(ISSN: 2356 - 9492)

حق الدفاع الشرعي في مواجهة الهجمات السيبرانية

في ضوء ميثاق الأمم المتحدة

دكتور/ محمد حسن أحمد جاد
أستاذ القانون الدولي العام المساعد
كليات عنيزة - المملكة العربية السعودية

المستخلص:

يهدف هذا البحث إلى تناول الهجمات السيبرانية بين الدفاع الشرعي وممارسات الدول الانفرادية، وهل تتوافق هذه الهجمات السيبرانية قانونياً مع حق الدفاع الشرعي طبقا للمادة (٥١) من ميثاق الأمم المتحدة أم يتعارض معه.

وتعد فكرة الهجمات السيبرانية من المسائل المستحدثة التي انتهجتها الدول العظمى والمتقدمة في المجال التكنولوجي لكونه سلاحا في يدها تستطيع من خلاله ضرب الدول الأعداء في أي وقت، ويترتب على ذلك إحداث خسائر وأضراراً خطيرة للدولة المستهدفة.

ويقع البحث في ثلاثة مباحث: يتناول الأول منها: تعريف الهجمات السيبرانية، ويعرض المبحث الثاني حق الدفاع الشرعي في ضوء قواعد القانون الدولي العام، ويبين المبحث الأخير نماذج واقعية للهجمات السيبرانية في وقتنا الراهن.

وتخلص الدراسة إلى أن الدول العظمي استغلت عدم وجود تنظيم دولي دقيق يحكم هذه الهجمات السيبرانية؛ فقامت بتوجيه الكثير من الهجمات التي ضد الدول المعادية لها، وقد ساعدها على ذلك القدرة التكنولوجية الهائلة التي تمتلكها هذه الدول التي بموجبها يمكن إخفاء الجهة التي أصدرت الهجوم أكثر من أي وقت سابق، ومن هنا يمكن تفعيل نص المادة (٥١) من ميثاق الأمم المتحدة.

الكلمات المفتاحية: الهجمات السيبرانية– الحرب السيبرانية – الدفاع الشرعي– الضرورة – التناسب– ميثاق– دليل تالين.

حق الدفاع الشرعي في مواجهة الهجمات السيبرانية في ضوء ميثاق الأمم المتحدة

دكتور/ محمد حسن أحمد جاد

مجلة الدراسات القانونية والاقتصادية

The Right of Legal Defense in the Confrontation of Cyber Attacks in Light of the Charter of the United Nations

Abstract

This research aims to address cyber-attacks between legitimate defense and the practices of unilateral states, and whether these cyber-attacks are legally compatible with the right of legitimate defense according to Article No. (51) of the Charter of the United Nations or contradict it. The idea of cyber-attacks is one of the emerging issues pursued by the great and advanced countries in the field of technology, as it is a weapon in their hand through which they can strike enemy countries at any time, and this results in serious losses and damage to the target country. The research falls into three sections; the first deals with the definition of cyber-attacks, the second section presents the right of legitimate defense in the light of the rules of public international law, and the last section shows realistic models of cyber-attacks in our time. The study concludes that the superpowers took advantage of the lack of accurate international regulation governing these cyber-attacks. It directed many attacks against the countries hostile to it, and this was helped by the enormous technological ability that these countries possess, according to which the party that issued the attack can be hidden more than ever before, and from here it is possible to activate the text of Article No. (51) of the Charter of the United Nations.

Keywords: Ccyber-attacks, Cyber Warfare, Legitimate Defense, Necessity, proportionality, Charter, .Tallinn Guide

(ISSN: 2356 - 9492)

مقدمة:

تبنت الولايات المتحدة الأمريكية وروسيا وغيرها من الدول الكبرى التي تمتلك قدرات تكنولوجية هائلة إستراتيجية جديدة تقوم على مبدأ الهجمات السيبرانية؛ فوجهت هذه الدول الكثير من الهجمات السيبرانية ضد بعضهما البعض، وضد الدول المعادية لهما التي يمكن أن تهدد أمن هذه الدول مستقبلا أو لتحقيق أهداف سياسية تسعى إليها هذه الدول(١).

وأكدت هذه الدول أنها تدافع عن نفسها مستخدمة مبدأ حق الدفاع الشرعي؛ واحتجت بهذا الحق تبريرا لمسلكها، ولكن الواقع يثبت خلاف ذلك حيث إن هذه الدول استخدمت حق الدفاع الشرعي بشكل يتنافى مع الغرض الذي وضع له، ويتعارض أيضا مع ميثاق الأمم المتحدة طبقاً لنص المادة (٥١) من ميثاق الأمم المتحدة التي حددت شروط حق الدفاع الشرعي(٢).

واستغلت هذه الدول عدم وجود تنظيم دولي دقيق لتجريم هذه الهجمات، ورأت أن طبيعة المخاطر تغيرت، وبالتالي يجب أن يكون الرد مغايراً، فتم توجيه هجمات سيبرانية ضد عدد من الدول مبررة أنها تدافع عن نفسها ضد أية دولة تهدد أمنها واستقرارها(٣).

فقد وجهت كل من الولايات المتحدة الأمريكية وروسيا هجمات سيبرانية تجاه بعضهما البعض وتجاه دول أخرى؛ ليكونا بذلك نموذجين لمفهوم الهجمات السيبرانية؛ لكونهما دولتين عظمتين تمتلكان قدرات هائلة في هذا المجال التكنولوجي يستطيعان من خلالها طمس هوية الفاعل الحقيقي لمرتكبي هذه الجرائم، ويزداد الأمر تعقيداً عندما يتم ارتكاب هذه الجرائم خارج نطاق الشبكات الإلكترونية(٤).

وللكيان الصهيوني دور بارز في هذا المجال إذ قام بتوجيه هجمات سيبرانية ضد إيران وبعض الدول العربية؛ مبرراً ذلك أن هذه الدول تمثل تهديداً لأمنه ومصالحه، وأنه يدافع عن نفسه طبقا لنص المادة (٥١) من ميثاق الأمم المتحدة(٥).

---

(١) أ. د. نورهان الشيخ: الإرهاب السيبراني ومستقبل العلاقات الأمريكية الروسية، آفاق استراتيجية – العدد (٤) أكتوبر، ٢٠٢١، ص ٦٢.

See: Jason Healey: Cyber Warfare in the 21st Century: Threats, Challenges, and Opportunities, Healey – Testimony to HASC, 1 March 2017, p. 2. See also Emily Crawford: Virtual Battlegrounds: Direct Participation in Cyber Warfare, I/S: A journal Of Law and Policy, Vol. 9: 1, 2013. p. 5 margin.
, p. 15.

(2) Matthew Borton, Samuel Liles, Sydney Liles: Cyberwar Policy, 27 J. Marshall J. Computer & Info. L. 303 (2010), Journal of Computer & information, Vol. xxvii, 2010, p. 311.

(3) Anna C. Mourlam: Unarmed attacks: cyber combatants and the right to defend, The California International Law Journal Vol. 26, No. 1, Winter, 2018, p. 23

انظر: د. رزق أحمد سمودي: حق الدفاع عن النفس نتيجة الهجمات الإلكترونية في ضوء قواعد القانون الدولي العام، بحث منشور في مجلة جامعة الشارقة لعلوم القانونية، المجلد ١٥، العدد ٢، ٢٠١٨، ص ٣٥٢.

(٤) سمودي: المرجع السابق، ص ٣٥٥.

تداعيات المواجهة السيبرانية بين إيران وإسرائيل، مجلة الدراسات الإيرانية، السنة الرابعة – : اللواء/ أحمد بن على الميموني: الجبهة النِشطة(5) العدد الثاني عشر – أكتوبر ٢٠٢٠م، ص ٨٢.

دكتور/ محمد حسن أحمد جاد

وقد أثار هذا الأمر لدى الباحثين عدة تساؤلات حول الأهداف الحقيقية لتلك الهجمات السيبرانية، وتبين أن هناك عدة أهداف رئيسة أهمها: إضعاف القوة العسكرية لهذه الدول المعتدى عليها، أو عدم قيام أجهزة الحاسب الآلي بوظائفها لتحقيق أهداف سياسية، أو إلحاق ضرر شامل للأشخاص أو الممتلكات للدولة المستهدفة[١].

(١) د. رزق أحمد سمودي: مرجع سابق، ص ٣٤٦ .

(ISSN: 2356 - 9492)

مشكلة البحث:

تتمحور المشكلة الرئيسة للبحث حول مدى إمكانية ارتقاء الهجمات السيبرانية إلى مستوى النزاع المسلح؛ لكي تستطيع الدولة تفعيل حق الدفاع الشرعي استناداً للمادة (٥١) من ميثاق الأمم المتحدة، ويتفرع عن هذه المشكلة عدة إشكاليات أهمها: الخلط بين مفهوم حق الدفاع الشرعي والهجمات السيبرانية، حيث دأبت بعض الدول الكبرى– وعلي وجه الخصوص الولايات المتحدة الأمريكية وروسيا – على توجيه هجمات سيبرانية تهدف إلى تعطيل نظم القيادة والمصالح الأساسية في الدول تحت ستار حق الدفاع الشرعي، ولكن الواقع يؤكد غير ذلك، وأن هناك خلطا بين مفهوم الدفاع الشرعي والهجمات السيبرانية؛ لذلك يجب التمييز بين الهجمات السيبرانية التي ترتقى إلى مستوى الهجوم المسلح وغيرها من الهجمات التي لا تصل إلى هذا المستوى.

وتبنت الولايات المتحدة الأمريكية وروسيا إستراتيجيات جديدة أثارت لبسا وغموضا وخلطا بين مفهوم الدفاع الشرعي والهجمات السيبرانية، وعلى الرغم من وجود فرق شاسع بين حق الدفاع الشرعي والهجمات السيبرانية، ومن هنا وجدنا أن هذا الموضوع جدير بالبحث والدراسة.

ومما يزيد أهمية هذا الموضوع ما يحدث في الوقت الراهن من هجمات سيبرانية متبادلة بين روسيا وأمريكا في ظل الحرب الروسية الأوكرانية، تلك الهجمات تؤكد عدم التزام تلك الدول بقوانين وأحكام القانون الدولي؛ لذلك لابد من دراسة هذه الجرائم والتمييز بين ما يعد دفاعا شرعيا للدولة وما يعد انتهاكا لسيادة الدول والقانون الدولي.

فرضيات البحث وتساؤلاته:

ينطلق البحث من سؤال رئيس مفاده: ما مدى شرعية الهجمات السيبرانية في القانون الدولي الإنساني؟ وينبثق من هذا الافتراض عدة تساؤلات فرعية أخري تتمثل في:

- ما هو مفهوم الهجمات السيبرانية؟
- ما هو الفرق بين الهجمات السيبرانية والحرب السيبرانية؟
- ما هو موقف القانون الدولي من الهجمات السيبرانية ؟
- ما هو مفهوم الدفاع الشرعي في القانون الدولي العام؟
- ما مدي توافق الهجمات السيبرانية مع حق الدفاع الشرعي؟

أهمية البحث:

يعد موضوع الهجمات السيبرانية من الموضوعات المهمة والمطروح بقوة على الساحة الدولية خصوصاً بعد تبني الدول العظمى – كالولايات المتحدة الأمريكية وروسيا – لهذه الهجمات، حيث لقى هذا الموضوع اهتماما واسعا لدى حكومة الدولتين، وقد لجأت هاتان الدولتان إلى تبني مفهوم الهجمات السيبرانية كجزء أساسي من إدارتها السياسية دفاعا عن نفسها، ومن هنا ظهر الخلط بين مفهوم الهجمات السيبرانية الذي تبنته هذه الدول وبين مفهوم الدفاع الشرعي عن النفس؛ لذلك لابد من توضيح هذين المفهومين.

حق الدفاع الشرعي في مواجهة الهجمات السيبرانية
في ضوء ميثاق الأمم المتحدة

دكتور/ محمد حسن أحمد جاد

مجلة الدراسات القانونية والاقتصادية

والجدير بالذكر أن مفهوم الهجمات السيبرانية للدفاع عن النفس هو من صنع الدول العظمى لكي تبرر للعالم أسباب شنها هجمات خاطفة وسريعة ضد دول معينة مدعيين أن ذلك يدخل في نطاق الدفاع الشرعي، وحقيقة الأمر أن هذا يعد اعتداءً وتدخلا سافرا في شؤون الدول وسياستها بالهجوم عليها إلكترونياً، مع عدم توافر شروط الحقيقية الدفاع الشرعي.

وتكمن أهمية البحث في دراسة مفهوم الهجمات السيبرانية مع بيان الحالات التي يبيح فيها الميثاق استخدام القوة السيبرانية لرد الاعتداء للدفاع عن النفس طبقا لنص المادة (٥١) من ميثاق الأمم المتحدة، وذلك حتى لا يساء استخدام حق الدفاع الشرعي.

أهداف البحث:

يرمي هذا البحث إلى تحقيق الأهداف التالية:

- التعرف على مفهوم الهجمات السيبرانية ومدي مطابقتها لحق الدفاع الشرعي.
- التعرف على مفهومي الهجمات السيبرانية والدفاع الشرعي من وجهة النظر الأمريكية والروسية.
- توضيح مفهوم الدفاع الشرعي طبقا لقواعد القانون الدولي الإنساني.
- التعرف على النماذج العملية للهجمات السيبرانية في ظل الأحداث الراهنة.

منهجية البحث:

يعتمد منهج الدراسة لهذه الورقة البحثية على المنهج الوصفي التحليلي حيث تعرض لنا واقع الهجمات السيبرانية ومدى مطابقتها لنص المادة (٥١) من ميثاق الأمم المتحدة والتطبيقات الحديثة لها، والتعقيب عليها بما يلزم، وذلك من خلال الاستعانة بالمراجع العامة والمتخصصة العربية والأجنبية ومواقع الإنترنت؛ حتى تتحقق أهداف البحث، ونتمكن من الوصول إلى أهم النتائج والتوصيات.

خطة البحث:

تحقيقاً لأهداف البحث فقد تم تقسيمه إلى مقدمة وثلاثة مباحث على النحو التالي:

مقدمة: مشكلة الدراسة فرضيات البحث وأهميتها وأهدافها ومنهجها.

المبحث الأول: مفهوم الهجمات السيبرانية والتكييف القانوني لها.

المبحث الثاني: حق الدفاع الشرعي في ضوء قواعد القانون الدولي العام.

المبحث الثالث: النماذج العملية للهجمات السيبرانية في الوقت الراهن.

الخاتمة.

(ISSN: 2356 - 9492)

المبحث الأول
مفهوم الهجمات السيبرانية والتكييف القانوني لها

شهد العالم نموذجا جديدا في سباق التسلح يتمثل في الهجمات الإلكترونية (السيبرانية)، وهذه الهجمات إما أن تكون ذات طبيعة عسكرية تتجسد في اتساع نطاق التدمير لقوات الدولة المعتدى عليها، أو يستهدف البنية التحتية لها كمحطات الطاقة أو الخدمات المالية والمؤسسات الأمنية أو العسكرية من خلال اختراق هذه الشبكات الخاصة للمؤسسات المستهدفة بقصد سرقة هذه المعلومات أو تدميرها الكترونيا(١).

وتختلف الحرب التقليدية عن الحرب السيبرانية في كون أن الحرب التقليدية تقوم على استخدام الجيوش النظامية، وتكون معلنة مسبقا، بيد أن الحرب السيبرانية تعد حرباً غامضة وغير محددة الأهداف؛ لأنها تتحرك عبر شبكة المعلومات الإلكترونية(٢).

وقد تكون تلك الحرب ذات طبيعة غير عسكرية سواء كانت اقتصادية أو اجتماعية كالإرهاب السيبراني، ويتحقق ذلك من خلال تنفيذ هجمات إلكترونية ضد أهداف ومؤسسات الدولة أو تشويه الرموز السياسية لمواقع التواصل للدولة المستهدفة باستخدام الهاشتاج لتشويه هذه الرموز أو الإساءة لها(٣).

---

(١) د. إيهاب خليفة: مرجع سابق، ص ٢، ٣. انظر: فيرونيك كريستوري: الحرب السيبرانية: القانون الدولي الإنساني يوفر طبقة إضافية من الحماية ، بيان ألقته السيدة "فيرونيك كريستوري"، كبيرة مستشاري الحد من التسلح في اللجنة الدولية أمام "الفريق العامل المفتوح العضوية المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي" – نيويورك، ١٠ أيلول/سبتمبر ٢٠١٩م، ص ٢.
https://www.icrc.org/ar/document/cyber-warfare-ihl-provides-additional-layer-protection

(2) Helen Wilson1 & Patrick van Esch: International Humanitarian Law: Attack of the Binary Bullet?، Journal of Politics and Law; Vol. 9, No. 4; 2016, p. 110.

انظر: د. يحي ياسين سعود: الحرب السيبرانية في ضوء قواعد القانون الدولي الإنساني، بحث منشور في المجلة القانونية بكلية الحقوق، جامعة القاهرة، المقالة ٣، المجلد ٤، العدد ٤، 2018م، ص ٨٤.
https://jlaw.journals.ekb.eg/article_45192_52d735c1a23cca2bf7dbbe56c4eb6846.pdf

انظر أيضا: الرائد/ حسن فياض: الهجمات السيبرانية من منظور القانون الدولي الإنسان، مجلة الدفاع الوطني، لبنان، العدد 14، ٢٠٢٠م، ص ١.

(٣) د. إيهاب خليفة: ما هو موقف ميثاق الامم المتحدة من استخدام القوة السيبرانية في التفاعلات الدولية – مقال صادر عن مركز المستقبل للأبحاث والدراسات المتقدمة – ابوظبي – الامارات العربية المتحدة، ٢٠١٩م، ص ٢، ٣.

See: Anna C. Mourlam: op. cit., p. 22.

حق الدفاع الشرعي في مواجهة الهجمات السيبرانية
في ضوء ميثاق الأمم المتحدة

دكتور/ محمد حسن أحمد جاد

ويختلف مفهوم الهجمات السيبرانية عن الحرب السيبرانية، فعندما تتحول الهجمات السيبرانية إلى نزاع مسلح يستهدف المواقع الإلكترونية والعاملين بها، فإننا نكون أمام حرب سيبرانية سواء كانت هذه الهجمات هجومية أو دفاعية، ويمكن أن يترتب عليها ضحايا أو أو قتل للأشخاص أو إصابتهم، الأمر الذي يمكن أن يترتب عليه نشوء أو قيام حرب عسكرية، ولذلك فإن الهجمات السيبرانية يمكن أن تكون أوسع نطاقاً من الحرب السيبرانية كما يمكن أن تحدث خارج إطار الحروب أو تكونسببا لنشوء الحرب[١]، ويتناول هذا المبحث: (مفهوم الهجمات السيبرانية وتكييفها القانوني) مطلبين على النحو الآتي:

المطلب الأول: تعريف الهجمات السيبرانية.

المطلب الثاني: التكييف القانوني للهجمات السيبرانية.

المطلب الأول
مفهوم الهجمات السيبرانية

يشتق لفظ السيبرانية في اللغة من الكلمة اليونانية (kybemetes) وهو يعني: القادة والتحكم عن بعد [٢].

أما في اللغة العربية فليس لكلمة (Cyber) المستخدمة بالإنجليزية أي لفظ مقارب لها في العربية؛ لذا توجد صعوبة في اختيار لفظ يقارب كلمة (Cyber)، وأن الترجمة العربية لعنوان "اتفاقية مجلس أوربا المتعلقة بالجريمة السيبرانية" غير صائبة، وترجم العنوان (Convention on Cybercrime) باللغة العربية إلى (الاتفاقية المتعلقة بالجريمة الإلكترونية)[٣].

وفى الاصطلاح، تعددت التعاريف للهجمات السيبرانية، فقد عرفها البعض بأنها: وسيلة إلكترونية تستخدم بذاتها للتسلل إلى أنظمة إلكترونية لتعطيلها أو تدميرها بهدف قومي أو سياسي عن طرق استغلال نقطة ضعف من خلالها يستطيع المهاجم التلاعب بالنظام. مثل: محطات توليد الطاقة النووية، أو وسائل النقل والمطارات[٤].

وعُرِّفت في دليل تالين بأنها: عملية إلكترونية هجومية كانت أم دفاعية يمكن أن تتسبب في إصابة أو قتل أشخاص أو الإضرار بالمنشآت أو تدميرها[٥].

---

(١) د. يحي ياسين سعود: مرجع سابق، ص ٨٤.

See: Lucian E. Dervan: Information Warfare and Civilian Populations: How the Law of War Addresses a Fear of the Unknown, Vol. 3, No. 1, 2011 ،p. 374.

(٢) د. أحمد عباس الفتلاوي: الهجمات السيبرانية : مفهومها والمسئولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر، مجلة المحقق الحلي للعلوم القانونية والسياسية، العدد ٤ السنة الثامنة ٢٠١٦م، ص ٦١٤.

(3) د. يحي ياسين سعود: مرجع سابق، ص ٨٣.

(٤) د. رغدة البهي: الردع السيبراني: المفهوم والإشكاليات والمتطلبات، مجلة العلوم السياسية والقانون، إحدى اصدارات المركز الديمقراطي العربي، العدد الأول، ٢٠١٧م، ص ٧.

See: Lucian E. Dervan: op. cit., p. 374.

(٥) د. طلال ياسين العيسى، عدي محمد غياب: المسئولية الدولية الناشئة عن الهجمات السيبرانية في ضوء القانون الدولي المعاصر، مجلة الزرقاء

(ISSN: 2356 - 9492)

ويشير مصطلح السيبرانية إلى عدة أشياء: كالإشارة إلى تنوع وسائل القتال التي يمكن أن تصل في النهاية إلى حد النزاع المسلح[١].

ويمكن وصف الهجمات السيبرانية بأنها أسلحة إلكترونية جديدة يتم استخدامها لضرب المنشآت الحيوية للعدو أو للدولة المعتدى عليها، كما يمكن أن توجه للعدو أو يتم دسها عن طريق عملاء أجهزة الاستخبارات[٢].

ومن المتفق عليه أن الهجمات السيبرانية واسعة النطاق، وقد ينتج عنها تدمير للبنية التحتية أو إصابات أو وفاة فإنها تخضع لقواعد القانون الدولي الإنساني[٣] .

ويهدف الهجوم السيبراني إلى سرقة البيانات والمعلومات أو تعطيلها أو تدميرها أو ضربها للدولة المعتدى عليها، أو الحصول على بيانات بالطرق غير الشرعية، كما يستهدف أنظمة المعلومات أو الشبكات أو البنية التحتية أيضا، كما يمكن أن يتم هذا الهجوم أو يتحقق عن طريق تثبيت برامج التجسس عن طريق وسائل مختلفة من الأفعال الخبيثة، وغالبا ترتكب هذه الأفعال ويكون المصدر مجهولاً[٤].

كما يهدف الهجوم السيبراني واسع النطاق إلى تدمير المنشآت الحيوية العامة التي قد يصيب مفاصل الدولة بشلل تام عند وقوعه، كما يصيب أجهزة الكمبيوتر للدولة المستهدفة، ويتميز هذه الهجوم بالسرعة والمراوغة[٥].

للبحوث والدراسات الإنسانية، الأردن، المجلد التاسع عشر، العدد الأول، ٢٠١٩م، ص ٨٨. للمزيد انظر: مكتب الأمم المتحدة المعني بالمخدرات الجريمة: دراسة شاملة عن الجريمة السيبرانية، فبراير ٢٠١٣م، ص ١٧،
https://www.unodc.org/documents/organized-crime/cybercrime/Cybercrime_Study_Arabic.pdf

(١) د. طلال ياسين العيسى، عدي محمد غياب: مرجع سابق، ص ٨٣.

(٢) د. يحي ياسين سعود: مرجع سابق، ص ٨٤.

See: Anna C. Mourlam: op. cit., p. 22.

(٣) I C R C : القانون الدولي الإنساني والعمليات السيبرانية خلال النزاعات المسلحة، موقف اللجنة الدولية للصليب الأحمر، ورقة مقدمة إلى فريق العمل المفتوح العضوية المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي، وإلى فريق الخبراء الحكوميين المعني بالارتقاء بسلوك الدول المسؤول في ميدان الفضاء السيبراني في سياق الأمن الدولي، ٢٠١٩م، ص ٧،
https://www.icrc.org/ar/document/

See: Lucian E. Dervan: op cit., p. 374.

(4) Herbert S. Lin: Offensive Cyber Operations and the Use of Force, Journal of national security law & Policy, Vol. 4:63, 2010, p. 63.

انظر: د. شريف نسيم قتلة: دليل "تالين" الهجمات الإلكترونية وخطر استخدام القوة في القانون الدولي"، المركز العربي للأبحاث الفضاء الإلكتروني، مصر، ٢٠١٧م، ص ١.

(5) Lucian E. Dervan: op. cit., p. 374.

انظر: م.م. علي عبدالرحيم العبودي: هاجس الحروب السيبرانية وتداعياتها على الأمن والسلم الدوليين، المجلة العلمية الأكاديمية العراقية، كلية العلوم السياسية، جامعة بغداد، العدد ٥٧، ٢٠١٩، ص ص ٨٩–١١٨، ص ٩٩.

https://cutt.ly/XkokTen

دكتور/ محمد حسن أحمد جاد

ونظراً لخطورة هذا الهجوم فقد نال اهتماما كبيرا لدى الأمم المتحدة، فقد عرفتها لجنة الأسلحة التابعة للأمم المتحدة الأسلحة غير التقليدية ١٩٦٨م، وبينت أشكالها، فهي تشمل" أسلحة الانفجارات الذرية، والأسلحة المصنوعة من مادة ذات نشاط إشعاعي، وأسلحة الفتك الكيمائية البيولوجية، وأي نوع من الأسلحة الأخرى التي يتم تصنيعها في المستقبل والتي تتشابه خصائصها في الأثر التدميري مع القنبلة الذرية أو الأسلحة الأخرى"(١).

وتضمنت المادة (٣٦) من البروتوكول الإضافي الأول ١٩٧٧م الملحق باتفاقية جنيف الرابعة المؤرخة في ١٢ أغسطس ١٩٤٩م الخاصة بالأسلحة الجديدة، والتي تنص على أنه عند تطوير أو اقتناء سلاح جديد يجب التحقق من هذا السلاح عما إذا كان محظورا أم لا، ويستفاد أيضاً من هذه المادة قابلية تطبيق القانون الدولي الإنساني على الحرب الفضائية؛ لأن هذا القانون لم يضع تعريفاً موحداً لفكرة النزاع المسلح، ولكنه فرق بين النزاع المسلح الداخلي والنزاعات المسلحة الدولية(٢).

وأشار بعض الباحثين إلى أن التقدم التكنولوجي والإنترنت والهجوم الذي يمكن أن يقع لم يكن متصورا عند التوقيع على الاتفاقيات التي تنظم حالة الحرب سواء قواعدها التي تبيح اللجوء إلى استخدام القوة أو قواعد إدارة المعارك أثناء الحرب؛ لأن هذه الاتفاقيات كانت وقتية، أي: تنظم حالة الحرب من حيث الزمان والمكان(٣).

وتهدف الهجمات السيبرانية التي تقوم بها الدولة أو إحدى مؤسساتها إلى إضعاف أو عدم قيام أجهزة الحاسب الآلي بوظائفه لتحقيق أهداف سياسية، أو إلحاق ضرر شامل بالأشخاص أو الممتلكات للدولة المقصودة، بينما الجريمة السيبرانية يقتصر ضررها على مستخدمين معينين فقط(٤).

كما تهدف هذه الهجمات إلى تدمير أو تعطيل شبكات الاتصال والمواقع الحكومية والطاقة الكهربائية وشبكات التوزيع وغيرها من المصالح المهمة والحيوية للدولة المستهدفة(٥).

وللجرائم السيبرانية صور متنوعة منها: الهجوم غير المشروع على الأمن العام والاستغلال للشباب بإنشاء موقع لمنظمات إرهابية على الشبكة المعلوماتية، والسطو السيبراني على أعمال البنوك والاعتداء على البنية التحتية للدولة المعتدى عليها، وغير ذلك من الأشكال(١).

---

(١) د. يحي ياسين سعود: مرجع سابق، ص ٨٤.

(٢) د. عمر محمود أعمر الحرب الإلكترونية في القانون الدولي الإنساني، دراسات علوم الشريعة والقانون، المجلد ٤٦، العدد ٣، ٢٠١٩م، ص ١٣٩.

(3) Matthew Borton, Samuel Liles, Sydney Liles: op. cit., p. 314.

(٤) د. رزق أحمد سمودي: مرجع سابق، ص ١٤٦.

(5) Lucian E. Dervan: op. cit., p. 378.

(ISSN: 2356 - 9492)

المطلب الثاني

التكييف القانوني للهجمات السيبرانية

تعددت آراء الفقهاء القانونيين حول بيان التكييف القانوني للهجمات السيبرانية، فذهب البعض إلى أن المدة التي جري فيها تقنين القواعد القانونية المنظمة لوسائل وطرق القتال لم يكن لاستخدام الأنظمة الإلكترونية أي وجود بمعنى أنها غير مقننة وغير منظمة وفقا للقواعد الدولية المعروفة، مما يعنى أنها خارج التنظيم القانوني الدولي(٢).

واستدل أصحاب هذا الاتجاه بالنظر إلى اتفاقيات لاهاي (١٨٩٩ – ١٩٠٧) واتفاقيات جنيف الأربع (١٩٤٩) والبروتوكولين الإضافيين (١٩٧٧) نجد أن هذه الاتفاقيات سابقة على هذه الجرائم(٣).

وذهب فريق آخر إلى أن الهجمات السيبرانية ينطبق عليها القانون الدولي الإنساني، ليس هذا فحسب، بل ينطبق عليها القانون الدولي العام لأن هذه الجرائم يمكن أن ترتكب أثناء النزاعات المسلحة وفى السلم أيضا، وأن هذه المبادئ والقواعد التي أكدها القانون الدولي الإنساني تنطبق عليها(٤).

ويستند القائلون بتجريم الهجمات السيبرانية إلى مبدأ الامتناع عن استخدام القوة بصفة عامة ضد أية دولة مستندين إلى نص المادة ٢ /٤ من ميثاق الأمم المتحدة "استخدام القوة أو التهديد بها"، واعتبرت هذه الهجمات بمثابة خرق واضح لحكم الفقرة الثانية من المادة الرابعة من ميثاق الأمم المتحدة(٥).

ويعد استخدام القوة طبقا لميثاق الأمم المتحدة عملا غير مشروع ووفقا لهذا الميثاق "يمتنع على أعضاء المنظمة جميعا في علاقاتهم الدولية التهديد باستعمال القوة أو استخدامها ضد سلامة الأراضي أو الاستقلال السياسي لأية دولة أو أي جهة أخرى لا يتعارض مع مقاصد الأمم المتحدة"(٦).

كما أن التكييف القانوني لهذه الهجمات يدور بين افتراضين:

---

(1) روان بنت عطية الله الصحفي: الجرائم السيبرانية، المجلة الإلكترونية الشاملة متعددة التخصصات، العدد ٢٤، ٢٠٢٠م، ص ١٩ وما بعدها.

See: John Richardson: stuxnet as cyberwarfare: applying the law of war to the virtual battlefield, Journal of computer & international law, volume 29 issue 1, 2011, p. 12.

(٢) د. أحمد عباس الفتلاوي: مرجع سابق، ص ٦٢٧، ٦٢٨.

(٣) د. طلال ياسين العيسى: مرجع سابق، ص ٨٧.

(4) Anna C. Mourlam: op. cit., p. 21.

انظر: د. أحمد عباس الفتلاوي: مرجع سابق، ص ٦٢٦.

(5) Lucian E. Dervan: op. cit., p. 382. See: Matthew Borton, Samuel Liles, Sydney Liles: op. cit., p. 315.

انظر: د. يوبي عبدالقادر: علاقة مجلس الأمن بالمحكمة الجنائية الدولية، رسالة دكتوراه (غير مشورة) كلية الحقوق، جامعة وهران، الجزائر، ٢٠١١، ٢٠١٢م، ص ٢٠٢ .

(6) Lucian E. Dervan: op. cit., p. 381, 382. Kamal Ahmad Khan: Use of Force and Human Rights under International Law, Athens Journal of Law - Volume 3, Issue 2 – Pages 141-164, April 2017, p. 145.

انظر: د. محمد حسن أحمد جاد: سلطة المحكمة الجنائية الدولية على الدول غير الأعضاء، دار النهضة العربية، مصر، ٢٠١٨م، ص ٤٨٠.

الافتراض الأول: صعوبة إثبات الدليل المادي لهذه الهجمات بخلاف وسائل القتال الأخرى، فيمكن إثبات الدليل المادي بسهولة لكونها تترك أثرا مباشرا أو غير مباشر بعد تنفيذ الهجوم، مثل: الدمار أو التعطيل الجزئي أو الكلي لبعض المواقع العسكرية أو المدنية، أو القتل أو الإصابة التي تحدث لبعض المدنيين أو المنفذين لهذه الجريمة.... الخ[١].

الافتراض الثاني: إثبات الدليل المادي لها من خلال ترك آثار مادية ملموسة سواء على المستوى الاقتصادي أو الأمني أو المستوى العسكري، وفى هذه الحالة إذا كانت هذه الهجمات المرتكبة من قبل التصرف العدائي أو كان هذا التصرف لرد العدوان ففي هذه الحالة يعتمد على القواعد ذات الصلة وخاصة الفقرة الرابعة من المادة (٢)، والمادة ٥١ من ميثاق الأمم المتحدة[٢].

وتعد أول محاولة للبحث عن التكييف القانوني لهذه الهجمات ما ورد في "دليل تالين" بالرغم من أنها وثيقة غير ملزمة وتم إعدادها من قبل مجموعة من الخبراء، إلا أنها كان لها دور فعال ومفيد عندما تم نقاش الموضوعات المثيرة للتحديات وكيفية تفسير القانون الدولي، وكذا القانون الدولي الإنساني وكيفية تطبيقه على الأفعال التي تصدر من الدول الأطراف وغير الأطراف في مجال هذه الجرائم[٣].

(١) د. طلال ياسين العيسى، عدي محمد غياب: مرجع سابق، ص ٨٨.

(٢) د. أحمد عباس الفتلاوي: مرجع سابق، ص ٦٢٨.

(٣) د. طلال ياسين العيسى، عدي محمد غياب: مرجع سابق، ص ٨٨.

(ISSN: 2356 - 9492)

ووفقا لدليل تالين فإن العمليات الإلكترونية وحدها قد تشكل نزاعا مسلحا طبقا للظروف لاسيما الآثار المدمرة لتلك العمليات التي تقوم بها الدول، ويعد هذا الهجوم الإلكتروني بمثابة استخدام للقوة طالما كان أثر هذا الهجوم مساويا للقوة أو مقاربا لها، وبالتالي يجب أن تخضع هذه الهجمات لقواعد النزاعات المسلحة(١).

وبالنظر إلى القرار الصادر من الجمعية العامة للأمم المتحدة رقم (٥٥/٣٦) لسنة ٢٠٠٠م، نجد أن هذه الهجمات متعددة، ويمكن أن تحدث دمارا لنواحي الحياة بأكملها، ورغم ذلك لم يتم مناقشة هذه الجرائم إلا على المستوى الأدنى من التنظيم الدولي، ولم توجد مبادرات لتحديد آثار هذه الهجمات في ظل اتفاقية دولية(٢).

كما أن التكييف القانوني لهذه الهجمات من حيث شرعيتها وعدم شرعيتها، يحكمه مبدأ حظر استخدام القوة في العلاقات الدولية طبقا لنص المادة ٢/ ٤ من ميثاق الأمم المتحدة باستثناء حق الدفاع الشرعي أو التدابير التي يتخذها مجلس الأمن(٣)؛ لذلك من حق أية دولة أن تدافع عن نفسها ضد أية هجوم يقع عليها، ولن تقف هذه الدول مكتوفة الأيدي في التقدم التكنولوجي الرهيب الذي قد يتسبب في شلل كامل للدولة المعتدى عليها، وهذا الحق نجده في المادة (٥١) من ميثاق الامم المتحدة(٤).

وهناك عدة مبادئ يجب أن تلتزم بها الدول طبقا لميثاق الامم المتحدة:

المبدأ الأول: مبدأ الامتناع عن استخدام القوة.

يعد مبدأ الامتناع عن استخدام القوة أو التهديد به مبدأ أساسيا وراسخا من مبادئ القانون الدولي العام، وتم النص عليه في الفقرة الرابعة من المادة (٢) من ميثاق الأمم المتحدة، وعند الخروج على هذا المبدأ تنشأ المسؤولية الدولية(٥).

وبينت هذه المادة أن استعمال القوة أو التهديد به لا يتفق مع أهداف ومبادئ ميثاق الأمم المتحدة حيث إن هذا الميثاق يهدف إلى حفظ السلم والأمن الدوليين، وأن لفظ القوة الوارد في الفقرة الرابعة من المادة (٢) لم يحدد نوع القوة حيث جاءت مطلقة، وبالتالي تشمل كل أنواع القوة(٦).

---

(١) د. عمر محمود أعمر: مرجع سابق، ص ١٣٩.

(٢) د. يحي ياسين سعود: مرجع سابق، ص ٨٦.

(3) Lucian E. Dervan: op. cit., p. 381. See also: Kamal Ahmad Khan: Use of Force and Human Rights under International Law, Athens Journal of Law - Volume 3, Issue 2 – Pages 141-164, April 2017, p. 142.

انظر: د. محمد حسن أحمد جاد: مدى تأثير قرارات المحكمة الجنائية الدولية على الدول غير الأعضاء، رسالة دكتوراه (غير منشورة)، جامعة أسيوط، كلية الحقوق، ٢٠١٦م، ص ٢٤٠.

(4) Anna C. Mourlam: op. cit., p. 21.

انظر: أ. صلاح حيدر عبدالواحد: حروب الفضاء الإلكتروني– دراسة في مفهومها وخصائصها وسبل مواجهتها، رسالة ماجستير (غير منشورة) قسم العلوم السياسية، كلية الآداب والعلوم، جامعة الشرق الأوسط، ٢٠٢١م، ص ٥٠.

(5) Sara Pangrazzi (MLaw): self-defense against cyberattacks? Digital and kinetic defense in light of article 51-charter, ICT4Peace Publishing, Geneva, February 2021, p. 7.

(6) د. علي فاضل على سليمان: حق الدفاع الشرعي اتجاه الهجمات السيبرانية، مجلة جامعة تكريت للحقوق، السنة (٤) المجلد (٤) العدد (٤) الجزء (١)، ٢٠٢٠م، ص ٢٥٢.

وقد جاء عن محكمة العدل الدولية في القضية المعروفة بـ "النشاطات العسكرية وشبه العسكرية في قضية نيكاراغوا" ١٩٨٦م مبدأ مهم يتمثل في حظر استخدام القوة، وهذا المبدأ مستمد من نص المادة (٤/٢) سالفة الذكر، وتطور هذا المبدأ، وأصبح عرفا دوليا يحتذي به وفقا لما جاء في محكمة العدل الدولية[١].

المبدأ الثاني: تكييف الهجمات السيبرانية بالتمييز بين المدنيين والمقاتلين.

جاء في المادة (٤٨) من البروتوكول الإضافي الأول ١٩٧٧م الملحق باتفاقيات جنيف التمييز بين المدنيين وغير المدنيين (المقاتلين) وبين الأعيان المدنية والأهداف العسكرية، وأكدت الفقرة الثانية من المادة (٥١) من هذا البروتوكول أنه لا يجوز أن يكون السكان المدنيين والأشخاص المدنيين هدفا للهجوم، وتحظر أيضا أعمال العنف و التهديد به أو الأشياء التي تبث الذعر بين المواطنين[٢].

وقد نصت الفقرة الرابعة من المادة (٥١) من هذا البروتوكول أيضا على حظر استخدام طرق قتالية من شأنها أن تؤدي الى هجمات عشوائية أو الهجمات التي لا يمكن توجيهها الى أهداف عسكرية محددة أو هجمات لا يمكن حصر آثارها أو الهجمات التي يمكن أن تصيب الأهداف العسكرية والمدنيين على حد سواء أو دون تمييز[٣].

وجاء في الفقرة الخامسة من المادة (٥١) من هذا البروتوكول أنه يحظر على أية دولة أن تقوم بهجوم يتسبب في أضرار أو إصابات أو خسائر في أرواح المواطنين أو أضرار بالأعيان المدنية[٤].

وقد أكد شرط مارتينز[٥] الذي يعد بمثابة شرط إضافي للمواد السابقة، على ضرورة تحديد الوضع القانوني للهجمات الإلكترونية[٦].

---

(١) تنص المادة (٢) الفقرة الرابعة من ميثاق الأمم المتحدة على أنه "على جميع الأعضاء في علاقاتهم أن يتخلصوا من التهديد باستخدام أو استخدام القوة ضد سلامة الإقليم أو الاستقلال السياسي لأي دولة، أو في أي حالة أخرى تتعارض مع مبادئ الأمم المتحدة". انظر: د. رزق أحمد سمودي: مرجع سابق، ص ٣٣٩.

(٢) موقع اللجنة الدولية للصليب الأحمر الإلكتروني، البروتوكول الأول الإضافي إلى اتفاقيات جنيف،

https://www.icrc.org/

انظر: أ. صلاح حيدر عبدالواحد: مرجع سابق، ص ٥١.

See: Laurent Gisel and other: The potential human cost of cyber operation, ICRC expert meeting 14- 16 November 2018- Geneva. p. 9.

(٣) أ. صلاح حيدر عبدالواحد: مرجع سابق، ص ٥١.

(٤) موقع اللجنة الدولية للصليب الأحمر الإلكتروني، البروتوكول الأول الإضافي إلى اتفاقيات جنيف،

https://www.icrc.org/

(٥) نسب هذا الشرط الى المندوب الروسي فريدريك مارتنز في مؤتمر السلام الذي عقد في مدينة لاهاى ١٩٨٨م.

(٦) ينص هذا الشرط على أنه "في الحالة التي لا تنطبق فيها معاهدة، أو قانون عرفي، فإن المدنيين والعسكريين يتمتعون بحماية مبادئ القانون

(ISSN: 2356 - 9492)

وطبقاً لهذا المبدأ يجب التمييز بين الاشخاص المدنيين وغيرهم من العسكريين، وهذا التمييز لا يوجد في الكثير من الهجمات السيبرانية، وبالتالي يترتب على ذلك تدمير للكثير من المنشآت الحيوية التي هي محمية ومحرم الاعتداء عليها طبق للقانون الدولي، والمبادئ الدولية التي تحظر ذلك(١).

وأثناء إبرام البروتوكولين الإضافيين ١٩٧٧م وكذلك اتفاقيات جنيف الأربعة ١٩٤٩م لم يكن للهجمات السيبرانية أي وجود، إلا أن ذلك لا يعني عدم خضوعها لقواعد القانون الدولي الإنساني، وهناك اتفاق على أن الهجمات السيبرانية واسعة النطاق يجب ألا تكون مقابل فكرة افتراضية، بل يجب مقارنتها بالبشر، وانطلاقا من ذلك يمكن القول أن القواعد الاتفاقية للقانون الدولي الإنساني معظمها أصبحت قواعد عرفيةً معرفاً بها من قبل الدول يمكن تطبيقها على الهجمات السيبرانية(٢).

وقد استبدلت اتفاقيات جنيف ١٩٤٩م مصطلح "الحرب" بمصطلح "النزاع المسلح" بهدف توسيع النطاق المادي لتطبيق الاتفاقيات الدولية، وجعل القانون الدولي الإنساني قابلا للتطبيق وتكييف كل حالة على حدة(٣).

ونجد أن المتخصصين في القانون الدولي يقولون أن الهجمات السيبرانية التي تتم خارج نطاق النزاع المسلح ليس من الضروري أن ينظمها القانون الدولي الإنساني بخلاف الهجمات التي في سياق النزاع المسلح(٤).

ومما تقدم يتضح لنا: أن الدول المتقدمة في المجال الإلكتروني لها مصالح خاصة بها في عدم تقنين قواعد قانونية لتنظيم هذه الهجمات، لكونه سلاحاً قوياً تمتلكه وتستخدمه حيثما شاءت لضرب الدول الأعداء، وبذلك تستطيع الدول المتقدمة في هذا المجال إحداث خسائر فادحة للدولة المستهدفة، بل يمكن أن تصبح ضحية نتيجة لهذه الهجمات.

الدولي المشتقة من العرف المستقر، ومن المبادئ الإنسانية، وما يمليه الضمير العام". انظر: أ. صلاح حيدر عبدالواحد: مرجع سابق ، ص ٥٠ .

(١) أ. صلاح حيدر عبدالواحد: مرجع سابق، ص ٥٢.

See: Laurent Gisel and other: op. cit., p. 12.

(٢) أ. نور أمير الموصلي: الهجمات السيبرانية في ضوء القانون الدولي الإنساني، رسالة ماجستير (غير منشورة) الجامعة الافتراضية السورية، قانون دولي انساني، ٢٠٢١م، ص ٣٣.

(٣) صدر عن دائر الاستئناف التابعة لمحكمة يوغسلافيا السابقة في قضية تاديتش أنه لكي نكون أمام نزاع مسلح يجب توافر عنصرين: أن يكون النزاع بين الدول وأقلها دولتين؛ وأن تلجأ هذه الدول الى استخدام القوة ويقصد بالقوة المسلحة اللجوء الى الأعمال العدائية ولا يقصد بهذه القوة استخدام الدولة لقواتها المسلحة وهذا ما تبناه أيضا دليل تالين حيث نص " يوجد نزاع دولي مسلح عندما تكون هناك أعمال عدائية، والتي قد تشمل أو تقتصر على العمليات السيبرانية، التي تحدث بين دولتين أو أكثر"، حيث يقصد بالأعمال العدائية التطبيق الجماعي لوسائل وأساليب الحرب." انظر: أ. صلاح حيدر عبدالواحد: مرجع سابق، ص ٦٧.

(٤) أ. نور أمير الموصلي: مرجع سابق، ص ٦٦، ٦٧.

حق الدفاع الشرعي في مواجهة الهجمات السيبرانية في ضوء ميثاق الأمم المتحدة

دكتور/ محمد حسن أحمد جاد

المبحث الثاني
حق الدفاع الشرعي في ضوء قواعد القانون الدولي العام

طبقا لميثاق الأمم المتحدة جاءت القاعدة العامة تؤكد على حظر استخدام القوة، وهذه القاعدة ورد عليها استثناء يتمثل في حق الدفاع الشرعي طبقا لنص المادة (٥١) من ميثاق الأمم المتحدة، وهذا الحق لا يتوافر إلا إذا اعتدت قوة مسلحة على إحدى دول أعضاء الأمم المتحدة [١].

وتضمنت المادة (٥١) من ميثاق الأمم المتحدة على أنه لا يوجد في هذا الميثاق ما ينقص أو يضعف الحق الطبيعي للدول في الدفاع عن نفسها عند تعرضها لاعتداء مسلح، ولكي تنطبق حالة الدفاع الشرعي لابد من وجود اعتداء مسلح ، وذلك حسب ما ورد في المادة (٥١) من ميثاق الأمم المتحدة ، وكذلك عند استخدام القوة أو التهديد حسب ما ورد في المادة (٢/ ٤) من ميثاق الأمم المتحدة[٢].

ومما يجب ملاحظته أن المادة (٥١) من ميثاق الأمم المتحدة استخدمت مصطلح الاعتداء المسلح، والمادة (٢/ ٤) من هذا الميثاق استخدمت مصطلح القوة، وهذا يعنى أن المادة (٥١) من هذا الميثاق أعطت الدولة المعتدى عليها حق الرد بدون استخدام القوة[٣].

وبناءً على ما تقدم، نتناول في هذا المبحث حق الدفاع الشرعي من خلال المطلبين الآتيين:

المطلب الأول: مدى انطباق حكم المادة (٢ / ٤) من ميثاق الأمم المتحدة على الهجمات السيبرانية.

المطلب الثاني: مدى انطباق حكم المادة (٥١) من ميثاق الأمم المتحدة على الهجمات السيبرانية.

المطلب الأول
مدى انطباق حكم المادة (٢/ ٤) من ميثاق الأمم المتحدة على الهجمات السيبرانية.

---

(١) د. فليج غزلان: التدخل العسكري المعاصر بين القانون الدولي والممارسة الدولية – العدوان المقنع– مجلة العلوم القانونية والاجتماعية جامعة زيان عاشور بالجلفة. الجزائر، المجلد الرابع، العدد الثالث، سبتمبر ٢٠١٩م، ص ١٣٤.

(2) Sara Pangrazzi (MLaw): op. cit., p. 7.

انظر: د. بودربالة صلاح الدين: استخدام القوة المسلحة في إطار أحكام ميثاق الأمم المتحدة، رسالة دكتوراه (غير منشورة)، جامعة الجزائر، كلية الحقوق، ٢٠١٠م، ص ٤٦.

(٣) د. إبراهيم رمضان عطا: الجريمة الإلكترونية وسبل مواجهتها في الشريعة الإسلامية والأنظمة الدولية، العدد الثلاثون– الجزء الثاني (دراسة تحليلية تطبيقية) ٢٠١٥م، ص ٣٣٠، ٤٠٤، ص ٣٦٠،
https://mksq.journals.ekb.eg/article_7802_c486775c9046bdaeb05a5de3a52784c0.pdf

(ISSN: 2356 - 9492)

يحظر استخدام القوة طبقا للمادة (٢/ ٤) من ميثاق الأمم المتحدة، وهذا مبدأ أساسي من مبادئ القانون الدولي العام إلا أنه يطبق في الحالات التي يقرها مجلس الأمن لحفظ السلم والأمن الدوليين، ومنها: حالة الدفاع الشرعي طبقا لميثاق الأمم المتحدة [١].

وقد تطور هذا الأمر وأصبح عرفا دوليا وفقا لما جاء عن محكمة العدل الدولية في القضية المعروفة بـ "النشاطات العسكرية وشبه العسكرية في قضية نيكاراغوا" ١٩٨٦م[٢].

واختلف الفقهاء بشأن المقصود بـ "القوة" الوارد في المادة (٤/٢) من ميثاق الأمم المتحدة إلى اتجاهين:

الاتجاه الأول:

يأخذ بالتفسير الضيق لهذه المادة، وهو أن المقصود بالقوة هنا هي القوة العسكرية فقط دون التهديد بها، وأن المقصود من نص المادة سالفة الذكر يجب أن تكون في حدود ديباجية الميثاق ونصوصه، ولكن غالبا ما يصطحب لفظ القوة في ميثاق الأمم المتحدة مصطلح "المسلحة" التي تم ذكرها في الديباجية في المادة (٤٤) من الميثاق، ويستند أنصار هذا الاتجاه إلى الاقتراح المقدم من البرازيل في مؤتمر سان فرانسوا بخصوص الضغط السياسي بحيث يكون من قبل الاستخدام غير المشروع للقوة، ولكن هذا المقترح قوبل بالرفض [٣].

الاتجاه الثاني:

يأخذ أنصار هذا الاتجاه بالمفهوم الواسع للمادة سالفة الذكر، وبموجبه تشمل القوة العسكرية كل أنواع التهديد؛ لأن المادة (٤/٢) من هذا الميثاق جاءت مرنة بلفظ "القوة أو التهديد به"، وأن للهجوم السيبراني آثار مشابهة لمفهوم القوة العسكرية، كما أن الكود الضار أو الفيروسات لها خصائص ضارة يمكن أن تكون أداة للدمار، مثلها مثل السلاح الحربى، واستدلوا أنصار هذا الاتجاه بأن ما صدر من محكمة العدل الدولية في الفتوى المتعلقة بشأن الأسلحة الدولية لا تشير إلى أسلحة محدودة، ومن ثم فإن ذلك ينطبق على الأسلحة السيبرانية أو على أنها قوة أيضا[٤].

وذهب فريق آخر إلى أن المقصود بالقوة هو جميع صور استخدام القوة المسلحة ليس هذا فحسب، بل يشمل المصطلح أي صور أخرى يكون لها تأثير أو انتهاك واضح للأمن القومي للدولة[٥].

([1]) Sara Pangrazzi (MLaw):, op. cit., p. 7. See: Anna C. Mourlam: op. cit., p. 24.

([2]) Herbert S. Lin: op. cit., p. 75.

انظر: د. رزق أحمد سمودي: مرجع سابق، ص ٣٣٩.

([٣]) د. علي فاضل على سليمان: مرجع سابق، ص ٢٥٢.

See: Matthew Borton, Samuel Liles, Sydney Liles: op. cit., p. 314.

([٤]) د. يحي ياسين سعود: مرجع سابق، ص ٨٧.

See: Herbert S. Lin: op. cit., p. 63.

([٥]) د. أحمد عباس الفتلاوي: مرجع سابق، ص ٦٣٠.

See: Matthew Borton, Samuel Liles, Sydney Liles: op. cit., p. 315.

وقد لعب الفضاء الإلكتروني دورا أساسيا في هذه الحرب حيث أصبح التفوق في هذا المجال عنصرا حيويا لهذه الهجمات التي يتم تنفيذها على الأرض أو الجو أو البحر من خلال التحكم والسيطرة التكنولوجية العالية الأمر الذي يستدعي بالضرورة تغيير مفهوم القوة[١].

وإذا نظرنا إلى ما ورد في دليل تالين نجد أنه "يوجد نزاع مسلح دولي عندما تكون هناك أعمال عدائية، والتي قد تشمل أو تقتصر على العمليات السيبرانية، التي تحدث بين دولتين أو أكثر"[٢].

والدليل على ذلك ما جاء في النسخة الأولى من دليل تالين ٢٠١١م في القاعدة ١١ منه، وهي التي تؤكد على "أن العمليات الإلكترونية تعد استخداما للقوة عندما يكون مستواها وتأثيرها متقاربا مع العمليات غير الإلكترونية"[٣] .

وتم إعداد النص من قبل مجموعة من الخبراء استندت إلى معيار الحجم والتأثير "Effect and Scale" لتحديد ما إذا كانت الهجمات الإلكترونية ترقى إلى الاستخدام غير المشروع للقوة – باستثناء ما ورد في المادة (٤/٢) من ميثاق الأمم المتحدة– وفيما إذا كان ذلك يعد هجوما عسكريا يبرر الدفاع عن النفس طبقا للمادة ٥١ من ميثاق الأمم المتحدة، وهذان المعياران نفسهما – في الحجم والتأثير – هما اللذان استندت إليهما محكمة العدل الدولية في قضية نيكاراغوا[٤].

وتصدت أيضا محكمة العدل الدولية لهذه الإشكالية في قضية نيكاراغوا حيث تبين أن مبدأ استخدام القوة أو التهديد به يتحول إلى قاعدة عرفية دولية تلتزم به جميع الدول– وهذا يتفق مع مبادئ الأمم المتحدة – ولا يجوز لأى دولة أن تخالفه[٥].

وقد اعتبرت كل من محكمة العدل الدولية ومجموعة لجنة الخبراء لدليل تالين أن الاعتداء على الدولة بأي شكل من أشكال الاعتداء بما فيها الهجمات السيبرانية يشكل انتهاكا لسيادة الدولة طالما وصل حجم الاعتداء أو الهجوم إلى مستوى معين[١].

---

(١) ويمكن تعريف القوة بأنها: مجموعة من الوسائل والطاقات والامكانات المادية وغير المادية المنظورة وغير المنظورة التي بحوزة الدولة ويستخدمها صانعي القرار في فعل مؤثر يحق مصالح الدولة ويؤثر في سلوك الوحدات السياسية الأخرى. د. يحي ياسين سعود: مرجع سابق، ص ٨٧.

(٢) أ. نور أمير الموصلي: مرجع سابق، ص ٦٧.

(٣) د. رزق أحمد سمودي: مرجع سابق، ص ٣٤٩.

(4) Sara Pangrazzi (MLaw): op. cit., p. 7.

انظر: هربرت لين: النزاع السيبراني والقانون الدولي الإنساني، مختارات من المجلة الدولية للصليب الاحمر المجلد ٩٤ (٨٨٦)، ٢٠١٢م، ص ٥٢٤.

(٥) د. أميرة عبدالعظيم محمد عبد الجواد: المخاطر السيبرانية وسبل مواجهتها في القانون الدولي العام، مجلة الشريعة والقانون، العدد ٥٣، الجزء ٣، ٢٠٢٠م، ص ٤٤٤.

See: Anna C. Mourlam: op. cit., p. 20.

(ISSN: 2356 - 9492)

وعلى ذلك يعد إرسال قوة نظامية أو غير نظامية خارج حدود الدولة أو أي وسيلة أخرى بمثابة هجوم مسلح، وهذا خروج واضح للمحكمة عن النهج المعروف لفهم استخدام القوة، والذى يتمثل في صدور قرار صريح من الدولة باستخدام القوة المسلحة[٢].

وتم التأكيد على ذلك عند صياغة المادة (٢/ ٤) من ميثاق الأمم المتحدة على أن أيه تهديد أو استخدام للقوة من قبل دولة يعد ذلك خرقا لهذه المادة يبرر حق الدفاع عن النفس[٣].

وأما القول بأن الميثاق اشترط استخدام القوة وأن الهجمات السيبرانية لا يتوافر فيها ذلك فهذا القول يتنافى مع مقاصد الأمم المتحدة الذى حظر في الفقرة الرابعة من المادة الثانية اللجوء إلى الحرب أو التهديد باستعمال القوة أو استخدامه ضد سلامة الأراضي أو على أية وجه آخر لا يتفق مع مقاصد الأمم المتحدة [٤]. ونجد أن ميثاق الأمم المتحدة ترك الأمر لمجلس الأمن ليقرر كل حالة على حدة تبعا للظروف المحيطة بها[٥].

وتم تجريم الهجمات التي ترتكب بشكل مباشر، ويكون لها تأثير مباشر أيضا مستندين إلى مبدأ التأثيرات؛ لكون أن هذه الأفعال يترتب عليها أضرار بالغة تلحق بالدولة[٦].

ويعد إرسال القوات من الدولة أو بالنيابة عنها سواء كانت هذه القوات على شكل مجموعات نظامية أو غير نظامية مخالفاً للمادة (٤/٢) من الميثاق، ويمكن لمثل هذا التصرف أن يعد هجوما مسلحا طبقا لحجم القوة والتأثير[٧].

وذهب كل من "شين، ورسيني" إلى أنه من الممكن أن تكون الهجمات بمثابة خرق واضح لأحكام الفقرة الرابعة من المادة الثانية من ميثاق الأمم المتحدة شريطة أن تتسبب هذه الهجمات في دمار واسع المدى أو تعطيل للبنية التحتية[٨].

وذهب "لوارن جيزيل"[١] إلى أن القانون الدولي الإنساني لا ينطبق على كآفة الهجمات السيبرانية التي تقع خارج النطاق المسلح، ولكن ما جاء في اتفاقية جنيف الرابعة من استبدال مصطلح الحرب بمصطلح النزاع المسلح بهدف توسيع

---

(١) د. رزق أحمد سمودي: مرجع سابق، ص ٣٥١.

(٢) د. سلافة طارق الشالان: تكييف استخدام الحرب الإلكترونية في النزاعات المسلحة وفقا للقانون الدولي الإنساني، مجلة الكوفة للعلوم القانونية والسياسية، العدد ٢٦، ٢٠١٦م، ص ١٢٥.

(3) Sara Pangrazzi (MLaw): op. cit., p. 7. Kamal Ahmad Khan: Use of Force and Human Rights under International Law, op. cit., p. 142.

(4) د. عمر محمود أعمر: مرجع سابق، ص ١٣٨. انظر: د. بودربالة صلاح الدين: استخدام القوة المسلحة في إطار أحكام ميثاق الأمم المتحدة، رسالة دكتوراه (غير منشورة)، جامعة الجزائر، كلية الحقوق، ٢٠١٠م، ص ٤٨.

(٥) حيث منحت المادة (٣٩) من ميثاق الأمم المتحدة مجلس الأمن سلطة تقرير الاجراءات القهرية، كما أن هذا النص ورد بصورة غير ملزمة باعتبار أن مجلس الأمن يتمتع بصلاحيات تقرير الحالات التي تهدد السلم والأمن الدوليين. انظر: المادة (٣٩) من ميثاق الأمم المتحدة. انظر أيضا: د. عمر محمود أعمر: مرجع سابق، ص ١٣٨.

(6) Anna C. Mourlam: op. cit., p. 20.

(٧) د. رزق أحمد سمودي: مرجع سابق، ص ٣٤٨.

See also: Matthew Borton, Samuel Liles, Sydney Liles: op. cit., p. 310, 314.

(٨) أ. صلاح حيدر عبدالواحد: مرجع سابق، ص ٥٠.

النطاق المادي لهذه الاتفاقيات لتطبيقها على هذه الهجمات، وجعل القانون الدولي الإنساني أيضا قابلا للتطبيق بناء على كل حالة على حدة[٢].

ولكن قد تحدث الهجمات السيبرانية خارج نطاق النزاع المسلح، ولكنها ترتقى إلى مستوى الهجوم المسلح، وينتج عنها أضرار مادية وخسائر في الأرواح والممتلكات، ويمكن إثباتها أو نسبها لدولة معينة، فعندئذ يمكن تطبيق قواعد القانون الدولي الإنساني، بخلاف ما إذا كان لا تستطيع الدولة نسب هذا الهجوم إلى دولة معينة فهنا يمكن تطبيق القانون الدولي لحقوق الإنسان بالإضافة الى تطبيق القانون المحلي للدولة المعنية[٣].

وقد فرقت محكمة العدل الدولية في قضية نيكاراغوا بين الأشكال الأكثر خطراً والأقل خطورة واعتبرت الأشكال الأكثر خطرا هي التي تبيح استخدام حق الدفاع عن النفس وفقا لنص المادة (٥١) من ميثاق الأمم المتحدة، بخلاف الأقل خطورة، وهذا ما سنتناوله في المطلب التالي[٤].

خلاصة القول: إن الدعم غير العسكري قد يشكل انتهاكاً للمادة(٤/٢) من ميثاق الأمم المتحدة، كما إن الاستخدام غير المشروع والاستغلال قد يشكل خطورة شديدة تضاهي في الحجم والأثر القوة العسكرية خاصة إذا كانت متعلقة بإصابات أو خسائر في أرواح المدنيين وفى هذه الحالة يمكن القول بأن ما ينطبق على الجرائم العسكرية ينطبق عليها باعتبارها جرائم لا تقل كثيرا عن الجرائم العسكرية.

المطلب الثاني
مدى انطباق حكم المادة (٥١) من ميثاق الأمم المتحدة على الهجمات السيبرانية

تعد الهجمات السيبرانية التي تحدث أثناء النزعات المسلحة من إحدى الدول المتنازعة أو بعض الدول الاطراف في هذا النزاع استخداما للقوة، يعطي للدولة الحق في أن تدافع عن نفسها ضد أية هجمات سيبرانية تقع عليها[٥].

---

(١) المستشار القانوني للجنة الدولية للصليب الأحمر.

(٢) أ. نور أمير الموصلي: مرجع سابق، ص ٦٦، ٦٧. انظر : I C R C : اللجنة الدولية للصليب الأحمر، ما هي القيود التي يفرضها قانون الحرب على الهجمات السيبرانية؟، مقال منشورة للجنة ٢٨/ ٦/ ٢٠١٣م،
https://www.icrc.org/ar/doc/resources/documents/faq/130628-cyber-warfare-q-and-a-eng.htm

(٣) أ. نور أمير الموصلي: مرجع سابق، ص ٦٨.

(٤) د. رزق أحمد سمودي: مرجع سابق، ص ٣٤٠.

(5) Matthew C. Waxman: Self-Defensive Force against Cyber Attacks: Legal, Strategic and Political Dimensions, Vol. 89, 2013, p. 109. See: Sara Pangrazzi (MLaw): op. cit., p. 4.

(ISSN: 2356 - 9492)

وبالرغم من عدم النص على هذه الهجمات ضمن قواعد ونصوص القانون الدولي الإنساني إلا أن ذلك لا يعنى عدم خضوعها لقواعد هذا القانون التي ينظم جميع أساليب الحرب ووسائلها[١].

ويعد حظر استخدام القوة أو التهديد الوارد في المادة (٢/ ٤) من ميثاق الأمم المتحدة ليس مطلقاً حيث يمكن إباحة واستخدام القوة في حالتين:

الحالة الأولى: وهي حالة الأمن الجماعي وفقا لقرار مجلس الأمن المادة: (٤/٢) من ميثاق الأمم المتحدة، والحالة الثانية: هي حالة الدفاع الشرعي طبقا لنص المادة (٥١) من ميثاق الأمم المتحدة[٢].

واستقر فقهاء القانون الدولي على أن التهديد لا يقوم إلا بقوة عسكرية، بينما ذهب شين (Shin) إلى اتجاه مغاير، حيث يقول: من الصعب القول بإقرار شرعية الهجمات السيبرانية، ولا يمكن أن تعفى الدولة استناد لنص الفقرة الرابعة من المادة (٢) من ميثاق الأمم المتحدة إذا أدت الهجمات السيبرانية إلى آثار ملموسة سواء في الأعيان المدنية أو الأعيان العسكرية[٣].

وذهب ماركوروسيني (Marco Rocini) إلى أن الهجمات السيبرانية تعد بمثابة خرق صريح لنص صريح للمادة الثانية من ميثاق الأمم المتحدة طالما ترتب على هذه الهجمات تعطيل أو دمار للبنية التحتية، كما يمكن أن يكون للقواعد العرفية دورٌ مميزٌ في تكييف تلك الهجمات خاصة في ظل عدم وجود تنظيم دولي صريح للهجمات السيبرانية[٤]؛ لذلك تصبح هذه الهجمات مجرمة متى تم استخدام القوة فيها، وبالتالي يحق للدولة أن تدافع عن نفسها ضد أية هجمات سيبرانية[٥].

وعندما تشكل الهجمات السيبرانية هجوما مسلحا فإن ذلك يكون استخداما للقوة يعطى الحق للدولة المعتدى عليها حق الدفاع عن النفس استنادا لنص المادة (٥١) من ميثاق الأمم المتحدة[٦].

انظر: د. يحيى بن سعود: مرجع سابق، ص ٨٩.

[1]) يرى بعض فقهاء القانون الدولي أنها تنطبق قواعد القانون الدولي الإنساني على هذه الجرائم، بينما يرى البعض الآخر أمثال: "إيميلى هاسلام" وغيرة من الفقهاء عدم انطباقها لأن المدة التي جرى فيها تقنين القواعد العسكرية لا يوجد فيها ما يسمى بالحروب السيبرانية أي لم يكن فيها استخدام في الانظمة الإلكترونية تستخدم لأغراض القتال والحروب بين الدول. انظر: أ. صلاح حيدر عبدالواحد: مرجع سابق، ص ٣١ .

[2]) د. أبوبكر المبروك بشير أبو عجيلة: أثر أحداث الحادي عشر من سبتمبر في السياسة الخارجية للولايات المتحدة الأمريكية تجاه منطقة الشرق بحث مقدم إلى جامعة الخرطوم لنيل درجة الدكتوراه في العلوم السياسية (غير منشورة)، ٢٠١٠م، ص ١٤٠. انظر: د.) الاوسط (٢٠٠١ –٢٠٠٨ يوبي عبدالقادر: مرجع سابق، ص ٢٠٢.

See: Lucian E. Dervan: op. cit., p. 315.

(٣) د. أحمد عباس الفتلاوي: مرجع سابق، ص ٦٣٠، ٦٣١.

(٤) المرجع سابق: ص ٦٣٠، ٦٣١.

(5) Sara Pangrazzi (MLaw): op. cit., p. 4.

انظر: د. يحيى بن سعود: مرجع سابق، ص ٩٠.

(6) Lucian E. Dervan: op. cit., p. 109.

وبالنظر إلى مصطلحي "الاعتداء المسلح" و "استخدام القوة أو التهديد بها" نجد أن المصطلح الأول يعطي الدولة الحق في استخدام القوة في الدفاع عن نفسها فرادي أو جماعات استنادا إلى المادة (٥١) من ميثاق الأمم المتحدة ، بينما نجد المصطلح الثاني الوارد في الفقرة الرابعة من المادة (٢) من ميثاق الأمم المتحدة، يعطي الدولة خيارات قانونية أخرى، أهمها: الإجراء المضاد الذى يعطي الدولة حق الرد بطرق أخري دون استخدام القوة[١].

وما يجب ملاحظته أن فكرة الإجراء المضاد[٢] للرد على الاعتداء جاء مقيداً بعدة شروط، أهمها: شرط الضرورة والتناسب، وهو ما أكدت عليه محكمة العدل الدولية في قضية كوبسكوفو ١٩٩٧م[٣].

ويجب على الدولة التي تدافع عن نفسها أن تكون ملتزمة بأحكام اتفاقية جنيف والتي بموجبها يجب ألا يتضرر السكان المدنيين من هذا الهجوم المسلح، كما يجب أن ألا تكون ممتلكات ومصالح الأشخاص المدنيين من بنوك ومستشفيات وكهرباء هدفاً للدولة صاحبة الحق في الرد حتى لا يكون حق استخدام القوة في الدفاع عن النفس من الدولة المعتدى عليها ذريعة لتدمير البنية التحتية للدولة المعتدية[٤].

ويؤكد بعض العلماء أن الاعتداء على شبكات الحاسب الآلي يشكل استخداما للقوة يعطي الحق للدولة المعتدى عليها حق الدفاع عن نفسها طبقا للمادة (٥١) من ميثاق الأمم المتحدة[٥].

كما يجب أن تكون القوة المستخدمة في الرد هي السبيل الوحيد لمواجهه الدولة المعتدية، ومما تم ملاحظته أن الرد يجب ألا يكون مطلقا، وإنما أتى مقيدا وفقا للمادة (٤٨) من الملحق الأصلي لاتفاقية جنيف والتي حددت الأهداف التي من الممكن استهدافا من قبل الدولة المعتدى عليها وهي الأهداف العسكرية[٦].

وهناك مجموعة من المبادئ الأساسية المهمة التي تحكم الهجمات السيبرانية، نتناولها على النحو الآتي:

المبدأ الأول: مبدأ الضرورة:

([1]) Anna C. Mourlam: op. cit., p. 23.

انظر: د. أميرة عبدالعظيم محمد عبد الجواد: مرجع سابق، ص ٤٥٠.

([٢]) انظر: المادة ٢٢ من مشروع مواد مسؤولية الدول عن الافعال غير المشروعة ٢٠٠١م.

([٣]) د. رزق أحمد سمودي: مرجع سابق، ص ٣٤١.

See: Anna C. Mourlam: op. cit., p. 23.

([٤]) د. علي فاضل على سليمان: مرجع سابق، ص ٢٥٤.

([5]) Lucian E. Dervan: op. cit., p. 382.

([٦]) د. علي فاضل على سليمان: مرجع سابق، ص ٢٥٤.

(ISSN: 2356 - 9492)

وهو يعني مبدأ الضرورة: الحالة التي تجبر الدولة على اللجوء للدفاع عن نفسها باستخدام القوة حيث إن الوسائل السلمية لحل المنازعات لم تعد لها جدوي في هذا التوقيت، ولم يعد أمام الدولة المعتدى عليها إلا اللجوء إلى القوة للدفاع عن نفسها استناد لمبدأ حق الدفاع الشرعي طبقا لميثاق الأمم المتحدة[١].

وجاء مبدأ الضرورة كمساحة إضافية لإعطاء الدولة المهاجمة فرصة يمكن أن تثبت فيها عدم نيتها في الهجوم، وأنها لا تريد حرباً مع هذه الدولة، وأن هذا الاعتداء لم يكن مقصودا[٢].

ويجب أن يكون رد الفعل للدفاع عن النفس ضد هذه الهجمات التي ترقى إلى الهجوم المسلح بمتطلبات الضرورة والتناسب، ولم يتم الإشارة إليهما في المادة (٥١) من ميثاق الامم المتحدة بشكل واضح لكن الرأي الاستشاري الخاص بالأسلحة النووية الصادر ١٩٩٦م عند ممارسة حق الدفاع عن النفس ذكر شرطين لابد من توافرهما، وهما الضرورة والتناسب، والتي تعد قاعدة من قواعد القانون الدولي العرفي[٣].

ويعد مبدأ الضرورة من المسائل التي تبرر حق الدفاع عن النفس، ولكن توجد صعوبة في تقديرها، فلكي يتم تطبيق هذا المبدأ يجب أن تكون القوة القاهرة هي الطريق الوحيد لرد العدوان، وأن يكون الرد على الهجوم السيبراني ضروريا[٤].

ولكي يكون الرد متفقا مع قواعد القانون الدولي لابد أن يكون استعمال القوة في الرد على الهجمات مقيدا وليس مطلقا طبقا لما ورد في المادة ٤٨ من الملحق الإضافي لاتفاقيات جنيف ١٩٤٩م والتي حددت الأهداف التي يمكن ضربها وهي الأهداف العسكرية[٥].

وفي سبيل تأمين المدنيين، أصدرت اللجنة الدولية للصليب الأحمر سنة ١٩٥٦م مسودة القواعد لتقييد الأخطار والتي نصت على أنه يجب ألا يكون المدنيين هدفا للحروب، وأن يكونوا خارج مجال الهجوم المسلح[٦].

فضلا عما ورد في اتفاقية لاهاي الرابعة التي بينت على أنه ليس للدولة المعتدى عليها استهداف أو تدمير الممتلكات الخاصة بالمدنيين، وإلا يعد هذا الانتهاك جريمة تعاقب عليها الدولة طبقا لاتفاقية روما المنشئة للمحكمة الجنائية الدولية[٧].

([1]) Anna C. Mourlam: op. cit., p. 23, 24.

([٢]) د. رزق أحمد سمودي: مرجع سابق، ص ٣٤٣.

([3]) Sara Pangrazzi (MLaw): op. cit., p. 9.

([٤]) د. أحمد عباس الفتلاوي: مرجع سابق، ص ٦٣٣.

See: Anna C. Mourlam: op. cit., p. 23.

([٥]) د. علي فاضل على سليمان: مرجع سابق، ص ٢٥٤.

See: Anna C. Mourlam: op. cit., p. 23.

([6]) Emily Crawford: Virtual Battlegrounds, op. cit., p. 5 margin.

([7]) Anna C. Mourlam: op. cit., p. 23.

انظر: د. علي فاضل على سليمان: مرجع سابق، ص ٢٥٤.

دكتور/ محمد حسن أحمد جاد

وقد أكدت محكمة العدل الدولية على ذلك أكثر من مرة وفى الكثير من المواقف أن الدفاع عن النفس يجب أن يكون مناسبا للهجوم المسلح والضروري للرد، وهذه قاعدة معروفة وراسخة من قواعد القانون الدولي العرفي التي يجب مراعاتها في جميع الأحوال(١).

ويجب على الدولة التي تستخدم حقها في الرد أن تكون ملتزمة بأحكام اتفاقيات جنيف والتي بموجبها يمتنع على الدول التي تستخدم حق الرد: ألا يلحق المدنيين أو ممتلكاتهم ضررٌ، وألا تكون المصالح الحكومية من مدارس ومستشفيات وبنوك وغيرها هدفا للدولة صاحبة الرد؛ لذلك فإن انتهاك هذه الممتلكات يوجب مسؤولية الدولة صاحبة الرد(٢).

كما أن استخدام القوة في الدفاع عن النفس وتدمير الممتلكات واستهداف المصالح المدنية قد يحول الدولة من دولة صاحبة حق إلى دولة مسؤولة؛ لذلك يجب أن يكون مبدأ التناسب حاضرا في جميع الأحوال حتى لا تقوم مسؤولية الدولة صاحبة الرد(٣).

وقد أكدت محكمة العدل الدولية على هذا الأمر لأن حق الدفاع عن النفس لابد أن يكون مناسبا مع الهجوم المسلح وضروري للرد عليه، وتم التأكيد عليه من قبل المحكمة في أحد الفتاوى الصادرة عنها باعتبار أن القوة المستخدمة لابد أن تكون بالحاجة التي تتناسب مع الهجوم(٤).

وهذه الهجمات يتوقع أن تسبب إصابات أو موت أو دمار أو ضرر كبير لذلك لابد أن يكون مبدأ الضرورة حاضرا في جميع الأحوال(٥).

المبدأ الثاني: مبدأ التناسب:

تم استخدام هذا المصطلح للمرة الأولى عام ١٩٢٢م أثناء تقنين قواعد الحرب الجوية، وأشير إلى هذا المبدأ في الفقرة (٥/ ب) من المادة (٥١) من البروتوكول الإضافي الأول لعام ١٩٧٧م والذي بموجبه يحظر على الدول التي تقوم باستخدام القوة التي يترتب عليها إصابات أو خسائر في أرواح المدنيين أو أضرار بالأعيان المدنية(٦).

---

(١) د. رزق أحمد سمودي: مرجع سابق، ص ٣٤١.

(٢) د. علي فاضل على سليمان: مرجع سابق، ص ٢٥٥.

(٣) د. فليج غزلان: مرجع سابق، ص ١٣٢.

(4) Elizabeth Wilmshurst: Self-Defense against Nonstate Actors: Reflections on the "Bethlehem Principles, American journal of international law, vol. 108, issue 2, 2017. An article published on the Internet without a page number, see the following site،
https://www.cambridge.org/core/journals/american-journal-of-international-law

(5) Anna C. Mourlam: op. cit., p. 19, 23. See: John Richardson: op. cit., p. 13.

(٦) د. أحمد عباس الفتلاوي: مرجع سابق، ص ٦٣٧.

(ISSN: 2356 - 9492)

ويعنى مبدأ التناسب في مصطلح الدفاع عن النفس اتخاذ الإجراءات الضرورية اللازمة لرد هذا الاعتداء دون تجاوز، ويتحقق ذلك التناسب عندما يكون رد الفعل متقارباً أو شبة متماثل مع الاعتداء، ولا يجاوزه حتى يتحقق السلم والأمن الدوليين(١).

ولا يكون هذا التناسب في استخدام القوة المسلحة مشروعا إلا عندما يتم توجيهه إلى القوات العسكرية أو الأشياء المتعلقة بالعمليات العسكرية والمؤسسات والمستودعات العسكرية والمصانع التي تستخدم لإنتاج الأسلحة ..... الخ(٢).

وقد تبنى دليل تالين هذا المبدأ، وذكر أن المواقف التي يتعرض فيها المدنيون أو الأعيان المدنية للأذى بشكل عرضي وأنهم غير مقصودين أثناء الهجوم السيبراني على هدف عسكري مشروع لا يجعل بالضرورة الهجوم غير قانوني(٣).

وتحظر الهجمات التي تلحق أضرارا بالمدنيين أو الأعيان المدنية بشكل مفرط، ويجب على الأطراف المتنازعة تقييم الضرر الذي ينتج عن هذا الرد كما يحظر الهجوم على الأهداف غير العسكرية التي يترتب عليها أذى أو وفاة أو تلف أو ضمار(٤).

كما يجب أن توجه الهجمات ضد المقاتلين والجيش بخلاف ما نراه من توجه ضربات تلحق بالمواطنين أذي أو ضرر، فهذا لا يجوز، ويوجب المسؤولية على الدولة المعتدية(٥).

ويثير مبدأ التناسب وتطبيقه على أرض الواقع بعض الصعوبات، وأهمها: الأضرار العرضية التي تحدث للمدنيين – بسبب استخدام الفضاء – من قبل الأطراف المتنازعة، ولكن دليل تالين حسم هذا الأمر من خلال حظر الهجمات التي من شأنها أن تسبب إصابات وقتل للمدنيين أو خسائر في الأعيان المدنية(٦).

وللدولة المعتدى عليها حق الرد في الدفاع عن النفس، ولكي يكون الرد قانونيا يجب أن يكون على هذه الهجمات التي ترتقى الى مستوى الهجوم المسلح بمتطلبات الضرورة والتناسب(٧).

وفيما يتعلق بمبدأ الضرورة العسكرية أشار "دليل تالين" إلى أنه عندما توجد عدة أهداف عسكرية بهدف الحصول على ميزة عسكرية مماثلة، فإن الهدف الذي يتم اختياره هو الهدف الذي يتوقع أن يكون خطره أقل على المدنيين، ولكن عندما

See: Matthew Borton, Samuel Liles, Sydney Liles: op, cit., p. 313.

(١) د. أميرة عبدالعظيم: مرجع سابق، ص ٤٥٤.

See: Anna C. Mourlam: op. cit., p. 24.

(٢) د. أحمد عباس الفتلاوي: مرجع سابق، ص ٦٣٧.

(٣) أ. نور أمير الموصلي: مرجع سابق، ص ٥١.

(4) Helen Wilson1 & Patrick van Esch: op. cit., p. 112.

انظر: د. عمر محمود أعمر: مرجع سابق، ص ١٤٥.

(5) Matthew Borton, Samuel Liles, Sydney Liles: op. cit., p. 313.

(6) د. يحي ياسين سعود: مرجع سابق، ص ٩٤. انظر: فيرونيك كريستوري: مرجع سابق، ص ٢.

(7) Sara Pangrazzi (MLaw): op. cit., p. 9.

انظر: د. علي فاضل على سليمان: مرجع سابق، ص ٢٥٦.

توجد عدة أهداف، أحدهما يحقق ميزة عسكرية أكبر يحق للمهاجم عند توجيه الهجمات السيبرانية المباشرة أن يختار الهدف الذي يحقق ميزة عسكرية أكبر مع مراعاة الضرر الذي يلحق المنشئات والبنية التحتية للطرف الآخر [١].

المبدأ الثالث: مبدأ الفورية:

يقصد بالفورية: عدم مرور فترة طويلة من الزمن على الاعتداء الواقع على الدولة التي تقوم بالدفاع عن نفسها، والسبب في ذلك أنه لو مرت فترة طويلة من الزمن فإن حقها يسقط في هذه الحالة؛ لأن مجلس الأمن هو صاحب الاختصاص الأساسي في حفظ السلم والأمن الدوليين[٢].

وعلى الرغم من ذلك يمكن أن تمتد هذه المدة لفترة زمنية معقولة للتأكد من نية الدولة المعتدية وهذا تحقيقا لشرط الضرورة الذى يوجب على الدولة المعتدى عليها التأكد من نية المعدية[٣].

وتظهر لنا المشكلة عند رسم الخط الذي يفصل بين استخدام القوة والاعتداء المسلح، لأن الاعتداء المسلح غير واضح في كثير من الحالات، ويمكن حل هذه الإشكالية من خلال الرجوع إلى محكمة العدل الدولية عند نظرها لقضية نيكاراغوا والتي تعد أن الاعتداء المسلح أخطر شكل من أشكال استخدام القوة، واعتبرت المحكمة أن المناوشات المسلحة على الحدود بين الدول لا ترقى أو لا تصل إلى الاعتداء المسلح[٤].

كما بينت المحكمة الفرق بين استخدام القوة والاعتداء المسلح في قضية منصات النفط بين الولايات المتحدة الأمريكية وإيران عام ٢٠٠٣م التي دمرت فيها الولايات المتحدة الأمريكية منصات النفط الإيرانية في منطقة الخليج عام ١٩٨٧م[٥].

وهناك مجموعة من الشروط يجب أن تتوافر في الهجمات السيبرانية حتى ترقى الى مرحلة الهجوم المسلح وهي:

الشرط الأول: الحدة.

يقصد بهذا الشرط أن يكون الهجوم قد وصل إلى درجة من الجسامة أو الحدة، وهذا ما اعتبرته مجموعة الخبراء لدليل تالين شرطا أساسياً حتى تصل العمليات السيبرانية إلى مستوى الهجوم المسلح[٦].

---

[1]) د. يحي ياسين سعود: مرجع سابق، ص ٩٤.

(٢) د. أميرة عبدالعظيم محمد عبد الجواد: مرجع سابق، ص ٤٥٣.

See: Anna C. Mourlam: op. cit., p. 24.

(٣) د. رزق أحمد سمودي: مرجع سابق، ص ٣٤٣.

(4) Anna C. Mourlam: op. cit., p. 20.

(٥) د. أميرة عبدالعظيم محمد عبد الجواد: مرجع سابق، ص ٤٥٥.

(6) Sara Pangrazzi (MLaw): op. cit., p. 9.

انظر: د. رزق أحمد سمودي: مرجع سابق، ص ٣٥٢.

(ISSN: 2356 - 9492)

ولكن هناك إشكالية تتمثل في مستوى الحدة، حتى يتم تكييف هذه العملية على أنها جسيمة، وفى هذا السياق رأت اللجنة أن الضرر المادي الناتج عن العمليات الإلكترونية هو الذي يسبب ضررا ماديا حالاً على الأفراد والممتلكات، وبالتالي ترقى إلى مستوى الهجوم المسلح الوارد في المادة (٥١) من ميثاق الأمم المتحدة[١].

أما بالنسبة للهجمات التي تقع دون أن ينتج عنها أضرار مادية على الأفراد والممتلكات والتي ينتج عنها إرباك بشكل جزئي للدولة المعتدى عليها، فإن ذلك لا ينطبق عليها نص المادة (٥١) من ميثاق الأمم المتحدة مثل: الهجوم الذي يقع على إحدى الإدارات الفرعية للدولة التي وقع عليها الهجوم[٢].

ويلاحظ أن الهجوم الذي يقع على المطارات والذى يمكن أن يسبب مقتل الآلاف من البشر بسبب تصادم الطائرات هبوطا وصعودا، أجابت اللجنة بأن ذلك من شأنه أن يعطي حق الدفاع عن النفس[٣].

لكن يخرج من ذلك "الأعمال الأقل خطورة" مثل: الهجوم الذي يسبب قلقا أو إزعاجا دون أن يقترن بمصلحة أساسية من مصالح الدولة، وكذلك المناوشات الحدودية لا يمكن أن تعد شكلا من أشكال القوة ولهذا لا يمكن تطبيق نص المادة (٥١) من هذا الميثاق[٤].

وفى ٢٠١١م، انعقد مؤتمر دولي للجنة الدولة للصليب الأحمر، وأكد المؤتمر أن الهجوم الذي يقع على الإنترنت ولا يترتب عليه دماراً فإن ذلك لا تندرج ضمن مفهوم القوة[٥].

وطبقاً لما ورد من هذه اللجنة، فأن الضرر المادي للأشخاص والممتلكات يتحقق به معيار الجسامة، وهذا ما جاء موافقا لمحكمة العدل قضية نيكاراغوا عندما فرقت بين الأعمال الخطرة والأعمال الأكثر خطورة، ورغم ذلك تبقى الحاجة قائمة إلى وضع معيار دقيق؛ لتحديد ما يعد جسيما وما يعد أقل جسامة حتى يتم تطبيق نص المادة (٥١) من هذا الميثاق بوضوح[٦].

ومما يجب ملاحظته أن العمليات التي تسبب تأثيراً مباشراً في حركة الطيران فإن ذلك يسبب إزعاج للدولة التي وقع عليها الاعتداء، بالإضافة إلى الضرر الملحق بمصلحة وطنية للدولة؛ وبالتالي ينطبق هنا نص المادة (٥١) من ميثاق الأمم المتحدة[٧].

([1]) Sara Pangrazzi (MLaw): op. cit., p. 9.

([٢]) د. رزق أحمد سمودي: مرجع سابق، ص ٣٥٢.

([3]) Anna C. Mourlam: op. cit., p. 19.

([٤]) د. رزق أحمد سمودي: مرجع سابق، ص ٣٥٢، ١٥٣.

([5]) Anna C. Mourlam: op. cit, p. 23.

([٦]) د. رزق أحمد سمودي: مرجع سابق، ص ٣٥٢.

See: Anna C. Mourlam: op. cit., p. 23.

([٧]) د. رزق أحمد سمودي: مرجع سابق، ص ٣٥٢.

الشرط الثاني: الضرر.

يعد شرط الضرر شرطا أساسيا وجوهريا حتى ترتقي الهجمات السيبرانية إلى مستوى النزاع المسلح، إذ أن القيد الكمي المفروض على التدابير المضادة هو شرط التناسب؛ لذلك نجد أن المادة ٥١ تنص على أنه يجب أن تكون التدابير المضادة متناسبة مع الضرر بمعنى أنه يجب الأخذ بعين الاعتبار أن يكون رد الفعل مناسبا مع الفعل نفسه[١].

وقد وضعت المادة (٥٠) مزيدا من الشروط الأساسية على التدابير المضادة " حظر التهديد باستعمال القوة أو استعمالها، والالتزامات الأساسية في مجال حقوق الإنسان، والالتزامات الإنسانية التي تحظر الأعمال الانتقامية، وعموما، الالتزامات الخاضعة للقواعد الآمرة "[٢].

ويتحقق الضرر في حالتين: الحالة الأولى: عندما يقع بالفعل، والحالة الثانية: هي الأكثر تعقيدا، عندما يكون الخطر وشيك الوقوع، وفى الحالة الثانية حسب ما أقرته لجنة الخبراء لدليل تالين يتحقق بها حالة الدفاع عن النفس وتفعيل نص المادة (٥١) من ميثاق الأمم المتحدة[٣].

والضرر سواء كان ضررا مباشراً أم غير مباشر وبكل صوره عند تطبيقه على الجرائم السيبرانية يتحقق من تلك الهجمات سواء كان مرتكب هذه الجريمة دولا: كالهجوم الفيروسي على البرنامج النووي الإيراني، أو منظمات إجرامية تلحق أضرار بالآخرين: كالهجمات التي تهدف إلى سرقة المعلومات أو إلى سرقة أرقام بطاقات الائتمان... الخ[٤].

الشرط الثالث: أن يكون أثر الهجوم مباشراً.

بالاستناد إلى شرط "الاتصال المباشر" الوارد في دليل تالين فإن ذلك لا يمكن أن يرتقي بالفعل إلى مرتبة الهجوم المسلح؛ بسبب عدم القدرة على تحديد العلاقة السببية بين الفعل والضرر، لذا يجب التفرقة بين الآنية والمباشرة لكونهما

---

(١) د. جيمس كرو فورد: المواد المتعلقة بمسؤولية الدول عن الأفعال غير المشروعة دوليا، مركز لاوت باخت لبحوث القانون الدولي – جامعة كمبردج، ٢٠١٧، ص ١٢.

(٢) A / C.6/55/SR.18

الجمعية العامة للأمم المتحدة ٢٠٠١م،

https://digitallibrary.un.org/record/436286

(٣) د. رزق أحمد سمودي: مرجع سابق، ص ٣٥٣.

(٤) د. طلال ياسين العيسى، عدي محمد غياب: مرجع سابق، ص ٨٩.

See: Landon J. Wedermyer: The Changing Face of War: The Stuxnet Virus and the Need for International Regulation of Cyber Conflict, Submitted in partial fulfillment of the requirements of the King Scholar Program Michigan State University College of Law under the direction of Professor Adam Candeub Spring, 2012, p. 6.

(ISSN: 2356 - 9492)

شرطين أساسين واردين في دليل تالين، فالآنية تتحقق عندما يخرج الضرر إلى حيز الوجود، وتتحقق المباشرة عندما يوجد ارتباط بين التصرف والضرر[١].

الشرط الرابع: وجود عداء بين الدولتين.

تضمن دليل تالين شرط وجود عداء بين الدولتين، ويتمثل هذا العداء في النية لارتكاب هذه الجرائم، وطبقاً لما ورد في دليل تالين أن العمليات السيبرانية ترتقي إلى مستوى الهجوم المسلح عند ارتكاب هذا التصرف، وتكون الدولة المعتدى عليها قادرة على إثبات أن هذا التصرف يسعى لتحقيق أهداف عدائية، مثل: إضعاف القدرة العسكرية للدولة المعتدي عليها[٢].

ولكن ما يثير التساؤل هنا في كيفية تحديد النية: هل هي نية عدائية أم لا؟ ويمكن الإجابة على هذا السؤال من خلال حكم محكمة العدل الدولية في قضية نيكاراغوا، حيث فرقت بين الأشكال الأكثر خطراً والأقل خطرا، وتعد الأشكال الأكثر خطرا هي التي تفعل حق الدفاع الشرعي بخلاف الأشكال الأقل خطرا فلا ترتقي إلى كونها اعتداءً يفعل حق الدفاع الشرعي وفقا للمادة (٥١) من ميثاق الأمم المتحدة[٣].

الشرط الخامس: أن يكون هذا الفعل منسوباً لدولة.

يعنى هذا الشرط أن يكون هذا التصرف متصلا بدولة معينة، وهو شرط جوهري من الشروط التي تقوم بها مسؤولية الدولة، بمعنى أن يكون الفعل صادرا عن سطلة من السلطات التي تمثل الدول سواء أكانت السلطة التشريعية أم السلطة التنفيذية أم السلطة القضائية[٤].

ولكن هذا الشرط تشوبه بعض الصعوبات، أهمها: صعوبة تحديد الدولة التي صدر عنها هذا الفعل خاصة إذا كانت هذه الدولة تمتلك قدرات تكنولوجية هائلة، وتستطيع من خلالها طمس هويتها الحقيقية، ويزداد الأمر صعوبة عندما تقع هذه الجرائم بعيدا عن الشبكات الإلكترونية[٥].

كما يزداد الأمر تعقيدا عندما ينسب هذا الهجوم إلى مجموعات خارجة عن سلطات الدولة، ولكن تم تنفيذ هذا الفعل على إقليم هذه الدولة، هذا الأمر لقي نقاشا مستفيضا من لجنة الخبراء حول دليل تالين، وفى النهاية قررت اللجنة أن التحكيم الفعال هو الذي يقرر ما إذا كان الفعل ينسب الى الدولة أم لا[٦].

وأشار دليل تالين إلى حظر الهجمات السيبرانية التي من شأنها أن تسبب خسارة في الأرواح للمدنيين أو أصابات أو أضرار بالأعيان المدنية ....الخ[٧].

---

(١) د. رزق أحمد سمودي: مرجع سابق، ص ٣٥٤.

(٢) د. أميرة عبد العظيم محمد عبد الجواد: مرجع سابق، ص ٥٠٩.

(٣) د. رزق أحمد سمودي: مرجع سابق، ص ٣٥٥.

(٤) د. أميرة عبد العظيم محمد عبد الجواد: مرجع سابق، ص٥١٠.

(٥) د. رزق أحمد سمودي: مرجع سابق، ص ٣٥٦.

(٦) د. أميرة عبد العظيم محمد عبد الجواد: مرجع سابق، ص ٥١٠، ٥١١.

(٧) د. يحي ياسين سعود: مرجع سابق، ص ٩٤.

دكتور/ محمد حسن أحمد جاد

كما أقر خبراء دليل تالين أنهم قد استندوا إلى معيار الحجم والتأثير في تحديد فيما إذا كانت الهجمة السيبرانية ترقى إلى الاستخدام غير المشروع للقوة الذي يبرر حق الدفاع الشرعي استنادا إلى المادة (٥١) من عدمه[١].

ورغم ذلك هناك خلط من جانب لجنة الخبراء بين الهجمات السيبرانية وبين الاستخدام التقليدي للقوة، الأمر الذي ترتب عليه نقاش مستفيض نحو هذا النوع المستحدث من "استخدام القوة" وظهر ذلك من خلال توجه لجنة الخبراء وتأثرهم بالفكرة التقليدية لاستخدام القوة واعتبارها مكافئة للقوة العسكرية[٢].

وهناك تناقض آخر بين المعيار الذي تبنته محكمة العدل الدولية – معيار الحجم والتأثير – وبين شرط اتصال التصرف بالدولة، ومما يدل على ذلك عندما تكون هناك هجمات ذات تأثير مدمر دون أن تكون هذه الهجمات هدفها عسكريا أو يكون مصدر هذه الهجمات وزارة الدفاع[٣].

ويرى الباحث أن الجرائم السيبرانية لا تقل أهمية عن الجرائم العسكرية لما فيها من أضرار بالغة الخطورة على الدول وتمثل انتهاكا لسيادة الدولة المعتدى عليها، ويصعب اكتشافها؛ لكونها جرائم ترتكب في أي مكان في العالم، كما أنها تسبب خسائر الارواح والممتلكات أو تلحق أضرارا بالبنية التحتية؛ وبالتالي يجب أن يطبق عليها ما ينطبق على الجرائم العسكرية.

---

(١) د. أميرة عبد العظيم محمد عبد الجواد: مرجع سابق، ص ٥١٠، ٥١١.

See: Sara Pangrazzi (MLaw): op. cit., p. 7.

(٢) د. رزق أحمد سمودي: مرجع سابق، ص ٢٥٧.

(٣) المرجع السابق، ص ٣٥٧، ٣٥٨.

(ISSN: 2356 - 9492)

المبحث الثالث
النماذج العملية للهجمات السيبرانية في الوقت الراهن

قبل التحدث عن الهجمات السيبرانية في الوقت الراهن بين روسيا وأوكرانيا، ويقتضي الأمر تناول الهجمات السيبرانية التي خاضتها روسيا والولايات المتحدة الأمريكية ضد بعضهما البعض؛ لأهميتها، وسنتناول النماذج العملية في هذا المبحث من خلال المطلبين الآتيين:

المطلب الأول: الهجمات السيبرانية بين الولايات المتحدة الأمريكية وروسيا.

المطلب الثاني: الهجمات السيبرانية الروسية على أوكرانيا.

المطلب الاول
الهجمات السيبرانية بين الولايات المتحدة الأمريكية وروسيا

دارت رحى الحرب الإلكترونية بين الدول الكبرى، وظهر أمام الولايات المتحدة الأمريكية تحديات كبرى مثل: الصين وروسيا، فهناك تحدٍ روسي للنظام العالمي دار من قبل، ولم يزل موجودا الآن، "بالإضافة إلى وجود تحدٍ صيني يتمثل في إمكانية منافسة الصين للولايات المتحدة في مجال العولمة. كما أن المراجعة الحالية بها نوع من اختبار القوة؛ مما يضع العالم أمام سيناريوهات للحرب الباردة، التي عاشت مراحل للتصعيد مسبقًا[١].

نفذت الولايات المتحدة الأمريكية الكثير من الهجمات السيبرانية ضد روسيا، وكان أول هذه الهجمات موجهاً إلى منظومة التحكم العالية صناعيا لأنبوب نفط تابع للاتحاد السوفيتي سنة ١٩٨٢م والمعروف باسم "chelyabinsk"، وترتب على هذا الهجوم انفجار كبير واشتعال النيران التي حرقت منه ثلاثة كيلو متراً من هذا الانبوب نتج عنه خسائر هائلة[٢].

وتدعى الولايات المتحدة الأمريكية أنها تدافع عن نفسها، وأنها دائما تتعرض لهجمات سيبرانية من دول أخرى، وأن من حقها الدفاع عن نفسها ضد الهجمات التي تتعرض لها استنادا للمادة (٥١) من ميثاق الأمم المتحدة[٣].

وقدر مجلس المستشارين الاقتصادي حجم الخسائر الأمريكية نتيجة الهجمات السيبرانية من عام ٢٠١٦م إلى ٢٠١٨م بما يتراوح ما بين ٩٧- ١٠٩ مليار دولار الأمر الذي يترتب عليه وضع ضوابط محددة لتجريم هذه الأفعال[٤].

وزادت الهجمات على الإنترنت في ٢٠١١م بنحو ٣٦% مقارنة بـ ٢٠١٠م وكذلك زادت كمية البرامج الخبيثة بنحو ٤١ % عن نفس الفترة[٥].

---

(١) د. عبدالمنعم سعيد: تداعيات الأزمة الأوكرانية على الشرق الأوسط، مقال منشور على شبكة الإنترنت بتاريخ ٢٣ فبراير ٢٠٢٢م، https://idsc.gov.eg/DocumentLibrary/View/6742

(٢) د. أحمد عباس الفتلاوي: مرجع سابق، ص ٦٢٣.

(3) Matthew Borton, Samuel Liles, Sydney Liles: op. cit., p. 311.

(٤) د. علم الدين بانقا: مخاطر الهجمات الإلكترونية (السيبرانية) وآثارها الاقتصادية: دراسة حالة دول مجلس التعاون الخليجي، دراسات تنموية، المعهد العربي للتخطيط، الكويت، العدد ٦٣، ٢٠١٩م، ص ١٠.

(5) Mohan B. Gazula: Cyber Warfare Conflict Analysis and Case Studies, Massachusetts Institute of Technology June 2017, p. 15.

وكان لا بد من وجود رد فعل للهجمات الأمريكية، فتم توجيه الكثير من الهجمات على وزارة الدفاع الأمريكية وغيرها من الوزارات والمصالح المهمة في الدول؛ ونتج عن ذلك خسائر فادحة لدى الولايات المتحدة الأمريكية(١).

كما تم توزيع برامج خبيثة لعرقلة شبكة الكهرباء الأمريكية، واستهدفت هذه البرامج شبكات الحاسب الآلي والبنية التحتية والبنوك وغيرها من المصالح الأساسية المهمة لدى الإدارة الأمريكية(٢).

وقد راجعت الحكومات نفسها على الصعيد الوطني والدولي لحماية الإنترنت؛ وبالتالي فإن هذه الحماية أصبحت من أولويات هذه الدول، كما أن الدول المتقدمة في هذا المجال التي تمتلك قدرات تكنولوجية هائلة غيرت اتجاهاتها من الحروب العسكرية إلى الحروب والهجمات السيبرانية(٣).

وقد استعدت الولايات المتحدة الأمريكية لمواجهة هجمات محتملة على الإنترنت حتى لا تتعرض لتوقف المصالح الحيوية لدى الإدارة الأمريكية بسبب أن الحرب على الإنترنت دخلت ترسانة الحرب الحديثة؛ وبالتالي يجب الاستعداد التام لمواجهة تلك الهجمات وحماية المصالح الحيوية للولايات المتحدة الأمريكية(٤).

وقد دعمت الولايات المتحدة الأمريكية أمن الإنترنت؛ لكونه مسألة أمن قومي، وأصبح من أولويات الإدارة الأمريكية؛ بسبب تعرضها لهجمات سيبرانية عديدة ترتب عليها خسائر فادحة، وحتى لا تتعرض لهذه الهجمات مرة أخرى(٥).

ولم تكن الولايات المتحدة الأمريكية هي الهدف الوحيد لروسيا بل قامت بالكثير من الهجمات على الدول الأخرى، ففي ٢٠٠٨م هاجمت جورجيا، وضربت أجهزة الحاسب الآلي لها، ووجهت الكثير من الهجمات ضد أوكرانيا(٦).

وفى مارس ٢٠٢١م، بدأت الولايات المتحدة إستراتيجية جديدة لمواجهة التهديدات السيبرانية بقيادة الرئيس الامريكي "جو بايدن" تعكس الركائز الأيديولوجية والتكنولوجية والدبلوماسية، وأكد وزير الخارجية الأمريكي (أنتوني بلينكن) على هذه

---

(1) Charles J. Dunlap, Jr: Meeting the Challenge of Cyberterrorism: Defining the Military Role in a Democracy, Meeting the Challenge of Cyberterrorism, international Law Studies - Volume 76, , without publication year , p. 357.

(2) Lucian E. Dervan: op. cit., p. 379.

(3) Thomas C. Wingfield3, Eneken Tikk: Frameworks for International Cyber Security: The Cube, the Pyramid, and the Screen, Frameworks for International Cyber Security: The Cube, the Pyramid, and the Screen, 2017, p. 16.

(4) Mohan B. Gazula: op. cit., p. 15.

(5) Thomas C. Wingfield3, Eneken Tikk: op. cit., p. 17.

(6) Lesley Swanson: The Era of Cyber Warfare: Applying International Humanitarian Law to the 2008 Russian-Georgian Cyber Conflict, The Era of Cyber Warfare, Vol. 32:303, 2010, p. 303. See: Landon J. Wedermyer: op. cit., p.14.

(ISSN: 2356 - 9492)

الإستراتيجية الجديدة للرئيس الأمريكي، وأن الأنشطة السيبرانية المناهضة للولايات المتحدة الأمريكية تستوجب علينا أن نعيد النظر في العلاقات الديمقراطية بالفضاء السيبراني الذي هو جزء من مشروع تجديد الديمقراطية في الولايات المتحدة الأمريكية؛ لتحسين الدفاعات السيبرانية، وردع أي عمليات سيبرانية معادية للولايات وكيفية مواجهتها(١).

ولم تقتصر الهجمات السيبرانية ضد الولايات المتحدة الأمريكية على البنية التحتية وشبكة الكهرباء فقط، وإنما استهدفت القوات العسكرية أيضا، ونتج عن ذلك إصابات وخسائر في الأرواح والممتلكات(٢).

وفى يونيو ٢٠٢١م، أكد الرئيس الامريكي جو بايدن على تعزيز الأمن السيبراني من خلال قيام الولايات المتحدة بشن هجمات على الخوادم المستخدمة في الهجمات السيبرانية ضد الولايات المتحدة الأمريكية، كما أنها ستسعى بكل قوة لحماية بنيتها التحتية وأمنها القومي ضد أية هجمات سيبرانية(٣).

وفى المقابل تعرضت روسيا لهجمات سيبرانية من قبل الولايات المتحدة، ففي ٢٠١٨م تم توجيه هجمات سيبرانية إلى شبكة الكهرباء الروسية من خلال زرع برامج ضارة لتعطيل عمل هذه الشبكة(٤).

وإذا تطرقنا إلى مسألة الدفاع الشرعي تجاه هذه الهجمات، نجد أن للولايات المتحدة الأمريكية الحق في الدفاع عن نفسها ضد هذه الهجمات استنادا لنص المادة (٥١) من ميثاق الأمم المتحدة(٥).

ويري الباحث أن كل هذه الهجمات السيبرانية لا تقل خطورة في حجمها الكبير وآثارها المدمرة عن الجرائم العسكرية خاصة إذا كانت هذه الهجمات موجهة ضد الأشخاص المدنيين كالعاملين بالمطارات وشركات الكهرباء والبنوك وغيرها مما يترتب عليها ضحايا في الأرواح وخسائر مادية، ويمكن القول بأنها أحياناً تتعدى في أضرارها وخسائرها المادية والبشرية الجرائم العسكرية، لأن الجرائم السيبرانية لا توجه إلى الأهداف العسكرية فحسب بل تشمل أهدافا غير عسكري كالمواطنين الآمنين، بعكس الجرائم العسكرية التي تستهدف جوانب عسكرية؛ من أجل ذلك يحق للدول التي تتعرض للهجمات السيبرانية أن تدافع عن نفسها طبقا لميثاق الأمم المتحدة.

---

(1) أ.م.د. كرار عباس متعب فرج: الحرب السيبرانية: دراسة في استراتيجية الهجمات السيبرانية بين الولايات المتحدة الأمريكية وإيران، مجلة حمورابي للدراسات، العدد ٤٠ – السنة العاشرة، ٢٠٢١م، ص ٢٠٧.

(2) James Andrew Lewis: Aux Armes, Citoyens: Cyber Security and Regulation in the United States (pre-print version of article published in Elsevier's Telecommunications Policy, Fall 2005, p. 8. see: Robert K. Knake : A Cyberattack on the U.S. Power Grid, Coucil on foreign relation , Copyright 2017 by the Council on Foreign Relations® Inc. All rights reserved , April 2017 , p. 6.

(3) أ.م.د. كرار عباس متعب فرج: مرجع سابق، ص ٢٠٨.

(٤) أ. صلاح حيدر عبدالواحد: مرجع سابق، ص ٣١.

(5) Charles J. Dunlap, Jr: op. cit., p. 356. See: Anna C. Mourlam: op. cit., p. 19.

المطلب الثاني

الهجمات السيبرانية الروسية على أوكرانيا

تعد روسيا من أكثر دول العالم نشاطا في القرصنة الإلكترونية، ولها قدرات سيبرانية هائلة، وقد وجهت الكثير من الهجمات السيبرانية ضد أوكرانيا، ومن ذلك: هجوم البرمجيات الخبيثة "نوتبيتيا" الذي تسبب في أضرار اقتصادية تقدر بنحو عشرة مليارات دولار، وكذلك توجيه الكثير من الهجمات الروسية الأخرى ضدها(١).

وتتواصل الحرب السيبرانية بين روسيا وأوكرانيا في هذا المجال، والتي أصبحت تشكل أدوات وأسلحة، وقد سببت هذه الهجمات أضرارا بالغة لديهما، ومع تواصل الحرب بين الطرفين اخترقت روسيا بعض المواقع الحكومية والبرلمان، وكذلك المصارف الكبيرة في أوكرانيا بعد أن شنت عليها سلسلة من الهجمات الإلكترونية على نطاق واسع(٢).

ومن أشهر البرامج الخبيثة التي أطلقتها روسيا قبيل ساعات من بدأ الحرب والتي لم يسبق لها مثيل: برامج تعرف باسم "Box Bade" واستهدفت هذه البرامج الوزارات الحكومية الأكرانية والمؤسسات المالية داخل أوكرانيا، وتعمل هذه البرامج على مسح البيانات لدى الكثير من أجهزة الكمبيوتر داخل أوكرانيا(٣).

وقد استخدمت روسيا تلك القوة للسيطرة على الأنظمة العسكرية، وسرقة المعلومات والبيانات العسكرية، وكذا إتلاف المعلومات أو تعديلها والتحكم والسيطرة عليها عن بعد(٤).

ومن أبرز الهجمات السيبرانية التي وقعت خلال الفترة الاخيرة ما قامت به روسيا من هجمات سيبرانية حول شبه جزيرة القرم والمناطق الشرقية من البلاد، وقد استهدفت هذه الهجمات البنوك والوزارات الاوكرانية وشركات الكهرباء وغيرها من المصالح الحيوية، وتم استخدام برامج خبيثة من نوع بيتا(٥).

---

(١) أ. د. نورهان الشيخ: مرجع سابق، ص ٦٢.

(2) Jason Healey: op. cit., p. 2.

انظر: د. أيمن سلامة: السيبرانية: جديد الحرب الباردة بين روسيا وأكرانيا، مقال منشور ١٩ ديسمبر ٢٠١٩م، https://www.skynewsarabia.com/blog/

(٣) انظر: تقرير: «مايكروسوفت» دخلت على خط الحرب بين روسيا وأوكرانيا قبل اندلاعها، نيويورك الشرق الأوسط، الثلاثاء ١ مارس ٢٠٢٢م، ص ١- ٢،

https://aawsat.com/home/article

(٤) د. أماني عصام محمد: استخدام روسيا للقوة السيبرانية في إدارة تفاعلاتها الدولية، دراسات: المجلد ٢٢، العدد ٤ أكتوبر ٢٠٢١م، ص ١٧٢.

(5) Lucian E. Dervan: op. cit., p. 378.

انظر: أ. صلاح حيدر عبدالواحد: مرجع سابق، ص ٢٩.

(ISSN: 2356 - 9492)

وفى ٦ مارس ٢٠١٤م بدأت روسيا عمليات عسكرية على شبه جزيرة القرم، ولم تكتفي روسيا بالهجمات السيبرانية فحسب، بل سيطرت على هذه المدينة في فترة وجيزة، ربما كان السبب في تأييد سكان القرم الانضمام لروسيا، لأمرين: الأول: تحسين الحالة المعيشية للقرم، والثاني: عدم الدخول في حروب عسكرية مؤلمة موجعة مع إيمانهم بقوة بوتين العسكرية(١).

وفي ٢٤ فبراير/شباط ٢٠٢٢، بدأت روسيا غزوا عسكريا واسعا لأوكرانيا، وشنت هجمات تسببت في مقتل وإصابة مدنيين، وألحقت أضرارا بالمباني المدنية، بما فيها المستشفيات، والمدارس، والمنازل. وقعت هجمات عشوائية تنتهك قوانين الحرب، وقد ترقى إلى جرائم الحرب. بحلول نهاية الأسبوع الأول من الأعمال العدائية، كان قد فر أكثر من مليون شخص في أوكرانيا من منازلهم، ولجأ الكثير منهم إلى خارج أوكرانيا(٢).

ولم تكن الحرب الروسية على أوكرانيا متوقفا على الجانب العسكري فقط، بل تعدت بصفة خاصة إلى الهجمات السيبرانية، شهدت الآونة الأخيرة حربا سيبرانية قوية بين روسيا وأوكرانيا، ففي خضم الحرب العسكرية بين البلدين، فقد أكدت شبكة BBC أن" روسيا قامت بهجوم إلكتروني شامل يستهدف مؤسسات وسفارات أوكرانيا، وكانت وزارتا الخارجية والتعليم، وكذلك السفارات في كل من المملكة المتحدة، والولايات المتحدة، والسويد، من بين المؤسسات الأوكرانية التي استهدفها الهجوم الإلكتروني، والتي زاد عددها على عشر مؤسسات. وقبل أن تسقط المواقع الإلكترونية، كانت تظهر عليها رسالة تحذيرية للأوكرانيين تقول: "انتظروا الأسوأ". ولم يتضح بعد مَن يقف وراء الهجوم، لكن متحدثا قال: إن هجمات إلكترونية سابقة كانت قد أتت من روسيا(٣).

ولم تقف حكومة أوكرانيا مكتوفة الأيدي أمام هذه الهجمات السيبرانية الروسية، فقد" أنشأت الجيش السيبراني الأوكراني على يدِ ميخايلو فيدوروف، النائب الأول لرئيس الوزراء ووزير التحوّل الرقمي، في ٢٥ فبراير ٢٠٢٢ وذلك تزامنًا مع الغزو الروسي لأوكرانيا، الهدف الأساس لهذا الجيش السيبراني بحسبِ ميخايلو هو: المساهمة وبقوّة في الحرب السيبرانيّة ضد روسيا، طلب فيدوروف المساعدة من خبراء التقنيّة من مختلف بقاعِ العالم، ثمّ نشرَ على حسابٍ رسمي في تيلي جرام قائمةً ضمَّت ٣١ موقعًا إلكترونيًا لمنظمات الأعمال والدولة الروسية من أجلِ استهدافها(٤).

تطورت الحرب العسكرية بين البلدين حاليا خاصة بعد تدخل أمريكا وإمدادها أوكرانيا ببطارية صواريخ باتريوت، فقد أكدت الأخبار الحالية أنه قد تعهد بايدن بتعزيز الدفاع الجوي الأوكراني، وقال: "لهذا السبب سنزود أوكرانيا ببطارية صواريخ باتريوت وندرب قواتك لتكون قادرة على استخدامها بدقة" (٥).

---

(١) مايكل كوفمان وآخرين: عبر من عمليات روسيا في شبه جزيرة القرم وشرق أوكرانيا، مؤسسة RAND، سانتا مونيكا، كاليفورنيا، ٢٠١٧، ص ١٠.

(٢) الحرب الروسية الاوكرانية: مقال منشور على شبكة الإنترنت، دون ناشر،

https://www.hrw.org/ar/tag/russia-ukraine-war

(3) مقال منشور على ويكيبيديا، (

https://m5.gs/a09CNn

(4) Pearson, James (27,February, 2022) "Ukraine launches 'IT army,' takes aim at Russian cyberspace. Reuters . Archived from the original on: 2022-03-01.

(5) مقال منشور على ويكيبيديا،)

دكتور/ محمد حسن أحمد جاد

وهذا ما أثار حفيظة الرئيس الروسي فلاديمير بوتين، وتأكد لديه أن الولايات المتحدة الأمريكية لن تدع أوكرانيا تعيش الحرب وحدها، وفي نفس اليوم أكد الرئيس الروسي فلاديمير بوتين، أن بلاده ستحافظ على استعدادها القتالي، وستعمل على تحسين "الثالوث النووي"، باعتباره الضمان الرئيسي لسيادة روسيا، وينذر إعلان بوتين عن أهداف الجيش في الفترة المقبلة مع اقتراب دخول العملية العسكرية بأوكرانيا عامها الأول، بانتقال الصراع إلى مربع أكثر تصعيدا في ٢٠٢٣، حسب خبراء تحدثوا لموقع "سكاي نيوز عربية"[١].

ومع تطور الحرب العسكرية بهذه الصورة السريعة والمدمرة، يتوقع الباحث أن الحرب السيبرانية ستكون قوية وأكثر ضراوة عما بدأت به، وذلك لأنها أشد تدميراً وفتكا بالمصالح الحكومية والعناصر البشرية، وشأنها في ذلك شأن سلاح النووي الذي أعلن بوتين عن تطويره، وتشير الأخبار الحالية بأن الحرب السيبرانية ستكون أشد قوة وضراوة بين روسيا من جهة وأمريكا وأوكرانيا من جهة أخرى، وأن الحرب الروسية السيبرانية تزامنت جنبا إلى جنب مع الحرب العسكرية على أوكرانيا، بل ربما سبقتها لتعطيل المصالح الحكومية، ثم تدميرها، وهذا مما دفع أوكرانيا إلى إنشاء الجيش السيبراني الأوكراني؛ وذلك لأمرين: الأول حماية مصالح الدولة الإلكترونية وبنتيها التحتية من هجمات روسيا، والثاني: الهجوم الأوكراني السيبرانيّة على روسيا، لتعطيل وتدمير أجهزة الإدارة الروسية.

---

https://m5.gs/a09CNn

(١) جريدة SKY NEWS العربية، الأربعاء ٢٠٢٢/١٢/٢٢م، عنوان: (روسيا تستعد لعام ٢٠٢٣ بالثالوث النووي. وزيادة عدد القوات)، https://2u.pw/FrODsa

(ISSN: 2356 - 9492)

الخاتمة

تعد دراسة الهجمات السيبرانية ضرورة ملحة؛ نظرا لما تقوم به الدول من الاستخدام السلبي للتقدم التكنولوجي، وقد تشكل الهجمات السيبرانية تهديدا للخدمات الأساسية في الدولة والبنية التحتية وتعطيل استخدام الدولة للآليات الإلكترونية بل قد يصل الأمر الى تدمير الأجهزة الإلكترونية الخاصة بالأمن القومي للدولة برغم الإجراءات الدفاعية لمواجهته باعتباره من الجرائم العابرة للحدود والتي ظهرت في الآونة الأخيرة مع الانتشار التكنولوجي الرهيب والتي يصعب على الدولة المعتدى عليها التصدي له.

وتثير هذه الهجمات في مجملها الكثير من الإشكالات من مختلف الجوانب كصعوبة اكتشافها أو الحيلة والدهاء من طرف مرتكبيها وذلك من خلال استعمال تقنيات معلوماتية ذو كفاءة عالية، مما يؤدي إلى اختراق هذه الشبكات، أو أجهزة الحاسب الآلي المرتبطة بالإنترنت، ويتم ذلك من خلال اختراق نظام الأمن الخاص بحماية الشبكة والدخول إلى الجهاز للكشف عن المعلومات، أو إتلافها, أو التلاعب بها.

وقد قامت بعض الدول بالعديد من الهجمات السيبرانية مستغلين عدم وجود تنظيم دول يحكمها معتبرين أن قواعد القانون الدولي الإنساني قواعد قديمة ومر عليها زمن وبالتالي لا تنطبق على الهجمات السيبرانية ووجدنا العديد من الهجمات التي قامت بها الدول ضد دول أخرى وهذا ما تم ذكره سابقا.

وبالرغم من ذلك فقد وجدنا جهود دولية ومحاولات عديدة لتنظيم هذه الهجمات حتى وأن كانت هذه الجهود بطيئة بسب تعطيل بعض الدول المتقدمة في المجال التكنولوجي والذي يعتبر التقدم في هذا المجال أداة قوية ووسيلة فعالة لضرب الدول الأعداء الا أن ذلك يدل على وعي المجتمع الدولي بخطورتها ومن أهم ما تم التوصل الية هو خضوع الهجمات السيبرانية التي تحدث في سياق النزاع المسلح ضمن قواعد القانون الدولي الإنساني.

ورغم ذلك تثير الهجمات السيبرانية التي تحدث خارج سياق النزاع المسلح الكثير من الأسئلة حول مدى إمكانية إلحاق هذا الهجمات لجهة معينة، ويعد نزاعاً مسلحاً، وبالتالي يمكن تطبيق القانون الدولي الإنساني عليها يواجه الكثير من الصعوبات، وهذا الأمر لا يزال بحاجة إلى دراسة حثيثة من قبل الخبراء المختصين في القانون.

النتائج :

١. يعد مفهوم الهجمات السيبرانية من المفاهيم الحديثة غير محدد المعالم دوليا، ويختلف عن مفهوم الجريمة السيبرانية، فالهجمات السيبرانية أهدفها سياسية تظهر عليه علامات سياسة الدولة، بخلاف الجريمة السيبرانية، فإنها تهدف الى أشياء مادية، وهي جرائم تتطور بسرعة فائقة من خلال استخدام واستحداث برمجيات وفايروسات خبيثة وهي جرائم أيضاً عابرة للحدود.
٢. يعد الهجوم السيبراني استخداما لقوة الدولة ضد أخرى، ويمكن أن يكون هذا الهجوم أكثر تدميرا وخطرا، ولذلك فهو يرتقي إلى مستوي الهجوم التقليدي، وجاءت الفقرة الرابعة من المادة (٢) من ميثاق الأمم المتحدة مرنة بالشكل الكافي؛ لاستيعاب الهجوم السيبراني، وجعله صورة من صور استخدام القوة بسبب الآثار المتشابهة مع القوة العسكرية التقليدية.

٣. عدم وجود تنظيم دولي دقيق يحكم الهجمات السيبرانية؛ وذلك لعدة أسباب أهمها: رغبة بعض الدول في البقاء على هذا الوضع الحالي من حالة الغموض الإلكتروني لإلحاق الضرر بدول أخرى من خلال تنفيذ هذه الهجمات، وجود القدرة التكنولوجية الهائلة التي تمكن الدول التي ترتكب هذه الهجمات من إخفاء الجهة والهوية التي أصدرت الهجوم أكثر من أي وقت في الماضي.

٤. هناك إجماع من الفقهاء الدوليين على خضوع الهجمات السيبرانية التي تقع في سياق النزاع المسلح الحركي لقواعد القانون الدولي الإنساني، ولكن التحدي الأكبر عندما تقع الهجمات خارج سياق النزاع المسلح الحركي، ومدى إمكانية وجود نزاع مسلح ينسب لدولة معينة ينطبق عليها القانون الدولي الإنساني من عدمه.

٥. على الرغم من عدم وجود تنظيم دولي دقيق توجد علاقة بين قواعد القانون الدولي العام الخاصة باستخدام القوة والدفاع عن النفس وبين الهجمات الإلكترونية كظاهرة متطورة في العلاقات الدولية؛ وذلك لأن الدول التي تقع عليها الهجمات السيبرانية تمتلك حق الدفاع عن النفس استنادا لنص المادة (٥١) من ميثاق الأمم المتحدة.

٦. ورد عن فقه محكمة العدل الدولية في قضية "النشاطات العسكرية وشبه العسكرية في وضد نيكاراغوا ١٩٨٦م"، وقضية "منصات النفط بين إيران والولايات المتحدة ٢٠٠٣م" من ضم فئات أخرى غير الهجوم الحركي، وهذا ما يؤيد انطباق حالة الدفاع الشرعي الواردة في المادة (٥١) على الهجمات السيبرانية بشروط أهمها شرطي الحجم والتأثير " Effect and Scale".

٧. برغم الاختلاف التفصيلي بين فقه محكمة العدل الدولية وبين مجموعة الخبراء لدليل تالين نجد أن هنالك اتفاقاً مشتركاً بينهم يتلخص في الحجم والتأثير كمعيارين يستند إليهما في تفعيل حق الدفاع عن النفس وفقا المادة ٥١ من ميثاق الأمم المتحدة.

٨. بذلت جهود دولية لتنظيم الأنشطة السيبرانية كاتفاقية بودابست ودليل تالين وبعض القرارات الصادرة عن الأمم المتحدة، وإن كان هناك بعض القوانين السابقة على ظهور الهجمات السيبرانية إلا إنها لم تصل إلى مستوى التنظيم الشامل لهذه الهجمات.

التوصيات

١. السعي إلى اعتماد اتفاقية دولية تنظيم الهجمات السيبرانية وإن كان هذا الأمر فيه الكثير من الصعوبة بسبب عزوف بعض الدول عن الانضمام إلى مثل هذه الاتفاقية؛ بسبب تعارضه مع بعض الدول الكبرى والمتقدمة في هذا المجال، ولكونه سلاحاً في أيدي هذه الدول لضرب الدول الأعداء.

(ISSN: 2356 - 9492)

٢. يجب أن يكون للمجتمع الدولي دور مهم في رفع الوعي بخطورة الاستخدامات غير المشروعة للتكنولوجيا، وتأثيرها على الصحة العامة والاقتصاد والأمن العالمي والتي يمكن أن تلحق أضرارا بالأشخاص أو بالبنية التحتية أو تعرض حياة المدنيين للخطر.

٣. يجب على المجتمع الدولي أن يعي خطورة هذه الهجمات، وأن يصدر بروتوكولاً إضافياً رابعاً يكون ملحقا باتفاقيات جنيف الرابعة لعام 1949م لتنظيم الهجمات السيبرانية وتجريم هذه الهجمات التي تكون خارج نطاق التنظيم الدولي.

٤. تفعيل الحوار والتنسيق وتبادل المعلومات بين الدول والمنظمات الدولية والإقليمية في مكافحة إساءة استخدام تكنولوجيا المعلومات والاتصالات، والعمل على تحديث أنظمة الحماية لتتضمن متطلبات الأمن السيبراني.

٥. يجب على الدول المتقدمة والدول العظمى أن تستخدم التطور التكنولوجي في مجال الثورة المعلوماتية بما يخدم هذه الدول بصفة عامة، والبشرية بصفة خاصة، بدلا من أن تستخدمها في الصراعات والحروب والانتقام من الدول الأعداء.

٦. يجب على الدول غير المتقدمة في المجال التكنولوجي وكذا الدول النامية أن تستفيد مما يحدث في الكثير من دول العالم من هجمات سيبرانية ترتب عليها اعتداء على البينة التحتية والمصالح المهمة والأساسية في هذه الدول.

٧. ضرورة تعديل ميثاق الأمم المتحدة ليشمل حظر الهجمات السيبرانية بشكل واضح وصريح بين الدول؛ لأنها أصبحت تمثل انتهاكاً سافراً لحقوق الانسان، وتعرض حياة الأشخاص للخطر أو تلحق أضراراً بهم أو تهدد الأمن والسلم الدوليين.

٨. يعد إخفاء الهوية في الفضاء السيبراني تحديا كبيراً يترتب عليه صعوبة في كشف مواقع الاتصال والتواصل أو التضليل بشأنه الأمر الذي يستوجب إنشاء إستراتيجية دولية لإنشاء نظام رقمي للحد من هذه الظاهرة، كما يجب إبعاد البنية التحتية والشبكات السيبرانية العسكرية عن المدينة لحماية السكان المدنيين وعدم تعرضهم للهجمات السيبرانية.

حق الدفاع الشرعي في مواجهة الهجمات السيبرانية
في ضوء ميثاق الأمم المتحدة

دكتور/ محمد حسن أحمد جاد

مجلة الدراسات القانونية والاقتصادية

(ISSN: 2356 - 9492)

قائمة المراجع

أولاً: - مراجع باللغة العربية:

أ-الكتب:

- مايكل كوفمان وآخرون: عبر من عمليات روسيا في شبه جزيرة القرم وشرق أوكرانيا، مؤسسة RAND، سانتا مونيكا،كاليفورنيا، ٢٠١٧م .
- أ . بشرى عواطة: حجية الدليل الالكتروني في الإثبات الجنائي، دار الجامعة، الجزائر، ٢٠١٧ م.
- د. جيمس كرو فورد: المواد المتعلقة بمسؤولية الدول عن الأفعال غير المشروعة دوليا، مركز لاوترباخت لبحوث القانون الدولي – جامعة كمبردج، ٢٠١٧.
- د. شريف نسيم قتلة: دليل "تالين" الهجمات الإلكترونية وخطر استخدام القوة في القانون الدولي، المركز العربي للأبحاث الفضاء الإلكتروني، مصر، ٢٠١٧م.
- أ . محمد أمين الشوابكة: جرائم الحاسوب والإنترنت (الجريمة المعلوماتية) – دار الثقافة للنشر والتوزيع، عمان، الأردن ٢٠٠٩م.
- د. محمد حسن أحمد جاد: سلطة المحكمة الجنائية الدولية على الدول غير الأعضاء، دار النهضة العربية، مصر، ٢٠١٨م.

ب- الرسائل العلمية:

- د. أبوبكر المبروك بشير أبو عجيلة: أثر أحداث الحادي عشر من سبتمبر في السياسة الخارجية للولايات المتحدة الأمريكية تجاه منطقة الشرق الأوسط (٢٠٠١ –٢٠٠٨) بحث مقدم إلى جامعة الخرطوم لنيل درجة الدكتوراه في العلوم السياسية (غير منشورة)، ٢٠١٠م.
- د. بو دربالة صلاح الدين: استخدام القوة المسلحة في إطار أحكام ميثاق الأمم المتحدة، رسالة دكتوراه (غير منشورة)، جامعة الجزائر، كلية الحقوق، ٢٠١٠م.
- د. محمد حسن أحمد جاد: مدى تأثير قرارات المحكمة الجنائية الدولية على الدول غير الأعضاء، رسالة دكتوراه (غير منشورة) جامعة أسيوط، كلية الحقوق، ٢٠١٦م.
- أ. نور أمير الموصلي: الهجمات السيبرانية في ضوء القانون الدولي الإنساني، رسالة ماجستير (غير منشورة) الجامعة الافتراضية السورية، قانون دولي انساني، ٢٠٢١م.
- د. يوبي عبدالقادر: علاقة مجلس الأمن بالمحكمة الجنائية الدولية، رسالة دكتوراه (غير مشورة) كلية الحقوق، جامعة وهران، الجزائر، ٢٠١١، ٢٠١٢م.

ج- المقالات والدوريات

- د. إبراهيم رمضان عطا: الجريمة الإلكترونية وسبل مواجهتها في الشريعة الإسلامية والأنظمة الدولية دراسة تحليلية تطبيقية، العدد الثلاثون، الجزء الثاني، ٢٠١٥م .

حق الدفاع الشرعي في مواجهة الهجمات السيبرانية في ضوء ميثاق الأمم المتحدة

دكتور/ محمد حسن أحمد جاد

مجلة الدراسات القانونية والاقتصادية

- اللواء/ أحمد بن على الميموني: الجبهـة النِشطـة: تداعيات المواجهة السيبرانية بين إيران وإسرائيل، مجلة الدراسات الإيرانية، السنة الرابعة – العدد الثاني عشر – أكتوبر ٢٠٢٠م.
- د. أحمد عباس الفتلاوي: الهجمات السيبرانية : مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر، مجلة المحقق الحلي للعلوم القانونية والسياسية، العدد ٤ السنة الثامنة ٢٠١٦م.
- د. أماني عصام محمد: استخدام روسيا للقوة السيبرانية في إدارة تفاعلاتها الدولية، دراسات: المجلد ٢٢، العدد ٤ أكتوبر ٢٠٢١م.
- د. أميرة عبد العظيم محمد عبد الجواد: المخاطر السيبرانية وسبل مواجهتها في القانون الدولي العام، مجلة الشريعة والقانون، العدد ٥٣، الجزء ٣، ٢٠٢٠م .
- د. إيهاب خليفة: ما هو موقف ميثاق الامم المتحدة من استخدام القوة السيبرانية في التفاعلات الدولية – مقال صادر عن مركز المستقبل للأبحاث والدراسات المتقدمة – أبوظبي – الإمارات العربية المتحدة، ٢٠١٩م.
- الرائد/ حسن فياض: الهجمات السيبرانية من منظور القانون الدولي الإنساني، مجلة الدفاع الوطني، لبنان، العدد ١٤ ، ٢٠٢٠م.
- د. رزق أحمد سمودي: حق الدفاع عن النفس نتيجة الهجمات الإلكترونية في ضوء قواعد القانون الدولي العام، بحث منشور في مجلة جامعة الشارقة لعلوم القانونية، المجلد ١٥، العدد ٢، ٢٠١٨م.
- د. رغدة البهي: الردع السيبراني: المفهوم والإشكاليات والمتطلبات، مجلة العلوم السياسية والقانون، إحدى إصدارات المركز الديمقراطي العربي، العدد الأول، ٢٠١٧م.
- روان بنت عطية الله الصحفي: الجرائم السيبرانية، المجلة الإلكترونية الشاملة متعددة التخصصات، العدد ٢٤، ٢٠٢٠م.
- د. سلافة طارق الشالان: تكييف استخدام الحرب الإلكترونية في النزاعات المسلحة وفقا للقانون الدولي الإنساني، مجلة الكوفة للعلوم القانونية والسياسية، العدد ٢٦، ٢٠١٦م.
- د. طلال ياسين العيسى ، عدي محمد غياب: المسؤولية الدولية الناشئة عن الهجمات السيبرانية في ضوء القانون الدولي المعاصر، مجلة الزرقاء للبحوث والدراسات الإنسانية، الأردن، المجلد التاسع عشر، العدد ١، ٢٠١٩م.
- د. علم الدين بانقا: مخاطر الهجمات الإلكترونية (السيبرانية) وآثارها الاقتصادية: دراسة حالة دول مجلس التعاون الخليجي، دراسات تنموية، المعهد العربي للتخطيط، الكويت، العدد ٦٣، ٢٠١٩م.
- م.م. علي عبدالرحيم العبودي: هاجس الحروب السيبرانية وتداعياتها على الأمن والسلم الدوليين، المجلة العلمية الأكاديمية العراقية، كلية العلوم السياسية، جامعة بغداد، العدد ٥٧، ٢٠١٩م.

(ISSN: 2356 - 9492)

- د. علي فاضل على سليمان: حق الدفاع الشرعي اتجاه الهجمات السيبرانية، مجلة جامعة تكريت للحقوق، السنة (٤) المجلد (٤) العدد (٤) الجزء (١)، ٢٠٢٠م.
- د. فليج غزلان: التدخل العسكري المعاصر بين القانون الدولي والممارسة الدولية – العدوان المقنع– مجلة العلوم القانونية والاجتماعية جامعة زيان عاشور بالجلفة. الجزائر، المجلد الرابع، العدد الثالث، سبتمبر ٢٠١٩م.
- أ.م.د. كرار عباس متعب فرج: الحرب السيبرانية: دراسة في إستراتيجية الهجمات السيبرانية بين الولايات المتحدة الأمريكية وإيران، مجلة حمورابي للدراسات، العدد ٤٠ – السنة العاشرة ٢٠٢١م.
- أ. د. نورهان الشيخ: الإرهاب السيبراني ومستقبل العالقات الأمريكية الروسية، آفاق إستراتيجية – العدد (٤) أكتوبر، ٢٠٢١م.
- د. يحي ياسين سعود: الحرب السيبرانية في ضوء قواعد القانون الدولي الإنساني، بحث منشور في المجلة القانونية بكلية الحقوق، جامعة القاهرة، المقالة ٣، المجلد ٤، العدد ٤، 2018م.
- هربرت لين: النزاع السيبراني والقانون الدولي الإنساني، مختارات من المجلة الدولية للصليب الأحمر المجلد ٩٤ (٨٨٦)، ٢٠١٢م.

د-الوثائق والقرارات:

- تقرير: «مايكروسوفت» دخلت على خط الحرب بين روسيا وأوكرانيا قبل اندلاعها، نيويورك الشرق الأوسط، الثلاثاء ١ مارس ٢٠٢٢م، ص ١- ٢،

https://aawsat.com/home/article

- فيرونيك كريستوري: الحرب السيبرانية: القانون الدولي الإنساني يوفر طبقة إضافية من الحماية، بيان ألقته السيدة "فيرونيك كريستوري"، كبيرة مستشاري الحد من التسلح في اللجنة الدولية أمام "الفريق العامل المفتوح العضوية المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي" – نيويورك، ١٠ سبتمبر ٢٠١٩م، https://www.icrc.org/ar/document/cyber-warfare-ihl-provides-additional-layer-protection
- I C R C : القانون الدولي الإنساني والعمليات السيبرانية خلال النزاعات المسلحة ورقة موقف اللجنة الدولية للصليب الأحمر، مقدمة إلى فريق العمل المفتوح العضوية المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي، وإلى فريق الخبراء الحكوميين المعني بالارتقاء بسلوك الدول المسؤول في ميدان الفضاء السيبراني في سياق الأمن الدولي، ٢٠١٩م، https://www.icrc.org/ar/document/
- جريدة NEWS BBC عربي، خبر: هجوم إلكتروني شامل يستهدف مؤسسات وسفارات أوكرانيا ورسالة مصاحبة تقول "انتظروا الأسوأ، بتاريخ: 14يناير ٢٠٢٢م،

https://www.bbc.com/arabic/world-59994442

- جريدة SKY NEWS العربية، الأربعاء ٢٠٢٢/١٢/٢٢م، خبر:(زيلينسكي يقدم لبايدن "هدية" من أرض المعركة) وخبر:(روسيا تستعد لعام ٢٠٢٣ بالثالوث النووي... وزيادة عدد القوات).

ثانياً: - مراجع باللغة الأجنبية:

- Anna C. Mourlam: Unarmed attacks: cyber combatants and the right to defend, The California International Law Journal Vol. 26, No. 1, Winter, 2018.
- Charles J. Dunlap, Jr: Meeting the Challenge of Cyberterrorism: Defining the Military Role in a Democracy, Meeting the Challenge of Cyberterrorism, international Law Studies - Volume 76, , without publication year.
- Elizabeth Wilmshurst: Self-Defense Against Nonstate Actors: Reflections on the "Bethlehem Principles, American journal of international law, vol. 108, issue 2, 2017.
- Emily Crawford: Virtual Battlegrounds: Direct Participation in Cyber Warfare, I/S: A journal Of Law And Policy, Vol. 9: 1, 2013.
- Thomas C. Wingfield3, Eneken Tikk: Frameworks for International Cyber Security: The Cube, the Pyramid, and the Screen, Frameworks for International Cyber Security: The Cube, the Pyramid, and the Screen, 2017.
- James Andrew Lewis: Aux Armes, Citoyens: Cyber Security and Regulation in the United States (pre-print version of article published in Elsevier's Telecommunications Policy, fall 2005.
- Jason Healey: Cyber Warfare in the 21st Century: Threats, Challenges, and Opportunities, Healey – Testimony to HASC, 1 March 2017.
- John Richardson: stuxnet as cyberwarfare: applying the law of war to the virtual battlefield, Journal of computer & international law, volume 29 issue 1, 2011.
- Helen Wilson1 & Patrick van Esch: International Humanitarian Law: Attack of the Binary Bullet? , Journal of Politics and Law; Vol. 9, No. 4; 2016.
- Herbert S. Lin: Offensive Cyber Operations and the Use of Force, Journal of national security law & Policy, Vol. 4:63, 2010.
- Kamal Ahmad Khan: Use of Force and Human Rights under International Law, Athens Journal of Law - Volume 3, Issue 2, April, 2017.
- Laurent Gisel and other: The potential human cost of cyber operation, ICRC expert meeting 14- 16 November- Geneva, 2018.
- Landon J. Wedermyer: The Changing Face of War: The Stuxnet Virus and the Need for International Regulation of Cyber Conflict, Submitted in partial fulfillment of the requirements of the King Scholar Program Michigan State University College of Law under the direction of Professor Adam Candeub Spring, 2012.
- Lesley Swanson: The Era of Cyber Warfare: Applying International Humanitarian Law to the 2008 Russian-Georgian Cyber Conflict, the Era of Cyber Warfare, Vol. 32:303, 2010.
- Lucian E. Dervan: Information Warfare and Civilian Populations: How the Law of War Addresses a Fear of the Unknown, Vol. 3, No. 1, 2011.

(ISSN: 2356 - 9492)

- Matthew Borton, Samuel Liles, Sydney Liles: Cyberwar Policy, 27 J. Marshall J. Computer & Info. L. 303 (2010), Journal of Computer & information, Vol. xxvii, 2010.
- Matthew C. Waxman: Self-Defensive Force against Cyber Attacks: Legal, Strategic and Political Dimensions, Vol. 89, 2013.
- Mohan B. Gazula: Cyber Warfare Conflict Analysis and Case Studies, Massachusetts Institute of Technology June 2017.
- Pearson, James (27, February, 2022) "Ukraine launches 'IT army,' takes aim at Russian cyberspace. Reuters. Archived from the original on: 03-2022.
- Robert K. Knake: A Cyberattack on the U.S. Power Grid, Coucil on foreign relation, Copyright 2017 by the Council on Foreign Relations® Inc. All rights reserved, April 2017.
- Sara Pangrazzi (MLaw): self-defense against cyberattacks? Digital and kinetic defense in light of article 51-charter, ICT4Peace Publishing, Geneva. February 2021.