

الحرب السيبرانية والقانون الدولي الإنساني

Cyber War and International Humanitarian Law

د. بن تغري موسى⁽¹⁾

أستاذ محاضر "أ"

كلية الحقوق

جامعة يحي فارس - المدية (الجزائر)

bentegri.moussa@yahoo.com

تاريخ النشر
05 أبريل 2020

تاريخ القبول:
04 مارس 2020

تاريخ الارسال:
08 نوفمبر 2019

الملخص:

أصبح الأمن السيبراني من الإهتمامات الكبرى للدول، خاصة بعد التهديدات والهجمات المختلفة التي تمس بأنظمة المعلومات ومراكز القوة والدفاع، ما جعلها تسعى لتطوير وتعزيز منظومتها الدفاعية في مواجهة الجرائم السيبرانية والهجمات الإلكترونية، سعيا منها لحماية أمنها القومي، وسلامة حدودها وحماية مواطنيها، وأمام هذا الواقع تحولت مخاوف الدول من الاعتداءات وواقعها المحتمل، إلى هاجس اسمه الحرب السيبرانية، ما فرض النظر إلى هذه الحرب على أنها حرب حقيقة حديثة، ولكن بوسائل غير الأسلحة والذخائر، فبدأ البحث عن مكانتها في قانون النزاعات المسلحة، ومدى إمكانية انطباق القانون الدولي الإنساني عليها، مع البحث عن المبادئ والقواعد الواجبة التطوير في هذا القانون لتتلاءم مع هذه الحرب.

الكلمات المفتاحية:

الحرب السيبرانية - الدفاع السيبراني - القانون الدولي الإنساني.

Abstract :

Cyber security has become one of the major concerns of states, especially after the various threats and attacks affecting information systems and centers of power and defense, which made them seek to develop and strengthen their defense system in the face of cyber crimes and electronic attacks, in an effort to protect their national security, the integrity of their borders and the protection of their citizens, and in front of this reality has transformed The countries' fears of the attacks and their potential reality, to an obsession called cyber warfare, which imposed this war as a true modern war, but by means other than weapons and ammunition, so he began searching for its place in the law of armed conflict, and the extent of the possibility of We apply international humanitarian law to them, with a search for principles and rules to be developed in this law to suit this war

key words :

Cyber War - Cyber Defense - International Humanitarian Law.



مقدمة:

تبرز أهمية الموضوع من خلال البحث في التهديد بالحرب السيبرانية الذي يلوح في الأفق أكثر من أي وقت مضى، خاصة أنه أصبحت التقدمات التكنولوجية والبنية الرقمية المتنامية تربط مجتمعات العالم بأكملها بعجلة أنظمة معقدة ومتشابكة، والطلب على الإنترنت والتوصيلة الرقمية يستدعي تكاملاً متزايداً باستمرار لتكنولوجيا المعلومات والاتصالات واندماجها في منتجات كانت تعمل من قبل بدونها، مثل السيارات والمباني بل وأنظمة المراقبة لشبكات الطاقة والنقل الشاسعة، فشبكات إمدادات الكهرباء وأنظمة النقل والخدمات واللوجستيات العسكرية، أي كل الخدمات المعاصرة تقريباً تتوقف على استعمال تكنولوجيا المعلومات والاتصالات واستقرار الفضاء السيبراني.

والفضاء السيبراني هو العالم المادي والمفاهيمي الذي توجد فيه جميع هذه الأنظمة، والبحث عن الأمن السيبراني في هذا الفضاء من أهم مجالات الأمن في القرن الحادي والعشرين، ومن المعروف أن الهيمنة السيبرانية ترسم ملامح الحروب في القرن القادم مما يستلزم تغيير الإستراتيجية في اتجاه التصعيد مع قوى أخرى معادية نشطة في ساحة الحرب السيبرانية التي تحارب عليها منذ أكثر من عشرة أعوام فرق من القوات الخاصة للدول الكبرى، ومجموعات من قراصنة الإنترنت المرتزقة المجندين حسب اللزوم، ويقصد بالحرب السيبرانية هنا عمليات في الفضاء الإلكتروني تستخدم وسائل وأساليب قتال ترقى إلى مستوى النزاع المسلح أو تُجرى في سياقه، ضمن المعنى المقصود في القانون الدولي الإنساني.

ولذلك فإن الحرب السيبرانية يمكن أن تُفهم بصورة واسعة على أنها حرب تجري في الفضاء السيبراني باستعمال واستهداف تكنولوجيا المعلومات والاتصالات، والاعتماد المتزايد بسرعة على الشبكات الذكية وغيرها من أنظمة المراقبة والرصد عن طريق الإنترنت، تضع مركز موارد الطاقة والنقل والدفاع في متناول هؤلاء الذين يسعون إلى إحداث الفوضى في الحكومة وبين السكان المدنيين، وهكذا فإن تعزيز الأمن السيبراني وحماية البنية التحتية الحرجة للمعلومات تمثل الآن عناصر حيوية في أمن كل دولة ورفاهها الاقتصادي¹.

ويثور القلق بشأنها بسبب ضعف الشبكات الإلكترونية والتكلفة الإنسانية المحتملة من جراء الهجمات السيبرانية، فعندما تتعرض الحواسيب أو الشبكات التابعة لدولة ما لهجوم أو اختراق أو إعاقة، قد يجعل هذا الأمر المدنيين والأعيان المدنية عرضة لخطر الحرمان من الاحتياجات الأساسية مثل مياه الشرب والرعاية الطبية والكهرباء وغيرها، لذا تظهر أهمية البحث في تسليط الضوء على مدى انطباق القانون الدولي الإنساني على الحرب السيبرانية في الوقت الراهن من خلال التطرق للجوانب القانونية المنظمة لمثل هذه الحروب وكيف تعامل

القانون الدولي مع آثار الحرب السيبرانية، مع محاولة إظهار قدره دليل تالين على رصد مختلف جوانب هذه الحرب والمبادئ الحاكمة لها في ضل المتغيرات الجديدة ومحاولة كل دولة تحقيق الأمن السيبراني.

هذه الجوانب السابق ذكرها قمنا برصدها وتحليلها وفق المنهج التحليلي عن طريق تحليل نصوص ومبادئ القانون الدولي الإنساني ومحاولة معرفة مدى إمكانية تطبيقها على مثل هذه الحروب، وهنا يثور التساؤل عن مدى انطباق القانون الدولي الإنساني على هذه الحروب، وكيف يمكن تطويره بما يتناسب والحرب السيبرانية؟.

ولدراسة هذه العناصر قمنا بتقسيم المقال إلى ثلاث مباحث رُتبت على الشكل التالي:

المبحث الأول: ماهية الحرب السيبرانية.

المبحث الثاني: واقع الحرب السيبرانية في القانون الدولي للمنازعات المسلحة.

المبحث الثالث: دليل تالين والقدرات الوطنية والدولية في مواجهة الحرب السيبرانية.

المبحث الأول: ماهية الحرب السيبرانية

يتبوأ أمن الفضاء الإلكتروني مكانة بارزة على جدول أعمال المسؤولين عن وضع السياسات العامة والقادة العسكريين في جميع أنحاء العالم، وقد أدرجت على وجه التحديد حرب الفضاء الإلكتروني أو الحرب السيبرانية في تخطيطها وتنظيمها العسكري، وأصبحت الدول تبحث عن نهج أمن الفضاء الإلكتروني المتبع، وتشمل هذه التدابير بيانات متطورة للغاية عن العقيدة والتنظيمات العسكرية وتوظيف مئات الأفراد بهذا الخصوص، مع إعداد ترتيبات أساسية تدمج الهجوم الإلكتروني في قدراتها الحالية الخاصة بالحرب السيبرانية، وتعمل عدد من الدول على إنشاء وحدات متخصصة داخل أو خارج قواتها المسلحة للتعامل مع العمليات والهجمات الإلكترونية، وورد أيضاً أن اثنتي عشرة من أقوى القوات المسلحة الخمس عشرة على مستوى العالم تعمل على بناء برامج لحروب الفضاء الإلكتروني²، لذا سنقوم بتعريف الحرب السيبرانية وبيان أنماطها المختلفة وفق قواعد القانون الدولي الإنساني.

المطلب الأول: مفهوم الحرب السيبرانية

يشمل مفهوم الحرب السيبرانية استهدافا للقدرات والأنظمة العسكرية واستهداف البنية التحتية الحيوية للمجتمع، بما في ذلك الشبكات الذكية وشبكات المراقبة الإشرافية وحيازة البيانات التي تسمح لها بالعمل والدفاع عن نفسها، وفي حين أن استخدام وسيط مختلف (الفضاء السيبراني وتكنولوجيا المعلومات والاتصالات العاملة فيه) فإن الأعداء يستطيعون مع ذلك نشر أسلحة والدخول في نزاع هجومي دفاعي يُشبه إلى حد بعيد الحرب التقليدية، وتكتيكات الحرب

السيبرانية تنطوي نمطياً على جمع البيانات أو التسلل إلى الأنظمة المحوسبة لإحداث الضرر في الأنظمة الحرجة³.

وتعبير الحرب السيبرانية يُستخدم للإشارة إلى أشياء مختلفة، ويُستخدم المصطلح هنا للإشارة إلى وسائل وأساليب القتال التي تتألف من عمليات في الفضاء الإلكتروني ترقى إلى مستوى النزاع المسلح أو تُجرى في سياقها، ضمن المعنى المقصود في القانون الدولي الإنساني، فعندما تتعرض الحواسيب أو الشبكات التابعة لدولة ما لهجوم أو اختراق أو إعاقة، قد يجعل هذا الأمر المدنيين عرضة لخطر الحرمان من الاحتياجات الأساسية مثل مياه الشرب والرعاية الطبية والكهرباء، وإذا تعطلت أنظمة تحديد المواقع GPS عن العمل، قد تحدث إصابات في صفوف المدنيين من خلال تعطيل عمليات إقلاع مروحيات الإنقاذ مثلاً⁴.

ويمكن أن تتعرض السدود والمحطات النووية وأنظمة التحكم في الطائرات لهجمات سيبرانية نظراً لاعتمادها على الحواسيب، وتكون الشبكات مترابطة إلى حد يجعل من الصعب الحد من آثار هجوم سيبراني ضد جزء من المنظومة دون الإضرار بأجزاء أخرى أو تعطيل المنظومة بأكملها، وقد يتضرر مئات الآلاف من الناس، وصحتهم وحتى حياتهم، فعلى أطراف النزاع توخي الحرص بشكل مستمر من أجل حماية المدنيين في الحروب السيبرانية، وهو أحد أهم الأدوار التي تقوم بها، فالحروب لها قواعد وحدود تنطبق على اللجوء إلى الحرب السيبرانية بنفس القدر الذي تنطبق به على استخدام البنادق والمدفعية والصواريخ وغيرها كما سنرى⁵.

وتعرف اللجنة الدولية للصليب الأحمر هذه الحرب بأنها الأفعال التي يتخذها أطراف نزاع ما، لتحقيق ميزة على خصومهم في الفضاء السيبراني باستخدام أدوات تقنية مختلفة وتقنيات تعتمد على البشر، ومن الناحية النظرية، يمكن تحقيق المزايا عن طريق إتلاف أو تدمير أو إعطاب أو نهب أنظمة الحاسوب لدى الخصم (الهجوم السيبراني)، أو بالحصول على معلومات يُفضّل الخصم أن تبقى سرية (التجسس السيبراني أو من خلال الاستغلال السيبراني⁶). فالعمليات والهجمات الإلكترونية التي تهدف إلى الإضرار بالخصم، سواء عن طريق التسبب في الوفاة أو الإصابة أو الدمار أو عن طريق التأثير سلباً على العمليات العسكرية أو القدرة العسكرية، يجب أن تعتبر عمليات عدائية، فعلى سبيل المثال، فإن العمليات الإلكترونية التي تهدف إلى تعطيل أو تعجيز نظم الرادار أو نظم الأسلحة أو الإمداد بالخدمات اللوجستية أو شبكات الاتصال التي يتحكم فيها العدو عن طريق الكمبيوتر، تُصنف على أنها عمليات عدائية حتى إذا لم تتسبب في ضرر مادي، أما العمليات الإلكترونية التي تنفذ لتحقيق الغرض العام

المتمثل في جمع المعلومات الإستخباراتية فلا تندرج ضمن العمليات العدائية بمفهوم القانون الدولي الإنساني⁷.

ومن وجهة نظر قانونية، من المهم التمييز بين الحرب السيبرانية بمفهوم العمليات الإلكترونية المنفذة في سياق النزاعات المسلحة في إطار المعنى المقصود في القانون الدولي الإنساني، والعمليات الإلكترونية خارج هذه السياقات، ولا تنطبق قواعد القانون الدولي الإنساني إلا في سياق النزاعات المسلحة، مما يفرض قيوداً محددة على الأطراف المشاركة في النزاع، وبالتالي، فإن مصطلح الحرب السيبرانية سيشير إلى وسائل وأساليب القتال التي تشمل العمليات الإلكترونية التي تصل إلى حد النزاع المسلح أو تنفذ في سياقه وذلك في إطار المعنى المقصود في القانون الدولي الإنساني فقط، وتوجه العمليات الإلكترونية المذكورة -التي يشار إليها كثيراً بوصفها هجمات على شبكات الكمبيوتر- ضد جهاز كمبيوتر أو نظام حاسوبي أو عبرهما من خلال مسار تدفق البيانات، ويمكن أن تسعى إلى تحقيق أهداف مختلفة، منها على سبيل المثال التسلل إلى نظام حاسوبي وجمع أو إخراج أو تدمير أو تعديل أو تشفير البيانات أو إطلاق عمليات أو تعديلها أو التلاعب بطريقة أخرى في هذه العمليات التي يسيطر عليها النظام المخترق، وبمعنى آخر، يتناول التحليل التالي العمليات العدائية التي تشمل تطوير شفرة حاسوبية وإرسالها من جهاز كمبيوتر أو أكثر إلى أجهزة الكمبيوتر المستهدفة⁸.

وتشمل الأسلحة السيبرانية المحتملة، الفيروسات والديدان الحاسوبية وعمليات جمع البيانات السيبرانية وأجهزة تشويش اتصالات البيانات اللاسلكية وبرمجيات الحاسوبية المزيفة المشبوهة وأسلحة النبض الكهرومغناطيسي وأدوات استطلاعات الحاسوب والشبكات والقنابل الزمنية الطروادية المدمجة ورغم أن المعالم الدقيقة لأي حرب سيبرانية لا تزال غير محددة فإن الهجمات الكبيرة ضد البنية التحتية للمعلومات وخدمات الإنترنت في العقد الأخير تُعطي صورة عن الشكل والنطاق المحتملين للنزاع في الفضاء السيبراني⁹.

وإطلاق اسم سلاح معلوماتي على أي نوع من أنواع الأسلحة، بما في ذلك التقليدية منها، القادرة على إلحاق الضرر بالبنية التحتية المعلوماتية، وعلى سبيل المثال، ليس هناك من أهمية لنوع الجهاز الذي يُستخدم في تعطيل نظام التحكم بالاقتصاد الوطني أو الأسلحة أو المعلومات القومية، سواء أكان هذا الجهاز شفرة برنامجية، أم نبضة إلكترونية شديدة، أم ضربة مباشرة من متفجرة تقليدية، وثمة نهج آخر يمكن بمقتضاه اعتبار الأسلحة المعلوماتية على أنها في النهاية كل وسائل التدمير التي تستخدم تكنولوجيا المعلومات والاتصالات وهنا تتفق جميع الدول على اعتبارها كذلك وفق هذا المنطق¹⁰.

المطلب الثاني: أنماط الحرب السيبرانية

تتنوع أنماط الحرب السيبرانية في أشكال متعددة تعود لطبيعة الصراع وللضرورة التي تفرض استخدام أي نمط من هذه الأنماط، وقدره العدو على التصدي لها، ومن خلال هذه الأنماط يكون انطباق القانون الدولي الإنساني، خاصة أن هذا القانون يميز بين أنواع النزاعات المسلحة لتحديد القانون المطبق وهو ما يمكن تطبيقه في الحرب السيبرانية على النحو التالي.

الفرع الأول: الحرب السيبرانية الباردة

حيث يتم استخدام الفضاء الإلكتروني كساحة للصراع منخفض الشدة، ويعبر هذا النمط عن صراع مستمر بين الفاعلين المتنازعين، وقد يكون ذا طبيعة ممتدة، ودائمة النشاط العدائي أو غير السلمي، بخلاف أنه عميق الجذور ومتداخل، وله نواح متعددة ثقافية، أو اقتصادية، أو اجتماعية، وعادة ما يتم اللجوء إلى القوّة الناعمة الحروب السيبرانية في مثل صراعات كهذه. وإن كانت لا تتطور بالضرورة إلى استخدام القوّة المسلحة بشكلها التقليدي، أو شن حرب إلكترونية واسعة النطاق¹¹.

ولهذه الحرب السيبرانية الباردة وسائل عدد، منها شن الحروب النفسية، والاختراقات المتعددة، والتجسس، وسرقة المعلومات، وشن حرب الأفكار، والتنافس بين الشركات التكنولوجية العالمية وأجهزة الاستخبارات الدولية.

وتجلى هذا النمط في حالات الحروب في الصراعات السياسية، ذات البعد الاجتماعي الديني الممتد، مثل الصراع العربي الإسرائيلي، أو الصراع الهندي الباكستاني، وغيرها، في مثل هذه الصراعات، تنشط جماعات دولية للقرصنة للتعبير عن مواقف سياسية، أو حقوقية، مثل جماعة ويكيليكس، وأنونيموس، وكذلك أيضا في حالات الأزمات الدولية، مثل التوتر بين استونيا وروسيا في عام 2007، وكذا الاختراقات المتبادلة بين الصين والولايات المتحدة وروسيا، أو ما بين طهران وواشنطن¹².

وقد تعرضت روسيا إلى اتهام بشن هجمات إلكترونية على الترويج، والتشيك، وبريطانيا، مما دفع الدول الأخيرة لإعلان أنها قادرة على الرد بالمثل، أيضا، شنت إيران هجمات إلكترونية على منشآت نفطية في منطقة الخليج العربي، احتجاجا على مزاعم بتعرض الأقليات الشيعية للتمييز، كما الحال مع هجمات فيروس دوكو في عام 2012¹³.

الفرع الثاني: الحرب السيبرانية متوسطة الشدة

حيث يتحول الصراع عبر الفضاء الإلكتروني إلى ساحة موازية لحرب تقليدية دائره على الأرض، ويكون ذلك تعبيرا عن حدّ الصراع القائم بين الأطراف، كما قد يمهّد لعمل عسكري، هنا تدور الحروب السيبرانية عن طريق اختراق المواقع الإلكترونية، وتخريبها، وشن

حرب معلوماتية وتجسسية ضد الخصوم، وغيرها، ويستمد ذلك النوع من الحروب السيبرانية شدته من قوّة أطرافه، وارتباطها بعمل عسكري تقليدي، خاصة في ظل بعض التقديرات التي تشير إلى أن تكلفة هذه الحروب قد تشكل 4 من إنفاق نظيراتها التقليدية، بما يمكن من تمويل حملة حربية كاملة عبر الإنترنت بتكلفة دبابه، وتاريخيا تم استخدام الحروب السيبرانية متوسطة الشدة في هجمات حلف الناتو في عام 1999 على يوغوسلافيا، حيث استهدفت الهجمات الإلكترونية تعطيل شبكات الاتصالات للخصوم، وأيضا، برزت خلال الحرب بين لبنان وإسرائيل في عام 2006، وكذلك بين روسيا وجورجيا في عام 2008، والمواجهات بين حماس وإسرائيل في عامي 2008 و2012¹⁴.

الفرع الثالث: الحرب السيبرانية الساخنة

ويعبر ذلك النمط عن نشوء حروب في الفضاء الإلكتروني منفردة، وغير متوازية مع الأعمال العسكرية التقليدية، ولم يشهد العالم هذا النوع من الحروب، وإن كانت احتمالات حدوثها وارده في المستقبل مع تطور القدرات التكنولوجية، واتساع الاعتماد بين الدول والفواعل من غير الدول على الفضاء الإلكتروني، وينطوي هذا النمط من الحروب على سيطرته البعد التكنولوجي على إدارة العمليات الحربية، حيث يتم استخدام الأسلحة الإلكترونية فقط ضد منشآت العدو، وكذا اللجوء إلى الروبوتات الآلية في الحروب والطائرات دون طيار، وإدارتها عن بعد، بخلاف تطوير القدرات في مجال الدفاع والهجوم الإلكتروني، والاستحواذ على القوّة الإلكترونية¹⁵.

وفي هذا السياق، يتم أيضا استخدام الفضاء الإلكتروني للاستعداد لحرب المستقبل، عبر قيام الدول بتدريبات على توجيه ضربة أولية لحواصب العدو، واختراق العمليات العسكرية عالية التقنية، أو حتى باستهداف الحياة المدنية، والبنية التحتية المعلوماتية¹⁶. والهدف من وراء ذلك تحقيق "الهيمنة الإلكترونية الواسعة" بشكل أسرع في حالة نشوب صراع، وقد شهدت الأسلحة الإلكترونية تطورا أكبر في قدرتها على التأثير في الخصوم، مثل أسلحة الميكروويف عالية القدرة، والهجمات الإلكترونية عبر الفيروسات، مثل شن إسرائيل هجمات فيروس ستاكسنت ضد المنشآت النووية الإيرانية بالتعاون مع الولايات المتحدة في عام 2010، وكان قد تم تطوير هذا الفيروس وتجربته في إسرائيل¹⁷.

المبحث الثاني: واقع الحرب السيبرانية في القانون الدولي للمنازعات المسلحة

من الخطير على الاستقرار الدولي أن تتم معاملة النزاعات التي لا تشتمل على تهديدات واضحة للأرواح البشرية أو الحرية الاجتماعية على أنها نزاع مسلح، وفضلاً عن ذلك، وبالنظر

إلى أن كل أنظمة السلاح المتطورة عملياً تستخدم تكنولوجيا المعلومات والاتصالات، فإن من العسير للغاية، إن لم يكن من المستحيل، أن نعزل الأسلحة المعلوماتية عن الطائفة الكاملة للأسلحة، وبما أن الحرب المعلوماتية هي ظاهرة مستمرة في تاريخ النزاع البشري، فإن من الصعب على وجه الخصوص تقديم وضع قاطع لهذه الحرب بالنظر إلى المستويات المتعددة للتعقيد المفاهيمي لها، لذا سنحاول تحديد وضع هذه الحرب في القانون الدولي الإنساني، ثم البحث عن إمكانية انطباق هذا القانون عليها¹⁸.

المطلب الأول: وضع الحرب السيبرانية في القانون الدولي الإنساني

الغالبية العظمى من الوسائل المتطورة للصراع المسلح التي تستخدم تكنولوجيا المعلومات والاتصالات هي ذات استخدامات متعددة، أي أنها ليست مصممة فحسب لتدمير البنى التحتية المعلوماتية بل لمهام قتالية أخرى أيضاً، وتتمتع البلدان التي تمتلك أنظمة أسلحة متطورة، ووسائل استطلاع، واتصال، وملاحقة، وتحكم مستندة إلى الاستخدام الواسع لتكنولوجيا المعلومات والاتصالات بتفوق عسكري حاسم؛ ومن ثم فإن من المشكوك فيه أن تنضم هذه الدول إلى اتفاقيات تحد من مزاياها الاستراتيجية¹⁹.

لذا فإن وضع هذه الحرب يقف موقف القانون الذي يحكمها وهو القانون الدولي الإنساني، فإذا ما دارت هذه الحرب في نزاع بين الدول قد يأخذ وصف الحرب يكون هذا القانون هو الذي يحكم سلوك أطراف النزاع، وعليه فإنه لا ينطبق القانون الدولي الإنساني إلا إذا نُفذت العمليات الإلكترونية في سياق نزاع مسلح وكانت مرتبطة به، وهذه أحد القواعد الواجب مراعاتها للبحث حول أثر تطبيق القانون الدولي الإنساني، وبالتالي ينبغي أن لا يُثار أي جدل إزاء الرأي القائل بأن العمليات الإلكترونية حين تُنفذ في سياق نزاع مسلح دائر، فإنها تخضع لقواعد القانون الدولي الإنساني ذاتها التي يخضع لها النزاع، على سبيل المثال، إذا قام أحد أطراف النزاع، بالتزامن مع قصف بالمدفعية أو القذائف أو بالإضافة إليها، أيضاً بإطلاق هجوم إلكتروني على النظم الحاسوبية لخصمه لأنه يوصف الفعل بأنه هجوم في نزاع وحتى إن لم يكن مسلحاً بمفهوم الحرب التقليدية²⁰.

كما أن ميثاق الأمم المتحدة، واتفاقيات جنيف لعام 1949 ولاهاي لعامي 1899 و1907، ومعاهد حلف شمال الأطلسي لا تتناول النزاع السيبراني، ويستخدم ميثاق الأمم المتحدة ومعاهد حلف شمال الأطلسي على حد سواء مصطلحات من قبيل السلامة الإقليمية، واستخدام القوة المسلحة، وعمل من جانب القوات الجوية أو البرية أو البحرية، و"هجوم مسلح"، وهي مصطلحات لا تنسجم مع التصورات السيبرانية مما يضعها ظاهرياً خارج نطاق القانون الدولي²¹.

ومع ذلك، فإن عدداً من العمليات التي يشار إليها على أنها من قبيل الحرب السيبرانية قد لا تُنفذ في سياق نزاع مسلح على الإطلاق، وقد تؤدي مصطلحات مثل الهجمات الإلكترونية أو الإرهاب الإلكتروني، إلى استدعاء فكرة أساليب الحرب، إلا أن العمليات التي تشير إليها لا تُنفذ بالضرورة في نزاع مسلح، ويمكن للعمليات الإلكترونية أن تستخدم، بل هي تستخدم فعل، في جرائم ترتكب في حالات يومية لا تتعلق بالحرب على الإطلاق، ولكن قبل الانتقال إلى القواعد التي تحكم سير العمليات العدائية -ولا سيما مبادئ التمييز والتناسب والاحتياط -من المهم معالجة مسألة ظلت موضوعاً للمناقشة لفترة من الوقت، ألا وهي نوع السلوك، ولا سيما نوع العملية الإلكترونية، الذي يؤدي إلى تطبيق القواعد التي تحكم سير العمليات العدائية²².

والسؤال بالغ الأهمية، فإذا كانت عملية إلكترونية معينة خاضعة لمبدأ التمييز، فمن المحذور توجيهها مباشرة ضد البنية الأساسية المدنية، وإذا وُجّهت صوب هدف عسكري، فإن التأثيرات العرضية التي تلحق بالبنية الأساسية المدنية يجب أن تؤخذ في الاعتبار إذا كانت العملية خاضعة لمبدأ التناسب²³، وهنا تكون في وضع الحرب ولكن بشكل مختلف ينظمها القانون الدولي الإنساني حتى لا تترك مثل هذه الحروب بلا قواعد ولا نظم، ويجب الإعداد لوضع القواعد الخاصة بهذه الحرب حتى لا يتذرع أي من كان بغياب النص.

المطلب الثاني: انطباق القواعد والمبادئ الإنسانية على الحرب السيبرانية

ثمة حاجة ملحة للقيام بموائمة الحرب السيبرانية مع القانون الدولي الإنساني، نظراً لأن أعمال الحرب السيبرانية ستسفر عن خرق أحكام عديدة في القوانين الحالية المسلحة أو أنها ستكون خارج نطاق هذه القوانين تماماً، فيجب احترام الأطر الكبرى والاتفاقية المهمة في هذا القانون، خاصة اتفاقيات جنيف لعام 1949 والبروتوكول الإضافي الأول الخاص بحماية ضحايا المنازعات الدولية المسلحة (البروتوكول الأول)²⁴، واتفاقيات لاهاي (1899 و1907) الخاصة باحترام قوانين وأعراف الحرب البرية، ونظام روما الأساسي للمحكمة الجنائية الدولية.

كما ينبغي احترام مبادئ القانون الدولي الإنساني الممكن انطباقها على الحرب السيبرانية، من خلال توفير قدر كاف من الحماية للبنية التحتية الحيوية لمنع أوجه التدمير والأذى والمعاناة غير الضرورية، وضمان الحد الأدنى من الاتصالات الأساسية ذات الصلة بحماية المدنيين، حيث أن البنى التحتية الحيوية المحمية ستشمل البنى التي تدعم المستشفيات، والمرافق الطبية ومراكز دور العجز، والنظم المالية، ونظم دعم الحياة والأجهزة الطبية الهامة، وسلاسل الإمداد، ووسائل النقل، ومرافق الأخبار ودور العبادة والمراكز الدينية، والمرافق التعليمية، والمسعفين، وأجهزة إنفاذ القانون، وليس المقصود بالقائمة المعروضة آنفاً أن تكون

كاملة، بل أن تقدم أمثلة على أنواع النظم التي تساند المدنيين الأبرياء وتكون النظم والأجهزة المعلوماتية التي تحميها عرضة للهجمات الإلكترونية، بما في ذلك صغار الأطفال، والعجزة، والجرحى، والعجائز، ومن المفروض أن تساعد مساهمات الجهات المعنية الدبلوماسية في رسم الحدود المقدسة للبنية التحتية الحيوية²⁵.

فيجب على الطرف المسؤول عن هجوم سيبراني ما اتخاذ التدابير إلى أقصى قدر ممكن، من أجل تفادي أو تخفيف الضرر العرضي الذي يلحق بالبنية التحتية المدنية أو يؤدي المدنيين، وهذا سيتطلب التحقق من طبيعة النظم التي تتعرض للهجوم والأضرار المحتملة التي قد تنجم عن أحد الهجمات، وهذا يعني أيضاً أنه عندما يصبح جلياً أن هجوماً سيتسبب بإصابات أو أضرار مدنية عرضية، يجب إلغاؤه أو العدول عنه.

علاوة على ذلك، يجب على أطراف النزاع أن تلتزم باتخاذ الاحتياطات اللازمة من آثار الهجمات، ونتيجة لذلك، تكون نظم الحواسيب العسكرية منفصلة بما يكفي عن تلك المدنية، بغية حماية السكان المدنيين من آثار الهجمات العرضية والعشوائية. ويمكن للاعتماد على نظم الحواسيب العسكرية والتوصيل بين نظم الحواسيب التي يديرها متقاعدون مدنيون وتستخدم أيضاً لأغراض مدنية أن يثير القلق، وعلى صعيد آخر، قد تساهم تكنولوجيا المعلومات أيضاً في الحد من الأضرار العرضية التي تلحق بالمدنيين أو البنية التحتية المدنية، وعلى سبيل المثال، قد يلحق تعطيل خدمات معينة تستخدم لأغراض عسكرية ومدنية أضراراً أقل مما يلحق تدمير البنية التحتية تماماً، وفي هذه الحالات، يفرض مبدأ الاحتياط القابل للجدل التزاماً على الدول باختيار الوسائل الأقل ضرراً بغية تحقيق أهدافها العسكرية²⁶.

لذا فإن الأذى والضرر الناجمين عن تدمير أو تعطيل نظم البنية التحتية الحيوية غير ضروريين وسيتسببان في معاناه ومصاعب جسيمة من النوع الذي هدفت قوانين النزاع المسلح إلى منعه، وفضلاً عن ذلك، ولأن هذه الشبكات تخدم أعداداً ضخمة من السكان، فإن الأذى والضرر المتأتين من مثل هذا الهجوم سيكونان على نطاق واسع وغير متناسبين مع المزايا العسكرية المستخلصة، وبالتالي، من المهم للغاية أن توضح هذه المسألة في حالة السكان المدنيين، فحسبما يرى الشخص، من منظور ضيق أو منظور واسع، أنواع العمليات الإلكترونية التي تخضع للقواعد التي تحكم سير العمليات العدائية، يمكن أن تكون الأعمال التالية محظورة أو قانونية في سياق نزاع مسلح:

- تعطيل شبكة الكهرباء المدنية أو نظام لمعالجة المياه (دون إلحاق أضرار مادية بها).
- توجيه هجوم يترتب عليه حرمان نظام مصرفي من خدمة الإنترنت مما يكون له تأثير كبير على قدرته عدد ملايين من عملاء المصرف على الحصول على الخدمات المصرفية.

- توجيه هجوم يترتب عليه الحرمان من الخدمات المقدمة عبر نظام خاص لحجز رحلات الطيران عبر الإنترنت من أجل التسبب في عدم تمكن السكان المدنيين من مغادرة مناطق النزاع.

- إغلاق شبكة الإنترنت وشبكات الهاتف المحمول في منطقة معينة من البلد لمنع الدعاية التي يطلقها الخصم²⁷.

كما أنه على البلدان أن تحترم حياد البلدان الأخرى وألا تنقل أي نوع من الهجمات عبر بناها التحتية الحيوية وهذا يتسق هذا مع اتفاقيات لاهاي 1899 و 1907 في المادة 05 و 13، التي تقيد نقل القوات أو قوافل الإمدادات أو الذخائر عبر الأقاليم أو المياه المحايدة، وبالمستطاع تدمير العديد من البنى التحتية الحيوية، مثل الشبكات الكهربائية، من خلال فرط تحميل النظام، وهكذا فإن السماح للبلدان بشن الهجمات السيبرانية التي يمكن أن تعبر من خلال العديد من شبكات البلدان الأخرى دون علمها لا يتسق ببساطة مع تاريخ القوانين الدولية للنزاع المسلح والغاية منها، وسيطلب هذا المبدأ المقترح الحصول على إذن من البلدان الأخرى قبل شن هجوم سيبراني، وبالتالي العمل كرادع ضد شن هجوم سيبراني²⁸.

كما أن مبدأ التمييز يلزم الدول بأن تميز في جميع الأحوال بين المدنيين والمقاتلين وبين الأعيان المدنية والأهداف العسكرية، وهو مبدأ أساسي من مبادئ القانون الدولي الإنساني، على حد قول محكمة العدل الدولية، ولا يجوز توجيه الهجمات إلا نحو المقاتلين أو الأهداف العسكرية، ويعني هذا أنه عند تخطيط وتنفيذ العمليات الإلكترونية، فإن الأهداف المسموح بها فقط في إطار القانون الدولي الإنساني هي الأهداف العسكرية، مثل أجهزة الكمبيوتر أو النظم الحاسوبية التي تحقق مساهمة فعالة في العمليات العسكرية للموسسة، ولا يجوز توجيه الهجمات عبر الفضاء الإلكتروني نحو النظم الحاسوبية المستخدمة في منشآت مدنية بحتة²⁹.

المبحث الثالث: دليل تالين والقدرات الوطنية والدولية في مواجهة الحرب السيبرانية

في هذا المبحث سنتناول دليلين تالين كأحد الأطر القانونية الجديدة لمواجهة الحرب السيبرانية من خلال مجموعة القواعد والمبادئ المتفق عليها والتي تشكل الأرضية الحقيقية لبداية البحث عن السبل من أجل تطوير قواعد القانون الدولي الإنساني لتستوعب مثل هذه الحروب، وصولاً إلى الحلول الموجودة لدى الدول أو المتفق عليها في القانون الدولي والتي يمكن التقيد بها في حال حدوث حرب سيبراني، وهي مجالات بدأ التوافق حولها ووجب تطويرها كما سنرى.

المطلب الأول: دليل تالين بشأن الحرب السيبرانية

يعد دليل تالين المتعلق بالقانون الدولي المنطبق على عمليات حرب الفضاء الإلكتروني أو الحرب السيبرانية المشار إليه باسم دليل تالين، هو الإجراء الأشمل الذي يسعى إلى تفسير قواعد القانون الدولي (الحق في الحرب وقانون الحرب). في إطار الحرب الإلكترونية، وقد صاغ هذا الدليل مجموعة من الخبراء بناءً على دعوة من مركز الامتياز التعاوني للدفاع عن الفضاء الإلكتروني التابع لمنظمة حلف شمال الأطلسي، وهو يقدم مجموعة مفيدة من القواعد التي تقترب بتعليق يعكس مختلف الآراء بشأن المسائل الشائكة التي تثيرها هذه التكنولوجيا الجديدة، وشاركت اللجنة الدولية للصليب الأحمر في مداولات مجموعة الخبراء بوصفها مراقباً، إلا أنها لا توافق على جميع الآراء الواردة في الدليل³⁰.

ويقدم دليل تالين رؤى مثيرة للاهتمام في هذا الصدد، فهو يتمسك على سبيل المثال بالثنائية التقليدية للنزاعات المسلحة الدولية والنزاعات المسلحة غير الدولية، ويقر بأن العمليات الإلكترونية وحدها قد تشكل نزاعات مسلحة تبعاً للظروف - لا سيما الآثار المدمرة لتلك العمليات-، ويقدم الدليل في هذا الصدد تعريفاً للهجوم السيبراني بموجب القانون الدولي الإنساني بوصفه "عملية إلكترونية سواء هجومية أو دفاعية يتوقع أن تتسبب في إصابة أو قتل أشخاص أو الإضرار بأعيان أو تدميرها.

ويكمن صلب الموضوع مع ذلك في التفاصيل أي ما ينبغي أن يفهم على أنه "ضرر" في العالم الإلكتروني، وبعد مناقشات مكثفة، اتفق أغلب الخبراء على أنه علاوة على الضرر المادي فإن توقف أحد الأعيان عن العمل قد يشكل ضرراً أيضاً، وتتمثل وجهة نظر اللجنة الدولية للصليب الأحمر مع مبادئ دليل تالين في أنه إذا تعطل أحد الأعيان، فليس من المهم كيفية حدوث ذلك سواء بوسائل حركية أو عملية إلكترونية، وهذه القضية مهمة للغاية في الممارسة العملية حيث أن أي عملية إلكترونية تستهدف تعطيل شبكة مدنية خلاف ذلك، لن يشملها الحظر الذي يفرضه القانون الدولي الإنساني على الاستهداف المباشر للأشخاص المدنيين والأعيان المدنية³¹.

ويذكر الدليل أيضاً أن مبدأي الاحتياط والتناسب، يجب احترامهما في حال تعرضت شبكة الإنترنت أو أجزاء كبيرة منها للهجوم، ولكن على الرغم من أن هذا قد يبدو مطمئناً للوهلة الأولى، فهو يترك إشكالية حول ما إذا كان من الممكن أو غير الممكن استهداف شبكة الإنترنت بالكامل، أو استهداف أجزاء منها إذا كانت تستخدم في الاتصالات العسكرية وكان تدميرها أو تعطيلها يوفر ميزة عسكرية أكيدة (مرة أخرى رهناً بالتناسب والاحتياطات).

وينص دليل تالين بشأن مبدأ الاحتياط على أنه بالنظر إلى تعقد العمليات الإلكترونية، وارتفاع احتمالات الإضرار بالنظم المدنية، والفهم المحدود في بعض الأحيان لطبيعتها وتأثيرها

لدى المسؤولين عن اعتماد العمليات الإلكترونية، ينبغي أن تتاح لمخططي المهام، حيثما أمكن، الاستعانة بالخبرة التقنية الموجودة لمساعدتهم في تحديد ما إذا كانت التدابير الاحتياطية الملائمة قد اتخذت، وإذا كانت الخبرة، ومن ثم القدرة على تقييم طبيعة الهجوم والخسائر والأضرار العرضية بين المدنيين، غير متاحة، فقد يتعين على المهاجم الامتناع عن الهجوم³².

المطلب الثاني: الأساليب الوطنية والدولية المقترحة لمواجهة الحرب السيبرانية

على المستوى الوطني فإن معظم الحكومات تعترف بضرورة إعادة توزيع الموارد وإصلاح استراتيجيات الأمن الوطنية على بعض المستويات، وتبادر كثير من البلدان إلى زيادة التمويل وبحث الموارد التكتيكية والدبلوماسية لتعزيز أمنها السيبراني، مما يجعلها تصمم أسلحة سيبرانية هجومية وقدرات دفاعية أيضاً، وهي تعتبر الأسلحة السيبرانية بمثابة "مضاعفات القوة" التي ينبغي استعمالها في المقام الأول بالاقتران مع الأعمال العسكرية الأكثر تقليدية من أجل تعزيز قدراتها الحربية بشكل كبير، ويمكن أن يشمل هذا النوع من التحويل تدريب الموظفين العسكريين (أو إعادة تدريبهم)، وتحديث خدمات الاستخبارات للتركيز على جمع المعلومات العلمية والتكنولوجية ذات الصلة وإجراء عمليات محاكاة للحرب السيبرانية والمناورات العسكرية مع إيلاء اهتمام خاص لتطبيقات تكنولوجيا المعلومات والاتصالات، كما قد يشمل إنشاء فرق حربية للإنترنت تكون مكرسة لتحقيق الأمن السيبراني، ويمكن دمجها في وكالات استخبارات الدول³³.

أما على المستوى الدولي فإنه نظراً لأن المعايير والصكوك القانونية الدولية الحالية غير مجهزة تجهيزاً كاملاً للتعامل مع التحديات الجديدة التي يطرحها الأمن السيبراني، يعتبر الحوار العالمي والتعاون من الأمور الضرورية بهذا الشأن، والطبيعة المتغيرة للتكنولوجيا ذاتها - مع تداخلات متزايدة بين السلطات القضائية الوطنية وتكنولوجيا المعلومات والاتصالات المرتبطة بها، والموارد والأنظمة على الخط - تجعل اعتماد استراتيجيات جديدة والتعاون الدولي يتسمان بأهمية أكثر لضمان السلام السيبراني³⁴.

ومن الضروري أن تعمل البلدان على تنسيق أطرها القانونية لمكافحة الجرائم السيبرانية وتيسير التعاون الدولي الدينامي متعدد الجوانب، ويتعين على الدول أن تعمل في سبيل وضع إطار قانوني وتنظيمي مشترك، وإقامة نظام لتحديث هذه القوانين على أساس منتظم لمعالجة الطبيعة المتغيرة للتهديدات التي يتعرض لها الأمن، وقد دعت بعض المجموعات بالفعل إلى إصدار معايير دولية وقواعد سيبرانية كوسيلة لتحسين الأمن السيبراني على الصعيد الدولي، فيتعين لدى إصدار مبادئ توجيهية لتحقيق الأمن السيبراني بين الدول، النظر في الخصائص المميزة للفضاء السيبراني وأبرز التحديات التي تطرحها هذه السمات، وذلك من خلال وضع

استراتيجيات من أجل تطوير نموذج للتشريعات المتعلقة بالجرائم السيبرانية يكون قابلاً للتطبيق والتنفيذ على الصعيد العالمي، ويساعد في فهم الجوانب القانونية للأمن السيبراني من أجل تنسيق الأطر القانونية لا سيما من خلال موارده المختلفة الخاصة بالتشريعات المتعلقة بالجرائم السيبرانية³⁵.

خاتمة:

من كل هذا نصل إلى أن الحرب السيبرانية تعد حرباً حقيقية بمفهوم النزاعات المسلحة في القانون الدولي الإنساني، لاعتمادها على الهجمات ولاستهدافها مجمل ما تستهدفه الحرب، كما أنها تلحق أضراراً قد تضاهي في جسامتها أضرار الحروب التقليدية، ما يظهر الحاجة العاجلة في الوقت الحاضر من حيث تحديد مجالات الحماية والأشخاص المحميين من أثار هذه الحرب السيبرانية، ونوع هذه الحماية المقدمة لهذه الفئات المحمية.

كما أن القانون الدولي الإنساني يمكن في شكله الحالي أو بعد تطويره أن ينطبق على الحرب السيبرانية بعد ضبط مدلولها ومجالاتها بشكل دقيق، خاصة أنه في الفضاء السيبراني كما أشار د. حمدون توريه، الذي تتسم كل دقيقة تمضي فيه بالأهمية، فإن الحل الواضح والأمثل يتمثل في تطوير اتفاقيات القانون الدولي الإنساني القائمة، وجعلها أكثر قابلية لتشمل كل أنواع الهجمات وكل أنواع المخاطر والأضرار الناتجة عن هذه الهجمات، خاصة أن إبرام معاهدات جديدة خاصة بالحرب السيبرانية فقط محفوفة بالمشكلات لتدخل هذه الحرب مع الحروب التقليدية؛ كما أن هذه الاتفاقيات تتطلب مداولات مطولة متعددة الأطراف في مرحلة الصياغة، لتفتح بعدها للتوقيع، وبعد هذا يتعين على الأطراف الموقعة المصادقة على المعاهدة قبل أن تدخل حيز التنفيذ، بل وحتى عقب ذلك فإنها لن تكون سارية المفعول إلا بالنسبة إلى تلك البلدان التي صادقت عليها وطبقته، وكل هذا يحتاج إلى وقت طويل، وهو ما سيكون في صالح الجهات الفاعلة والجرائم السيبرانيين³⁶.

ومن التوصيات المقترحة في هذا الشأن أن تضم البلدان القومية صفوفها، بمساهمة من الجهات المعنية، لإدخال التعديلات التالية على القوانين الدولية القائمة للنزاع المسلح:

- يجب على الدول التي تسعى لتطوير قدراتها الدفاعية في مجال الحرب السيبرانية أن تجعل توسيع قدراتها العسكرية مرسوماً مع الحدود الموضوعة لحماية ضحايا النزاعات المسلحة وضحايا الحرب السيبرانية، حيث تعترف بوجود مستوى جديد من "الحد الأدنى الجوهرى من الخدمات" التي تحظى بالحماية من النزاع، وهذا الإجراء سيمنع التدمير والمعاناة بدون داع بين المشاركين في النزاع، وسيؤدي إلى حماية البلدان الأخرى غير المشاركة في هذه الحرب من الضرر،

ووجود هذا المستوى من الاستقرار السيبراني أمر حيوي، لكي لا تضيق فوائد الإنترنت في خضم قوى التكنولوجيا المدمرة.

- كما ينبغي تحديد المقصود بالسلامة الإقليمية المدرجة في ميثاق الأمم المتحدة لتشمل البنى التحتية الحيوية، والإتاحة والمنعة والسرية السيبرانية، وهي مفاهيم تحتاج إلى دقة تحديدها خاصة أن الحرب السيبرانية قد تكون أثارها أشمل وأعم.

- ينبغي إحداث تعديل جوهري على اتفاقيات لاهاي الخاصة بتنظيم وسائل وطرق الحرب، بغرض تحريم استخدام القوات غير النظامية في القتال السيبراني وحظر نقل الهجمات السيبرانية عبر شبكات البلدان المحايدة تحت أي ظرف كان.

- ينبغي تعديل اتفاقيات جنيف بغرض تحريم الهجمات على البنية التحتية الحيوية التي يمكن أن تعطل الاتصالات الأساسية الدنيا وتعرض السكان المدنيين للخطر، خاصة أن تدمير الاتصالات قد يمس الأنظمة الصحية وأنظمة معالجة المياه وغيرها، وهي في النهاية ضرورية لبقاء السكان المدنيين أحياء.

- ينبغي أن يلتزم كل بلد بألا يكون الطرف الذي يبدأ بشن هجوم سيبراني على غيره من البلدان إلا في الحدود الضيقة والمسموح بها دفاعا عن النفس، تجنباً لانتشار هذه الهجمات إلى مجالات ودول ومنظمات، ويكون من الصعب التحكم في أثارها.

- كما يلتزم كل بلد بالتعاون مع غيره ضمن إطار دولي للتعاون لضمان الأمن في الفضاء السيبراني، وتطوير نظام الأمم المتحدة وقوات حفظ السلام ليستوعب مثل هذه الهجمات وهذه الحروب مستقبلاً.

قائمة المصادر والمراجع:

أولا / قائمة المصادر:

أ- الاتفاقيات:

1- الاتفاقية المتعلقة بقوانين وأعراف الحرب البرية (اتفاقية لاهاي الثانية)، 29 يوليو 1899، الرابط الإلكتروني: http://avalon.law.yale.edu/19th_century/hague02.asp.

2- البروتوكول الإضافي لاتفاقيات جنيف الصادر في 12 أغسطس عام 1949 والمتعلق بحماية ضحايا المنازعات الدولية المسلحة (البروتوكول الأول)، 8 يونيو، 1977، الرابط الإلكتروني: www.icrc.org/ihl.nsf/7c4d08d9b287a42141256739003e636b/ff6c8b9fee14a77fdc125641e0052b079

03- قوانين وأعراف الحرب البرية (اتفاقية لاهاي الرابعة)، 18 أكتوبر 1907، الرابط الإلكتروني: http://avalon.law.yale.edu/20th_century/hague04.asp ثانياً / قائمة المراجع:

أ- الكتب:

1- أميرفرج يوسف، مكافحة الإرهاب الإلكتروني، الإرهاب الرقمي في ظل اتفاقية دول مجلس التعاون الخليجي، دار الكتب والدراسات العربية، 2016.

- 2- خالد وليد محمود، الهجمات عبر الانترنت ساحة الصراع الإلكتروني الجديد، الطبعة الأولى، المركز العربي للأبحاث ودراسة السياسات، دون بلد النشر، 2013.
 - 3- د. عادل عبدالصالح، الإرهاب الإلكتروني، القوة في العلاقات الدولية، نمط جديد وتحديات مختلفة، الطبعة الأولى، مركز الدراسات السياسية والاستراتيجية، القاهرة، مصر، 2009.
 - 4- د. عادل عبد الصالح، هل يمثل الإرهاب الإلكتروني شكلاً جديداً من أشكال الصراع الدولي، الطبعة الأولى، مركز الدراسات السياسية والاستراتيجية، القاهرة، مصر، 2017.
 - 5- عباس بدران، الحرب الإلكترونية، الاشتباك في عالم المعلومات، دون طبعة، مركز دراسات الحكومة الإلكترونية، بيروت، 2010.
 - 6- د. علي حسين باكير، الحروب الإلكترونية في القرن الواحد والعشرين، دون طبعة، مركز الجزيرة للدراسات قطر، 2010.
 - 7- محمد سعادي، أثر التكنولوجيا المستحدثة على القانون الدولي العام، الطبعة الأولى، دار الجامعة الجديدة، الإسكندرية، مصر، 2014.
 - 8- نوران شفيق، أثر التهديدات الإلكترونية على العلاقات الدولية، دراسة في أبعاد الأمن الإلكتروني، الطبعة الأولى، المكتب العربي للمعارف، 2016.
- ب- المقالات على مواقع الانترنت:**
- 1- إيهاب شوقي، الحرب السيبرانية حرب المستقبل المفزعة، مقال إلكتروني، 2015/02/19. اطلع عليه بتاريخ 2019/07/04، الرابط الإلكتروني: <http://www.annntv.tv/new/showsubject.aspx?id=101954>
 - 2- الحرب السيبرانية وتداعياتها على الأمن العالمي، الموسوعة الجزائرية للدراسات السياسية والاستراتيجية، دراسات اقليمية، دراسات الشرق الأوسط وشمال أفريقيا ANEM، مقال منشور بتاريخ 9102/60/72، متوفر على الموقع الإلكتروني، اطلع عليه بتاريخ 9102/11/41.
- <https://www.politics-dz.com>
- 3- جانكارلو أ. بارليتتا، ووليام أ. بارليتتا، وفيتالي تسيجيشكو، النزاع السيبراني والاستقرار الجيوسياسي، مقال إلكتروني منشور على الرابط الإلكتروني، جانفي 2011، اطلع عليه بتاريخ 2019/9/5، الرابط الإلكتروني: https://www.itu.int/dms_pub/itu-s/opb/gen/S-GEN-WFS.01-1-2011-MSW-A.docx
 - 4- جودي ر. وستبي، دعوى إلى الاستقرار الجيوسياسي، الاتحاد الدولي للاتصالات، مقال منشور على الرابط الإلكتروني، جانفي 2011، اطلع عليه بتاريخ 2019/7/20، الرابط الإلكتروني: https://www.itu.int/dms_pub/itu-s/opb/gen/S-GEN-WFS.01-1-2011-MSW-A.docx
 - 5- حمدون إ. توريه، البحث عن السلام السيبراني، الاتحاد الدولي للاتصالات، مقال إلكتروني، منشور عام 2011، اطلع عليه بتاريخ 2019/7/20، الرابط الإلكتروني: https://www.itu.int/dms_pub/itu-s/opb/gen/S-GEN-WFS.01-1-2011-MSW-A.docx
 - 6- حمدون إ. توريه، الفضاء السيبراني وتهديد الحرب السيبرانية، الاتحاد الدولي للاتصالات، مقال إلكتروني، اطلع عليه بتاريخ 2019/7/20، الرابط الإلكتروني: https://www.itu.int/dms_pub/itu-s/opb/gen/S-GEN-WFS.01-1-2011-MSW-A.docx
 - 7- حمدون إ. توريه، الاستجابة الدولية للحرب السيبرانية، مقال إلكتروني، اطلع عليه بتاريخ 2019/10/14، https://www.itu.int/dms_pub/itu-s/opb/gen/S-GEN-WFS.01-1-2011-MSW-A.docx
 - 8- حماية الأشخاص المدنيين والسكان في وقت الحرب، المقتطف من القواعد الأساسية لاتفاقيات جنيف وبروتوكولها، اللجنة الدولية للصليب الأحمر، 31 ديسمبر 1988.

www.icrc.org/web/eng/siteeng0.nsf/html/57JMJV

09- عمر محمود اعمر، الحرب الإلكترونية في القانون الدولي الإنساني، دراسات علوم الشريعة والقانون، المجلد 46 عدد 03، 2019، اطلع عليه بتاريخ 2019/10/12، الرابط الإلكتروني.

<https://journals.ju.edu.jo/DirasatLaw/article/viewFile/101907/10621?target=blank>

10- كوردولا دوريجي، لا تقترب من حدود فضائي الإلكتروني، الحرب الإلكترونية والقانون الدولي الإنساني وحماية المدنيين مجلة اللجنة الدولية للصليب الأحمر، مجلد 94 صيف 2012، اطلع عليه بتاريخ 2019/10/12، الرابط الإلكتروني.

https://www.icrc.org/ar/download/file/86667/12825_-get_off_my_cloud_cyber_warfare-opt_05.pdf

11- كوردولا دروغيه المستشارة القانونية في اللجنة الدولية، ما من فراغ قانوني في الفضاء السيبراني، مقال منشور على موقع اللجنة الدولية للصليب الأحمر بتاريخ 2011/08/16، اطلع عليه بتاريخ 2019/10/10، الرابط الإلكتروني.

<https://www.icrc.org/ar/doc/resources/documents/interview/2011/cyber-warfare-interview-2011-08-16.htm>

12- ما هي القيود التي يفرضها قانون الحرب على الهجمات السيبرانية، اللجنة الدولية للصليب الأحمر، مقال منشور على موقع اللجنة بتاريخ 2013/06/28، اطلع عليه بتاريخ 2019/11/10، الرابط الإلكتروني.

<https://www.icrc.org/ar/doc/resources/documents/faq/130628-cyber-warfare-q-and-a-eng.htm>

13- محمد الدوراني، ترجمة: كريم الماجري، قتال غير مرئي، الحرب السيبرانية في الأزمة الخليجية، مركز الجزيرة للدراسات، مقال منشور بتاريخ 2018/05/13، اطلع عليه بتاريخ 2019/10/12، الرابط الإلكتروني.

http://studies.aljazeera.net/mritems/Documents/2018/5/15/5ef5853e7c2f461ea24c2feb73448543_100.pdf

14- هيربرت لين، النزاع السيبراني والقانون الدولي الإنساني، مجلة اللجنة الدولية للصليب الأحمر، 2012/06/30، مقال منشور على الرابط الإلكتروني، اطلع عليه بتاريخ 2019/10/12، الرابط الإلكتروني.

<https://www.icrc.org/ar/international-review/article/cyber-conflict-and-nternational-humanitarian-law>

15- يحيى مفرح الزهراني، الأبعاد الاستراتيجية والقانونية للحرب السيبرانية، مجلة البحوث والدراسات، مجلة دورية أكاديمية دولية نصف سنوية محكمة تعنى بنشر البحوث والدراسات في العلوم الشرعية والقانونية والاقتصادية والاجتماعية والإنسانية، جامعة الوادي، الجزائر، المجلد 14 العدد الأول، الصفحة 237، الرابط الإلكتروني.

<https://www.asjp.cerist.dz/en/downArticle/202/14/1/25280>

الهوامش:

¹ - حمدون إ. - توريه، البحث عن السلام السيبراني، الاتحاد الدولي للاتصالات، مقال منشور عام 2011، اطلع عليه بتاريخ 2019/7/20، الرابط الإلكتروني.

https://www.itu.int/dms_pub/itu-s/opb/gen/S-GEN-WFS.01-1-2011-MSW-A.docx

² - كوردولا دوريجي، لا تقترب من حدود فضائي الإلكتروني، الحرب الإلكترونية والقانون الدولي الإنساني وحماية المدنيين، مجلة اللجنة الدولية للصليب الأحمر، مجلد 94 صيف 2012، ص 03، اطلع عليه بتاريخ 2019/10/12، الرابط الإلكتروني.

https://www.icrc.org/ar/download/file/86667/12825_-get_off_my_cloud_cyber_warfare-opt_05.pdf

- ³ - يحيى مفرح الزهراني، الأبعاد الاستراتيجية والقانونية للحرب السيبرانية، مجلة البحوث والدراسات، مجلة دورية أكاديمية دولية نصف سنوية محكمة تعنى بنشر البحوث والدراسات في العلوم الشرعية والقانونية والاقتصادية والاجتماعية والإنسانية، جامعة الوادي، الجزائر، المجلد 14، العدد 1، الصفحة 237، الرابط الإلكتروني: <https://www.asjp.cerist.dz/en/downArticle/202/14/1/25280>
- ⁴ - محمد سعادي، أثر التكنولوجيا المستحدثة على القانون الدولي العام، الطبعة الأولى، دار الجامعة الجديد، الإسكندرية، مصر، 2014، ص 13.
- ⁵ - إيهاب شوقي، الحرب السيبرانية حرب المستقبل المفزعة، مقال إلكتروني، 2015/02/19، اطلع عليه بتاريخ 2019/07/04، الرابط الإلكتروني: <http://www.annetv.tv/new/showsubject.aspx?id=101954>
- ⁶ - هريبرت لين، النزاع السيبراني والقانون الدولي الإنساني، مجلة اللجنة الدولية للصليب الأحمر، مقال منشور على الرابط الإلكتروني 2012/06/30، اطلع عليه بتاريخ 2019/10/12، الرابط الإلكتروني: <https://www.icrc.org/ar/international-review/article/cyber-conflict-and-international-humanitarian-law>
- ⁷ - خالد وليد محمود، الهجمات عبر الانترنت ساحة الصراع الإلكتروني الجديد، الطبعة الأولى، المركز العربي للأبحاث ودراسة السياسات، دون بلد المنشأ، 2013، ص 20.
- ⁸ - كوردولا دوريجي، المرجع السابق، ص 538.
- ⁹ - حمدون إ. توريه، الفضاء السيبراني وتهديد الحرب السيبرانية، الاتحاد الدولي للاتصالات، مقال إلكتروني، منشور في 2011/01/01، اطلع عليه بتاريخ 2019/7/20، الرابط الإلكتروني: https://www.itu.int/dms_pub/itu-s/opb/gen/S-GEN-WFS.01-1-2011-MSW-A.docx
- ¹⁰ - جانكارلو أ. بارليتتا، ووليام أ. بارليتتا، وفيتالي تسيجيشكو، النزاع السيبراني والاستقرار الجيوسياسي، مقال إلكتروني منشور على الرابط الإلكتروني، جانفي 2011، اطلع عليه بتاريخ 2019/9/5، الرابط الإلكتروني: https://www.itu.int/dms_pub/itu-s/opb/gen/S-GEN-WFS.01-1-2011-MSW-A.docx
- ¹¹ - الحرب السيبرانية وتداعياتها علي الأمن العالمي، الموسوعة الجزائرية للدراسات السياسية والاستراتيجية، 9102/60/72، دراسات اقليمية، دراسات الشرق الأوسط وشمال أفريقيا ANEM، مقال متوفر على الموقع الإلكتروني، اطلع عليه بتاريخ 9102/11/41.
- ¹² - الحرب السيبرانية وتداعياتها علي الأمن العالمي، المرجع السابق.
- ¹³ - د. عادل عبد الصادق، هل يمثل الإرهاب الإلكتروني شكلا جديدا من أشكال الصراع الدولي، مركز الدراسات السياسية والاستراتيجية، القاهرة، 2017، ص 06.
- ¹⁴ - الحرب السيبرانية وتداعياتها علي الأمن العالمي، المرجع السابق.
- ¹⁵ - عباس بد ران، الحرب الإلكترونية، الاشتباك في عالم المعلومات، بيروت، مركز دراسات الحكومة الإلكترونية، 2010، ص 22.
- ¹⁶ - نوران شفيق، أثر التهديدات الإلكترونية على العلاقات الدولية دراسة في أبعاد الأمن الإلكتروني، الطبعة الأولى، المكتب العربي للمعارف، 2016، ص 9.
- ¹⁷ - د. علي حسين باكير، الحروب الإلكترونية في القرن الواحد والعشرين، قطر، مركز الجزيرة للدراسات، 2010، ص 23.

- 18 - محمد الدوراني، قتال غير مرئي، الحرب السيبرانية في الأزمة الخليجية، مركز الجزيرة للدراسات ترجمة كريم الماجري، مقال منشور بتاريخ 2018/05/13، اطلع عليه بتاريخ 2019/10/12، الرابط الإلكتروني. http://studies.aljazeera.net/mritems/Documents/2018/5/15/5ef5853e7c2f461ea24c2feb73448543_100.pdf
- 19 - بقلم جانكارلو أ. بارليتتا، ووليام أ. بارليتتا، وفيتالي تسيجيشكو، المرجع السابق، ص 55.
- 20 - كوردولا دوريجي، المرجع السابق، ص 542.
- 21 - جودي ر. وستبي، دعوة إلى الاستقرار الجيوسبراني، الاتحاد الدولي للاتصالات، مقال منشور على الرابط الإلكتروني، جانفي 2011، اطلع عليه بتاريخ 2019/7/20، الرابط الإلكتروني. https://www.itu.int/dms_pub/itu-s/opb/gen/S-GEN-WFS.01-1-2011-MSW-A.docx
- 22 - أمير فرج يوسف، مكافحة الإرهاب الإلكتروني، الإرهاب الرقمي في ظل اتفاقية دول مجلس التعاون الخليجي، دار الكتب والدراسات العربية، 2016، ص 253.
- 23 - حماية الأشخاص المدنيين والسكان في وقت الحرب، المقتطف من القواعد الأساسية لاتفاقيات جنيف وبروتوكولها، اللجنة الدولية للصليب الأحمر، 31 ديسمبر 1988 www.icrc.org/web/eng/siteeng0.nsf/html/57JM.JV
- 24 - البرتوكول الإضافي الثاني الملحق باتفاقيات جنيف والمتعلق بحماية ضحايا المنازعات المسلحة غير الدولية، 8 حزيران/يونيه 1977، تاريخ بدء النفاذ، 7 كانون الأول/ديسمبر 1978، الرابط الإلكتروني. <https://www.legal-tools.org/doc/0453fb/pdf/>
- 25 - جودي ر. وستبي، المرجع السابق، ص 65.
- 26 - كوردولا دروغيه المستشارة القانونية في اللجنة الدولية، ما من فراغ قانوني في الفضاء السيبراني، مقال منشور على موقع اللجنة الدولية للصليب الأحمر بتاريخ 2011/08/16، اطلع عليه بتاريخ 2019/10/10، الرابط الإلكتروني. <https://www.icrc.org/ar/doc/resources/documents/interview/2011/cyber-warfare-interview-2011-08-16.htm>
- 27 - عمر محمود اعمر، الحرب الإلكترونية في القانون الدولي الإنساني، دراسات علوم الشريعة والقانون، المجلد 46 عدد 03، 2019، اطلع عليه بتاريخ 2019/10/12، الرابط الإلكتروني. https://journals.ju.edu.jo/DirasatLaw/article/viewFile/101907/10621?target=_blank
- 28 - جودي ر. وستبي، المرجع السابق، ص 68.
- 29 - حماية الأشخاص المدنيين والسكان في وقت الحرب، المرجع السابق.
- 30 - كوردولا دوريجي، المرجع السابق، ص 541.
- 31 - ما هي القيود التي يفرضها قانون الحرب على الهجمات السيبرانية، اللجنة الدولية للصليب الأحمر، مقال منشور على موقع اللجنة بتاريخ 2013/06/28، اطلع عليه بتاريخ 2019/11/10، الرابط الإلكتروني. <https://www.icrc.org/ar/doc/resources/documents/faq/130628-cyber-warfare-q-and-a-eng.htm>
- 32 - كوردولا دوريجي، المرجع السابق، ص 574.
- 33 - حمدون إ. توريه، الاستجابة الدولية للحرب السيبرانية، مقال إلكتروني ص 102، اطلع عليه بتاريخ 2019/10/14.
- 34 - حمدون إ. توريه، الاستجابة الدولية للحرب السيبرانية، المرجع السابق، ص 105. https://www.itu.int/dms_pub/itu-s/opb/gen/S-GEN-WFS.01-1-2011-MSW-A.docx

³⁵ - عادل عبدالصادق، الإرهاب الإلكتروني: القوّة في العلاقات الدولية، نمط جديد وتحديات مختلفة، القاهرة، مركز الدراسات السياسية والاستراتيجية، الطبعة الأولى، 2009، ص 156.

³⁶ - حمدون إ. توريه، الفضاء السيبراني وتهديد الحرب السيبرانية، المرجع السابق، ص 69.