" الحرب السيبرانية في ضوء أحكام القانون الدولي العام "

Cyber war in light of the provisions of public international law

د. نورية الساعدي المقريف

محاضر بكلية القانون / جامعة بنغازي

nouriaalsaade@yahoo.com

الملخص

تطورت أساليب الحروب وأدواتها عبر التاريخ تطوراً كبيراً، وواكب هذا تطور مماثل للقواعد القانونية الدولية التي وضعتها الدول لمنع اندلاع الحروب والنزاعات، ولقد مكّن التقدم العلمي والتكنولوجي الهائل، الذي تحقق من تطوير القدرات الحربية والعسكرية على نحو سمح باستحداث أساليب ، وفضاءات جديدة يشكل الاستخدام العسكري للفضاء السيبراني نموذجاً لها.

وأصبح استخدام العمليات السيبرانية أثناء النزاع المسلح من سمات الكثير من النزاعات المعاصرة، وهو ما يدعو إلى ضرورة تطويع قواعد القانون الدولي لتتناسب مع الظروف الدولية المعاصرة ، وتتمكن من شمول المفاهيم المستحدثة والوسائل المتطورة للحروب .

الكلمات الدالة :الحرب السيبرانية. ضبط العمليات الحربية. آليات تعزيز قدرات الدول للوقاية وردع التهديدات السيبرانية .

Summary

The methods and tools of war have developed greatly throughout history, and this has coincided with a development similar to the international legal rules established by states to prevent the outbreak of wars and conflicts. Cyber is an example.

The use of cyber operations during armed conflict has become a feature of many contemporary conflicts, which calls for the necessity of adapting the rules of international law to suit contemporary international circumstances, and to be able to include innovative concepts and advanced means of war.

Keywords: cyber warfare. Regulating military operations. Mechanisms to enhance the capabilities of countries to prevent and deter cyber threats.

المقدمة

تطورت أساليب الحروب وأدواتها عبر التاريخ تطوراً كبيراً، وواكب هذا التطور والتنوع تطور مماثل للقواعد القانونية الدولية التي وضعتها الدول لمنع اندلاع الحروب، والنزاعات فيما بينها، تفادياً للكثير من آثارها الوخيمة على البشرية إذا ما عجزت عن منع وقوعها.

فلقد انتهت واستقرت قواعد القانون الدولي منذ فترة طويلة إلى تحريم وتجريم لجوء الدول إلى شن الحروب، وألزمتها باتباع النهج السلمي لحل ما يثور بينها من نزاعات، وحتى في الأحوال التي أجازت فيها أحكام القانون الدولي استخدام القوة ، ضبطت نصوصه ذلك ، ببيان مبررات هذا الاستخدام وحدوده . وتمكنت أيضاً عند وقوع الصراعات المسلحة من وضع أطر

تحكمها وتكفل قدراً من الحماية الإنسانية لضحاياها، وهو ما تضمنه فرع القانون الدولي المسمى بالقانون الدولي الإنساني.

ولقد مكّن التطور العلمي والتكنولوجي الهائل، من تطوير القدرات الحربية والعسكرية على نحو سمح باستحداث أساليب، وفضاءات جديدة تشن من خلالها أنواع غير تقليدية للحروب، يشكل الاستخدام العسكري للفضاء السيبراني نموذجاً لها.

وأصبح استخدام العمليات السيبرانية أثناء النزاع المسلح من سمات الكثير من النزاعات المعاصرة، التي تعتمد في جزء من استراتيجيتها على هذه العمليات، وهو ما يدعو إلى ضرورة أن تطوع قواعد القانون الدولي لتتناسب مع الظروف الدولية المعاصرة، وتتمكن من شمول المفاهيم المستحدثة والوسائل المتطورة للحروب.

أهمية الدراسة:

رغم الاتفاق على نبذ فكرة الحرب إلا أن واقع المجتمع الدولي يشهد الكثير من النزاعات المسلحة، ونظراً لتطور العمليات العسكرية ومغايرته لما نظمته القواعد الأساسية للقانون الدولي، وجب العمل على تطوير قواعد القانون الدولي لتتواءم مع الظروف الدولية المعاصرة وصولاً للهدف الأسمى وهو تحقيق الحماية الإنسانية.

إشكالية الدراسة:

يثير شن الدول لهجمات سيبرانية العديد من التساؤلات حول التكييف القانوني لهذه الهجمات في ضوء قواعد القانون الدولي ، وهذه التساؤلات كثيرة جداً غير أن هذه الدراسة

ستحاول بحث بعض منها ، لعل أهمها يقتضي بيان مدلول هذه الهجمات ، ومدى اعتبار لجوء الدول لها استخدام للقوة بالمخالفة للحظر العام لاستخدامها الراسخ كمبدأ أساسي من مبادئ القانون الدولي لا يجوز الخروج عنه إلا في أحوال استثنائية محددة ، ثم البحث عن إمكانية إجبار الدول بالالتزام بمراعاة أحكام القانون الدولي الإنساني المطبق في النزاعات المسلحة ، عندما تستخدم الدول الهجوم السيبراني ضمن استراتيجيتها في نزاع مسلح قائم .

منهج الدراسة:

تتناول هذه الورقة الحرب السيبرانية في ضوء قواعد القانون الدولي للبحث عن إطار قانوني يمكننا من بيان موقف القانون الدولي من هذا النوع من الحروب بتحليل العديد من النصوص لاستنباط الأحكام.

خطة البحث:

سنقسم البحث في ثلاثة مطالب، الأول يخصص لتوضيح مفهوم الحرب السيبرانية لتمييزها عن الحرب التقليدية، والمطلب الثاني يناقش مدى خضوع الحرب السيبرانية لقواعد القانون الدولي المنظمة للعمليات الحربية، أما المطلب الثالث مخصص لبيان التدابير الوطنية التي تتخذها كل دولة منفردة، والتدابير الدولية التي تتعاون فيها الدول لمواجهة الحرب السيبرانية .

المطلب الأول

مفهوم الحرب السيبرانية

خلال هذا المطلب نحاول بيان المقصود بالحرب السيبرانية بشكل واضح يمكننا من تمييزها عن غيرها من المفاهيم المرتبطة بالاستخدام غير المشروع للفضاء السيبراني، ثم نبيّن الآليات التي تدار بها، مع الإشارة لنماذج وأمثلة لحروب سيبرانية، وذلك على النحو التالي:

الفرع الأول: تعريف الحرب السيبرانية:

يعد منع استخدام القوة في العلاقات الدولية من المبادئ الرئيسة الراسخة في القانون الدولي، والتي تشكل التزاماً أساسياً يقع على عاتق كل الدول، تمكنت من إرسائه بعدما أنهكتها الحروب والصراعات، وكلفتها أرواحاً وأموالاً باهظة.

ولقد حرص ميثاق الأمم المتحدة على إقرار هذا المبدأ بنصه في الفقرة الرابعة من مادته الثانية على أن " يمتنع أعضاء الهيئة جميعاً في علاقاتهم الدولية عن التهديد باستعمال القوة أو استخدامها ضد سلامة الأراضي أو الاستقلال السياسي لأي دولة أو على وجه آخر لا يتفق ومقاصد الأمم المتحدة. " كما أكدته العديد من الإعلانات والمواثيق الدولية العالمية منها والإقليمية وحتى في تلك الأحوال التي تجيز فيها أحكام القانون الدولي اللجوء إلى القوة يكون ذلك بشروط وضوابط وفي حالات محددة.

وعلى الرغم من استقرار تحريم استخدام القوة كقاعدة قانونية دولية آمرة ، إلا أن ذلك لم يمنع نشوب حروب ونزاعات مسلحة، دفعت الدول لتطوير قدراتها العسكرية وتنويع أسلحتها لتجنب تعرضها لأي اعتداء، وكان للتطور العلمي والتكنولوجي الهائل الذي تحقق أثر كبير في استحداث أسلحة، وفي اكتشاف طرق وأساليب تشن وتدار من خلالها الحروب . ويعد تسخير

الفضاء السيبراني في المجال العسكري تطبيقاً للاستفادة من هذه التطورات، والتي مكنت من إدارة العمليات والهجمات أثناء النزاعات بوسائل وآليات تعتمد على تقنيات مغايرة تماماً لوسائل الحرب التقليدية ،حتى أصبحت الحرب السيبرانية من سمات الحروب المعاصرة .

والفضاء السيبراني هو " مجال مادي وغير مادي يشمل مجموعة من العناصر وهي: أجهزة الكمبيوتر، وأنظمة الشبكات والبرمجيات، وحوسبة المعلومات، ونقل وتخزين البيانات، ومستخدمو كل هذه العناصر.

ونظراً لأن الفضاء السيبراني مجال مفتوح تصعب السيطرة عليه، تزايدت المخاطر التي تنتج عن استعماله، وتنوعت التهديدات المرتبطة به من جرائم إلكترونية، وهجمات سيبرانية، مرورا بالتجسس السيبراني، والإرهاب الإلكتروني، والقرصنة السيبرانية ، بل أصبح هذا الفضاء أيضا ساحة جديدة للحرب ، توصف العمليات العسكرية التي تدار فيه بالحرب السيبرانية، كما هو شأن الحرب البرية والبحرية والجوية. وهو ما دفع البحاث والخبراء في القانون الدولي، والدول والمنظمات الدولية إلى الاهتمام بهذا النوع المتطور للحروب، ومحاولة ضبطها وفقا لأحكام القانون الدولي.

وبداية تجدر الإشارة إلى أن مصطلح الحرب السيبرانية له مدلول محدد يختلف عن مصطلح الهجوم السيبراني أو الهجمات السيبرانية التي تشنها دولة ضد الأنظمة الإلكترونية لدولة أخرى، حيث يقصد بالهجوم السيبراني" تلك الإجراءات التي تتخذها الدولة من أجل الهجوم على

نظم المعلومات للعدو لهدف التأثير والإضرار فيها والدفاع عن نظم المعلومات الخاصة بالدولة المهاجمة [1].

ويعرَف أيضاً بأنه: استخدام أنشطة متعمدة لتغيير أو إفساد أو خداع أو إضعاف أو تدمير أنظمة الحاسوب، أو شبكات الحاسوب للخصم، أو المعلومات، والبرامج المدرجة في هذه الأنظمة، أو الشبكات، أو تُرسل من خلالها. [2]

أما الحرب السيبرانية فلم تتضمن المواثيق الدولية سواء تلك التي شكلت قواعد القانون الدولي الأساسية، أو تلك المتعلقة بالقانون الدولي الإنساني على تعريف للعمليات السيبرانية، أو الحرب السيبرانية، أو القتال السيبراني، مما جعل الفقه الدولي يجتهد في محاولة للوقوف على معنى واضح لها، وهو ما أدى إلى تعدد وتنوع التعريفات بتعدد وكثرة الدراسات التي تناولتها. فيعرفها البعض بأنها " أساليب الحرب ووسائلها التي تعتمد على تكنولوجيا المعلومات وتستخدم في سياق نزاع مسلح، أو هي الهجمات والعمليات التي ترتكب ضد أو بواسطة شبكات الحواسيب وأنظمة البيانات بين الدول أو الجماعات المسلحة المنظمة في سياق نزاع مسلح، أو سياسات الردع المتبادل. [3]

---

[1] Michael N. Schmitt، Computer network attack and the use of force in international law:Thoughts on a normative framework، Columbia journal of transnational law، 1998– 1999 available at : https://apps.dtic.mil/sti/pdfs/ADA471993.pdf

[2] هربرت لين " النزاع السيبراني والقانون الدولي الإنساني" مختارات من المجلة الدولية للصليب الأحمر ، مجلد94 (886) صيف 2012 ص 518.

[3] هالة أحمد الرشيدي" هل من حرب سيبرانية بين الولايات المتحدة وروسيا" منشور في جريدة الأهرام ، العدد48972 السنة 145 بتاريخ 4 يناير 2021 ، متاح على الرابط

https://gate.ahram.org.eg/daily/News/203620/4/792352/

وعرفها دليل "تالين" المتعلق بتطبيقات القانون الدولي في مجالات الصراع والحروب بأنها " كل العمليات السيبرانية سواء كانت دفاعية أو هجومية، والتي يعتقد أنها قد تسبب إصابات أو وفيات للبشر، أو تلف وضرر للأشياء المادية [1].

ومما سبق يتضح أن مفهوم الهجوم السيبراني أوسع من مفهوم الحرب السيبرانية، فالهجوم السيبراني قد يقع في أي وقت وقد يكون شرارة البدء للحرب أو إعلاناً لها، لكنه إذا وقع أثناء النزاع المسلح يوصف بأنه حرب سيبرانية، باعتباره جزء من حرب قائمة.

ولهذا التمييز إذا ما أخذنا به أهمية كبيرة في البحث عن طبيعة الحروب السيبرانية في إطار قواعد القانون الدولي، فهو من ناحية يوجب التطرق إلى تكييف الحرب السيبرانية وفقا لمبدأ حظر استخدام القوة في العلاقات الدولية، ومن ناحية أخرى سيمكننا من المطالبة بتطبيق قواعد القانون الدولي الإنساني كونها القواعد الواجبة التطبيق عند وقوع الحرب.

الفرع الثاني: طبيعة وآليات الحرب السيبرانية:

تتميز الحرب السيبرانية عن الحرب التقليدية، في أن المفهوم التقليدي للحرب، ينطوي على استخدام الجيوش النظامية ويسبقها إعلان واضح لحالة الحرب وميدان قتال محدد، بينما تبدو هجمات الفضاء الإلكتروني غير محددة المجال وغامضة الأهداف، كونها تتحرك عبر شبكات المعلومات والاتصالات المتعدية للحدود الدولية، إضافة إلى اعتمادها على ما يمكن وصفه بأسلحة إلكترونية جديدة تلاءم طبيعة السباق الإلكتروني لعصر المعلومات، حيث يتم

[1] درويش سعيد "الحروب السيبرانية وأثرها على حقوق الإنسان" المجلة الجزائرية للعلوم القانونية والاقتصادية والسياسية ، ص 181 الرابط:

https://www.asjp.cerist.dz/en/downArticle/32/54/5/83205

توجيهها ضد المنشئات الحيوية أو دسها عن طريق عملاء لأجهزة الاستخبارات، وعليه فإن أحد معايير التمييز بين الحرب السيبرانية والحرب التقليدية يمكن أن يكون بالاستناد إلى طبيعة السلاح المستخدم[1].

ومن أمثلة استخدام العمليات السيبرانية أثناء النزاعات التجسس، وتحديد الأهداف، والعمليات المعلوماتية الرامية إلى التأثير على معنويات العدو وإرادته إزاء القتال، وقطع نظم اتصالات العدو أو تضليلها أو التشويش عليها ابتغاء إعاقة تنسيق القوات، والعمليات السيبرانية الرامية إلى دعم العمليات الحركية كتعطيل محطات الرادار العسكرية للعدو لدعم الضربات الجوية، ومفهوم الحرب السيبرانية لا يستهدف القدرات والأنظمة العسكرية وحسب، ولكنه أيضاً قد يستهدف البنية التحتية الحيوية للمجتمع [(2)].

[1] يحي بياسين سعود" الحرب السيبرانية في ضوء قواعد القانون الدولي الإنساني" المجلة القانونية ، المجلد 4، العدد 4، 2018، متاح على الرابط : https://jlaw.journals.ekb.eg/article_45192.html

[(2)] لور انجيزلو تيلمان رودنها وسرو كنوتد ورمان "القانون الدولي الإنساني وحماية المدنيين من آثار العمليات السيبرانية أثناء النزاعات المسلحة "المجلة الدولية للصليب الأحمر ، مجلد 102 (913) 2020 ص 291.

وتشمل الأسلحة السيبرانية الفيروسات والديدان الحاسوبية وعمليات جمع البيانات السيبرانية، وأجهزة تشويش اتصالات البيانات اللاسلكية، وبرمجيات الحاسوبية المزيفة المشبوهة وأسلحة النبض الكهرمغناطيسي، وأدوات استطلاعات الحاسوب، والشبكات والقنابل الزمنية الطروادية المدمجة [1].

ويرى البعض أنه يمكن تحديد ثلاثة مستويات رئيسة للحرب السيبرانية أو الهجمات السيبرانية المستوى الأول: ويتمثل في تلك العمليات المصاحبة للحروب التقليدية كمهاجمة نظام الدفاع الجوي، والذي يؤدي إلى خسائر إستراتيجية واسعة النطاق نتيجة لأهمية الدفاع الجوي بالنسبة للدول، أما المستوى الثاني: فيتمثل في الحرب الإلكترونية المحدودة، والتي تتعرض فيها البنية التحتية والأهداف المدنية للهجمات السيبرانية، والمستوى الثالث: يتمثل في الحرب الإلكترونية غير المحدودة والتي يسعى من خلالها القائم بالهجوم إلى تعظيم الآثار التدميرية للبنية التحتية، حيث يؤثر سلباً في البناء الاجتماعي للدولة ، كمهاجمة أسواق المال، وخدمات الطوارئ، والأنظمة الإلكترونية الخاصة بمولدات الطاقة، وغيرها من الأهداف التي يترتب عليها آثار تدميرية واسعة النطاق، ويكون الهدف من هذا النوع من الحروب هو توسيع نطاق الخسائر المادية قدر الإمكان[2].

لقد أضحى استخدام العمليات السيبرانية أثناء النزاع المسلح سمة واقعية من سمات النزاعات المسلحة، ويرى البعض أن أول مرة نفذت فيها الهجمات السيبرانية، كانت في حرب كوسوفو

---

[1] حمدون إ. توريه " البحث عن السلام السيبراني" يناير 2011 ، ص 9.

[2] طلال ياسين العيسى، عدي محمد عناب "المسؤولية الدولية الناشئة عن الهجمات السيبرانية في ضوء القانون الدولي المعاصر" مجلة الزرقاء للبحوث والدراسات الإنسانية، المجلد19 العدد الأول ،2019، ص 85 متاح على الرابط:
https://doi.org/10.12816/0054788

عام1999، من خلال استهداف سلاح الجو التابع لحلف شمال الأطلسي "الناتو"لشبكات الهاتف في يوغسلافيا السابقة [1].

وأقرت بعض الدول علناً بأنها أجرت عمليات سيبرانية في نزاعات مسلحة جارية. فقد كشفت الولايات المتحدة، والمملكة المتحدة، وأستراليا على وجه الخصوص أنها لجأت إلى العمليات السيبرانية في نزاعها ضد تنظيم الدولة الإسلامية، ونشرت تقارير تشير إلى أن إسرائيل استخدمت عمليات سيبرانية ضد حماس، وأثرت العمليات السيبرانية على بلدان أخرى مشاركة في نزاعات مسلحة، مثل جورجيا في عام 2008 وأوكرانيا في الفترة بين2015 و2017[2].

وأكدت التقارير الاستخبارية الأمريكية في عام 2009، بقيام بعض من المجموعات المسلحة في أثناء احتلال العراق باختراق مواقع الكترونية كانت تستقبل بيانات غاية في الأهمية تنقلها الطائرات بدون طيار لتحديد تحركات هذه المجموعات، ما ساعد الأخيرة في مراقبة التحركات العسكرية الأمريكية لموجهة ضدهم [3].

وفي النزاع الروسي الأوكراني بدأت الهجمات الإلكترونية الروسية في وقت مبكر من عام 2014، بهدف تدمير البنية التحتية، والبيانات أو إتلافها، وحاولت القيام بذلك مرة أخرى في عام 2022، بقصد خلق الفوضى والتغلب على الدفاعات الأوكرانية، وسعت روسيا إلى تعطيل الخدمات، وتثبيت برامج ضارة مدمرة على الشبكات الأوكرانية، مستهدفة مواقع الحكومة الأوكرانية، ومقدمي خدمات الطاقة والاتصالات، والمؤسسات المالية، ووسائل الإعلام [4].

---

[1] احمد عبيس نعمة الفتلاوي، الهجمات السيبرانية: مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر، مجلة المحقق الحلي للمعلومات قانونية والسياسية، جامعة بابل كلية القانون، العدد الرابع،السنة الثامنة، 2016 ،ص 623 .

[2] لورا نجيزلو تيلمان رودنها وسروكنوتد ورمان، المرجع الساب، ص 290.

[3] احمد عبيس نعمة الفتلاوي، المرجع السابق، ص 625.

[4]James Andrew Lewis " Cyber War and Ukraine" available at https://www.csis.org/analysis/cyber-war-and-ukraine.

المطلب الثاني

مدى خضوع الحرب السيبرانية لقواعد القانون الدولي المنظمة للعمليات الحربية

إن تسخير الفضاء السيبراني في المجال العسكري واعتباره ساحة جديدة للحروب، أوجب ضرورة البحث وبيان بداية مدى ضبط هذا الاستخدام بمبادئ القانون الدولي المنظمة لاستعمال القوة في العلاقات الدولية، وأيضاً مدى إمكانية تطبيق قواعد القانون الدولي المتعلقة بالحرب، والتي تعرف بالقانون الدولي الإنساني على العمليات السيبرانية التي تقع أثناء النزاعات المسلحة، وهو ما سنحاول بيانه فيما يلي:

الفرع الأول: الحرب السيبرانية ومبدأ حظر استخدام القوة:

إن إقرار مبدأ حظر استخدام القوة في العلاقات الدولية الذي تضمنه نص الفقرة الرابعة من المادة الثانية من ميثاق الأمم المتحدة، وترسخه كمبدأ أساسي من مبادئ القانون الدولي، قد فرض التزاماً أساسياً يوجب على الدول الامتناع عن اللجوء إلى الحرب لأي مبرر، ورتب بذلك نتيجة تقضي بعدم مشروعية استعمالها للقوة في غير الأحوال الاستثنائية التي أجاز فيها الميثاق استعمالها.

غير أن عدم تعريف الميثاق لمصطلح استخدام القوة، أوجد تباين في الآراء بينم تمسك بالتفسير الضيق لهذا الاصطلاح، وبالتالي ذهب إلى عدم مشروعية استخدام القوة المسلحة، أو التهديد باستخدامها، وآخر اعتبر كافة صور الضغوط الأخرى ومنها السياسي والاقتصادي من صور القوة التي تم حظر استخدامها أو التهديد باستخدامها.

وفي كل مرة تتغير فيها طبيعة العمليات الحربية ونوع الأسلحة، عن تلك المستخدمة فيما يمكن وصفه بالحروب التقليدية، يثار النقاش مجدداً عن مدى اعتبار نوع ما من العمليات أو الهجمات

انتهاك لمبدأ الحظر، وما إذا كانت قواعد القانون الدولي تتواءم مع هذه المعطيات المتغيرة، فيغطيها المبدأ العام للحظر.

وقد أثار اللجوء إلى العمليات السيبرانية بدوره التساؤل عن مدى شمول حظر استخدام القوة لهذا النوع من العمليات.

ويقول البعض أن العملية السيبرانية التي تنفذها دولة ضد أخرى تنتهك حظر استخدام القوة إذا كانت آثارها مماثلة للآثار الناجمة عن استخدام الأسلحة التقليدية، ويعكس عدد من الأمثلة التي ساقتها الدول على استخدام القوة في الفضاء السيبراني على ما يبدو هذا الفهم، مثل العمليات السيبرانية التي تتسبب في إصابة الأشخاص أو موتهم أو إلحاق الضرر بالممتلكات أو تدميرها؛ والتسبب في انهيار محطة نووية؛ وفتح سد فوق منطقة مأهولة، الأمر الذي يؤدي إلى الدمار؛ وتعطيل خدمات مراقبة الحركة الجوية، الأمر الذي يؤدي إلى حوادث الطائرات؛ وإعاقة الأنظمة اللوجستية للقوات المسلحة، وتفسر بعض الدول على ما يبدو الحظر المفروض على استخدام القوة على نطاق أوسع، مشيرة إلى أنه لا يمكن استبعاد أن" توصف عملية سيبرانية لا تخلف آثاراً مادية أيضاً بأنها استخدام للقوة" وأن عملية سيبرانية لها أثر مالي واقتصادي خطير للغاية قد توصف بأنها استخدام للقوة[1].

وهناك من يرى أن محكمة العدل الدولية في قضية نيكاراغوا العام1986 أقرت بشمولية المادة(4/2) من الميثاق، وعدم اقتصارها على استخدام القوة بالمعنى التقليدي، والمتمثل في استخدام قوات عسكرية نظامية خارج حدود الدولة وهو ما يعني أنها كانت مهيأة لضم فئات أخرى غير الهجوم العسكري التقليدي في إطار التصرفات التي يمكن أن تشكل خرق للمادة(4/2) من الميثاق، إلى جانب ذلك جاءت النسخة الأولى من دليل تالين للعام 2011 لكي

[1] لورا نجيزلو تيلمان رودنها وسروكنوتد ورمان ، المرجع السابق ، ص 307 .

تدعم هذه النتيجة حين جاءت القاعدة 11 من هل تؤكد على أن" العمليات الإلكترونية تعتبر استخداماً للقوة عندما يكون مستواها وتأثيرها متقارباً مع العمليات غير الإلكترونية" ففي سياق هذا النص أقرت مجموعة من الخبراء أعدت هذا الدليل أنها قد استندت إلى معيار الحجم والتأثير في سياق تحديد في ما إذا كانت الهجمة الإلكترونية ترقى إلى استخدام غير مشروع للقوة خلافاً للمادة (4/2)من الميثاق[1].

الفرع الثاني: انطباق القانون الدولي الإنساني على العمليات العسكرية السيبرانية.

أشرنا فيما سبق إلى أن أحكام القانون الدولي قد استقرت على تحريم وتجريم لجوء الدول للحروب، غير أن ذلك لا ينفي وقوع عمليات حربية سواء أكان ذلك ضمن الاستثناءات التي سمحت باستخدام القوة، أو في تلك الأحوال التي تخرق فيها الدول هذه القاعدة فتقع منازعات مسلحة فيما بينها، أو تحدث صراعات مسلحة داخل الدولة الواحدة.

وقد بذلت العديد من الجهود للحد من مخاطر النزاعات المسلحة ومحاولة ضبطها للتقليل من آثارها الوخيمة، ولاسيما أن هذه الآثار قد تمتد لأشخاص لم يشاركوا بها وهذه الجهود قد أثمرت الاتفاق على مجموعة من القواعد القانونية المعروفة بقواعد القانون الدولي الإنساني والتي تعنى بضبط العمليات الحربية، وهي قواعد واجبة التطبيق على كافة العمليات التي تقوم بها الأطراف أثناء النزاع المسلح.

[1] رزق أحمد سمودي "حق الدفاع عن النفس نتيجة الهجمات الإلكترونية في ضوء قواعد القانون الدولي العام "مجلة جامعة الشارقة للعلوم القانونية ، المجلد(15) العدد(2) 2018 ، ص 348،349 .

وتعد اتفاقيات جنيف الأربع المبرمة عام 1949 والبرتوكولان الملحقان المضافان لها عام 1977، المصدر الأساسي لقواعد القانون الدولي الإنساني، وهي قواعد واجبة التطبيق على كافة الأنشطة التي تقوم بها الأطراف أثناء النزاع المسلح وينبغي احترامها.

ونظراً لتغير صور الحروب عن تلك التي كانت في زمن إبرام هذه الاتفاقيات، وتعدد وتطور أسلحتها وامتداد مجالاتها – والذي كان نتاجاً للتطور العلمي الكبير الذي حققته الدول، والذي سخرته لتطوير القدرات الحربية فقد كان هناك سعي مستمر لأن تظل كل هذه المتغيرات والتطورات الحربية، مشمولة بالضوابط ومحصورة في الحدود التي أرستها أحكام القانون الدولي الإنساني.

ويعد استخدام الفضاء السيبراني في المجال العسكري ، والنظر إليه كساحة جديدة قد تدور من خلالها نزاعات ، بنوع مغاير من الأسلحة ، نموذجاً لهذه التطورات التي نتجت عن تكنولوجيا المعلومات، حتى صارت هذه التكنولوجيا تستخدم في إدارة القوات العسكرية في القيادة والتحكم وفي الأمور اللوجستية، وفي توجيه الذخائر الحديثة بشكل دقيق يزيد من قوة فتكها ، ويقلل من الأضرار التي تصاحب استخدام مثل هذه الأسلحة، ويمكن هذا الاستخدام أيضاً من تنسيق تحركات وأفعال القوات العسكرية من خلال شبكات الاتصال التي تتيح تبادل المعلومات والصور المشتركة لميدان المعارك على نطاق واسع[1].

وقد أثار هذا التسخير للفضاء السيبراني في الأغراض العسكرية، النقاش حول مدى شمول أحكام القانون الدولي الإنساني لما يطلق عليه وصف بالحرب السيبرانية، إذ لم تتضمن أي وثيقة من مواثيقه صراحة مثل هذا النوع من العمليات المتطورة.

[1] هربرت لين ، المرجع السابق ، ص 516 .

ولكن قبل أن نبحث مدى خضوع العمليات السيبرانية لمبادئ القانون الدولي الإنساني، تجب الإشارة إلى أن القانون الدولي الإنساني ينطبق عند قيام نزاع مسلح وفقا لما قررته المادة الثانية المشتركة في اتفاقيات جنيف لعام 1949[1]. وهو ما يدعو إلى التساؤل حول ما إذا كانت العمليات السيبرانية لوحدها، أي دون أن تكون جزءاً من عمليات عسكرية قائمة، ينبغي أن تخضع لقواعد القانون الدولي الإنساني؟ وهنا يرى البعض خضوع الهجمات السيبرانية وحدها ولو لم يقترن بها استخدام القوات المسلحة التقليدية للقانون الدولي الإنساني، إذ يرى أن خضوع هذه الهجمات أو عدم خضوعها إنما يعتمد على طبيعتها، وعلى النتائج المتوقعة منها ، فمبادئ القانون الدولي الإنساني تنطبق عندما تعزي أي هجمات على شبكات الحاسوب إلى دولة ، مادامت الهجمات أكثر من مجرد حوادث متفرقة، أو معزولة وتهدف إلى الأذى أو الوفاة أو إحداث التلف أو الدمار[2].

بينما يرى البعض الآخر أن الهجمات السيبرانية ليست من النزاعات المسلحة التي تحكمها قواعد القانون الدولي الإنساني، إذ لا يوجد نص قانوني بأي وثيقة من مواثيق القانون الدولي الإنساني تعالج الهجوم على شبكات الحاسوب، أو تتحدث عن حرب المعلومات أو العمليات المعلوماتية، كون الاستخدام التكنولوجي للإنترنت هو حديث نسبياً، والقانون الدولي الإنساني القائم لا يتلاءم مع وسائل وأساليب الحرب الإلكترونية. بالإضافة إلى أن المعاهدات القائمة حالياً يرجع تاريخها إلى ما قبل وجود أو ظهور الهجمات عبر شبكات الحاسوب [3].

---

[1] تنص هذه المادة على " أن هذه الاتفاقيات تنطبق في حالة النزاع المسلح بين "الأطراف السامية المتعاقدة" حتى لو لم يعترف أحدها بحالة الحرب ".

[2] مايكل ن سميث ، " الحرب بواسطة شبكات الاتصال : الهجوم على شبكات الكمبيوتر (الحاسوب) والقانون في الحرب "المجلة الدولية للصليب الأحمر مختارات من أعداد 2002 ، ، ص 90. الرابط :

https://www.icrc.org/ar/doc/resources/documents/misc/5x6lsp.htm

[3] عمر محمود أعمر "الحرب الإلكترونية في القانون الدولي الإنساني" دراسات، علوم الشريعة والقانون، المجلّد 46 ،عدد3 ، 2019 ص 136. الرابط : https://journals.ju.edu.jo

أما عن امتداد تطبيق قواعد القانون الدولي الإنساني على العمليات السيبرانية التي تتم ضمن نزاع مسلح، فإن الاتجاه الغالب يدعو لتطبيق قواعد القانون الدولي الإنساني على هذه العمليات، منطلقاً من فكرة أن غياب معالجة نصوص القانون الدولي الإنساني للعمليات السيبرانية، أمر يبرر بعدم حدوثها زمن صياغة تلك الصكوك. وقد جاء في تعليق اللجنة الدولية للصليب الأحمر على اتفاقية جنيف الأولى " عندما تنفذ إحدى الدول عمليات سيبرانية ضد دولة أخرى واقترن ذلك ودعمه بعمليات عسكرية أكثر تقليدية، فهذه الحالات، بلا ريب، هي بمثابة نزاع مسلح دولي [1].

ويضيف أنصار هذا الاتجاه أن غياب إشارات محددة في القانون الدولي الإنساني لا يعني عدم خضوع هذه العمليات لقواعده، وذلك من خلال قواعده العامة التي تنظم جميع أساليب الحرب ووسائلها بما فيها استخدام الأسلحة، حيث جاءت تلك القواعد لتشتمل على كافة التطورات ذات الصلة، وهو ما تشير إليه المادة (36) من البروتوكول الإضافي الأول الملحق باتفاقيات جنيف الأربعة لعام1977إذ نصت على "يلتزم أي طرف سام متعاقد، عند دراسة أو تطوير أو اقتناء سلاح جديد، أو أداة للحرب، أو إتباع أسلوب للحرب، بأن يتحقق مما إذا كان ذلك محظوراً في جميع الأحوال أو في بعضها بمقتضى هذا الملحق " البروتوكول " أو أية قاعدة أخرى من قواعد القانون الدولي التي يلتزم بها الطرف السامي المتعاقد[2].

---

[1] تعليق اللجنة الدولية على اتفاقية جنيف الأولى،الفقرة 254 . الرابط:

https://www.icrc.org/ar/commentaries-geneva-convention-i

[2] يحيى ياسين سعود ، المرجع السابق ، ص 90.

كما يؤكد البعض على أن شرط مارتينز وهو من المبادئ الأساسية في القانون الدولي الإنساني، يقرر بأنه "في حالة عدم وجود قاعدة معينة في القانون التعاهدي، يظل محارب ونفي حمى، وتحت سلطة القانون العرفي ومبادئ الإنسانية وما يمليه الضمير العام [1].

وتؤكد أيضاً اللجنة الدولية للصليب الأحمر أيضاً أنه ليس ثمة شك في أن القانون الدولي الإنساني ينظم العمليات السيبرانية أثناء النزاعات المسلحة أو الحرب السيبرانية بشأن السلاح أو أساليب ووسائل القتال التي يلجأ إليها أي طرف من الأطراف المتحاربة في النزاع، سواء كانت قديمة أو حديثة واعتماد العمليات السيبرانية على تقنية جديدة ومتطورة باستمرار لا يحول دون تطبيق القانون الدولي الإنساني على استخدام هذه التقنيات باعتبارها من وسائل أو أساليب القتال [2].

ويمكن كذلك الاستدلال كذلك بالرأي الاستشاري لمحكمة العدل الدولية الصادر عام 1996 والمتعلق بمشروعية التهديد بالأسلحة النووية أو استخدامها والذي ذهبت فيه إلى القول" إن التهديد بالأسلحة النووية ،أو استخدامها مخالف بصورة عامة لقواعد القانون الدولي المنطبقة في أوقات النزاع المسلح وخاصة مبادئ القانون الإنساني وقواعده " وذلك لقياس استخدام الأسلحة السيبرانية على استخدام الأسلحة النووية – بوصف الأخيرة نموذجاً لتطور لم تتضمنه القواعد الأساسية للقانون الدولي الإنساني وبذلك يمكننا تأييد خضوع الدول عند استخدام الأسلحة السيبرانية في النزاعات المسلحة لأحكام القانون الدولي الإنساني.

---

[1] مايكل ن سميث ، المرجع السابق ، ص 94 ، 95.

[2] لوران جيزلو تيلمان رودنها وسروكنوتد ورمان، المرجع السابق، ص 297 و 298 .

أخيرا يمكننا القول أن هناك تأييد كبير من قبل العديد من الدول والمنظمات الدولية وخبراء القانون الدولي لوجوب خضوع العمليات السيبرانية لقواعد القانون الدولي الإنساني ، وهو ما خلص إليه تقرير فريق الخبراء الحكوميين المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدول التابع للأمم المتحدة، عامي 2013 و2015، إذ جاء به أن"أحكام القانون الدولي، وخاصة ميثاق الأمم المتحدة ينطبق على استخدام لتكنولوجيا المعلومات والاتصالات، وهو عنصر لابد منه لحفظ السلام والاستقرار وتهيئة بيئة لتكنولوجيا المعلومات والاتصالات[1].

المطلب الثالث

الآليات الوطنية والدولية لمواجهة الحرب السيبرانية

تدرك الدول الخطر الكبير الذي تشكله الهجمات السيبرانية بمختلف أشكالها على أمنها الوطني، لذلك تسعى لمجابهة هذه المخاطر سواء بإجراءات انفرادية تتخذها داخل إقليمها، أو بالتعاون فيما بينها لوضع إطار يكفل الحماية للجميع. ونحاول في هذا المطلب الإشارة إلى بعض من التدابير التي تتخذها الدول في هذا الشأن.

الفرع الأول: التدابير الوطنية لدرء مخاطر العمليات السيبرانية:

شكلت مسألة كيفية الرد على أعمال عدائية في الفضاء السيبراني شاغلاً للكثير من الدول دفعها لاتخاذ جملة من الإجراءات لردع مخاطر هذه الأعمال، والتقليل من نتائجها.

وتعتبر الدول أن الأمن السيبراني جزء لا يتجزأ من أمنها القومي، وتعمل على مواصلة تقييم الأخطار والتحديات المحتملة التي تصاحب التكنولوجيا الحديثة في ميدان أمن المعلومات،

[1] وثيقة الأمم المتحدة A/68/98 24حزيران/يونيو 2013 ،الفقرة19 .

ودراسة ما يمكن اتخاذه من تدابير واستراتيجيات على مختلف المستويات للتصدي لهذه الأخطار.

وفي المجال العسكري حولت بعض البلدان موارد الميزانية إلى مبادرات الفضاء السيبراني، حيث وضعت جانباً مبالغ كبيرة خصصتها للبحث وتطوير قدرات الحرب السيبرانية، كما تعمل على إقامة العُدة العسكرية السيبرانية من خلال تحديث خدمات الاستخبارات للتركيز على جمع المعلومات العلمية والتكنولوجية ذات الصلة وإجراء عمليات محاكاة للحرب السيبرانية والمناورات العسكرية ،و تكليف عدد كبير من الأفراد العسكريين بمهمة القتال الافتراضي، وتدريبهم على ذلك، ويمكن أن يشمل هذا التحول إنشاء فرق حربية للإنترنت تكون مكرسة لتحقيق الأمن السيبراني، ويمكن دمجها في وكالات استخبارات أخرى، أو حتى إنشاء قطاعات جديدة تماماً ضمن الهيكل العسكري المكرس للنشاط السيبراني.فقد أعلنت الولايات المتحدة على سبيل المثال، إنشاء وحدة جديدة للشؤون العسكرية السيبرانية في 2009، وأعلنت المملكة المتحدة مؤخراً إنشاء مركز لعمليات الأمن السيبراني كجزء من استراتيجيتها للأمن السيبراني[1].

وتستعمل بعض الحكومات بالفعل تكنولوجيا المعلومات والاتصالات بالاقتران مع موظفين عسكريين متخصصين في التكنولوجيا لمراقبة الحدود الوطنية، ويمكن أن تشمل النُهج الأخرى عمليات التحكم والمراقبة التي تركز على تعطيل تدفق معلومات العدو واستهداف والبنى التحتية لتكنولوجيا المعلومات والاتصالات المعادية لإتلاف أو تدمير الأجهزة الوظيفية والشبكات والبيانات الحيوية. وتركز هذه التغييرات على شن هجمات على نقاط الضعف المحتملة للخصوم[2].

---

[1] حمدون إ. توريه" الاستجابة الدولية للحرب السيبرانية " ضمن مؤلف"البحث عن السلام السيبراني" الصادر عن الاتحاد الدولي للاتصالات والاتحاد العالمي للعلماء ،2011،ص 79-81.

[2] المرجع السابق ، ص 82،82.

وأخيراً من المهم الإشارة إلى أن بعض الدول اعتبرت تعرضها لهجمات سيبرانية بمثابة أعمال عسكرية عدائية، تجيز لها استخدام وسائل ردع العدوان المقررة بموجب أحكام القانون الدولي بما فيها اللجوء إلى القوة المسلحة ، فقد نشر البيت الأبيض فيعام 2011 " الاستراتيجية الدولية للفضاء الإلكتروني" والذي أعلن فيها احتفاظ الولايات المتحدة الأمريكية بالحق في استخدام القوة العسكرية رداً على هجوم إلكتروني[1]. وبالمثل اعتبرت الدول في حلف شمال الأطلسي "الناتو" الهجمات الإلكترونية بمثابة هجمات مسلحة تستدعي الدفاع المشترك، حيث جاء في البيان المشترك الصادر عن الحلف في 14 من يونيو 2021 "أن تأثير الأنشطة السيبرانية الكبيرة الخبيثة التراكمية يمكن، في ظروف معينة، اعتباره بمثابة هجوم مسلح، وهو تقييم يمكن أن يؤدي إلى تطبيق بند الدفاع عن النفس المشترك للمنظمة، بموجب المادة الخامسة [2].

الفرع الثاني: التدابير الدولية للحد من الهجمات السيبرانية:

إن الترابط الذي يميز الفضاء السيبراني يعني أن أي شيء لمواجهة بيئية تتطلب الإنترنت يمكن أن يتأثر بالعمليات السيبرانية التي تُنفذ في أي مكان في العالم وقد يخلف الهجوم السيبراني الذي يستهدف نظاماً معيناً تداعيات على نظم أخرى مختلفة، بغض النظر عن مكان وجود تلك النظم وثمة خطر حقيقي من أن تؤدي الأدوات السيبرانية – سواء عمدًا أو خطأً – إلى آثار واسعة النطاق ومتنوعة على البنية التحتية المدنية الحيوية، وترابط الفضاء السيبراني يعني أيضًا أن جميع الدول ينبغي أن تهتم بالرقابة الفعالة عليه، فالهجمات التي تُشن ضد دولة واحدة

---

[01] الاستراتيجية متاحة على الرابط :

https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/International_Strategy_Cyberspace_Factsheet.pdf

[2] https://arabic.cnn.com/world/article/2021/06/14/nato-cyber-attacks-article-5-russia

يمكن أن تؤثر على العديد من الدول الأخرى، بغض النظر عن مكان وجودها وعن مشاركتها في النزاع[1].

ونظرا لما تتضمنه الهجمات السيبرانية من خصائص، أهمها صعوبة إن لم يكن استحالة نسبة هذه العمليات إلى جهة محددة، والتكلفة الكبيرة التي تلحقها وخاصة الاقتصادية، كان لزاماً على الدول أن تكثف جهودها، وتعزز التعاون فيما بينها لدرء هذه المخاطر، ومحاولة منع لجوء الدول إلى استخدام العمليات السيبرانية في سياق النزاعات المسلحة، وإخضاع ما يقع منها لقواعد القانون الدولي الإنساني كما وضحنا فيما سبق .

ورغم أن المجتمع الدولي لم يتوصل –إلى الآن –إلى إبرام اتفاقية دولية تحظر استخدام الهجمات السيبرانية أو تضبطها، إلا أن هناك اهتمام دولي متزايد يدفع الدول نحو وجوب اتخاذ خطوات عملية في مواجهة خطورة الهجمات السيبرانية انطلاقاً من تحملها لمسؤولياتها في تعزيز السلم والأمن الدوليين.

ولقد أولت الجمعية العامة للأمم المتحدة اهتماماً كبيراً بالعمليات السيبرانية، وبدأت المناقشات حول المسائل المتعلقة بأمن المعلومات عندما دعت روسيا في عام 1998، الجمعية العامة للأمم المتحدة إلى إبرام اتفاقية دولية معنية بالهجمات السيبرانية، وهو ما دفع الجمعية العامة عام 2000 إلى إصدار قرار يدعو إلى دراسة التهديدات التي تصاحب استخدام المنظومات الإلكترونية لأغراض عسكرية [2].

وقد تكونت مجموعة من الفرق تضم خبراء حكوميين، وتعمل على مناقشة المسائل المتعلقة بالمعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي، وفي عام 2012 وعملاً بقرار الجمعية العامة للأمم المتحدة 24/66 الصادر في 2011 تم إنشاء فريق الخبراء

---

[1] لوران جيزلو تيلمانرو دنهاو سروكنو تدورمان، المرجع السابق، ص294 .

[2] احمد عبيس نعمة الفتلاوي ،المرجع السابق ، ص 656.

الحكوميين المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي ، والذي خلص في تقريريه لعام 2013 [1]و2015[2] إلى أن القانون الدولي وبخاصة ميثاق الأمم المتحدة ينطبق على استخدام الدول لتكنولوجيا المعلومات والاتصالات وهو عنصر لابد منه لصون السلام والاستقرار، وأن من شأن وضع معايير وقواعد لسلوك الدول أن يحد من المخاطر التي تهدد السلام ،والأمن والاستقرار على الصعيد الدولي .

وفي عام2018، أنشأت الجمعية العامة للأمم المتحدة أيضاً الفريق العامل المفتوح العضوية، والذي أتاح للجمعية العامة إمكانية عقد اجتماعات تشاورية بين الدورات مع الأطراف المعنية، وهي الشركات والمنظمات غير الحكومية والأوساط الأكاديمية، من أجل تبادل الآراء بشأن القضايا التي تدخل في نطاق ولاية الفريق.

وفي الإطار الإقليمي نفذ الناتو السياسة الخاصة به في مجال الدفاع السيبراني في عام 2008 من أجل حماية مواردها التكنولوجية وتلك الخاصة بالأعضاء ، وكجزء من هذه السياسة أنشأ الحلف هيئة معنية بإدارة الدفاع السيبراني، وفريقاً للاستجابة للحوادث الحاسوبية يكفل إرسال فرق الدعم السريع إلى فرادى البلدان الأعضاء، ومركزاً للتميز من أجل الدفاع السيبراني التعاوني، ويضم خبراء يضطلعون بالبحث والتدريب في مجال الأمن السيبراني، وإضافة إلى ذلك أجرى الناتو تدريبات في مجال الدفاع السيبراني حيث تقوم فرق من الدول الأعضاء بمحاولة الدفاع عن الشبكات الحاسوبية الافتراضية من الهجوم السيبراني[3]، كما نشر الحلف في عام

---

(1) A/68/98 .

(2) A/70/174 .

(3) حمدون إ. توريه، المرجع السابق ، ص 86

2013 دليلا باسم"تالين" يحتوي على 95 مادة للقوانين الدولية المطبقة في حال نشوب حروب الكترونية وتنظيم قواعد الاشتباك عبر الإنترنت، ويقسم هذا الدليل إلى قسمين:

الأول: يعالج قانون الأمن الإلكتروني، والثاني قانون النزاعات الإلكترونية، ويقر هذا الدليل بأن العمليات الإلكترونية قد تشكل نزاعات مسلحة تبعاً للظروف، لا سيما الآثار المدمرة لتلك العمليات، والمبادرة الأكثر نجاحاً التي تضمنها هي إشارته إلى أن القانون الدولي الإنساني ينطبق على الحرب الإلكترونية، مع تحديدها للدور الذي ستلعبه قواعد القانون الدولي الإنساني [1].

وعلى الصعيد الإقليمي أيضا سبق للدول الأعضاء في منظمة شنغهاي للتعاون أن قررت في عام 2009 أن تطوير واستخدام أسلحة المعلومات، والتحضير لحرب المعلومات وتنفيذها، يشكلان تهديداً رئيساً في مجال أمن المعلومات الدولي، إلا أنها التزمت الصمت بشأن الإطار القانوني المنطبق. وقد أجريت مناقشات بشأن تطبيق القانون الدول بما في ذلك القانون الدولي الإنساني، في المنظمة الاستشارية القانونية الآسيوية الأفريقية(آلكو) التي أنشأت في عام 2015 فريقًا مفتوح العضوية بشأن القانون الدولي في الفضاء السيبراني[2].

وأخيراً على الصعيد العربي فقد بذلت جهود كبيرة في مكافحة الجرائم السيبرانية والإلكترونية، أسفرت عن وضع اتفاقية عربية لمكافحة جرائم تقنية المعلومات، والتي انبثقت عن الاجتماع المشترك لمجلس وزراء الداخلية والعدل العرب، الذي عُقد بمقر الأمانة العامة لجامعة الدول العربية في عام2010 بهدف تعزيز التعاون بين الدول العربية في مكافحة جرائم تقنية المعلومات، والجرائم السيبرانية التي تهدد أمنها ومصالحها وسلامة مجتمعاتها، وتلبية الحاجة إلى تبني سياسة جنائية مشتركة تهدف إلى حماية المجتمع العربي ضد جرائم تقنية المعلومات، وقد

---

[1] عمر محمود أعمر ، المرجع السابق ، ص 135.

[2] لورا نجيز لوتيلما نرودنها وسروكنوتد ورمان، المرجع السابق، ص293 .

جاءت هذه الاتفاقية من منطلق الالتزام بالمعاهدات، والمواثيق العربية والدولية المتعلقة بهذا الشأن[1].

[1] طلال ياسين العيسى، عدي محمد عناب ، المرجع السابق، ص 90 .

الخاتمة

من خلال هذا البحث يتبين أنه لا يوجد تعريف اصطلاحي لمفهوم الهجوم السيبراني، إنما هناك عدة تعريفات معظمها فقهية حاولت توضيح المقصود به، مستهدفة الوصول إلى نوع من التنظيم القانوني لمثل هذا النوع من الهجمات، والتي باتت تشكل خطراً إضافياً متزايداً يهدد السلم والأمن الدوليين، لاسيما بعد أن أصبح استخدام العمليات السيبرانية أثناء النزاع المسلح سمة واقعية من سمات النزاعات المسلحة.

قد تتسبب العمليات السيبرانية التي تستهدف البنية التحتية للدول، مثل الكهرباء والمياه والصرف الصحي، في إحداث أضرار جسيمة بالبشر، ويمثل وجوب توجيه الهجمات ضد الأهداف العسكرية فقط تحدياً رئيساً للحد من التكلفة البشرية المحتملة من جراء العمليات السيبرانية أثناء النزاعات المسلحة.

وكل ما سبق يشكل تحديات حقيقة تحتم على الدول ضرورة التعاون والتضافر فيما بينها لإقامة نظام قانوني يرتكز على أسس تكفل مواجهة وردع مخاطر الهجمات السيبرانية. وعليه يمكننا تقديم التوصيات التالية:

- تعديل ميثاق الأمم المتحدة لاستيعاب النزاع السيبراني، والتطورات الأخرى التي لحقت في طبيعة الصراعات والنزاعات، لتتمكن الجماعة الدولية من اتخاذ التدابير اللازمة لمواجهة مخاطر هذه الحروب.
- العمل على وضع إطار محدد يتفق من خلاله على تعريف واضح لمفهوم النزاع المسلح، والهجوم السيبراني وكيفية اعتباره نزاعاً مسلحاً، أو استخدام للقوة، وحالات الدفاع عن النفس ضد الهجمات الإلكترونية أو السيبرانية.

- الاتفاق بين الدول على وضع اتفاقية دولية شاملة تعالج استخدام الأسلحة السيبرانية، شأنها شأن الأسلحة النووية والكيماوية والبيولوجية وغيرها من الأسلحة المتطورة.
- فرض المزيد من القيود على استخدام الدول في الفضاء السيبراني، وإلزامها بفرض ضوابط على استخدام أفرادها، للوصول إلى آلية تمكن من إسناد المسؤولية وتحمل تبعات ذلك.

المراجع

باللغة العربية:

- أحمد عبيس نعمة الفتلاوي، الهجمات السيبرانية مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر، مجلة المحقق الحليل لعلوم القانونية والسياسية، جامعة بابل كلية القانون، العدد الرابع، السنة الثامنة، 2016.
- حمدون إ. توريه "الاستجابة الدولية للحرب السيبرانية " ضمن مؤلف "البحث عن السلام السيبراني" الصادر عن الاتحاد الدولي للاتصالات والاتحاد العالمي للعلماء، يناير 2011.
- درويش سعيد "الحروب السيبرانية وأثرها على حقوق الإنسان" المجلة الجزائرية للعلوم القانونية والاقتصادية والسياسية، متاح على الرابط:

https://www.asjp.cerist.dz/en/downArticle/32/54/5/83205

- رزق أحمد سمودي "حق الدفاع عن النفس نتيجة الهجمات الإلكترونية في ضوء قواعد القانون الدولي العام "مجلة جامعة الشارقة للعلوم القانونية، المجلد(15) العدد(2) 2018 .
- طلال ياسين العيسى، عدي محمد عناب "المسؤولية الدولية الناشئة عن الهجمات السيبرانية في ضوء القانون الدولي المعاصر" مجلة الزرقاء للبحوث والدراسات الإنسانية، المجلد19 العدد الأول ،2019، متاح على الرابط:

https://doi.org/10.12816/0054788

- عمر محمود أعمر "الحرب الإلكترونية في القانون الدولي الإنساني" دراسات، علوم الشريعة والقانون، المجلّد46 ، عدد3 ، 2019. متاح على الرابط: https://journals.ju.edu.jo

- قادير إسماعيل، إدارة الحروب النفسية في الفضاء الإلكتروني: الاستراتيجية الأمريكية الجديدة في الشرق الأوسط، (ندوة دولية بعنوان : عولمة الإعلام السياسي وتحديات الأمن القومي للدول النامية، الجزائر:2017، متوفر على الرابط : https://manifest.univ-ouargla:
- لورا نجيز لوتيلما نرودنها وسروكنوتد ورمان "القانون الدولي الإنساني وحماية المدنيين من آثار العمليات السيبرانية أثناء النزاعات المسلحة" المجلة الدولية للصليب الأحمر، مجلد 102 (913) 2020.
- مايكل سميث" الحرب بواسطة شبكات الاتصال: الهجوم على شبكات الكمبيوتر (الحاسوب) والقانون في الحرب "المجلة الدولية للصليب الأحمر مختارات من أعداد 2002، متاح على الرابط:
- https://www.icrc.org/ar/doc/resources/documents/misc/5x6lsp.htm
- هالة أحمد الرشيدي" هل من حرب سيبرانية بين الولايات المتحدة وروسيا" منشور في جريدة الأهرام، العدد48972 السنة 145 بتاريخ 4 يناير 2021، متاح على الرابط

https://gate.ahram.org.eg/daily/News/203620/4/792352

- هربرت لين " النزاع السيبراني والقانون الدولي الإنساني" مختارات من المجلة الدولية للصليب الأحمر، مجلد94 (886) صيف 2012.
- يحيى ياسين سعود" الحرب السيبرانية في ضوء قواعد القانون الدولي الإنساني" المجلة القانونية، المجلد 4، العدد 4، 2018، متاح على الرابط:

https://jlaw.journals.ekb.eg/article_45192.html

المراجع الأجنبية:

- James Andrew Lewis " Cyber War and Ukraine" available at https://www.csis.org/analysis/cyber-war-and-ukraine
- Michael N. Schmitt، Computer network attack and the use offorce in international law: Thoughts on a normative framework، Columbia journal of transnational law، 1998– 1999 available at : https://apps.dtic.mil/sti/pdfs/ADA471993.pdf

.