدفاع عن النفس ضد العمليات السيبرانية

بالرغم من أن ميثاق الأمم المتحدة حظر استخدام القوة أو التهديد بها، إلا أنه اقر بالحق الاساسي للدول في الدفاع عن النفس بموجب المادة (٥١)، إذ وردت فيه "ليس في هذا الميثاق ما يضعف أو ينتقص الحق الطبيعي للدول، فرادى أو جماعات، في الدفاع عن أنفسهم إذا اعتدت قوة مسلحة على أحد أعضاء الأمم المتحدة وذلك إلى أن يتخذ مجلس الأمن التدابير اللازمة لحفظ السلم والأمن الدولي، والتدابير التي اتخذها الأعضاء استعمالاً لحق الدفاع عن النفس تبلغ إلى المجلس فورا..."، وممارسة هذا الحق يتطلب وجود بعض الشروط منها ما يتعلق بفعل العدوان الذي يبرر ممارسة هذا الحق، ومنها ما يتطلب توافرها في فعل الدفاع التي تلجأ إليه الدولة الضحية لصد العدوان، ويثير التساؤل في مجال العمليات السيبرانية حول مدى امكانية تطبيق هذه الشروط وبالتالي وجود حق الدفاع عن النفس ضد العمليات السيبرانية، ولتوضيح ذلك سنقسم هذا المبحث إلى مطلبين، في المطلب الأول سنبين الشروط المتعلقة بفعل العدوان، أما المطلب الثاني فسنتناول فيه الشروط المتعلقة بفعل الدفاع.

(١) المنظمة الاستشارية القانونية الآسيوية -الإفريقية، القانون الدولي في الفضاء السيبراني، وثيقة رقم AALCO/59/HONG KONG/2021/SD/S17 الصادرة في ٢٠٢١، فق ٥٥- ٦٥، ص ١٩.

## II.أ. المطلب الأول

## الشروط المتعلقة بفعل العدوان

هناك عدة شروط يجب أن تتوافر في فعل العدوان لكي يكون الدفاع ضده مشروعاً، ولم تتضمن المادة (٥١) جميع هذه الشروط، فبعض منها وردت فيها، إلا أن البعض الآخر مصدره القواعد العرفية بالإضافة إلى قرار الجمعية العامة للأمم المتحدة بشأن تعريف العدوان (رقم ٣٣١٤) لعام (١٩٧٤)[١]، وسنبين فيما يلي هذه الشروط:-

### أولاً: أن يكون هناك عدوان مسلح

لم يعرف ميثاق الأمم المتحدة مصطلح العدوان، ومرت تعريف العدوان بمراحل تاريخية عديدة[٢]، إلا أن تبنت الجمعية العامة للأمم المتحدة قرار رقم (٣٣١٤/ ٢٩) في (١٤ ديسمبر/ كانون الأول ١٩٧٤) بشأن تعريف العدوان، حيث عرف العدوان بأنه "استعمال القوة المسلحة من قبل دولة ما ضد سيادة دولة أخرى أو سلامتها الإقليمية أو استقلالها السياسي، أو بأية صورة أخرى تتنافى مع ميثاق الأمم المتحدة"[٣].

وبالتالي يجب لاعتبار الفعل عدواناً أن يكون استخداماً للقوة المسلحة، وبينا سابقاً إمكانية اعتبار العمليات السيبرانية استخداماً للقوة المسلحة، ولكن بالإضافة إلى اشتراط وقوع فعل عدوان يجب أن يكون العدوان مسلحاً، ويعتبر الفعل عدواناً مسلحاً عندما يكون هناك هجوم مسلح من دولة أخرى، وذلك لأن الغاية من وضع المادة (٥١) من الميثاق هو حفظ السلم والأمن الدوليين لذا نص على حظر استخدام القوة في العلاقات الدولية، لهذا فالحالات التي لا تعد هجوماً مسلحاً لا تبرر فعل الدفاع عن النفس كالتهديد للأمن والسلم والعدوان الاقتصادي والفكري[٤].

لذلك وبالرغم من أنه في قضية نيكاراغوا، أشارت محكمة العدل الدولية إلى تعريف الجمعية العامة للعدوان لعام ١٩٧٤ من أجل تحديد مفهوم هجوم مسلح، إلا أن (العدوان) مفهوم أوسع من (الهجوم المسلح)، حيث يعتبر الأخير فئة فرعية من الأولى. من بين الحالات

---

(١) د. محمود حسين الشرقاوي، مصدر سابق، ص ٢٤٦.

(٢) في ذلك ينظر:- د. صلاح الدين احمد حمدي، *العدوان في ضوء القانون الدولي العام*، ط ١، (بيروت: منشورات زين الحقوقية)، ص ٢٩- ٤٤.

(٣) المادة (١)، من قرار رقم ٣٣١٤/ ٢٩ الصادرة من الجمعية العامة للأمم المتحدة، الوثيقة (A/RES/3314(XXIX))، في ١٤ ديسمبر/ كانون الأول ١٩٧٤.

(٤) د. صلاح الدين أحمد حمدي، مصدر سابق، ص ٦٦، د. سامي السعد، "حق الدفاع الشرعي في القانون الدولي العام"، *بحث منشور في مجلة القانون المقارن، جمعية القانون المقارن العراقية*، العدد ٣، (١٩٧٠): ص ١٩٠.

المدرجة في القرار (٣٣١٤/ ٢٩)، يعتبر فقط الفقرة (أ، ب، د، ز) من المادة (٣) هجوماً مسلحاً يبرر الدفاع عن النفس أما الفقرات الأخرى فلا تعتبر كذلك، وبالتالي عمل دولة ما بالسماح باستخدام أراضيها، التي وضعتها تحت تصرف دولة أخرى من قبل تلك الدولة الأخرى لارتكاب عمل عدواني ضد دولة ثالثة لا يرقى إلى مستوى هجوم مسلح، فالدولة التي تسمح عن علم لدولة أخرى باستخدام بنيتها التحتية السيبرانية من أجل شن عملية سيبرانية ترقى إلى حد العمل العدواني، تخرق حظر استخدام القوة ولكنها لن تعتبر هجوماً مسلحاً[١].

ومن أجل اعتبار استخدام القوة هجوماً مسلحاً يجب أن تكون على درجة من الخطورة، حيث من المعروف أن محكمة العدل الدولية اعتبرت أن الهجوم المسلح هو أخطر أشكال استخدام القوة، في حين القوة المسلحة يعتبر الأقل خطورة، واعتمدت معيار (النطاق والآثار) من أجل التمييز بينهما[٢]، وبالإضافة إلى ذلك ورد في (المادة (٢) من قرار تعريف العدوان بأنه "المبادأة باستعمال القوة من قبل دولة ما خرقا للميثاق تشكل بينة كاقية مبدئيا على ارتكابها عملا عدوانياً، وإن كان لمجلس الأمن، طبقا للميثاق، أن يخلص إلى أنه ليس هناك عملاً عدوانياً قد ارتكب وذلك في ضوء ملابسات أخرى وثيقة الصلة بالحالة، بما في ذلك أن تكون التصرفات محل البحث أو نتائجها ليست ذات خطورة كافية"، فإن كان العدوان يتطلب الخطورة الكافية فمن باب أولى يجب أن يكون الهجوم المسلح كذلك لأنه يعتبر فرعاً من العدوان كما اشرنا إليه سابقاً، وبالتالي استخدام القوة المسلحة هو (هجوم مسلح) فقط عندما يكون نطاقه وآثاره خطيرة بما فيه الكفاية، ولكن يلاحظ بأن الفجوة بين (استخدام القوة) و (الهجوم المسلح) ليست واسعة بالضرورة، كما أكدت محكمة العدل الدولية في قضية منصات النفط حيث لم تستبعد احتمال أن يكون تفجير سفينة عسكرية واحدة كافياً لنشوء الحق في الدفاع الشرعي[٣].

ومن أجل بيان المقصود بـ (النطاق والآثار) يؤكد البعض بأن هناك إجماع دولي على أن المعايير التي ذكرها (pictet) يمكن الأخذ بها لتقييم ما إذا كان استخدام معين للقوة المسلحة قد تصل إلى ستوى الهجوم المسلح، حيث أشار (pictet) إلى وجود نزاع مسلح دولي بموجب المادة (٢) المشتركة لاتفاقيات جنيف لعام (١٩٤٩) بغض النظر عن معايير ثلاثة وهي "المدة التي تستغرقها النزاعات، أو مقدار المذابح التي تحدث، أو عدد القوات

(1)Marco Roscini, Cyber Operations and the Use of Force in International Law, Op. Cit. p 71.
(2)Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), Merits, Judgment. I.C.J. Reports, 1986, p. 14. para 191.
(3)Marco Roscini, Cyber Operations and the Use of Force in International Law, Op. Cit. p 72- 73.

المشاركة"[١]. لذلك وكما يؤكد (Ruys) بأنه يقصد بالنطاق مقدار القوة المسلحة المستخدمة ومدتها ومكانها، في حين أن المقصود بالآثار هو الضرر الناجم عن استخدام هذه القوة أي الاصابات التي وقعت[٢]. وبالتالي مثلاً عملية DDoS التي تتم عن طريق استخدام ملايين شبكات الروبوت وينتج عنها مجرد تعطيل البنية التحتية الحيوية المتعلقة بصفحات الويب ولفترة محدودة هي بالتأكيد خطيرة فيما يتعلق بالنطاق ولكن آثارها ليست كذلك وبالتالي لا تعتبر هجوماً مسلحاً[٣].

فالعمليات السيبرانية التي تنطوي على انقطاع صغير للخدمات الإلكترونية غير الأساسية من الواضح أنها لا تعتبر هجوماً مسلحاً، وعلى العكس من ذلك فالعمليات السيبرانية التي تؤدي إلى إصابة عدد من الأشخاص بإصابات خطيرة أو قتلهم أو تتسبب في إلحاق ضرر جسيم بالممتلكات أو تدميرها من شأنها أن تفي بمتطلبات النطاق والآثار وبالتالي تعتبر هجوماً مسلحاً[٤].

وبسبب هذا الشرط لا يوجد اتفاق بالإجماع على اعتبار حادثة ستوكسنت هجوماً مسلحاً، ففي حين ذهب بعض الخبراء من الفريق المعد لدليل تالين إلى اعتبار حالة ستوكسنت هجوماً مسلحاً نظراً لأضرارها المادية التي لحقت بالأجهزة الموجودة في محطة نطنز النووي، إلا أن البعض الآخر منهم وكذلك غالبية الباحثين يذهبون إلى عدم وصفها بهجوم مسلح مع أن هناك اتفاق على اعتباره استخداماً للقوة المحظورة كما اشرنا إليه سابقاً وذلك نظراً لآثارها المحددة على البرنامج النووي الإيراني بالرغم من وجود اضرار مادية، فقد ترتبت عليها مجرد ابطاء البرنامج النووي الإيراني دون توقفها وبالتالي لا يبدو أن آثار الحادثة كانت كافية لاعتباره هجوماً مسلحاً[٥].

(1)Jean S. pictet, The Geneva Conventions of 12 August 1949. Commentary. Volume III: Relative to the Treatment of Prisoners of War, ICRC, 1960, p 23; David E. Graham, Cyber Threats and the Law of War, Journal of National Security Law & Policy, Vol. 4:87,2010, p 90; jeffrey Carr, Inside cyber warfare: mapping the cyber underworld, O'Reilly Media, 2011, p 58.

(2)Tom Ruys, Armed Attack and Article 51 of the UN Charter, Cambridge University Press, 2010, p 139.

(3)Duncan Blake and Joseph S Imburgia, Bloodless Weapons? The Need to Conduct Legal Reviews of Certain Capabilities and the Implications of Defining Them as Weapons, Air Force Law Review, Vol. 66, 2010, p 186.

(4) Michael N. Schmitt (GEN. ED.), Tallinn manual on the international law applicable to cyber warfare, Op.Cit. commentary to Rule 13, para 6.

(5)Heather Harrison Dinniss, Op. Cit. p 81- 82; François Delerue, Op. Cit. p 333, Michael N. Schmitt (GEN. ED.), Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, Op. Cit. commentary to Rule 71, para 10.

وفي الحقيقة للتمييز بين العدوان المسلح والعدوان الذي لا يصل لمستوى الهجوم المسلح أهمية كبيرة، وذلك لانه في حالة العدوان المسلح يكون للدولة المعتدية الحق في استخدام القوة في سياق الدفاع عن النفس، أما استخدام القوة الذي لا يرتقي إلى الهجوم المسلح لا يكون للدولة المعتدية الحق في الدفاع عن النفس بل يحق لها عدة خيارات قانونية أخرى منها التدابير المضادة التي تعطي للدولة المتضررة القدرة على رد الاعتداء بطرق أخرى دون استخدام القوة[١].

**الشرط الثاني: يجب أن يكون العدوان المسلح حالاً**

ومعنى ذلك أن يكون العدوان المسلح قد وقع فعلاً وبالتالي إذا كان العدوان لم يقم بعد أو أنه وقع وانتهى وتمت آثاره فلا مجال لإثارة حق الدفاع عن النفس[٢]، وفي هذا الشأن ظهر خلاف فقهي حول مدى شرعية الدفاع عن النفس الوقائي، بمعنى آخر جواز الدفاع عن النفس ضد عدوان مسلح قبل وقوعه[٣]، ولكن الراجح عند الغالبية هو عدم جوازه وذلك لعدة حجج منها[٤]:

- ادراج حق الدفاع عن النفس في الميثاق بحد ذاته يعتبر تضييقاً لنطاقه وطالما انه تم تنظيمه بعدما كان معترف بها في القانون الدولي التقليدي فهذا يعني وضع القيود على ممارستها.

- بالرغم من وجود تناقض بين عبارات النص حيث تناقض عبارة "الحق الطبيعي الراسخ" مع "إذا وقع هجوم مسلح" إلا أن تفسير النص يجب أن يتم بأكمله فالعبارة الثانية تعد تضييقاً للعبارة الأولى أي أنها مكملة لها، فعبارات النص تفسر بعضها البعض.

- لم يتم شمول حق الدفاع عن النفس للمواطنين في الخارج على الرغم من الاعتراف به في القانون الدولي التقليدي.

وفي السياق السيبراني أقرت بعض الباحثين بوجود هذا الحق وذلك أخذاً بنظر الاعتبار طبيعة العمليات السيبرانية التي يتسم بالسرية، والمفاجئة، والفورية، والتي يصعب

(١) أ د. صلاح عبدالرحمن الحديثي وكاميران عزيز حسن، *التفصيل الشامل لتطور القواعد القانونية الخاصة بالحرب السيبرانية*، ط ١، (الجيزة: مجموعة ثري فريندز للنشر والتوزيع والمجموعة العلمية للنشر والتوزيع، ٢٠٢١)، ص ٢٣٠.

(٢) د. ابراهيم الدراجي، *جريمة العدوان ومدى المسؤولية الدولية عنها*، ط ٢، (بيروت: منشورات الحلبي الحقوقية، ٢٠١٩)، ص ٢٣٤.

(٣) ينظر في هذه الاتجاهات: د. عباس المراغي ناصر، *القضاء الجنائي الدولي (حق الدفاع الشرعي عن النفس والاباحة الجنائية في إطار القانون الدولي)*، (الاسكندرية: مكتبة الوفاء القانونية، ٢٠١٧)، ص ١٦٣-٢٠٨.

(٤) للمزيد ينظر استاذنا د. قاسم أحمد قاسم، مصدر سابق، ص ١٧- ٢١.

تحديد مصدرها، أو نسبتها إلى جهة معينة بشكل مؤكد في وقت مناسب، علاوة على أنها يمكن أن تؤدي إلى عواقب يتعذر تدارك أثارها، وعلى ضوء ذلك، يكون الالتزام الصارم بالمعيار الزمني غير منطقي لأن الوقت بين اتخاذ قرار إجراء هجوم عبر الفضاء السيبراني ، وتنفيذه، وتحقق عواقبه يمكن قياسه بالملي ثانية، فإذا كان للحق في الدفاع عن النفس أي مضمون، فيجب أن تكون الدولة قادرة على التصرف لتفادي مثل هذا الهجوم، بمجرد علمها بأنه على وشك التنفيذ وأنها إذا ترددت في الاستجابة فإنها تخاطر بفقدان فرصة الدفاع عن نفسها بفعالية(١).

ومن أبرز الباحثين الذين يؤيدون حق الدفاع عن النفس الوقائي هو (Schmitt) الذي وضع اختباراً يتضمن عدة شروط للقول بنشأة حق الدفاع عن النفس الوقائي للدولة الضحية أطلق عليها (نافذة الفرصة الأخيرة- last window of opportunity)، فهو يذهب بأنه باعتبار أن الخطر يكون وشيكاً، عندما تكون نافذة الفرصة لاتخاذ إجراء منعه على وشك الإغلاق وبالتالي، يجوز للدولة أن تمارس حقها في الدفاع عن النفس لأن عدم القيام بذلك يمثل مخاطرة فقدان فرصة منع تلك العمليات بشكل فعال(٢).

وهذا هو توجه فريق الخبراء المعني بإعداد دليل تالين (١ و٢) أيضاً إذ وضعوا قاعدة خاصة بهذا الشأن التي تنص على أنه "ينشأ الحق في استخدام القوة في الدفاع عن النفس في حالة وقوع هجوم مسلح سيبراني أو وشيك"، وفي التعليق على القاعدة المذكورة أكدوا على اختبار (Schmitt)(٣).

(١) ينظر: د. محمد عادل محمد عسكر، مصدر سابق، ص ٢٩٩؛ د. محمود حسين الشرقاوي، مصدر سابق، ص ٢٩٤.

(٢) أكدت "Schmitt" هذا المعيار في عدة من مؤلفاته، ينظر:
Michael N. Schmitt, Responding to Transnational Terrorism Under the Jus Ad Bellum: A Normative Framework, Naval Law Review, Vol. 1, 2008, p 16- 20; Michael N. Schmitt, Cyber Operations and the Jus Ad Bellum Revisited, Villanova Law Review, Vol. 56, 2011, p 592; Michael N. Schmitt, Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework. Op. Cit. p 932.

(3)Michael N. Schmitt (GEN. ED.), Tallinn manual on the international law applicable to cyber warfare, Op. Cit. commentary to Rule 15, para 4; Michael N. Schmitt (GEN. ED.), Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, Op. Cit. commentary to Rule 73, para 4.

ويميز الباحثين بين حالتين في هذا الشأن وهما: أولاً، عندما يكون العملية السيبرانية بمثابة تهديد وشيك لهجوم مسلح تقليدي، وثانياً، عندما تشير العملية السيبرانية إلى عملية سيبرانية يرتفع إلى مستوى هجوم مسلح وشيك الحصول[١].

ففي الحالة الأولى يتطلب اختبار (Schmitt) ثلاثة شروط يجب توافرها للقول بوجود عملية سيبرانية وشيكة يؤدي إلى تفعيل حق الدفاع عن النفس وهي: أولاً، يجب أن تكون العملية السيبرانية جزءٌ من عملية شاملة تنتهي بوجود هجوم مسلح، ثانياً: يجب أن تشكل العملية السيبرانية خطوة لا رجوع عنها في هجوم وشيك (على المدى القريب) وربما لا مفر منه، وثالثاً: أن تكون المبادرة بالهجوم تمثل آخر فرصة لدى الدولة للدفاع أو كما يسمى (Schmitt) (آخر نافذة لها)، وإذا لم تغتنمها فلن تتمكن من درء الخطر[٢]، ويؤكد (Delerue) بأنه من الواضح أنه سيكون من المستحيل تقريباً في معظم الحالات تحديد أن العملية السيبرانية جزءًا من عملية شاملة تنتهي بوجود هجوم مسلح، وبالتالي يبدو الشروط المذكورة صعب التطبيق للغاية إن لم يكن مستحيلا. والمثال عليها هو العمليات السيبرانية ضد استونيا عام (٢٠٠٧) فيمكن اعتبارها بمثابة الخطوة الأولى لتدخل وشيك من قبل روسيا ضد إستونيا، ومع ذلك لم يحدث أي هجوم مسلح تقليدي. وبالتالي، فإن أي رد عسكري من إستونيا ضد روسيا على أساس الدفاع الوقائي عن النفس سيكون غير مبرر وغير قانوني[٣].

أما الحالة الثانية فتتعلق باكتشاف عملية سيبرانية موجودة ومن المحتمل أن تشكل الخطوة الأولى لعملية سيبرانية تصل لمستوى هجوم مسلح، والمثال على ذلك أن تكتشف الدولة وجود فيروس في النظام قبل حصول أية هجوم مسلح سيبراني ففي هذه الحالة هل يمكن أن نعتبر مجرد وجود الفيروس دليلاً على اقتراب هجوم مسلح سيبراني، الجواب بالطبع هو سلبي وذلك لأن وجود الفيروس قد يكون لمجرد التجسس فقط[٤]، أما في حالة وجود قنبلة مؤقتة، يذهب (Schmitt) بأنه يجب أن تتأكد الدولة الضحية بأنه: ١) قرر المهاجم استغلال نقاط الضعف هذه فعلياً ٢) من المحتمل أن تصل نطاق وآثار العملية السيبرانية لمستوى الهجوم المسلح، ٣) تنشيط البرامج الضارة وشيكاً[٥].

(1)Marco Roscini, Cyber Operations and the Use of Force in International Law, Op. Cit. p 79; Heather Harrison Dinniss, Op. Cit. p 88.
(2) Michael N. Schmitt, Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework, Op. Cit. p 932- 933.
(3)François Delerue, Op. Cit. p 474.
(4)ibid, p 475.
(5)Michael N. Schmitt, Cyber Operations and the Jus Ad Bellum Revisited, Op. Cit. p 592- 593.

وفي هذه الحالة وكما أشار إليه (Delerue) ومن الواضح بأنه حالة الدفاع الشرعي غير مبرر فاكتشاف دولة ما وجود عملية سيبرانية ضدها ستصل لمستوى هجوم مسلح ولكنها لم تصل بعد سيكون بإمكانها ازالتها بدلاً من اللجوء لاستخدام القوة وبالتالي في هذه الحالة ليست مسألة مدى شرعية حق الدفاع عن النفس الوقائي بل هي مسألة عدم تماثلها لشرط الضرورة الذي تفرض على الدولة عدم اللجوء لاستخدام القوة للدفاع عن نفسها إذا كان بإمكانها درء الخطر بوسائل غير قسرية[١]، وذهب (Focarelli) بأنه القول بجواز الدفاع عن النفس الوقائي في السياق السيبراني وجهة نظر تخمينية بحتة، لأنه من الصعب للغاية تتبع العمليات السيبرانية حتى بعد حدوثها ومن الصعب تحديد الجهة الصادرة عنها فعل العدوان المسلح[٢].

وبناء على ما تقدم تبينت لنا بان حق الدفاع عن النفس الوقائي مشروع في السياق التقليدي أما في السياق السيبراني فعلاوة على عدم مشروعيته تبدو وكأنه من الصعب إن لم يكن مستحيلاً القول بوجوده، فحتى الباحثين الذين يتجهون نحو القول بشرعيته يضعون شروط مستحيلة التطبيق.

**الشرط الثالث: يجب أن يكون العدوان مباشراً**

يقصد بهذا الشرط استعمال الدولة لقواتها المسلحة بطريقة غير مشروعة ضد دولة أخرى[٣]. أما العدوان غير المباشر فيقصد بها العدوان الذي لا تستخدم فيه الدولة القوة المسلحة ومن اكثر صور العدوان غير المباشر انتشاراً واثارة للجدل هو تقديم العون للجماعات المسلحة[٤]، في هذه الحالة يشترط أن يكون العدوان المسلح منسوباً للدولة، فالرأي السائد بأنه يشترط العدوان أن يكون صادراً من الدولة وذلك استناداً إلى المادة الأولى من قرار الجمعية العامة للأمم المتحدة رقم (٣٣١٤ لسنة ١٩٧٤) بشأن تعريف العدوان التي تنص على أنه "العدوان هو استعمال القوة المسلحة من قبل دولة ما.."[٥]، كما أكدت ما وردت في المادة (٣/ ز) من قرار تعريف العدوان ذلك فمن خلال دراسة هذا النص يتبين بأن مجرد الدعم لا يعتبر عدواناً ففي الجزء الأول يشترط الإرسال والتي تعني إتيان فعل مادي المكون لجريمة

(1)François Delerue, Op. Cit. p 475- 476.

(2) Carlo Focarelli, Self-defence in cyberspace. IN Research Handbook on International Law and Cyberspace, Nicholas Tsagourias and Russell Buchan (eds.), Edward Elgar Publishing, 2021, p 335.

(٣) د. كمال حماد، *النزاع المسلح والقانون الدولي العام*، ط ١، (بيروت: مجد المؤسسة الجامعية للدراسات والنشر والتوزيع، ١٩٩٧)، ص ٣١.

(4) Hans Kelsen, international law studies, 1956, p 63.

(٥) ينظر: د. محمود حسين الشرقاوي، مصدر سابق، ص ٢٦٠.

العدوان ويختلف ذلك عن الدعم والجزء الثاني من الفقرة نص على أن تلك الجماعات تعمل باسم الدولة[١].

وكذلك أقرت محكمة العدل الدولية هذا الحكم عندما قررت بأنه لا يشترط لاعتبار فعل العدوان هجوماً مسلحاً أن تنفذه الدولة مستعملاً جيشها النظامي بل يعتبر كذلك إرسال عصابات أو جماعات مسلحة، من قبل دولة أو بالنيابة عنها، غير النظاميين أو المرتزقة، الذين ينفذون أعمال القوة المسلحة ضد دولة أخرى من الخطورة بحيث ترقى إلى (من بين أمور أخرى) هجوم مسلح فعلي تقوم به القوات النظامية أو مشاركتها الكبيرة فيها هجوماً مسلحاً[٢]، وجدير بالذكر بأن محكمة العدل الدولية ميزت في قضية نيكاراغوا ضد الولايات المتحدة الأمريكية بين مجرد تقديم العون المالي واعتبرها انتهاكاً لعدم التدخل دون أن يكون استخداماً للقوة، وبين تقديم الأسلحة والتدريب للجماعات المسلحة حيث اعتبرها استخداماً للقوة ولكن ليس هجوماً مسلحاً يؤدي إلى تفعيل حق الدفاع عن النفس[٣].

أما مدى جواز الدفاع عن النفس ضد العمليات التي لا تثبت إسنادها للدولة حتى ولو تم تقديم العون من قبل الدولة أو بدونه، أثارت جدلاً واسعاً ولا نخوض في تفاصيلها، ونكتفي بالإشارة إلى أنه لم يتم تسوية الجدل في هذا الشأن، ولا يمكن تأكيد ما إذا كان حق الدفاع عن النفس يمتد بعد ليشمل العمليات التي تشنها جهات فاعلة من غير الدول لا تُنسب إلى دولة أم لا[٤].

وبالتالي فإن مجرد انطلاق بعض الجماعات المسلحة من فوق اقليم الدولة لشن العمليات السيبرانية ضد دولة اخرى لم يثبت باليقين انتساب تلك الجماعات المسلحة الى الدولة التي انطلقت منها لا تعتبر العملية منسوباً للدولة، وفي هذه الحالة قد تكون الدولة الأولى متواطئة مع تلك الجماعات المسلحة ولم يتم بعد اثبات انتمائها إلى تلك الدولة، أو قد تكون الدولة لا تعلم بانطلاق هذه الجماعات من اقليمها ولا تعلم بوجودها أصلاً، في الحالة الأولى تكون الدولة مسؤولة عن التدخل المحظور في المادة (٢/ ٧) من ميثاق الأمم المتحدة، أما الحالة الثانية فتقوم مسؤوليتها وفقاً للعناية الواجبة بسبب تقصيرها في اتخاذ واجب الحيطة

(١) ينظر استاذنا: د. قاسم أحمد قاسم، مصدر سابق، ص ١٢١.

(2)Military and Paramilitary Activities in and against Nicaragua, Op. Cit. para 195.

(٣) ينظر: أ.د صلاح عبدالرحمن الحديثي وكاميران عزيز حسن، مصدر سابق، ص ٢٤١.
Military and Paramilitary Activities in and against Nicaragua, Op. Cit. para. 228, 230.

(4) François Delerue, Op. Cit. p 463; Michael N. Schmitt (GEN. ED.), Tallinn manual on the international law applicable to cyber warfare, Op. Cit. commentary to Rule 13, paras 2, 15- 18.

لمنع استخدام أراضيها لهذه العمليات، ولكن في كلتا الحالتين لا تعتبر العملية منسوبة للدولة طبقاً لقواعد الإسناد وبالتالي لا يحق للدولة استعمال حق الدفاع عن النفس[١].

## II.ب. المطلب الثاني

## الشروط المتعلقة بفعل الدفاع

فعل الدفاع عن النفس ضد العمليات السيبرانية التي ترقى إلى العدوان المسلح، مثل أي رد فعل للدفاع عن النفس ضد الدول أو الجهات الفاعلة غير الحكومية، يجب أن يفي بشرطي الضرورة والتناسب، على الرغم من أن المادة (٥١) لا تشير إلى هذه الشروط، إلا أنه في الرأي الاستشاري بشأن مشروعية التهديد بالأسلحة النووية أو استخدامها، أكدت محكمة العدل الدولية أن "إخضاع ممارسة حق الدفاع عن النفس لشرطي الضرورة والتناسب هو قاعدة من قواعد القانون الدولي العرفي، وينطبق هذا الشرط المزدوج بالتساوي على المادة (٥١) من الميثاق مهما كانت وسائل القوة المستخدمة"[٢].

ويرجع الأصل العرفي لهذه الشروط إلى (حادثة كارولين) في عام (١٨٣٧)، الذي اعتاد الكتاب والدول الرجوع إليها لدعم الادعاء بحق الدفاع عن النفس، حيث أوضحت المحكمة الأمريكية في قضية كارولين بأن الدفاع عن النفس مقيد بشرطي الضرورة والتناسب بين العدوان وفعل الدفاع[٣]، وفيما يلي نوضح هذين الشرطين.

### الشرط الأول: الضرورة

يهدف شرط الضرورة إلى تحديد ما إذا كان التدبير المعين المعتمد في الدفاع عن النفس ضروريًا لتحقيق الغرض المشروع للدفاع عن النفس. وبعبارة أخرى، يجب أن يكون التدبير المحدد ضروريًا لصد الهجوم المسلح، ويتضمن شرط الضرورة عدة متطلبات وهي: -

**أولاً: يجب أن يكون الدفاع الوسيلة الوحيدة**: ومعنى ذلك عدم وجود وسائل اخرى غير اللجوء للقوة المسلحة لصد العدوان أي عدم وجود بدائل اخرى وعلى ذلك متى ما وجدت وسائل أخرى ولم تلجأ اليها الدولة فإنها تكون قد ارتكبت فعلاً غير مشروع بمعنى أنها تقوم بالعدوان ويحق للطرف الاخر في هذه الحالة استخدام القوة دفاعاً عن النفس، وعليه إذا تمكنت الدولة المعتدى عليها من الاستعانة في وقت مناسب بمعونة منظمة دولية وكانت هذه المعونة

(١) د. مرابط وسيلة، *استخدام القوة في العلاقات الدولية وأثره على فرض الشرعية*، ط ١، (الجيزة: مركز الدراسات العربية للنشر والتوزيع، ٢٠٢١)، ص ٢٠٤.

(2) Legality of the Threat or Use of Nuclear Weapons, Op. Cit. Para 41.

(٣) د. محمد خليل الموسى، *استخدام القوة في القانون الدولي المعاصر*، ط ١، (عمان: دار وائل للنشر والتوزيع، ٢٠٠٤)، ص ٩٨.

كافية لحمايتها من العدوان المسلح المرتكب ضدها فلا يكون للدفاع عن النفس محل في هذه الحالة [١]، وبالتالي يجب أن لا يمكن تسوية الأمر بوسائل أقل تدخلاً والتي تحتوي على تدابير غير قسرية، وفي الحقيقة يمنع اللجوء إلى الدفاع عن النفس في معظم العمليات السيبرانية وذلك لأنه في معظم الحالات ستكون التدابير غير القسرية متاحة لصد العمليات السيبرانية، مما يجعل الدفاع عن النفس غير ضروري، وهذا يرجع لسببين، الأول قد تكون الدولة المستهدفة قادرة على تعديل الميزات الأمنية لنظامها الخاص أو تصحيح نقاط الضعف التي تستغلها العملية السيبرانية، وبالتالي يصبح الدفاع عن النفس زائداً عن الحاجة. أما الثاني فينبغي للدولة المستهدفة أولاً أن تنظر في إمكانية اتخاذ تدابير مضادة ضد الدولة المستهدفة قبل التفكير في اتخاذ تدابير للدفاع عن النفس. وبالتالي، إذا كان لدى الدولة المستهدفة إمكانية اتخاذ إجراء مضاد سيبراني، مثل إيقاف تشغيل الكمبيوتر المستخدم في تقييم العملية السيبرانية، فإن هذا هو الخيار المفضل على استخدام القوة في الدفاع عن النفس. فقط إذا كانت جميع الخيارات غير القسرية غير كافية لصد العملية السيبرانية، فسيكون للدولة الضحية الحق في اللجوء إلى القوة دفاعاً عن نفسها[٢]، ويلاحظ بأنه يجب أن تكون الوسيلة الوحيدة ممكنة بالفعل وأن تكفل الحفاظ على حقوق الدولة وسلامتها واستقلالها وأن تكون مشروعة، وبالتالي اذا وجدت وسائل اخرى لكن لا تتمتع بتلك الصفات فإن وجودها لا يمنع الدولة المستهدفة بالعدوان من استخدام حقها في الدفاع الشرعي[٣].

**ثانياً: يجب أن يوجه الدفاع ضد الدولة المعتدية دون غيرها**: فلا يجوز أن يكون مصدر العدوان دولة ما ويوجه الرد الى دولة اخرى وإلا كان الرد عدواناً، فلا يجوز الدفاع ضد دولة أخرى أو انتهاك حياد دولة غير مشتركة في فعل العدوان المسلح، ومن أجل تحقيق هذا الشرط يجب تحديد هوية الفاعل[٤]، وبالرغم من أن الإسناد صعب في السياق السيبراني، إلا أن هذه الصعوبة لا يجب أن تكون ذريعة لعدم القيام بمعالجة الجوانب القانونية الدولية للعمليات السيبرانية، حيث أن مشكلة الاسناد موجودة بالفعل في العديد من السياقات الأخرى وليست سمة فريدة للعمليات السيبرانية فهي موجودة على سبيل المثال في الإرهاب الدولي أو في بعض الظروف الحرب التقليدية بشكل خاص في المجال البحري، إلا أن ذلك لم يمنع من وضع إطار قانوني لها، بالإضافة إلى أن إلا أنها ليست مستحيلة فهي تحتاج للعمل على

(١) د. محمد محيي الدين عوض، "دراسات في القانون الدولي الجنائي"، *بحث منشور في مجلة القانون والاقتصاد*، العدد الثانية، السنة الخامسة والثلاثون، (١٩٦٥): ص ٦٥٦.

(2)François Delerue, Op. Cit. p 480.

(٣) د. ابراهيم الدراجي، مصدر سابق، ص ٢٤٢.

(٤) محمد محمود خلف، "حق الدفاع الشرعي في القانون الدولي الجنائي"، (اطروحة دكتوراه مقدمة لجامعة القاهرة، ١٩٧٣)، ص ٤٤٥.

التطور التكنولوجي مما يتطلب تكاليف كبيرة، بالإضافة إلى جمع المعلومات الاستخباراتية سواء على طريقة التقليدية أو السيبرانية[١].

**ثالثاً: الفورية:** يؤدي مبدأ الضرورة أيضًا إلى نشوء مبدأ ذي صلة، وهو أن الإجراءات المتخذة دفاعًا عن النفس يجب عموماً أن تُتخذ دون تأخير لا داعي له وهو ما يسمى ب (شرط الفورية)[٢]، وبمعنى آخر حق الدفاع عن النفس يبدأ مع بداية الهجوم المسلح وينتهي بانتهائه، وفي الحقيقة إن الأخذ بهذا الشرط بشكل صارم يؤدي بنا إلى القول بعدم وجود حق الدفاع عن النفس ضد العمليات السيبرانية، وذلك لأنه العمليات السيبرانية تبدأ وتنتهي خلال مدة زمنية تستغرق بضع ثواني أي لا يستمر لفترة زمنية بحيث تستطيع الدول الدفاع عن نفسها لحين تدخل مجلس الأمن بشكل ملائم وفي ذلك تشبه العمليات السيبرانية مع العمليات الإرهابية[٣]، وعليه ومن الناحية العملية يفترض بأن شرط الفورية لا يعني أن يتم الرد على الفور، ولكن يجب تفسيرها بطريقة أكثر مرونة، فالدولة الضحية وكما ذهب إليه (Dinstein) حتى في المجال التقليدي تحتاج لفترة زمنية معقولة للقيام ببعض الاستعدادات قبل اتخاذ تدابير الدفاع عن النفس. وبالتالي يجب ألا يكون هناك فارق زمني غير مبرر بين الهجوم المسلح وممارسة الدفاع الشرعي ردا على ذلك وبخلاف ذلك يعتبر إجراءاً انتقامياً وليس رداً على هجوم مسلح فبمرور فترة زمنية طويلة وبشكل غير معقول سوف ينتفي المنطق من إعطاء الدولة الحق في الدفاع عن نفسها دون اللجوء إلى مجلس الأمن صاحب السلطة الأساسية في حفظ الأمن والسلم الدوليين[٤]، وبالتالي تطبيق هذا الشرط يجب أن يفسر في مجال التطبيق العملي بشكل مرن طبقاً للظروف والملابسات المحيطة بكل حالة على حدة وبشكل خاص بعد التطور التكنولوجي الهائل الذي حصل للوسائل الحربية ومنها العمليات السيبرانية[٥].

---

(1)Yoram Dinstein, Cyber War and International Law: Concluding Remarks at the 2012 Naval War College International Law Conference, Op.Cit. p 281; Marco Roscini, Op. Cit. p 33.

(2)Heather Harrison Dinniss, Op. Cit. P 103.

(٣) ينظر استاذنا د. قاسم أحمد قاسم، مصدر سابق، ص ١٢٧؛

François Delerue, Op. Cit. p 477.

(٤) د. أميرة عبد العظيم محمد عبد الجواد، "المخاطر السيبرانية وسبل مواجهتها في القانون الدولي العام"، *بحث منشور في مجلة البحوث الفقهية والقانونية تصدرها كلية الشريعة والقانون في جامعة الأزهر*، العدد الخامس والثلاثون، ج ٣، (٢٠٢٠): ص ٤٥٨؛ د. محمود حسين الشرقاوي، مصدر سابق، ص ٢٩٤؛

Yoram Dinstein, War- Aggression and Self-Defence, Cambridge University Press, 2011, p 233; Heather Harrison Dinniss, Op. Cit. p 103; Marco Roscini, Cyber Operations and the Use of Force in International Law, Op. Cit. p 91; François Delerue, Op. Cit. p 477.

(٥) د. وليد الدرديري عبدالحميد، *حق الدفاع الشرعي (دراسة تطبيقية مقارنة في ضوء اراء الفقه الاسلامي واحكام القانون الدولي العام)*، ط ١، (الجيزة: مركز الدراسات العربية للنشر والتوزيع، ٢٠٢٠)، ص ٢٤٣.

**رابعاً: يجب أن يكون فعل الدفاع مؤقتاً:** وهذا ما نستخلصه من نص المادة (٥١) عندما جاء فيها عبارة "... إلى أن يتخذ مجلس الأمن التدابير اللازمة لحفظ السلم والأمن الدولي"، ولا يعني هذا الشرط أنه رهن فترة زمنية قصيرة تعد بالساعات أو الأيام أو الشهور بل العكس قد تقوم أفعال الدفاع لسنوات طويلة انتهاء حالة الدفاع الشرعي مرتبطة إما برد العدوان وانسحاب قوات المعتدي وإعادة الحال إلى ما كان عليه قبل وقوع العدوان أو قيام مجلس الأمن بوضع يده على الموقف واتخاذ التدابير اللازمة، وفي غياب أحد هاتين الحالتين فإن حالة الدفاع عن النفس تبقى مستمرة وقائمة، ويتأخر الوقت الذي يتدخل فيه مجلس الأمن وذلك بسبب الصعوبة في عملية التدخل إذ لابد من مرور فترة زمنية بين فعل العدوان وفعل التدخل، إذ يتم إبلاغ المجلس أولاً بالوقائع، ثم يجتمع لدراستها ثم يقرر ما إذا كانت تشكل عدواناً أم تهديدا للسلم أو إخلالاً به[١].

**الشرط الثاني: التناسب**

يقصد بشرط التناسب أن تكون الأفعال التي تتخذ في حالة الدفاع الشرعي عن النفس متناسبة مع أعمال العدوان الواقع على الدولة وأن تكون غير متجاوزة الحدود المعقولة لرد العدوان المسلح، ويترتب على ذلك أن هذه الأفعال يجب أن تقتصر على دفع العدوان الحال والمباشر الواقع على الدولة، بمعنى يجب أن يتحقق التناسب بين جسامة وحجم ونوع أعمال العدوان مع أعمال الدفاع وهذا الشرط لا يعني التماثل التام بينهما [٢]، ولا يعني اشتراط تحقيق التناسب بين جسامة أعمال العدوان وجسامة أعمال الدفاع هذا التماثل التام، فاختلاف وسيلة الدفاع عن وسيلة العدوان لا يعني انتفاء شرط التناسب بل المقصود هو أن تكون أعمال الدفاع متناسبة في حجمها وجسامتها مع أعمال العدوان غير متجاوزة الحدود المعقولة لرد العدوان الواقع عليها[٣].

وبالتالي لا يعني التناسب التماثل بين نوعية السلاح المستخدم في الدفاع وتلك المستخدم في العدوان، مما يعني أنه يجوز الرد سواءاً كان حركياً أو سيبرانياً على أي عملية سيبرانية[٤]، ولكن يلاحظ بأنه في بعض الأحيان العمليات السيبرانية فقط متناسبة وضرورية للرد على عملية سيبرانية، على سبيل المثال للدولة الضحية خياران لإغلاق الخوادم التي يستخدمها الدولة المهاجمة لتنفيذ العمليات السيبرانية وهما: إما قصف الخوادم فعليًا أو ايقافها وتعطيلها عن طريق عملية سيبرانية، ففي هذه الفرضية، يبدو أن استخدام الخيار الأول غير

(١) د. مرابط وسيلة، مصدر سابق، ص ٢١٨.
(٢) د. ابو الخير احمد عطية عمر، *نظرية الضربات الاستباقية (الدفاع الوقائي) في ضوء قواعد القانون الدولي المعاصر*، (القاهرة: دار النهضة العربية، بدون سنة نشر)، ص ٦٢.
(٣) د. وليد الدرديري عبدالحميد، مصدر سابق، ص ٢٤٤.
(4)Marco Roscini, Cyber Operations and the Use of Force in International Law, Op. Cit. p 90; Heather Harrison Dinniss, Op. Cit. p 104.

متناسب وغير ضروري، حيث يوجد خيار أقل ضرراً[١]، وعلى عكس ذلك قد لا يكون الرد العيني ضد عملية سيبرانية ممكنا أو فعالاً، وذلك يرجع لسببين، السبب الأول افتقار الدولة الضحية للتكنولوجيا اللازمة للاختراق، أو قد يكون السبب راجع إلى كون المعتدي دولة ذات تكنولوجيا منخفضة أو جهة فاعلة غير حكومية، وبالتالي لا يمتلك البنية التحتية السيبرانية لضربها[٢].

وجدير بالذكر بأنه توافر شرط التناسب للدفاع عن النفس ممكنة في الفضاء السيبراني إذا تمت كتابة البرنامج مع وضع هذا الغرض في الاعتبار. فيمكن على سبيل المثال تصميم الكود بطريقة لا يمكن تفعيلها إلا بوجود خصائص معينة. يتطلب ذلك درجة عالية من المعلومات حول الأنظمة المستهدفة، والتي يمكن الحصول عليها من خلال جمع المعلومات الاستخبارية التقليدية أو الاستغلال السيبراني [٣].

بناء على ما تقدم نرى بأن جميع شروط حق الدفاع عن النفس ينطبق في الفضاء السيبراني وبالتالي يحق للدول ممارستها ضد العمليات السيبرانية عند توافر الشروط المذكورة السابقة جميعها، وهذا ما أكدته أغلب الدول، فعلى سبيل المثال ذكرت سنغافورة بأن الدولة تتمتع بالحق المتأصل في الدفاع عن النفس في حالة حدوث عملية سيبرانية ترقى إلى مستوى هجوم مسلح[٤]، كما ترى كندا أن الحق الطبيعي في الدفاع عن النفس في حالة وقوع هجوم مسلح ضد دولة ما ينطبق أيضاً على الفضاء السيبراني وأكدت أنها سترد على العمليات السيبرانية التي ترقى إلى مستوى هجوم مسلح بطريقة تتسق مع القانون الدولي[٥]، وسويسرا أيضاً ذهبت إلى أن حظر استخدام القوة وحق الدفاع عن النفس ينطبقان على الفضاء السيبراني[٦]، وأكدت يابان كذلك على أنه عندما تشكل العملية السيبرانية هجومًا مسلحًا

(1)François Delerue, Op. Cit. p 482.

(2)Lawrence T. Greenberg. And others, Information Warfare and International Law, National Defense University Press, 1998, p 32; Laurie R. Blank, International Law and Cyber Threats from Non-State Actors, International Law Studies 89, 2013, p 419.

(3) William A. owens and others, Op. Cit. p 123.

(4)UNGA, Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States, Op. Cit. P 84.

(5)Government of Canada, international law applicable in cyberspace, 22 April 2022, paras 46- 47.

(6)Federal Department of Foreign Affairs (FDFA), Switzerland's Position Paper On The Application Of International Law in Cyberspace, 2021, P 4.

بموجب المادة (٥١) من ميثاق الأمم المتحدة، يجوز للدول ممارسة الحق الطبيعي في الدفاع عن النفس الفردي أو الجماعي المعترف به بموجب المادة (٥١) من ميثاق الأمم المتحدة[١].

**خلاصة القول:**

جميع شروط حق الدفاع الشرعي سواء المتعلقة بفعل الدفاع أو العدوان بالإمكان تطبيقها في ممارسة هذا الحق ضد العمليات السيبرانية نظرياً، إلا أنه من الناحية العملية والى الوقت الحالي نستطيع القول بأنه نادراً ما تلجأ دولة ما إلى ممارستها وذلك لعدم وجود درجة كافي من اليقين بشأن مدى توافر شروطها والتي يرجع لطبيعة هذه العمليات التي تتسم بالسرعة ومجهولية المصدر والآثار المتعددة التي تترتب عليها، لذلك يتطلب لجوء الدولة لهذا الحق أن تمتلك امكانيات ومهارات عالية في التكنولوجيا والفضاء السيبراني بالإضافة إلى فهم منطقي وواقعي للقواعد القانونية من أجل:-

١- تحديد درجة الخطورة الكافية لوصول العملية السيبرانية لمستوى الهجوم المسلح: والحقيقة هذا الشرط وكما رأينا حتى في العمليات التقليدية يثير اشكالية حيت الفجوة بين استخدام القوة التي لا يعتبر هجوماً مسلحاً والتي يعتبر كذلك غير واسع، ولكن ما يصعب ذلك في السياق السيبراني هو تعدد الآثار التي يترتب عليها وعدم وجود اجماع حول بعض الحالات كحالة تعطيل البنية التحتية الحيوية واتلاف البيانات دون وجود أضرار مادية، أما في حالة وجود الأضرار المادية وبالرغم من وجود اجماع على اعتبارها هجوماً مسلحاً إلا أن وجود درجة الخطورة الكافية من الصعب تحديدها من عدمه وهذا واضح من حالة ستوكسنت والخلاف الحاصل عليه في مدى امكانية وصفها هجوماً مسلحاً نظراً لخطورتها وعدم وجود اجماع عليها لاعتباره هجوم مسلح.

٢- تحديد مصدر العدوان: مسألة الإسناد في الفضاء السيبراني تثير اشكالية حيث يصعب تحديد القائم بالعملية السيبرانية وبالتالي وجود الصعوبة في الامتثال لشرط الضرورة التي يعتبر من متطلباته أن توجه فعل الدفاع إلى الجهة القائمة بفعل العدوان.

٣- مدى وجود المدة المعقولة والمبررة للدفاع: فالسرعة التي يتسم بها تنفيذ العمليات السيبرانية حيث تكون المدة التي يمتد بين بدء تنفيذ العمليات السيبرانية وانهاءها قصيرة للغاية إذ تكون ذلك في ثوان معدودة، يترتب عليها صعوبة الامتثال لشرط الفورية وإن كان المعيار مرناً لأنه عدم امتلاك الدولة لمهارات عالية من التطور والتكنولوجيا وعدم قدرتها لتحديد الجهة الفاعلة والوسيلة المناسبة للدفاع في وقت معقول ومبرر قد يجعل في غالب الأوقات المدة المعقولة اللازمة للدفاع منتفية.

(1)Ministry of Foreign Affairs of Japan, Op. Cit. P 6.

ومع ذلك نرى بأنه مازالت هذه العمليات في بدايتها لذلك وبمرو الوقت وفي المستقبل سيكون هناك تطورات كبيرة في هذا المجال وستعمل الدول من أجل القضاء على المشاكل المذكورة من تحديد الجهة الفاعلة والسرعة في الاستجابة وممارسة حقها في الدفاع عن نفسها، ذلك الحق الأصيل والمعترف به منذ القدم، وبخصوص تحديد درجة الخطورة الكافية نرى وبأنه وفي ضوء ممارسات الدول سواء العملية أو النظرية سيكون هناك وضوح أكثر حول مدى توافر الخطورة المطلوبة، وذلك لأنه نعتقد وبأن سبب الاعتماد المتزايد والمستمر على الفضاء السيبراني من قبل الدول لإدارة شؤونها سيوجد عمليات سيبرانية بكثرة وبدرجات متفاوتة من الخطورة.

## الخاتمة

بعد تحليل مشكلة الدراسة توصلنا إلى العديد من النتائج والتوصيات يمكن إجمالها كالآتي:

### أولاً: النتائج

١- بالرغم من أن الحظر الوارد في (المادة ٤/٢) يشمل القوة المسلحة فقط إلا أنه يمكن تطبيق القاعدة على العمليات السيبرانية واعتبارها استخداماً للقوة المسلحة نظراً لإمكانية تشابه آثارها مع آثار القوة المسلحة وذلك استنادا إلى ما ورد في فتوى محكمة العدل الدولية بشأن مشروعية التهديد بالأسلحة النووية أو استخدامها ومشيراً إلى أنه المواد (٢/ ٤) و (٥١) و (٤٢) من ميثاق الأمم المتحدة لا تُشير إلى أسلحة محددة حيث قررت بأنه "وليس في تلك الأحكام ما يشير إلى أسلحة معينة. وانما هي تنطبق على أي استعمال للقوة. بصرف النظر عن الأسلحة المستخدمة. والميثاق لا يحظر صراحة، ولا هو يبيح استخدام أية أسلحة معينة بما فيها الأسلحة النووية والسلاح الذي هو بحد ذاته محرم سواء بموجب معاهدة أو عرف، لا يغدو مشروعاً بسبب كونه يستخدم لفرض مشروع بموجب الميثاق"، وهذا ما أكدته غالبية الدول والفقهاء.

٢- بالرغم من وجود اتفاق عام على تطبيق قواعد اللجوء لاستخدام القوة على العمليات السيبرانية إلا أن هناك عدم الوضوح بشأن كيفية التطبيق هذا وذلك نظراً لاختلاف الآثار التي يترتب على العمليات السيبرانية، فإذا كان هناك إجماع على اعتبار تلك العمليات السيبرانية التي يتسبب في الأضرار المادية استخداماً للقوة المسلحة إلا أن الوضع ليست كذلك في حال التسبب بتعطيل البنية التحتية الحيوية للدول أو اتلاف بياناتها دون وجود أضرار المادية، والراجح عندنا أنه:

أ- نظراً لأنه وفي المجتمع الرقمي المعاصر لا يستبعد أن يترتب على تعطيل البنى التحتية الحيوية للدولة آثار خطرة ومدمرة دون وجود آثار مادية، فالنظر إلى وجود الآثار المادية أم لا لاعتبار عملية سيبرانية استخداماً للقوة لا يفسر التطور الذي حصل بالمجتمعات المعاصرة، ولكن اعتبار ذلك استخداماً للقوة المسلحة مقيد بتوافر شرطين وهما: أولهما أن يستهدف العملية بنية تحتية حيوية في غاية الأهمية بحيث يترتب على تعطيلها عرقلة الوظائف الأساسية للدولة وأمنها القومي، وثانيهما أن يكون التعطيل واسعة النطاق بحيث يتعدى كونها مجرد تعطيل مؤقت.

ب- إن اقتصار مصطلح "الملكية" على الأشياء الملموسة لا يفسر العصر الرقمي الذي أصبحت فيه البيانات فيه ذات أهمية بالغة، ذلك العصر التي تعتمد غالبية الدول على الفضاء السيبراني لحفظ بياناتها.

٣- إن كافة شروط حق الدفاع الشرعي سواء المتعلقة بفعل الدفاع أو العدوان بالإمكان تطبيقها في ممارسة هذا الحق ضد العمليات السيبرانية نظرياً، إلا أنه من الناحية العملية نادراً من المتوقع أن تلجأ دولة ما إلى ممارستها وذلك لعدم وجود درجة من اليقين الكافية بشأن مدى توافر شروطها والتي يرجع لطبيعة هذه العمليات التي تتسم بالسرعة ومجهولية المصدر والآثار المتعددة التي تترتب عليها.

**ثانياً: التوصيات**

١- نوصي الدول أن تبين موقفها بوضوح فيما يتعلق بتحديد قاعدة حظر استخدام القوة وبشكل خاص فيما يتعلق بتحديد الحد الأدنى لاعتبار العمليات السيبرانية استخداماً للقوة ومن بينها العراق حيث لم نرى موقفها بهذا الخصوص.

٢- انطلاقاً من ضرورة الحفاظ على السلم والأمن الدوليين من جانب والأمن القومي للدول واستقلالها من جانب آخر، نوصي فيما يلي:

أ- أن يتم مراجعة مفهوم السلاح بحيث يشمل بالإضافة إلى حدوث آثار مادية وملموسة مفهوم التعطيل أيضاً نظراً للتطورات التكنولوجية التي امكنت ايجاد وسائل تؤدي إلى تعطيل شيء ما دون اتلافها مادياً.

ب- أن يتم تنظيم معاهدة دولية خاصة بالبيانات الدول وأن يتم الاعتراف بملكية الدولة لها وتوفير الحماية القانونية لها.

ت- تعمق المناقشات بين المختصين في مجال التكنولوجي والقانوني والتعاون الدولي من أجل القضاء على المشاكل االمتعلقة بممارسة حق الدفاع عن النفس ضد العمليات السيبرانية من الصعوبة في تحديد الجهة الفاعلة والسرعة في الاستجابة، تحديد الدرجة الخطورة الكافية.

## قائمة المصادر

### أولا: المصادر العربية

**الكتب**


١. د. ابراهيم الدراجي، *جريمة العدوان ومدى المسؤولية الدولية عنها*، ط ٢، بيروت: منشورات الحلبي الحقوقية، ٢٠١٩.

٢. د. ابو الخير احمد عطية عمر، *نظرية الضربات الاستباقية (الدفاع الوقائي) في ضوء قواعد القانون الدولي المعاصر*، القاهرة: دار النهضة العربية، بدون سنة نشر.

٣. د. حسن الجلبي، *مبادئ الأمم المتحدة وخصائصها التنظيمية*، القاهرة: معهد البحوث والدراسات العربية، ١٩٧٠.

٤. د. زينب رياض جبر، *التجسس الرقمي في ضوء قواعد القانون الدولي العام*، ط ١، القاهرة: المركز العربي للدراسات والبحوث العلمية للنشر والتوزيع، ٢٠٢٣.

٥. د. سامي جاد عبدالرحمن واصل، *ارهاب الدولة في اطار قواعد القانون الدولي العام*، الاسكندرية: دار الجامعة الجديدة للنشر والتوزيع، ٢٠٠٨.

٦. د. السيد مصطفى أحمد أبو الخير، *المبادئ العامة في القانون الدولي المعاصر*، ط ١، مصر: ايتراك للطباعة والنشر والتوزيع، ٢٠٠٦.

٧. د. صالح جواد الكاظم، *دراسة في المنظمات الدولية*، بغداد: مطبعة الارشاد، ١٩٧٥.

٨. د. صلاح الدين احمد حمدي، *العدوان في ضوء القانون الدولي العام*، ط ١، بيروت: منشورات زين الحقوقية.

٩. أ. د. صلاح عبدالرحمن الحديثي وكاميران عزيز حسن، *التفصيل الشامل لتطور القواعد القانونية الخاصة بالحرب السيبرانية*، ط ١، الجيزة: مجموعة ثري فريندز للنشر والتوزيع والمجموعة العلمية للنشر والتوزيع، ٢٠٢١.

١٠. د. عباس المراغي ناصر، *القضاء الجنائي الدولي (حق الدفاع الشرعي عن النفس والاباحة الجنائية في إطار القانون الدولي)*، الاسكندرية: مكتبة الوفاء القانونية، ٢٠١٧.

١١. د. كمال حماد، *النزاع المسلح والقانون الدولي العام*، ط ١، بيروت: مجد المؤسسة الجامعية للدراسات والنشر والتوزيع، ١٩٩٧.

١٢. د. محمد خليل الموسى، *استخدام القوة في القانون الدولي المعاصر*، ط ١، عمان: دار وائل للنشر والتوزيع، ٢٠٠٤.

١٣. د. محمد سعادي، *أثر التكنلوجيا المستحدثة على القانون الدولي العام*، ط ١، الإسكندرية: دار الجامعة الجديدة للنشر، ٢٠١٤.

١٤. محمود حسين الشرقاوي، *الهجمات السيبرانية في ضوء أحكام القانون الدولي الإنساني*، ط ١، القاهرة: دار النهضة العربية، ٢٠٢٢.

١٥. د. مرابط وسيلة، *استخدام القوة في العلاقات الدولية وأثره على فرض الشرعية*، ط ١، الجيزة: مركز الدراسات العربية للنشر والتوزيع، ٢٠٢١.

١٦. د. وليد الدرديري عبدالحميد، *حق الدفاع الشرعي (دراسة تطبيقية مقارنة في ضوء اراء الفقه الاسلامي واحكام القانون الدولي العام)*، ط ١، الجيزة: مركز الدراسات العربية للنشر والتوزيع، ٢٠٢٠.

**الاطاريح:**

١. د. قاسم أحمد قاسم، "حق الدفاع عن النفس في القانون الدولي المعاصر (دراسة تحليلية مقارنة)"، اطروحة دكتوراه مقدم إلى كلية القانون- جامعة صلاح الدين، ٢٠٠٨.

٢. د. محمد محمود خلف، "حق الدفاع الشرعي في القانون الدولي الجنائي"، أطروحة دكتوراه مقدمة لجامعة القاهرة، ١٩٧٣.

**البحوث**

١. د. أميرة عبد العظيم محمد عبد الجواد، "المخاطر السيبرانية وسبل مواجهتها في القانون الدولي العام"، *بحث منشور في مجلة البحوث الفقهية والقانونية تصدرها كلية الشريعة والقانون في جامعة الأزهر*، العدد ٣٥ ، ج ٣، (٢٠٢٠).

٢. د. سامي السعد، "حق الدفاع الشرعي في القانون الدولي العام"، *بحث منشور في مجلة القانون المقارن، جمعية القانون المقارن العراقية*، العدد ٣، (١٩٧٠).

٣. د. سمعان بطرس فرج الله، "تعريف العدوان"، *بحث منشور في المجلة المصرية للقانون الدولي*، المجلد ٢٤ ، (١٩٦٨).

٤. د. محمد عادل محمد عسكر، "وضع العمليات السيبرانية في القانون الدولي مع التطبيق على ممارسة التجسس في وقت السلم (دراسة على ضوء دليل تالين بشأن القانون الدولي المطبق على العمليات السيبرانية ٢٠١٣- ٢٠١٧)"، *بحث منشور في مجلة البحوث القانونية والاقتصادية تصدرها كلية الحقوق بجامعة بني سويف*، المجلد ٣٣، العدد ١، (٢٠٢١).

٥. د. محمد محيي الدين عوض، "دراسات في القانون الدولي الجنائي"، بحث منشور في *مجلة القانون والاقتصاد*، العدد ٢، السنة ٣٥، (١٩٦٥).

**الاتفاقيات والقرارات والاعلانات الدولية**

١. ميثاق الأمم المتحدة ١٩٤٥.

٢. اتفاقية فيينا لقانون المعاهدات لعام ١٩٦٩.

٣. اتفاقية الجوانب المتصلة بالتجارة من حقوق الملكية الفكرية (تريبس) لسنة ١٩٩٤.

٤. اتفاقية بودابست المتعلقة بالجريمة الالكترونية لعام ٢٠٠١.

٥. الجمعية العامة للأمم المتحدة، قرار (رقم ٢٦٢٥)، (الدورة ٢٥)، لاعتماد إعلان مبادئ القانون الدولي المتصلة بالعلاقات الودية والتعاون بين الدول وفقا لميثاق الأمم المتحدة، الوثيقة ((A/RES/2625(XXV) في 24 تشرين الأول/أكتوبر ١٩٧٠.

٦. الجمعية العامة للأمم المتحدة، قرار (رقم ٣٣١٤/ ٢٩) بشأن تعريف العدوان، الوثيقة ((A/RES/3314(XXIX، في ١٤ ديسمبر/ كانون الأول ١٩٧٤.

٧. الجمعية العامة للأمم المتحدة، قرار (رقم ٥٨/ ١٩٩) بشأن إرساء ثقافة عالمية لأمن الفضاء الحاسوبي وحماية الهياكل الأساسية الحيوية للمعلومات، وثيقة رقم A/RES/58/199، في ٢٣ / كانون الأول ديسمبر ٢٠٠٣.

**الوثائق الدولية**

١. الجمعية العامة للأمم المتحدة، نزع السلاح العام الكامل- فتوى محكمة العدل الدولية بشأن مشروعية التهديد بالأسلحة النووية أو استخدامها، وثيقة رقم A/51/218 الصادرة بتاريخ ١٥ اكتوبر ١٩٩٦.

٢. الأمم المتحدة، موجز الأحكام والفتاوى والأوامر الصادرة عن محكمة العدل الدولية ١٩٩٢- ١٩٩٦، نيويورك، وثيقة رقم ST/LEG/SER.F/1/Add.1 الصادرة في ١٩٩٨.

٣. الجمعية العامة للأمم المتحدة، تقرير فريق الخبراء الحكوميين المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي، ١٤ يوليو ٢٠٢١، وثيقة رقم A/76/135..

٤. المنظمة الإستشارية القانونية الآسيوية – الإفريقية، القانون الدولي في الفضاء السيبراني، وثيقة رقم AALCO/59/HONG KONG/2021/SD/S17، ٢٠٢١.

٥. المنظمة الإستشارية القانونية الآسيوية – الإفريقية، القانون الدولي في الفضاء السيبراني، وثيقة رقم AALCO/58/DAR ES SALAAM/2019/SD/S17، ٢٠١٩.

**ثانياً: المصادر الأجنبية**

**الكتب**

1. François Delerue, Cyber Operations and International Law, Cambridge University Press, Cambridge, 2020.
2. Hans Kelsen, international law studies, 1956.
3. Hans Kelsen, Principles of International Law, 2nd Edition, 1967.
4. Heather Harrison Dinniss, Cyber Warfare and the Laws of War, Cambridge University Press, Cambridge, 2012.
5. Jean s. pictet, The Geneva Conventions of 12 August 1949. Commentary. Volume III: Relative to the Treatment of Prisoners of War, ICRC, 1960.
6. jeffrey Carr, Inside cyber warfare: mapping the cyber underworld, O'Reilly Media, 2011.
7. Katharina Ziolkowski, Confidence Building Measures for Cyberspace– Legal Implications, NATO CCDCOE, Tallinn, 2013.
8. Katharina Ziolkowski, Confidence Building Measures for Cyberspace – Legal Implications, NATO CCD COE, Tallinn, 2013.
9. Lawrence T. Greenberg. And others, Information Warfare and International Law, National Defense University Press, 1998.

10. Marco Roscini, Cyber Operations and the Use of Force in International Law, Oxford University Press, 2014.
11. Michael N. Schmitt (GEN. ED.), Tallinn manual on the international law applicable to cyber warfare, prepared by the International Group of Experts at the invitation of the NATO CCDCOE, Cambridge University Press. Cambridge, 2013.
12. Tom Ruys, Armed Attack and Article 51 of the UN Charter, Cambridge University Press, 2010.
13. Walter Gary Sharp, Sr., Cyberspace and the Use of Force, Aegis Research Corporation, Virginia, 1999.
14. William A. Owens and others (eds.), Technology- Policy- Law and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities, National Academies Press, Washington, 2009.
15. Yoram Dinstein, War- Aggression and Self-Defence, Cambridge University Press, 2011.

**البحوث**

1. Daniel B. Silver, Computer Network Attack as a Use of Force under Article 2(4) of the United Nations Charter, International Law Studies Series US Naval War College, Vol. 76, 2002.
2. David Albright and others, Did Stuxnet Take out 1,000 Centrifuges at the Natanz Enrichment Plant?, Institute for Science and International Security's REPORT, **December 22, 2010**, p 1_ 2.
3. David E. Graham, Cyber Threats and the Law of War, Journal of National Security Law & Policy, Vol. 4:87,2010.
4. Duncan Blake and Joseph S. Imburgia, Bloodless Weapons? The Need to Conduct Legal Reviews of Certain Capabilities and the Implications of Defining Them as Weapons, Air Force Law Review, Vol. 66, 2010.

5. Duncan Hollis, Why States Need an International Law for Information Operations, Lewis and Clark Law Review, Vol. 11, 2007.

6. Gary Brown and Keira Poellet, The Customary International Law of Cyberspace, Strategic Studies Quarterly, Vol. 6 No. 3, 2012.

7. Herbert S. Lin, Offensive Cyber Operations and the Use of Force, Journal Of National Security Law & Policy, Vol. 4:63

8. Jason Barkham, Information Warfare and International Law on the Use of Force, New York University Journal of International Law and Politics, Vol. 34/ 58, 2001.

9. Laurie R. Blank, International Law and Cyber Threats from Non-State Actors, International Law Studies, Vol. 89, 2013.

10. Marco Roscini, World Wide Warfare – Jus ad bellum and the Use of Cyber Force, Max Planck Yearbook of United Nations Law, Vol. 14, 2010.

11. Matthew C Waxman, Self-Defensive Force against Cyber Attacks: Legal- Strategic and Political Dimensions, International Law Studies, Vol. 89, 2013.

12. Melzer Nils, Cyberwarfare and International Law, United Nations Institute for Disarmament Research, Geneva, 2011.

13. Michael Gervais, Cyber Attacks and the Laws of War, Berkeley Journal of International Law, Vol. 30, 2012.

14. Michael N. Schmitt, Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework. Columbia Journal of Transnational Law, Vol. 37, 1999.

15. Michael N. Schmitt, Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework. Columbia Journal of Transnational Law. Vol. 37, 1999.

16. Michael N. Schmitt, Cyber Operations and the Jus Ad Bellum Revisited, Villanova Law Review, Vol. 56, 2011.

17. Michael N. Schmitt, Responding to Transnational Terrorism Under the Jus Ad Bellum: A Normative Framework, Naval Law Review, Vol. 1, 2008.

18. Oona A. Hathaway and others, The Law of Cyber-Attack, California Law Review, vol. 100:817, 2012.

19. Scott J. Shackelford, From Nuclear War to Net War: Analogizing Cyber Attacks in International Law, Berkeley Journal of International Law, Vol 27: 1, 2009.

20. Todd A Morth, Considering Our Position: Viewing Information Warfare as a Use of Force Prohibited by Article 2(4) of the U.N. Charter, Case Western Reserve Journal of International Law, Vol. 3: issue 2, 1998.

21. William H. Boothby, Methods and Means of Cyber Warfare, International Law Studies Series US Naval War College, Vol. 89, 2013.

22. Yoram Dinstein, Computer Network Attacks and Self-Defense, International Law Studies, Vol. 76, 2002.

23. Yoram Dinstein, Cyber War and International Law: Concluding Remarks at the 2012 Naval War College International Law Conference, International Law Studies, Vol. 89, 2013.

**الأحكام والفتاوى الدولية**

1. Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, I. C.J. Reports 1996, p. 226.
2. Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), Merits, Judgment. I.C.J. Reports, 1986, p .14.

**المواقع الإلكترونية**

1. Explosive Growth of Digital Technologies Creating New Potential for Conflict, Disarmament Chief Tells Security Council in First-Ever Debate on Cyberthreats, 29 June 2021, https://press.un.org/en/2021/sc14563.doc.htm

2. James Lewis, To Protect the U.S. Against Cyberwar, Best Defense Is a Good Offense, 29 March 2010,

https://www.usnews.com/opinion/articles/2010/03/29/to-protect-the-us-against-cyberwar-best-defense-is-a-good-offense

3. The CCDCOE Invites Experts to Contribute to the Tallinn Manual 3.0:

https://ccdcoe.org/news/2021/the-ccdcoe-invites-experts-to-contribute-to-the-tallinn-manual-3-0/.