مجلـــة العلـــوم التربـــوية والدراســـات الإنســـانيـــة
ISSN: 2709-0302 (online)

Humanities and Educational Sciences Journal
ISSN: 2617-5908 (print)

أنسنة الحرب الإلكترونية(*)

أ.د/ محمد محمد سعيد الشعيبي
أستـاذ بكليــة الحقوق – جــامعة تعز
رئيس الجامعة

د/نادية محمد سعيد النقيب
أستاذ مشارك بكلية الحقوق - جامعة عدن

*) تاريـخ تسليم البحث 1/8/2022 تاريـخ قبوله للنشر 24/8/2022
*) موقع المجلة: http://hesj.org/ojs/index.php/hesj/index

أنسنة الحرب الإلكترونية

أ.د/ محمد محمد سعيد الشعيبي
أستاذ بكلية الحقوق
جامعة تعز
د/ نادية محمد سعيد النقيب
أستاذ مشارك بكلية الحقوق
جامعة عدن

ملخص

أنسنة الحرب الإلكترونية مصطلح حديث حداثة الانتقال النوعي الذي أبدعه التطور الإلكتروني والمدى الذي بلغه في التأثير على حياة الإنسان سلما وحربا، وأهداف البحث تجتمع في سؤال المعالجة النظرية والعملية لتأطير هذا المستجد في مجال القانون الدولي الإنساني، ثم في تفعيل قواعد القانون الدولي الإنساني وحقوق الإنسان لتشمل الحماية للإنسان أثناء النزاع الإلكتروني، مع بيان مفهوم الحرب الإلكترونية، ومدى كفاية قواعد القانون الدولي لشمول هذا النوع من الحروب.

وبحسب مادة الدراسة تنقل البحث بين المنهج الوصفي في عرض المعطيات المتداولة للمضمون، والمنهج التحليلي في تفكيك الرؤى النظرية المعروضة، والمنهج النقدي في المناقشة والاستنتاج.

توصل البحث إلى أن الخلاف في إمكانية تطبيق القانون الدولي الإنساني على النزاعات الإلكترونية لا زال في بواكيره، ويحتاج المزيد من الإثراء الكفيل بتجلية متعلقات الموضوع، وأن غياب الإشارة في القانون الدولي الإنساني إلى الاستهداف المباشر للأشخاص والأعيان المدنية للعمليات الدائرة في الفضاء الإلكتروني، لا يعني أن قواعد القانون الدولي الإنساني لا تغطي وسائل وأساليب الحرب الإلكترونية.

ثم إن صفة العمومية التي يتمتع بها القانون الدولي لحقوق الإنسان يجعله شبه قادر على احتواء وفهم أغلب ظواهر الحرب الإلكترونية وعواقبها.

ويوصي البحث بضرورة تحليل مختلف العناصر والظروف لتحديد إمكانية تطبيق القانون الدولي الحالي على النزاعات الإلكترونية، لاعتبار إشكالات التطبيق يمكن تجاوزها من خلال إبرام اتفاقية دولية خاصة بالحرب الإلكترونية.

وضرورة تكاتف الجهود الدولية والإقليمية، من أجل وضع تنظيم دولي ملزم للدول ينظم النزاعات الدولية المسلحة التي يتم فيها استخدام الأسلحة الإلكترونية، وتمنع التسلح السيبراني خلافًا لمبادئ القانون الدولي الإنساني.

ويوصي البحث بالاهتمام بالشروط التي وضعها دليل تالين الذي نص على "أن أطراف النزاع ملزمة بمراعاة آثار الأسلحة السيبرانية على العسكريين والمدنيين على حد سواء".

الكلمات المفتاحية: أنسنة – الحروب – الالكترونية.

Humanization of Electronic Warfare

Prof. Dr. Mohammed Mohammed Saeed Al-Shuaibi
Professor at the Faculty of Law Taiz University

Dr. Nadia Mohammad Saeed Al-Naqeeb
Associate Professor at the Faculty of Law
Aden University

Abstract:

Humanization of electronic warfare is a modern term, such as the modernity of qualitative transition created by electronic development and the extent it reached in affecting human life in peace as well as in war. The objectives of the research meet in the question of theoretical and practical treatment to frame this modern term in the field of international humanitarian law, then in activating the rules of international humanitarian law and human rights to include the protection for Man, during the electronic conflict, showing the concept of electronic war, and the extent of the sufficiency of the rules of international law to include this type of war.

According to the subject matter of the study, the research moves between the descriptive approach in presenting the current data of the content, the analytical approach in deconstructing the presented theoretical perspectives, and the critical approach in discussion and conclusion.

The research has concluded that the disagreement over the applicability of international humanitarian law on electronic disputes is still in the beginning and needs more enrichment to clarify the subject matter and that the absence of the reference in the international humanitarian law to the direct targeting of persons and civilian objects and the operations in the Cyberspace, does not mean that the rules of the international humanitarian law do not cover the methods and techniques of electronic warfare.

The inclusiveness feature of the international humanitarian law makes it almost capable to include and understand most of the phenomena of electronic warfare and its consequences.

The research recommends the necessity of analyzing various elements and conditions to determine the possibility of applying the current international law on the electronic disputes, for considering application problems can be by passed through concluding an international agreement related to electronic warfare.

The need for the collaboration of regional and international efforts in order to set out an international organization binding for the countries that regulate international armed disputes in which electronic weapons are used, and it prevents cyber weapons contrary to the principles of international humanitarian law.

The research recommends paying attention to the conditions set by the Tallinn Guide, which states “that the dispute parties are committed to consider the effects of cyber weapons on both the military and civilian personnel.

Keywords: Humanization, Electronic Warfare.

مقدمة

التعريف بالموضوع وأهميته:

أحدثت التطورات العلمية والتكنولوجية التي وصل إليها الإنسان تحولاً كبيرًا في وسائل القتال والصراعات البشرية، وآخر ما شهده العالم منها دخول وسائل الاتصال الإلكتروني ساحة الحروب، وما أحدثته من تغيير عملاق في القطاعات الأمنية والعسكرية والسياسية، الأمر الذي أدى إلى نقلة فارقة في مفهوم الصراع؛ فبعد أن كانت الحشود العسكرية والآلات الحربية هي لغة الحرب ووسيلتها أرضًا وجوًا وبحرًا، دخلت وسائل الاتصال الإلكتروني ساحتها لتضيف بعدًا جديدًا من أبعاد الصراع البشري، وهو ما يعرف اليوم بالحرب الإلكترونية Electronic Warfare، وفي موضوعها يعرض هذا البحث إمكان تطبيق قواعد القانون الدولي الإنساني والقانون الدولي لحقوق الإنسان وما في سياقهما من البروتوكولات والمبادئ والاتفاقيات على الحرب الإلكترونية، ويرصد البحث المدى التطبيقي الذي يصله شمول تلك القوانين والمبادئ للحرب الإلكترونية، وإمكانية أنسنة هذا النوع من الحروب بمعنى إدخالها في مشمولات القانون الدولي الإنساني، والقانون الدولي لحقوق الإنسان لما أضحى لها من الأهمية والتأثير.

إشكالية البحث:

لأهمية الصراع الإلكتروني وعلاقته المؤثرة بالإنسان، ولكونه من المستجدات التي لم تعرف من قبل، ولم تكن محلاً لمدارسات قانونية متخصصة؛ يعمل هذا البحث لمعالجة الإمكان النظري والعملي لتأطير هذه الظاهرة في مجال القانون الدولي الإنساني، ويسير باتجاه اختبار إمكان تفعيل قواعد القانون الدولي الإنساني وحقوق الإنسان لتشمل الحماية للإنسان في واحد من أهم ما يؤثر في حياته سلباً، ويتتبع لأجل ذلك موقف الفقه المعاصر من شمول القانون الدولي الإنساني وقانون حقوق الإنسان لمتغير حادث لم يكن له وجود في واقع الحروب وآثارها.

أسئلة البحث:

يسعى البحث للإجابة عن الأسئلة التالية:

١. ما هي الحرب الإلكترونية؟ وما آثارها، وهل يستوعب مفهوم الحرب الوارد في القواعد التقليدية الحرب الإلكترونية؟

٢. ما هو موقف الفقه والوثائق الدولية من خضوع الحرب الإلكترونية لقواعد القانون الدولي الإنساني؟ وما مدى كفاية تلك القواعد لاستيعاب مفاهيم الحرب الإلكترونية؟

٣. ما إمكانية تطبيق القانون الدولي لحقوق الإنسان على الحرب الإلكترونية؟ وما مدى ملاءمة تطبيقه؟

٤. هل يمكن إخضاع أسلحة الحرب الإلكترونية للقواعد الدولية المتعلقة بحظر وتقييد بعض الأسلحة أم لا؟

أهداف البحث:

يسعي البحث لبيان مفهوم الحرب الإلكترونية باعتبارها نوعًا جديدًا من الحروب التي تهدد العلاقات الدولية والسلم والأمن الدوليين، لاسيما بعد التطور التقني الذي شهدته الدول في مجال الإنترنت، مع بيان مدى خضوعه لقواعد القانون الدولي الإنساني والقانون الدولي لحقوق الإنسان، ومدى كفاية تلك القواعد وملائمتها لشمول الحرب الإلكترونية قانونًا، كل ذلك في ضوء آراء الفقه والقضاء والاتفاقيات الدولية.

منهج البحث:

يعتمد البحث على المنهج التحليلي من خلال تتبع مفهوم الحرب الإلكترونية والوقوف عند تحليل النصوص وبيان مدى تطبيق قواعد القانون الدولي الإنساني والقانون الدولي لحقوق الإنسان على الحرب الإلكترونية، لمعرفة مدي فاعليته وإمكانية تطبيقه على النزاعات ذات الطابع الإلكتروني، ويعتمد أيضًا على المنهج الوصفي من خلال وصف القواعد الدولية التقليدية وبيان مدى انطباقها على الحرب الإلكترونية.

خطة البحث:

وزعت محاور البحث في مقدمة سبقت الإشارة لأهم مضامينها وتمهيد ومبحثين رئيسيين تحتهما مطالب، وخاتمة بأهم نتائج البحث وتوصياته، وفهرس بأهم المراجع على النحو التالي:

التمهيد: في مفهوم الحرب الالكترونية وآثارها، وفيه:

أولاً: مفهوم الحرب الإلكترونية

ثانياً: أهم آثار الحرب الإلكترونية على الإنسان

المبحث الأول: تطبيق قواعد القانون الدولي الإنساني والمبادئ الأساسية على الحرب الإلكترونية، وفيه:

المطلب الأول: نطاق الحرب الإلكترونية

المطلب الثاني: موقف الفقه من تطبيق القانون الدولي الإنساني على الحرب الإلكترونية

المبحث الثاني مدى تطبيق المبادئ الأساسية والقواعد التقليدية وقانون حقوق الإنسان على الحرب الإلكترونية.

وفيه:

المطلب الأول: مدى ملائمة تطبيق المبادئ الأساسية على الحرب الإلكترونية

المطلب الثاني: مدى تطبيق القواعد التقليدية على الحرب الإلكترونية

المطلب الثالث: إمكانية تطبيق القانون الدولي لحقوق الإنسان على الحرب الإلكترونية

خاتمة:

مراجع البحث:

التمهيد

في مفهوم الحرب الإلكترونية وآثارها

أولاً: مفهوم الحرب الإلكترونية

الحرب لفظ مؤنث، وقد يذكر بمعنى القتال، ومعناه الصراع بين فئتين أو أكثر، وهي صدام مسلح يعتمد على قوة الآلة الحربية وقوة الإنسان المادية، ثم ظهرت لها صورة الصراع الخالي من صدام القوة، بما عرف بالحرب الباردة، وهي أن يكيد كل من الطرفين المتعاديين لخصمه دون أن يؤدي ذلك إلى تصادم(١).

واليوم يخرج لنا التقدم العلمي نوعاً ثالثاً من الحروب هو حرب المعلومات، أو الحرب الإلكترونية، ولا يوجد للحرب الإلكترونية تعريف محدد ودقيق متفق عليه دوليا، إنما اجتهد عدد من الباحثين فعرفها بأنها "نوع من النزاعات يحدث في الفضاء الإلكتروني، وتكون ذات طابع سياسي يتمثل بمجموعة من الإجراءات التي تقوم بها إحدى الدول بغية اختراق أجهزة الكمبيوتر والشبكات العائدة لدول أخري بقصد إلحاق الضرر بها"(٢).

ومما عرفت به كذلك أنها "مجموعة من الإجراءات الإلكترونية التي تستخدم فيها النظم والوسائل التقنية للاستطلاع والاشعاعات الكهرومغناطيسية الصادرة من نظم العدو ومعداته الإلكترونية والاستخدام المتعمد للإشعاع والتأثير المباشر على شكل النظم الحربية(٣).

كما يستخدم هذا المصطلح للإشارة إلى وسائل وأساليب القتال التي تتألف من عمليات في الفضاء الإلكتروني ترقى إلى مستوى النزاع المسلح، أو تجري في سياقه ضمن المعنى المقصود في القانون الدولي الإنساني(٤).

ويذهب جانب من الفقه إلى أن الحرب الإلكترونية (إجراء، أو استعداد لإجراء عمليات عسكرية بالاعتماد على المبادئ والآليات المعلوماتية، ما يعني تعطيل، إن لم يكن تدمير، نظم المعلومات والاتصالات على أوسع نطاق لتشمل حتى العقيدة العسكرية التي يعتمد عليها العدو لتحديد أهدافه والتحديات التي تواجهه)(٥).

---

(١) انظر: المعجم الوسيط، مجمع اللغة العربية بالقاهرة، ١٦/١.

(٢) الحرب الإلكترونية، مقال منشور في موقع ويكيبيديا.
http://ar.wikipedia.org/wiki/%D8%AD%D8%B تاريخ الزيارة ٢٠٢٠/٧/١.

(٣) فيصل محمد الغفار، الحرب الإلكترونية، ط١، الجنادرية للنشر والتوزيع ، الأردن، لبنان، ٢٠١٦ ، ص٦.

(4) ما هي القيود التي يفرضها قانون الحرب على الهجمات السيبرانية؟ اللجنة الدولية للصليب الأحمر، ٢٨-٦.
https://www.icrc.org/ara/resources/documents/faq/130628-cyber-warfare-q-and-a-eng.htm
2013 Schmitt, M., (2013), Tallinn Manual on the International Law

(5)John Arquilla and David Ronfeldt, Cyberwar Is Coming, Comparative Strategy, Vol.12, No.2, Spring 1993, P.146.

ويمكن تعريف الحرب الإلكترونية بأنها: عبارة عن هجمات تتم بواسطة استخدام الكمبيوتر أو الشبكات أو الأنظمة ذات الصلة، وتهدف إلى تعطيل أو تدمير أنظمة الإنترنت، أو الممتلكات أو الوظائف الحاسوبية الخاصة بالعدو.

ثانياً: أهم آثار الحرب الإلكترونية على الإنسان

لنقف على آثار الحرب الإلكترونية ينبغي التنبيه إلى أن مصطلح الحرب الإلكترونية يغطي مجموعة واسعة من الإجراءات تتراوح بين المجسمات البسيطة المستخدمة لمحو المواقع على شبكة الإنترنت، والحرمان من الخدمة، والتجسس والتدمير، وعلى نحو مماثل يستخدم لتغطية مجموعة واسعة من السلوكيات(١).

وسعة الوسائل والأهداف في الحرب الإلكترونية ينعكس على آثارها التي تغطي جوانب ممتدة من مصالح الإنسان وحركته في الحياة، ومعلوم مدى ارتباط مصالح الإنسان المعاصر بشبكة المعلومات التي اقتحمت كل خفايا حياته كفرد، ومدى علاقتها بالبنى التحتية للمدن، وهي في التأثير تشمل المجتمع والدولة، ونسبة الضرر الجزئي الذي تحدثه الحرب التقليدية لا يقل عن أضرار الحرب الإلكترونية.

وفي الحرب الإلكترونية تكون الدولة/ الدول الطرف الرئيس فيها، عندما توظف أجهزتها الحاسوبية وشبكاتها العنكبوتية للقيام بهجمات ضد دولة أخرى مستهدفة منظومة حواسيبها ونظم معلوماتها المتعلقة بالبنية التحتية الحيوية سواء كانت مدنية أو عسكرية(٢).

والهجوم على البنى التحتية يخلف أضرارًا كاسحة تدمر الكثير من المصالح الحيوية للفرد والمجتمع والدولة، من ناحية أخرى، لا تقتصر قواعد الاشتباك في الحرب الإلكترونية على الدول، إنما أضيف إليها فاعلون من غيرها، منهم الأفراد العاديون الذين يكون بمقدورهم امتلاك وسائل القوة السيبرانية، ويتمتعون بمهارات فنية وتقنية تمكنهم من ابتكار وتطوير برامج إلكترونية رقمية معقدة لاختراق المواقع والشبكات وشن الهجمات السيبرانية، وهم ما اصطلح على تسميتهم ب(الهاكرز) أو (القراصنة)، أو الميليشيات السيبرانية)(٣).

---

(١) انظر:
Joseph S. Nye, Cyber War and Peace, project syndicate, 10 April 2012, p.2
http//:www.project-syndicate.org/commentary/cyber-war-and-peace

(٢) صفات أمين سلامة، أسلحة حروب المستقبل بين الخيال والواقع، أبو ظبي، مركز الامارات للدراسات والبحوث الاستراتيجية، ٢٠١١، ص ٩.

(٣) التفاصيل حول هذه المجموعات من غير الدول والنشاطات التي تقوم بها، انظر:
Nicolo Bussolati, The Rise of Non-State Actors in Cyberwarfare, in Jens David Ohlin, Kevin Govern and Claire Finkelstein (eds.), Cyberwar: Law and Ethics For Virtual Conflicts, (Oxford: Oxford University Press, 2015), P. 106.
عبد الله بن عبدالعزيز العجلان، الإرهاب الإلكتروني في عصر المعلومات، بحث مقدم إلى المؤتمر الدولي الأول حول "حماية أمن المعلومات والخصوصية في قانون الإنترنت"، و المنعقد بالقاهرة، يونيو ٢٠٠٨م.

كانت تلك إشارة موجزة لمفهوم الحرب الإليكترونية وأهم آثارها لتكون بمثابة التوطئة بين يدي هذه الدراسة، وفي المبحثين التاليين عرض للجانب التطبيقي لقواعد القانون الدولي الإنساني والمبادئ الأساسية من حيث الإمكانية النظرية والمدى المجالي لتفعيله في حماية الإنسان مهما تنوعت صور الحروب واختلفت وسائلها.

المبحث الأول

تطبيق قواعد القانون الدولي الإنساني والمبادئ الأساسية على الحرب الإلكترونية

يسعى القانون الدولي الإنساني أو (قانون النزاعات) إلى تحقيق التوازن بين قاعدة الضرورة العسكرية والمتطلبات الإنسانية، وهذا التوازن يهدف لحماية الإنسان من كوارث النزاعات المسلحة، فهل يمكن تفعيل هذا التوازن بأهدافه السامية التي لا خلاف فيها على الحرب الإلكترونية؟

بداية نذكر بأن القانون الدولي الإنساني قائم على أساس اتفاقيات لاهاي (١٨٩٩ و١٩٠٧) واتفاقيات جنيف الأربع لعام (١٩٤٩م) وبروتوكليها الملحقين بها، ويسعى إلى تقييد مبدأ الضرورة العسكرية في حالة تجاوزه الطابع الإنساني في وسائل القتال، وبالتطور الحاصل في الوقت الحالي وتطور وسائل الحرب وظهور وسائل حرب إلكترونية حديثة يمكن التحكم بها عن بعد، يثار التساؤل حول مدى إمكانية تطبيق مبادئ القانون الدولي الإنساني والقانون الدولي لحقوق الإنسان والمبادئ الأساسية على هذه الوسائل، وسأبين ذلك في مطلبين، الأول عن النطاق ببعديه الزماني والشخصي للحرب الإلكترونية، باعتبار الحديث عن النطاقين الزمني والشخصي مقدمة ضرورية لمعرفة المجال الحيوي للقانون، والثاني عن موقف الفقه من تطبيق القانون الدولي الإنساني على الحرب الإلكترونية بمقارنة تطوف على أقوالهم وأدلتهم بغية الوصول إلى الرأي الأكثر قوة وملائمة.

المطلب الأول

نطاق الحرب الإلكترونية

لا يمكن الحديث عن تطبيق قواعد القانون الدولي الإنساني على الحرب الإلكترونية بدون الإشارة إلى النطاقين الزمني والشخصي لهذه الحروب.

ومعلوم أن القانون الدولي الإنساني أحد فروع القانون الدولي العام، وهو: "مجموعة من القواعد الدولية العرفية والمكتوبة، التي تهدف إلى حماية المحاربين والمدنيين أثناء النزاعات المسلحة، لاعتبارات إنسانية، وصيانة الأموال التي ليس لها علاقة مباشرة بالعمليات العسكرية أو مجموعة القواعد القانونية، العرفية أو المكتوبة، التي تم التوصل إليها، بهدف حماية حقوق الإنسان، وحرياته الأساسية أثناء النزاعات المسلحة، تلك القواعد والأعراف المكتوبة أصبحت تسمى بالقانون الدولي الإنساني، الذي يتضمن في معناه الواسع النصوص القانونية الدولية التي تؤمن الحماية للفرد"[١].

(١) محمد الطراونة: القانون الدولي الإنساني- النص وآليات التطبيق على الصعيد الوطني الأردني، مركز عمان لدراسات حقوق الإنسان، عمان- الأردن(٢٠٠٣)، ص ٣٣.

ويهدف القانون الدولي الإنساني إلى الحد من آثار النزاعات المسلحة الدولية وغير الدولية وحماية السكان المدنيين والأهداف المدنية من خلال وضع القواعد والضوابط التي تنظم وتحكم سير العمليات العسكرية.

وهنا يتكرر السؤال عن مدى إمكانية تطبيق القانون الدولي الإنساني على النزاعات الجديدة أو بالأحرى النزاعات الإلكترونية، حيث إنه لا تملك دولة من الدول القدرة على فرض سيادتها وسيطرتها على الفضاء بشكل كامل مع إمكان استخدامها بشكل يضر بالإنسانية!.

ولأجل التخفيف والحد من الخسائر الناجمة عن النزاعات الإلكترونية سعت بعض الدول إلى اعتبارها نزاعات مسلحة ويطبق عليها قانون الحرب المطبق على النزاعات التقليدية، غير أن الجدل الفقهي لا يزال قائمًا حول مسألة تطبيق القانون الدولي الإنساني على الحروب الإلكترونية، ولكل اتجاه حججه، وهذا ما نمهد له بالحديث عن النطاقين الزمني والشخصي للحروب الإليكترونية من خلال الجزئيتين التاليتين:

النطاق الزمني للحرب الإلكترونية

بموجب اتفاقيات جنيف فإنه يتم تحديد تطبيق القانون الدولي الإنساني منذ بداية النزاع المسلح سواء تم الإعلان عنه أو لم يتم ذلك[١]، وقد تضمنت المادة (٥) من اتفاقية جنيف الأولى على أنه: "بالنسبة للأشخاص المحميين الذين يقعون في قبضة العدو، فتطبق هذه الاتفاقية إلى أن تتم إعادتهم إلى أوطانهم"، وأيضا نصت المادة (٦) من الاتفاقية الرابعة على أن (تطبق هذه الاتفاقية بمجرد بدء أي نزاع ...) ويتم تطبيق هذه الاتفاقيات في أراضي الدول الأطراف في النزاع بعد عام واحد من توقف العمليات الحربية[٢].

يفهم من تلك النصوص أن القانون الدولي الإنساني يحدد نطاقاً زمنيًا لتطبيق مواده على النزاع المسلح، وهو البداية الفعلية للحرب أعلن عنها أم لم يعلن، والمجال الزمني لمن وقع في قبضة العدو من المشمولين بالحماية القانونية هو تاريخ عودتهم إلى أوطانهم، فإذا توقفت الحرب فالاتفاقيات ساري العمل بها بعد عام من توقف العمليات العسكرية.

وإذا كانت الدول تستخدم وسائل حرب إلكترونية، كأن تبدأ دولة ما بالتعدي على الأنظمة المعلوماتية، أو هددت أمن وسلامة واستقرار دولة أخرى، كأن تقوم بتعطيل الجهاز الحكومي الإلكتروني، أو استخدمت برامج التجسس والهكر للاستيلاء على معلومات عسكرية حساسة للدولة، أو قامت بقصف منشآت عسكرية عن بعد باستخدام طائرة بدون طيار، ففي هذه الحالة كيف سيتم تحديد بداية النزاع المسلح الدولي وسريان اتفاقيات جنيف لعام (١٩٤٩م) هل من بداية عمليات

(١) جان بكتيه، مبادئ القانون الدولي الإنساني، بحث منشور في كتاب محاضرات في القانون الدولي الإنساني، خرير شريف غتلم، منشورات اللجنة الدولية للصليب الأحمر، ص ٤٩. انظر أيض: ضوابط تحكم الحرب، مدخل للقانون الدولي الإنسانية ص ١١١.

(٢) المادة (٥) من اتفاقية جنيف الأول لعام ١٩٤٩. والمادة (٦) من اتفاقية جنيف الرابعة لعام ١٩٤٩.

التعدي على البيانات المعلوماتية أم يتطلب ذلك وجود هجوم عسكري يلحق آثاراً مادية من تدمير البنى التحتية للدولة الطرف في النزاع؟

للإجابة على السؤال يمكن القول إن النطاق الزمني للحرب الإلكترونية يبدأ مع أول عمليات التعدي على المعلومات الرقمية، ولا يشترط للحكم ببداياته انتظار آثاره المادية على الأرض، وطبقاً لتقرير اللجنة الدولية فإن العمليات السيبرانية التي تلجأ لها الدول في أثناء النزاعات المسلحة هي وسائل مطابقة لأي أسلحة أو وسائل أو أساليب حرب أخرى تلجأ إليها الدول المتحاربة في النزاع سواء كانت جديدة أم قديمة وتكون خاضعة في تنظيمها للقانون الدولي الإنساني(١).

هذا عن النطاق الزمني، والقول فيه مبني في الأساس على ما يترجح في أصل مسألة المبحث وهي تطبيق قوانين النزاعات الحربية التقليدية على الحرب الإلكترونية، وإنما اقتضى تراتب البحث أن نبدأ بالحديث عن النطاقين الزمني والشخصي.

النطاق الشخصي للحرب الإلكترونية

النطاق الشخصي يعني جملة من يستهدفون بالحماية القانونية أثناء النزاع الإلكتروني، وهم المتضررون من النزاع المسلح، سواء كانوا مدنيين أم مقاتلين، وهذا ما يطلق عليه النطاق الشخصي للقانون، والفئات المحمية بموجب القانون المذكور وبموجب اتفاقيات جنيف (١٩٤٩م)، هم الجرحى والمرضى والمنكوبون في البحار، وأسرى الحرب والمدنيون، والمفقودون والقتلى.

يمكن القول إن الحماية التي فرضتها اتفاقيات جنيف الأربع لعام (١٩٤٩م)، مبنية على أساس مبدأ حماية الأشخاص المشمولين بالحماية بموجب هذه الاتفاقيات، ومعاملتهم معاملة إنسانية بدون تمييز على أساس الجنس أو الدين أو الجنسية أو اختلافات أخرى، وهذا ما نصت عليه (المواد: (١٢) من الاتفاقيتين الأولى والثانية، و(١٦) من الاتفاقية الثالثة، و(٢٧) من الاتفاقية الرابعة.

حتى في حالة عدم وجود قاعدة قانونية لحماية الفئة المعنية بالقانون الدولي الإنساني في وقت النزاع تبقى الحماية القانونية مكفولة لهم بموجب القانون العربي ومبادئ الإنسانية، والضمير العام، وهذا ما نصت عليه المادة (١) الفقرة (٢) من البروتوكول الإضافي الأول لعام (١٩٧٧م)، وكذلك أشارت اتفاقية (١٩٨٠م) الخاصة بتقييد استعمال الأسلحة التقليدية إلى أنه يتوجب أن يظل المدنيون والمقاتلون متمتعين في كل الأوقات بحماية وسلطان مبادئ القانون الدولي.

وتلزم اتفاقية دبلن لعام (٢٠٠٨م) الخاصة بحظر الذخائر العنقودية، في ديباجتها أن (يظل المدنيون والمحاربون مشمولين بحماية وسلطة مبادئ القانون الدولي المنبثقة عن العرف والمبادئ الإنسانية)(٢).

(١) شافان دي يونس، تقرير اجتماع خبراء اللجنة الدولية للصليب الأحمر، الأسلحة المتفجرة في المناطق المأهولة، الجوانب الإنسانية والقانونية والتقنية والعسكري، سويسرا، ٢٠١٣.

(٢) المادة (١) من البروتوكول الإضافي الأول لعام ١٩٧٧، انظر أيضًا: ديباجة اتفاقية ١٩٨٠ الخاصة بتقييد استعمال الأسلحة التقليدية، ديباجة اتفاقية دبلن ٢٠٠٨ الخاصة بحظر الذخائر العنقودية.

وتلزم اتفاقيات جنيف طرف النزاع المسلح، الذي يقع تحت سلطته، مرضى وجرحى أن يقوم بعلاجهم، وتحظر القيام بمحاولات الاعتداء على حياتهم، واستعمال العنف معهم، أو قتلهم أو إبادتهم، أو تعريضهم للتعذيب، وأيضًا ألزمت الاتفاقيات الطرف الخصم في النزاع البحث عن جثث الموتى وتحديد هويتهم لتسهيل مهمة التعرف عليهم من قبل ذويهم بعد تسليمهم لدولتهم.

ولم تترك الاتفاقيات أي شاردة وواردة تخص حماية الأشخاص المشمولين بالاتفاقيات، لكن في حالة استخدام الأسلحة المتطورة وأغلب هذه الأسلحة تكون عن طريق التحكم بها عن بعد، وعن طريق أشخاص مجهولين متخفين خلف الأجهزة الإلكترونية، أو يصعب تحديد الدولة الجهة المنفذة للعمليات العسكرية في حالة كانت الدولة طرف النزاع المسلح في نزاع مسلح مع أكثر من دولة طرف في النزاع، أو من الممكن تنفيذ هذه العمليات من قبل دولة خارج أطراف النزاع وليست طرفًا في النزاع المسلح، وفي هذه الحالة سيكون هناك انتهاك لاتفاقيات جنيف وعدم الالتزام بها من قبل الأطراف المتنازعة والتنصل من كل ما تفرضه هذه الاتفاقيات في حالة إلحاقها الأذى بالفئات المحمية بموجب هذه الاتفاقيات.

هذا ما يفي بهدف التوطئة للسؤال الأكثر أهمية، وهو موقف الفقه القانوني من تطبيق القانون الدولي الإنساني على الحرب الإلكترونية، وهو محل المباحثة في المطلب التالي.

المطلب الثاني

موقف الفقه من تطبيق القانون الدولي الإنساني على الحرب الإلكترونية

إذا كان الفضاء الإلكتروني هو مكان أو قارة أو فضاء مستقل في حد ذاته عن كل الفضاءات الأخرى، بما فيها فضائنا المادي الملموس، وعرف الفضاء بأنه كل مكان أو حيز أو مجال يمكن من قيام الحياة فيه بمختلف تشعباتها وعلاقاتها[1]، فهل ذلك كاف للقول بأن الفضاء الإلكتروني هو في الحكم كالفضاء المحسوس الذي نعيش فيه؟

لو كانت الإجابة بإثبات المساواة بين الفضائيين محل اتفاق لما كانت لنا حاجة في المقارنة بين أقوال الفقهاء، غير أن المساواة المطلقة محل اختلاف؛ وهذا ما يفرض عرض آراء الفقهاء في خضوع الحرب الإلكترونية بفضائها الافتراضي المؤثر لأحكام القانون الدولي الإنساني، وفي العرض التالي حديث عن الاتجاهين الرئيسيين في المسألة:

الاتجاه الأول: يرى عدم خضوع الحرب الإلكترونية لأحكام القانون الدولي الإنساني

ذهب جانب من الفقه الأوروبي والأمريكي إلى اعتبار منطقة الفضاء الإلكتروني منطقة خاليه من القانون، وكل شيء فيها مباح، حيث يمكن لأي شخص القيام بأنشطة معاديه من دون قواعد أو ضبط النفس، وقيل بأن كلمات المرور وألواح المفاتيح وأجهزة الحواسيب هي التي تشكل حدودًا

(١) د. طالب حسن موسى، ود. عمر محمود أعمر، الإنترنت قانونا، مجلة الشريعة والقانون، جامعة الإمارات العربية المتحدة، العدد السابع والستين، ص.٣٣٩. (١٦) (٢٠١٦، ص. ٣٤٠.

وفواصل بين العالمين، ولا بد من الولوج إلى هذا العالم من خلالها، فهذا العالم لا يمكن أن يتحدد بدولة معينة، وبالتالي لا يمكن إخضاعه حتى للقانون الدولي العام التقليدي، فهذا القانون لم ينجح حتى الآن بحكم الفضاء البحري أو الجوي الخارجيين(١).

وعليه فأنصار هذا الاتجاه الذي يوصف بالحر يرفضون التعامل القانوني مع الإنترنت، ويتزعم هذا الاتجاه بعض السياسيين الأمريكيين وبعض علماء التقنية، وتساندهم فئة قليلة من فقهاء القانون، يذهبون إلى القول بأن الإنترنت لا يخضع لأي قانون، وحجتهم أن الإنترنت عالم جديد لا يتفق والواقع المادي التقليدي(٢).

ويرى مؤيدوا هذا المذهب أنه لا يوجد نص قانوني أو وثيقة من مواثيق القانون الدولي الإنساني تعالج الهجوم على شبكات الحاسوب، أو تتحدث عن حرب المعلومات أو العمليات المعلوماتية، كما لم يتم وضع قواعد للهجوم على شبكات الحاسوب أثناء النزاعات المسلحة، كون استخدام تكنولوجيا الإنترنت حديث نسبيا، والقانون الدولي الإنساني القائم لا يتلاءم مع وسائل وأساليب الحرب الإلكترونية، بالإضافة إلى أن المعاهدات القائمة حاليا يرجع تاريخها إلى ما قبل وجود أو ظهور الهجمات عبر شبكات الحاسوب(٣).

ويضيف أصحاب هذا الرأي أن تطبيق المبادئ العامة في القانون الدولي الإنساني على الفضاء الإلكتروني تبدو غير واقعية، لأن وسائل وأساليب الحرب الإلكترونية غير واضحة ومفهومة بشكلٍ كافٍ، ولأنها تتم في سرية تامه ولا يزال فهم الاستخدامات المحتملة لهذه التكنولوجيا وأثارها المتمثلة في الصراع المسلح غير جلي(٤).

كما أن المقاتلين السيبرانيين "ليس لهم مكان ثابت، ولا يحتاج المهاجمون" السيبرانيون إلى التواجد في المكان الذي يحدث فيه الهجوم، أو حتى في المكان الذي يظهر أن الهجوم ينشأ فيه، ويمكن للمهاجمين استعمال تكنولوجيا اتصال مجهولة الهوية والتشفير لإخفاء هويتهم(٥).

كما أن هناك صعوبة تكمن في تحديد مصدر هذه الهجمات، والذي تتم عادة من غير ذكر أسماء أو من خلال برنامج تسلل "روبوتي" آلي وصعوبة تتبع أصحابها الإسناد المسؤولية إلى دولة من الدول أو منظمة أو فرد، وإيجاد رابطة ما بين تلك العمليات، والصراع المسلح الذي يعقد للغاية

(١) نفس المرجع السابق، ص. ٣٤٠.

(2) Lavenue, J., Cyberspace ET Droit International: pour UN nouveau Jus Communications: Revue de la Recherche ,(1996),p.3.

(3) Brown, D., Proposal for an international convention to regulate the use of information System in Armed Conflict, Harvard International Law review, Vol (2006).47, p. 179.

(٤) د. عمر محمود أعمر، الحرب الإلكترونية في القانون الدولي الإنساني، الجامعة الأردنية، مج ٦٦، ع ٣، ٢٠١٩م، ص ١٣٧.

(٥) نفس المرجع، ص ١١.

تحديد ما إذا كان القانون الدولي الإنساني ينطبق أم لا على هذا الوضع، بالإضافة إلى أن الترابط بين أنظمة الكمبيوتر المدنية والعسكرية يعقد تطبيق القواعد الأساسية للقانون الدولي الإنساني(١).

لكل ذلك اعتبر الفقه الأمريكي والأوربي الفضاء الخارجي غير خاضع لأي قانون معين وأن أي تصرف أو عمل مباح فيه، وبالتالي لا يمكن تطبيق قوانين الحرب على النزاعات التي تحدث فيه، كما رفض أصحاب هذا الاتجاه التعامل القانوني مع الانترنت لكونه لا يتفق مع الواقع التقليدي، إضافة إلى ما سبقت إليه الإشارة من كون نصوص القانون الدولي الإنساني تخلو من الإشارة إلى الهجمات الإلكترونية على شبكات الحاسوب أو الحرب المعلوماتية، وأن هذا القانون لا يتلاءم مع وسائل الحرب الإلكترونية(٢).

ومن الحجج التي استند إليها أصحاب هذا الرأي عدم وجود أي مفهوم أو مصطلح يشير إلى الحرب الإلكترونية في ميثاق الأمم المتحدة واتفاقية لاهاي، إذ أنها أوردت مفهوم الهجوم المسلح واستخدام القوة في النزاعات وغيرها من المفاهيم، وخير مثال على ذلك النزاع بين استونيا وجورجيا والتي استمرت الهجمات الإلكترونية فيها لفترة معينة وألحقت أضرارًا جسيمة بالطرفين ومع ذلك لم تعد نزاعًا مسلحًا بالمعنى الحقيقي، ولم تخضع لقواعد الحروب(٣).

وباعتبار أن إي نشاط إلكتروني استخدم لأغراض عسكرية لا يعد هجوما ولا ينطبق عليه مفهوم الهجوم المسلح وفقًا للمادة (٤٩) من البروتوكول الإضافي الأول والذي نص على أن (الهجوم المسلح هو الهجمات وأعمال العنف الدفاعية والهجومية ضد الخصم) وأن هذا الأمر لا يتحقق لكون الهجوم الإلكتروني لا يصاحبه أو لا ينتج عنه عنف مسلح وتأثير مباشر(٤).

ويخلص البحث في هذه الجزئية إلى أن أصحاب هذا الرأي استبعدوا إمكانية تطبيق القانون الدولي الإنساني على النزاعات الإلكترونية؛ لأنهم يرون بأن الحرب تتطلب جيوشًا نظامية وميدانًا للقتال والمواجهة وتسبقها مرحلة إعلان، على عكس الحرب الإلكترونية التي تتم عبر شبكات المعلومات وتوجه نحو المنشآت الحيوية فهي أقرب إلى الإرهاب، إلى جانب خلو ميثاق الأمم المتحدة وقانون الحرب من الإشارة إلى الحرب الإلكترونية.

ومع أن القانون الدولي الإنساني خلى من الإشارة إلى الحرب الإلكترونية صراحة، وليس فيه أي نص يشير إليها بوجه الخصوص، غير أننا لا نتفق معهم، ونرى إمكانية تطبيق قواعده ومبادئه المطبقة على النزاعات التقليدية، لاسيما وتلك المبادئ تشمل كل التطورات ذات العلاقة بالنزاع والتي

---

(١) الحرب الإلكترونية تشن من خلال الجيش والمجتمع المدني والذي يشكل أسلوبًا عسكريًا غير نمطي لإدارة الصرعات المسلحة من خلال اشتراك منظمات غير حكومية وأفراد مدنيين عبر الفضاء الإلكتروني.

(٢)عمر محمود عمر، الحرب الإلكترونية في ضوء القانون الدولي الإنساني، بحث منشور في مجلة دراسات علوم الشريعة والقانون، مج ٤٦، ع٣، ٢٠١٩ ص١٣٦.

(٣) وليام، بارليتا، النزاع السيبراني والاستقرار الجيوسيبراني، ط١، الاتحاد الدولي للاتصالات والاتحاد العالمي للعلماء، ٢٠١١، ص ٥١- ٥٢.

(٤) أحمد عبيس نعمة، مصدر سابق، ص١١٨. وشيماء جمال محمد، الحرب الإلكترونية واسترتيجية الدول لمواجهتها، مجلة كلية القانون والعلوم السياسية، جامعة كركوك، مج ١٠، ع ٣٦، ٢٠٢١م، ص ٢٥٠.

أكدها البروتوكول الإضافي الأول الملحق باتفاقيات جنيف لعام (١٩٤٩م) من حيث التزام الدول عند اقتناء الأسلحة التحقق من كونها محظورة أم لا[١].

الاتجاه الثاني: خضوع الحرب الإلكترونية لأحكام القانون الدولي الإنساني

يذهب أنصار هذا الاتجاه إلى عدم الاعتراف بوجود فراغ قانوني في الفضاء الافتراضي "Cyberspace is not a law-free zone" واعتبار القواعد القانونية القائمة كافية لتنظيم الفضاء الإلكتروني، وأنه يمكن تطبيقها على الفضائيات الحديثة، وسمي هذا الرأي بالمذهب القانوني.

ووضح المستشار القانوني للجنة الدولية للصليب الأحمر Cordula Droege أن الإطار القانوني الدولي الإنساني القائم يطبق على النزاعات "السيبرانية" ويجب احترامه، بمعنى أن القانون القائم قادر على التعامل مع هذه التطورات الجديدة دون الحاجة إلى إشعار أو وضع قواعد قانونية خاصة بالفضاء الإلكتروني[٢].

ويمكن القول بإجماع الفقه الدولي على أن الحرب الإلكترونية تعد حربًا بالمعنى الصحيح عندما تكون أثارها على العالم المادي أثارًا مدمرة، وأن استخدام القوة من خلال هذه الآلية الحديثة ضد دولة ما يشكل حقًا وطنيًا للدولة المعتدى عليها للدفاع عن نفسها[٣].

وبناء على ذلك أكد الفريق الثاني على إمكانية تطبيق القانون الدولي الإنساني على الحرب الإلكترونية وضرورة احترامه من قبل كل الأطراف، ولا حاجة إلى وضع قواعد ومبادئ جديدة، واستند بذلك إلى ما جاء في المادة (٤) من ميثاق الأمم المتحدة التي حظرت على الدول الأطراف

---

(١) يلتزم أي طرف سام متعاقد عند دراسة أو تطوير أو اقتناء سلاح جديد أو أداة للحرب إن يتحقق مما إذا كان محظورًا في جميع الأحوال أو بعضها بمقتضى البروتوكول أو أية قاعدة أخرى من قواعد القانون الدولي التي يلتزم بها الطرف السامي المتعاقد، المادة ٣٦ من البروتوكول الإضافي الأول الملحق باتفاقية جنيف لعام ١٩٤٩.
وراجع د. علي عبد المعطي الحمدان، الحرب المعلوماتية وإمكانية تطبيق قواعد حقوق الإنسان، مجلة العلوم الشرعية، جامعة القصيم، مج ١٢، ع ١، ٢٠١٨م، ص ٧٧٤.

(2) Cordula Droege, conseillere juridique au CICR.Pas de vide juridique dans le cyberspace, CICR Comité international de la Croix-Rouge: https://www.icrc.org/.../interview/.... cyber-warfare-interview-2011-0.
شمال الأطلسي مناقشة مسألة انطباق القانون الدولي ما خلقت الثورة الرقمية شكلا جديدا من أشكال التهديدات مما دفع مركز الدفاع في حلف عدم وجود فراغ قانوني. والواقع أن في ذلك قانون النزاعات المسلحة والقانون الدولي الإنساني) على الهجمات الإلكترونية وتم التأكيد على بعض المنظمات الدولية مثل اللجنة الدولية للصليب الأحمر وبعض الدول مثل الولايات المتحدة الأمريكية وأستراليا تعد أن القانون الدولي القائم كافي لتنظيم الهجمات الإلكترونية.
(٣) في حال وقوع هجمات إلكترونية من دولة فان للدولة المعتدى عليها الحق في الدفاع عن نفسها استنادا لنص المادة ٥١ من ميثاق الأمم المتحدة سواء كان ذلك ناتج عن عدوان مسلح في العالم الحقيقي أو في الفضاء الإلكتروني وهنا يكون الرد فردي أو جماعي، ويكون من حق الدولة الضحية اتخاذ تدابير للدفاع عن النفس في الفضاء الإلكتروني أو في العالم الحقيقي ولكنها يجب أن تكون ضرورية ومتناسبة لمواجهة الهجوم المفاجئ:
Schmitt, M., International Law in Cyberspace the Koh Speech and. Tallinn Manual Juxtaposed. Harvard International Law Journal, December, 2012, Volume 54.... www.harvardilj.org/wp-content/.../12/HILJ-Online_54_Schmitt.pdf
شميت، مايكل.، الحرب بواسطة شبكات الاتصال: الهجوم على شبكات الكمبيوتر (الحاسوب) والقانون في الحرب، المجلة الدولية الصليب الأحمر، (٢٠٠٢) ص ٨٧.

اللجوء إلى الحرب باستخدام القوة أو التهديد ضد الدول واستقلالها السياسي وسلامة أراضيها وبشكل لا ينسجم مع مقاصدها(١).

كما فعلت أمريكا في سنة (٢٠١١م)، والهجمات ضد استوانيا (٢٠٠٧م) إذ عدت من قبيل أعمال العدوان وتجيز حق اللجوء إلى الحرب خاصة أن ميثاق الأمم المتحدة في المادة (٥١) لم يشر إلى نوع الأسلحة المستخدمة والتي تجيز حق الدفاع واستخدام القوة للرد(٢).

ومما استدل به أصحاب هذا الاتجاه ما يلي:

١. **تشابه آثار الحربين التقليدية والإلكترونية**، فالحرب الإلكترونية حرب حقيقية بالمعنى الدقيق لما لها من آثار مدمرة على العالم المادي، وقد بينت محكمة العدل الدولية أن المادة (٥١) من الميثاق لا تشير إلى نوع محدد من الأسلحة، وطبقته على قضية نيكاراغوا ضد الولايات المتحدة الأمريكية في عام (١٩٨٦م) بشأن الأنشطة العسكرية المستخدمة(٣).

وعليه فخلو القانون الدولي الإنساني من الإشارة إلى الاستهداف المباشر للأشخاص المدنيين والأعيان المدنية للعمليات التي تدور في الفضاء الإلكتروني، لا يعني أن قواعد القانون الدولي الإنساني لا تغطي وسائل وأساليب الحرب الإلكترونية ما دامت هذه الوسائل تنتج نفس الآثار التي يمكن أن تنتج عن الأسلحة التقليدية من دمار وانقطاع الخدمات الحيوية وكافة الأضرار والإصابات والوفيات، فالقانون الدولي الإنساني واسع بما فيه الكفاية لاحتضان التقدم الحاصل في التكنولوجيا، بالإضافة إلى أنه يمكن الرجوع إلى شرط مارتينز كأساس لتفسير معاهدات القانون الدولي الإنساني كلما وجدت الشكوك حول معنى بعض الأحكام الواردة فيها(٤).

واستنادًا إلى هذه القاعدة، فإن كل ما يقع أثناء المنازعات يخضع لمبادئ القانون الدولي الإنساني، مما يعني عدم خلو الهجوم على شبكات الحاسوب من القانون أثناء النزاع المسلح.

ويوضح الرأي الاستشاري لمحكمة العدل الدولية في مشروعية التهديد بالأسلحة النووية أو استخدامها، أن المادة (٢) ٤ والمادة (٥١) من ميثاق الأمم المتحدة تحظر استخدام القوة بغض النظر عن الأسلحة المستخدمة، فالمبادئ والقواعد الإنسانية قد وضعت قبل الأسلحة النووية، ومع ذلك فإنه لا يوجد شك بانطباق القانون الدولي الإنساني على الأسلحة النووية، وليس هناك ما يدعو للتمييز بين الأسلحة النووية وأسلحة الحاسوب، من حيث الزمن الذي استحدثت فيه، وهذا يعني إمكانية تطبيق القانون الدولي الإنساني عليها(٥).

---

(١) احمد عبيس نعمة، الهجمات السيبرانية، ط١، منشورات زين الحقوقية، بيروت، ٢٠١٨، ص٤٩.

(2) see seg Schmitt «m 1999 computer network atatck and the use of forse ininternational law. thoughts on a normative framework ،37، colum j trananat 1.885.1.

(٣) عمر محمود عمر، مصدر سابق، ص١٣٨.

(٤) انظر: Roscini, M., (2014), Cyber Operations and the Use of Force in International Law. Oxford:Oxford University Press, p. 22

(٥) سميث، مايكل، الحرب بواسطة شبكات الاتصال، مرجع سابق ص. ٩٣.

وعليه يمكن القول: إن أي هجوم "سيبراني" على دولة ما له عواقب في دولة أخرى هو بمثابة" هجوم مسلح "أو معادل له[١]، على الأقل عندما يحدث دمارًا كبيرًا، أو خسائر في الأرواح البشرية وهذا ينسجم مع المعنى الوارد في ميثاق الأمم المتحدة ومعاهدة الناتو والقانون الدولي العام، وذلك لتمكين الدول من الدفاع الفردي والجماعي المشروع بواسطة الوسائل العسكرية، ويترتب على ذلك رجحان تطبيق القانون الدولي الإنساني على الحرب الإلكترونية[٢].

يضاف إلى ذلك أن الأنشطة التي تؤدي إلى الموت تقريبًا أو الإصابة أو التدمير الكبير ينظر إليها على أنها استخدام للتوتر، وينطبق عليها القانون الدولي الإنساني أيضًا[٣]، فالفكرة الرئيسة تقوم على وضع معيار يعتمد على آثار العمل والنتائج المتوقعة منه[٤].

وهنا يمكن القول إن الأخذ بهذا الاتجاه سيوسع وبشكل كبير من تعريف النزاع المسلح، والذي يعني تغيير جوهري في نطاق القواعد القانونية التي تحكم النزاع المسلح، وليس كما ذهب إليه أصحاب هذا الرأي من القول بإمكانية تطبيق قواعد القانون الدولي الإنساني التقليدية، دون حاجة إلى إضافة نصوص أو تعديل ما هو موجود.

٢. شمول النطاق المكاني للحرب الإلكترونية

عرف البروتوكول الأول الإضافي (١٩٧٧م) الهجمات بأنها: "أعمال العنف الهجومية والدفاعية ضد الخصم، وتنطبق أحكام هذا البروتوكول المتعلقة بالهجمات على كافة الهجمات في أي إقليم تشن منه بما في ذلك الإقليم الوطني لأحد أطراف النزاع... وتسري أحكام هذا القسم عليه".

ويؤكد جانب من الفقه على أن الفضاء الإلكتروني لا يمكن أن يكون منطقة غير خاضعة للقانون، ووفقًا للقواعد التقليدية للقانون الدولي الإنساني، فإن تطبيق القواعد الخاصة بالنزاعات المسلحة غير الدولية، يلزم تحديد النطاق الجغرافي ليكون ضمن حدود الدولة التي حدث النزاع الداخلي فيها، ويستحيل ذلك في هذا النوع من النزاعات، رغم أن بعض الفقهاء يرون أن من الممكن أن يمتد النزاع الداخلي إلى خارج حدود الدولة الإقليمية[٥].

---

(1) Lovan, M., Vittor, F., intervention militaire en Iraq et le droit international, La doctrine europeenne, Annuaire francais de droit international, Volume (2003) 49, P. 17-13.

(٢) هينين وينجر، مفهوم بشأن السلام السيبراني، البحث عن السلام السيبراني، البحث عن السلام السيبراني، الناشر الاتحاد الدولي.

(٣)انظر: Koh, H, International Law in Cyberspace, Harvard International Law Journal, Online, volume., (2012) , p.54.

(٤) سميث، مايكن، (٢٠٠٢) الحرب بواسطة شبكات الاتصال: الهجوم على شبكات الكمبيوتر (الحاسوب والقانون الدولي)، مرجع سابق. ص. ٩٤.

(5) Michael N. Schmitt, Tallinn Manual on the International Law Applicale to Cyber Warfare...., Op.Cit, p.145.

٣. مبدأ تفسير المعاهدة بحسن نية

ووفقًا لهذا المبدأ وفي ضوء موضوعها والغرض منها المنصوص عليه في اتفاقية فيينا لعام (١٩٦٩م) المادة (٣١/ ١)، فإن المعنى العادي "للقوة" هو العنف أو الضغط الموجه ضد دولة، وهو واسع بما يكفي لتغطية ليس فقط القوة المسلحة التقليدية، ولكن أيضًا أنواع أخرى من الإكراه بقدر ما يتعلق بالسياق.

وتعبير "القوة" يظهر أيضًا في ديباجة الميثاق وفي المواد (٤١ و٤٦) حيث يسبقها صفة" مسلح"، بينما في المادة (٤٤) فقد تمت الإشارة إلى القوة العسكرية، والميثاق يشير صراحة في مواده عندما يريد واضعوه إلى الإشارة إلى القوة المسلحة"، وبما أن الأمر لم يكن كذلك في الفقرة (٢) من المادة، فربما أراد واضعوه الرجوع إلى نطاق أوسع في تفسيره ليتماشى مع الهدف العام للميثاق هو "إنقاذ" الأجيال من ويلات الحرب(١).

٤. **تطويع القضاء الدولي لمفاهيم مشابهة لفكرة أنسنة الحرب الإلكترونية**؛ فبالنسبة لنوع الأسلحة المستخدمة إذا أمعنا النظر في التعريف الذي أوردته لجنة الأسلحة التقليدية عام (١٩٨٦م) بأن أسلحة الانفجارات الذرية والمصنوعة.... وأسلحة الفتك الكيميائية والبيولوجية وأي نوع أخر من الأسلحة التي يتم تصنعيها في المستقبل وتتشابه خصائصها في الأثر التدمري مع القنبلة.

وبالتالي فإن إيراد عبارة أي نوع من الأسلحة يتم صنعها في المستقبل تتسع لتشمل الهجمات الإلكترونية التي تحدث في الفضاء من اختراق شبكة المعلومات والحواسيب وينجم عنها أضرارًا تلحق بالمدنيين من جراء تعطل السدود والاحتياجات الأساسية والتي يصعب فيها الحد من أثرها التدميري وبالتالي تشمل العبارة الأسلحة الإلكترونية المستخدمة في نطاق النزاعات الحديثة، والسلاح الإلكتروني منها(٢).

وفي قضية نيكاراغوا ضد الولايات المتحدة الأمريكية المتعلقة بالأنشطة العسكرية وشبه العسكرية في عام (١٩٨٦م)، بينت محكمة العدل الدولية أن المادة (٥١) لا تشير إلى أسلحة محددة وأن مفهوم الأسلحة ينطبق على "أي استخدام للقوة، وبغض النظر عن حقيقة أن الهجمات "السيبرانية" لا تستخدم الأسلحة الحركية التقليدية، فإن ذلك لا يعني بالضرورة أنها لا يمكن أن تكون "مسلحة"، ويمكن اعتبار استخدام أي جهاز ينتج عنه خسائر كبيرة في الأرواح أو تدمير واسع للممتلكات مستوف لشروط الهجوم المسلح".

ويدعم هذا الاستنتاج تأكيد مجلس الأمن على ذلك الحق في الدفاع عن النفس ردًا على هجمات ١١ سبتمبر (٢٠٠١م) على الولايات المتحدة(٣).

---

(1) Roscini, M. World Wide Warfare -Jus ad bellum and Use of Cyber Force, Op. Cit, p. 108.

(٢) يحى ياسين سعود، مصدر سابق، isnn ٢٥٣٧ – ٧٥٨، ص٨٤-٨٥.

(٣) انظر: ICJ Reports 1986, see note 64, 94 para. 176

يضاف إلى ذلك أن المحكمة الجنائية الدولية الخاصة ليوغوسلافيا سابقًا، وفي حكمها في قضية "تاديتش" قضت، بأن النزاع المسلح يكون دوليًا إذا وقع بين دولتين أو أكثر، وكذلك يمتد ليشمل حالة النزاع المسلح غير الدولي إذا تدخلت دولة أخرى بقوة عسكرية، أو إذا كانت مشاركة إحدى الفصائل المحلية المتنازعة تدخل "بالنيابة عن دولة أخرى، حيث أصبحت النزاعات المسلحة الداخلية ذات الطابع الدولي السمة الغالبة على النزاعات في الوقت الحالي"[١].

وفي إطار الأخذ باعتبار الهدف والضرر المتوقع (إن لم تكن الوسيلة محرمة قانونا) بسبب حداثتها، فإن محكمة العدل الدولية في فتواها بشأن مشروعية استخدام الأسلحة النووية، استنتجت تحريم استخدام السلاح النووي بسبب طبيعته التدميرية، ونظرت إلى نتائج استخدام هذا السلاح والأضرار التي يمكن أن يسببها للبشرية، بغض النظر عن الوسيلة، خصوصًا وأن للطاقة النووية استخدامات سلمية أيضًا، وفي رأيها المشار إليه وضعت المحكمة تفسيرات جديدة لقواعد القانون الدولي الإنساني ومبادئه، ليتم تطبيقها على جميع الأسلحة التي لم يتمكن المجتمع الدولي من وضع قيود على استخدامها أو تحريمها فيما بعد لكي تمتنع الدول عن استخدام الأسلحة الفتاكة الجديدة ولا تتذرع بعدم وجود نص قانوني يحرم استخدامها[٢].

وقد رأت محكمة العدل الدولية أنه أيًا كانت طبيعة الصراع وأيًا كان حجم التباين بين القوى المتنازعة فإن على جميع القوى احترام المبادئ التي تحظر المعاناة[٣]، وتكفل المعاملة الإنسانية، وتعمل على التمييز بين المقاتلين والمدنيين، إذ أن استهداف المدنيين محظور على الدوام، وعلى القوات المسلحة الحكومية والجماعات المسلحة غير التابعة للدولة أخذ كل الاحتياطات الممكنة لتقليل الأضرار التي قد تلحق بالمدنيين إلى أقل حد ممكن.

ورغم عدم وجود اتفاقية دولية تعنى بالحد من أخطار السلاح النووي إلا أن المحكمة أشارت إلى مجموعة من المبادئ (التي تكفل حماية المدنيين من جميع الأخطار التي تسببها الأسلحة الحديثة التي لم تنظمها اتفاقيات دولية للحد من أخطارها بعد)، وقد صيغت هذه المبادئ بشكل عام ليشمل كل المستجدات والأخطار التي قد تؤدي إلى الفتك بالبشرية مستقبلاً ويمثل شرط مارتنز النص المثالي الذي يضمن هذه الحماية للمدنيين[٤].

---

(1) Schindler, D. International Humanitarian Law and Internationalized Internal Armed Conflicts, International. (1982) p.37.

(٢) لويز دوسوالد بيت، القانون الدولي الإنساني وفتوى محكمة العدل الدولية بشأن مشروعية التهديد بالأسلحة النووية أو استخدامها المجلة الدولية للصليب الأحمر العدد ٣١٦ ، ١٩٩٧ – ص٣٥.

(٣) المصدر نفسه، ص ٢.

(٤) ويعد هذا الشرط على جانب كبير من الأهمية، لكن تفسيره الدقيق يخضع لتباين كبير، وقد وضع هذا الشرط أصلا في ديباجة اتفاقية لاهاي الرابعة لعام ١٨٩٩ وعام ١٩٠٧. ودخل بعد ذلك في صلب نص البروتوكول الإضافي الأول لعام ١٩٧٧ وفي ديباجة البروتوكول الثاني لويز دوسوالد بيت، مرجع سابق، ص٣٥. وقد أثارت اللجنة الدولية للصليب الأحمر تساؤلا حول حقيقة وجود الآلام.

كما بينت المحكمة أن المبادئ الأساسية للقانون الدولي الإنساني تظل منطبقة على جميع الأسلحة الجديدة، وذكرت أنه لا توجد دولة تجادل في ذلك(١).

بناءً على ما تقدم لا يمكن وفقًا لقواعد القانون الدولي الإنساني القول بأن ما لم يحظر صراحة في المعاهدات أو العرف يكون مباحًا، لأن مبدأ الإنسانية وما يمليه الضمير العام يمثلان عوامل تقييدية قانونية، ولا شك أن هذه العوامل هي التي منعت الدول في الواقع من استخدام الأسلحة النووية منذ عام (١٩٤٥م) نظرا لآثارها المدمرة(٢).

فذريعة استخدام الدول لسلاح جديد لم يتم تجريمه مباشرة بموجب قواعد القانون الدولي لم تعد مقبولة مطلقًا، وبنفس هذه المقاييس فإن استخدام الحرب الإلكترونية للتسبب بمعاناة إنسانية غير ضرورية أو لاستهداف السكان المدنيين هو أمر غير جائز بموجب قواعد القانون الدولي الإنساني(٣).

٥. **تأكيد بعض الأعمال الدولية على فكرة أنسنة الحرب الإلكترونية**، من ذلك دليل تالين(٤) الذي منح الدولة الحق في الرد على الهجمات الإلكترونية التي تتعرض لها من الدولة المعادية والتي تتسبب بخسائر كبيرة في الأرواح أو تسبب تعطل في أنظمة الكومبيوتر والحوادث الهندسية المتعمدة التي تستهدف شبكة المعلومات(٥).

كما أكدت اللجنة الدولية للصليب الأحمر شرعية وضرورة تطبيق القانون الدولي الإنساني على الهجمات الإلكترونية، لكون العمليات والهجمات التي ترتكب أثناء النزاعات شأنها شأن أسلحة الحرب الأخرى، بغض النظر عن نوع النزاع، وتخضع في تنظيمها للقانون ذاته، وأكدت المواثيق الدولية الأخرى المعنية بتنظيم السلاح والنزاعات المسلحة أن على المتحاربين احترام وحماية المرافق المدنية الضرورية والمواد التي لا غني عنها لبقاء السكان المدنيين (وأن الاعتداء عليها من خلال الهجمات الإلكترونية يشكل انتهاكا للقانون الدولي الإنساني(٦).

---

(1) International humanitarian law and the Advisory Opinion of the International Court of Justice on the legality of the threat or use of nuclear weapons- p.1.

(2)Ibid.p.3.

(3)Lesley Swanson, The Era of Cyber Warfare: Applying International Humanitarian Law to the 2008 Russian-Georgian Cyber Conflict, Loyola of Los Angeles International and Comparative Law Review Law Reviews, 2010, p. 316.

(٤) دليل تالين مكون من ٢٨٢صفحة وبواقع ٩٥ مادة متضمنا القوانين الدولية الواجبة التطبيق على الحرب الإلكترونية، والدليل يقع في قسمين: الأول اختص بالأمن الإلكتروني والثاني خاص بالنزاعات الإلكترونية.
ينظر شريف نسيم قلته، دليل تالين والهجمات الإلكترونية وحظر استخدام القوة في القانون الدولي، بحث منشور في مركز الفضاء العربي للأبحاث الفضاء الإلكتروني، ع ١٦٤، ٢٠١٧، ص ٢.

(٥) ينظر شريف نسيم قلته، دليل تالين والهجمات الإلكترونية وحظر استخدام القوة في القانون الدولي، بحث منشور في مركز الفضاء العربي للأبحاث الفضاء الإلكتروني، ع ١٦٤، ٢٠١٧، ص ٢.

(٦) فرونيك كريستوري، القانون الدولي الإنساني توفر طبقة إضافية من الحماية، تقرير عن الحد من التسلح في اللجنة الدولية للفريق العامل المفتوح العضوية المعني بالتطورات في ميدان المعلومات والاتصالات في سياق الأمن الدولي، ١٠ أيلول، ٢٠١٩.

٦. **شمول فكرة حظر بعض الأسلحة**، بمعنى أن فكرة حظر بعض أنواع الأسلحة لخطرها يشمل السلاح الإلكتروني فالمقصد واحد والسبب واحد، فكل سلاح تكنلوجي أو أسلوب من أساليب الحرب يتوجب على الأطراف التأكد من مشروعيته قبل استخدامه وفقا لقواعد القانون الدولي العام، كما يمكن الاستدلال بالمبادئ الأساسية للقانون الدولي الإنساني وفي مقدمته شرط مارتينز باعتباره الحجر الأساس له، وتم وضعه في ديباجة اتفاقية لاهاي الرابعة لعام (١٨٩٩و ١٩٠٧م) بحيث نص على أنه في حالة عدم وجود قاعدة محددة في القانون التعاهدي فإن للمحاربين حق الحماية بموجب القانون العرفي ومبادئ الإنسانية التي يمليها الضمير العام(١).

وعليه فإن الأطراف المتحاربة لا تمتلك حرية اختيار وسائل الحرب، فالمادة (٣٣) الفقرة (ب) من لائحة لاهاي (١٩٠٧م) المتعلقة بأعراف الحرب البرية حرمت اللجوء للغدر، كذلك المادة (٣٧) الفقرة (١) من البروتوكول الأول لعام (١٩٧٧م)، لاتفاقيات جنيف (١٩٤٩م) أجازت لأطراف النزاع استعمال خدع الحرب(٢).

وفي حالة استخدام الأسلحة الإلكترونية من قبل دول النزاع المسلح يثار التساؤل عن قيام المسؤولية الدولية على الدولة المتهمة في حالة ممارسة الأفعال المذكورة؟

وليس من الميسر إثبات نسبة الهجوم السيبراني لدولة بعينها حتى في حالة قيام الدولة المتضررة من الهجوم، بتعقب مصدر الهجوم لما يتطلب من الوقت والجهد، وفي أغلب الحالات يكون مصدر الهجوم الذي سير طائرات ألحقت الأذى بالأشخاص والمدن، أو استخدم فايروسات لضرب مواقع الأنترنت الأمنية للدولة الخصم من فاعل مجهول، لكن في حالة افتراض أن الدولة المتضررة تمكنت من إثبات قيام دولة معينة بهجمات سيبرانية، ففي هذه الحالة تحققت عناصر المسؤولية الدولية، ويتم تقدير الضرر الناتج لتحمله الدولة المتهمة، وتعوض الدولة المتضررة، لكن في بعض الأحيان يكون المتهم بالاختراق أو بالهجوم فردًا أو جماعة؟ وهنا تكون المسؤولية غير مباشرة وتسأل الدولة عن أفعال رعاياها، في حالة عدم بذل الدولة العناية اللازمة لتمنع إلحاق الضرر بالدولة الأخرى، خاصة وأن معظم الدول تفتقر إلى سن التشريعات الوطنية التي تحرم استخدام الأسلحة الإلكترونية وفق مبادئ القانون الدولي الإنساني، كما أنها لم تضع حدودًا للاستخدام الإلكتروني، ولا تفرض عقوبات على المتسببين بهذه الهجمات(٣).

ما يجب مراعاته عند تطبيق القانون الدولي الإنساني على الحرب الإلكترونية

عند تطبيق القانون الدولي الإنساني على الحرب الإلكترونية يجب التمييز بين المدنيين والعسكريين حيث توجب اتفاقية جنيف على أطراف النزاع التمييز بين السكان المدنيين والمقاتلين

(١) ينظر الموقع الإلكتروني: https://www.ahewar.org/debat/show.art.asp?aid= ٥٩١٧٩ تاريخ الزيارة ٢٠٢٠/٨/١٠.

(٢) د. أحمد فتحي سرور، القانون الدولي الإنساني دليل للتطبيق على الصعيد الدولي، ط١، القاهرة، ٢٠٠٣، ص٤٥.

(٣) د. أحمد فتحي سرور، القانون الدولي الإنساني، مرجع سابق، ص٤٥.

وبين الأعيان المدنية والأهداف العسكرية، هذا فضلاً عن إلزامها بتوجيه عملياتها ضد الأهداف العسكرية دون غيرها، وذلك من أجل تأمين حماية المدنيين والأعيان المدنية(١)، وقد تم التأكيد على الالتزام بهذا المبدأ في البروتوكولين الإضافيين (١٩٧٧م) لاتفاقيات جنيف(٢).

كما نص البروتوكول الإضافي الأول الملحق باتفاقيات جنيف على مبدأ المعاناة غير الضرورية ووضع قيودا على أساليب ووسائل القتال(٣)، وقد أثارت اللجنة الدولية للصليب الأحمر تساؤلا حول حقيقة وجود الآلام المفيدة والآلام غير مفيدة في الحرب؟ إن عبارة "الآلام التي لا فائدة منها" أو "الآلام التي لا مبرر لها" التي هي موضع متعمق في اللجنة الدولية للصليب الأحمر إذ يصعب على الكثيرين أن يتفهموا إمكانية وجود آلام "مفيدة" وآلام "ضرورية"، بيد أن هذه العبارة تستمد وجودها من فكرة أساسية مؤداها أن الحرب ليست غاية بالذات، ولا تسمح إلا بما هو ضروري لإحراز النص(٤).

وعليه فاستهداف المدنيين في النزاعات المسلحة في الحروب الإلكترونية يعد انتهاكا لقواعد القانون الدولي الإنساني(٥).

ويعتبر المقاتلون والأهداف العسكرية أهدافًا مشروعة وفقًا لقوانين الحرب، ويعد توجيه الهجمات باستخدام شبكة الحاسوب ضد المقاتلين، على سبيل المثال للتسبب بفقدان سيطرة الملاحة الجوية العسكرية على نظام إرسال المعلومات الملاحية ليتم إرسال معلومات خاطئة تتسبب في نقل قوات جيش لتدميرها (بعيدا عن المدنيين) جائز ومشروع بموجب هذا المفهوم(٦).

يتضح مما تقدم أن المشكلة في استخدام الحاسوب والانترنت في الحرب هي مشكلة عملية، وليست قانونية فقط، فقد يعتمد الجيش على الأهداف المزدوجة الاستعمال كشبكة الاتصالات والطرق والجسور، معرضا المدنيين إلى ضرر حتمي، ولكن ينبغي ملاحظة أن قواعد القانون الدولي الإنساني تحرم التسبب "بالآلام التي لا مبرر لها" لتحقيق الأهداف العسكرية المحددة إذ أن الحرب ليست غاية بذاتها ولذلك لا يسمح إلا بما هو ضروري لتحقيق الهدف المحدد(٧).

---

(١) البروتوكول الاضافي الأول ١٩٧٧، م/٤٨.

(٢) البروتوكول الإضافي الأول ١٩٧٧، م/٥١(٢)، والبروتوكول الثاني، المادة (١٣٠٢).

(٣) نصت المادة ٣٥ من البروتوكول الاضافي الأول ١٩٧٧ على الآتي:

١) إن حق أطراف أي نزاع مسلح في اختيار أساليب ووسائل القتال ليس حقا لا تقيده قيود.

٢) يحظر استخدام الأسلحة والقذائف والمواد ووسائل القتال التي من شأنها إحداث إصابات أو آلام لا مبرر لها.

٣) يحظر استخدام وسائل أو أساليب للقتال، يقصد ما أو قد يتوقع منها أن تلحق بالبيئة الطبيعية أضرار بالغة واسعة الانتشار وطويلة الأمد.

(٤) إيف ساندوز، حظر وتشييد استعمال أسلحة معينة، ثلاثة أسئلة جوهرية، المجلة الدولية للصليب الأحمر العدد ٣٧، ١٩٩٤، ص ٢.

(5) Michael N. Schmitt, Tallinn Manual on the International Law Applicale to Cyber Warfare.... Op.Cit, p.145.

(6)International humanitarian law and the Advisory Opinion of the International Court of Justice on the legality of the threat or use of nuclear weapons, p.7.

(7) Michael N. Schmitt, Heather A. Harrison Dinniss, Thomas C. Wingfield, Background Paper prepared for Informal High-Level Expert Meeting on Current Challenges to

وعليه يمكن القول بحرمة التسبب بالآلام التي لا مبرر لها لتحقيق أي هدف عسكري بسلاح إلكتروني، وينبغي أثناء الحرب الإلكترونية الالتزام بمبادئ القانون الدولي الإنساني المتعلقة بالتمييز والتناسب وأخذ الحيطة اللازمة، وهكذا نخلص مما تقدم إلى جدارة الرأي القائل بخضوع الحرب الإلكترونية لأحكام القانون الدولي الإنساني، وفي المبحث التالي نتطرق لمدى تطبيق المبادئ الأساسية والقواعد التقليدية وقانون حقوق الإنسان على الحرب الإلكترونية.

المبحث الثاني

مدى تطبيق المبادئ الأساسية والقواعد التقليدية وقانون حقوق الإنسان على الحرب الإلكترونية

لما كان شمول القانون الدولي الإنساني للحروب الإلكترونية من الضروريات التي أثبتها الاتجاه الفقهي الأقوى حجة أصبح التمكين لذلك الاتجاه منسحباً بالتلازم على المبادئ الأساسية والقواعد التقليدية وقانون حقوق الإنسان، ولا تكتمل صورة هذه الخلاصات إلا بالتعرف على المدى الذي يبلغه التطبيق العملي لتلك القوانين والقواعد والمبادئ، والمدى حديث عن المجال العملي الذي ينبغي تدعيمه بالحديث عن خاصية ملائمة المبادئ الأساسية لأن تطبق على الحرب الإلكترونية، وهذا ما يعرضه البحث في المطلبين التاليين:

المطلب الأول

مدى ملائمة تطبيق المبادئ الأساسية على الحرب الإلكترونية

سعى القانون الدولي الإنساني منذ نشوئه لوضع القواعد والضوابط التي تحكم سير العمليات العسكرية خلال النزاعات المسلحة بنوعيها الدولية وغير الدولية، وعلى الرغم من عدم قدرة هذا القانون على منع الحرب إلا أنه يسعى للحد من آثار النزاع المسلح بين الأطراف المتنازعة ويعمل بشكل خاص لحماية المدنيين الذين لا يشاركون في القتال، والأشخاص الذين أصبحوا عاجزين عن المشاركة في القتال والسعي لتحييد الأعيان المدنية عن سير الأعمال العدائية خلال العمليات القتالية التقليدية، وفي العرض التالي يقف البحث على مدى صلاحية المبادئ الأساسية المطبقة على الحروب التقليدية للتطبيق على الحرب الإلكترونية:

١. مدى ملائمة مبدأ الضرورة العسكرية للتطبيق على الحرب الإلكترونية

الضرورة العسكرية – بحسب تعريف قانون ليبر عام (١٨٦٣م) – هي "التدابير التي لا غنى عنها لتأمين انتهاء الحرب"[١].

International Humanitarian Law, Cambridge, June 25-27, 2004 – p.14 www.hsph.harvard.edu.

(1) LIEBER, Francis, Instructions for the Government of Armies of the United States in the field, 1898, Article14, 15, 16.

وأُشير لهذا المبدأ في اتفاقية لاهاي الخاصة باحترام قوانين وأعراف الحرب البرية لعام (١٩٠٧م) وفي المواد (٤٣ و ٥٤) من ذات الاتفاقية، وحدد البروتوكول الإضافي الأول لاتفاقيات جنيف لعام (١٩٤٩م) الضرورة العسكرية كحالة استثنائية في النزاعات المسلحة، فقد نصت المادة ٥٢/٢ بأن الأهداف العسكرية هي التي "تقصر الهجمات على الأهداف العسكرية فحسب[١]، أما الأهداف المحمية فهي الأهداف التي تحميها اتفاقيات جنيف، مثل المستشفيات، ووسائل نقل الجرحى أو المرضى، والمواقع الدينية أو الثقافية، ومناطق السلامة، غير أنه في حال استخدام أي من هذه المواقع لأغراض عسكرية فإن من الجائز مهاجمتها، وعلى سبيل المثال فإذا ما استخدمت الهيئات العسكرية كنيسة كقاعدة للعمليات، فإنها يمكن أن تصبح هدفا عسكريا مشروعا"[٢].

والضرورة المقصودة هي الضرورة التي لا مفر من ملابساتها، وليست كل ضرورة، هذا ما نبه عليه البروتوكول الإضافي الأول الذي وصف الضرورة العسكرية بأنها تلك التي توصف بالضرورة، الملحة في حالات اتباع سياسة "الأرض المحروقة في الأراضي الواقعة تحت سيطرة الخصم[٣].

وهذا يعني أن الضرورة المعتبرة مقيدة بوصف الإلحاح، ولها شروط إضافية أهمها:

١. أن يكون هذا التجاوز مؤقتًا ومرتبطًا بمدة قيام الضرورة.
٢. أن يكون على أهداف محددة.
٣. أن يكون الغرض منه تحقيق ميزة عسكرية أكيدة.
٤. أن يتم مراعاة القانون الدولي الإنساني.

ولا نرى بأساً من تطبيق مبدأ الضرورة العسكرية على النزاعات الإلكترونية المستخدمة في الأعمال العدائية، وبالتالي يتم تطبيق المبادئ الأساسية الراسخة في القانون الدولي الإنساني، ويمكن الدفاع عن النفس والرد بوسائل إلكترونية أو تقليدية، حيث يتم اللجوء لمعايير الهجوم العسكري التقليدي لتقييم الهجمة الإلكترونية[٤].

فقد اعتبر "شميث" و"كوه" ومجموعة من الخبراء في حلف شمال الأطلسي ممن وضعوا ما يسمى بدليل تالين أن الهجوم الإلكتروني هو بمثابة استخدام القوة، إذا كان أثر الهجوم عند مقارنته بالاستخدام الفعلي للقوة مساويًا له أو قريبًا منه فعند وقوع هجمة إلكترونية على الدولة ترقى إلى

(١) لقد تم الإشارة لمبدأ الضرورة العسكرية في المواد المؤرخة في ١٢ أغسطس/ آب ١٩٤٩ والمتعلق بحماية ضحايا النزاعات المسلحة الدولية.

(2)Wingfield, T.,The Law of information Conflict: National Security Law in Cyberspace, Aegis ResearchCorp., Falls Church, VA, 2000; The Law of Armed Conflict: Basic Knowledge, international Committee of the Red Cross, June 2002. http:/www.icrc.org.

(٣) البروتوكول الإضافي الأول ٥٤/٢.

(4) Kelsey, J., (2008) Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare, Michigan Law Review, Volume 106, Issue 7. (p. 1427- 1452), P.1437.

الاستخدام الفعلي للقوة فإن هذه الهجمة تخضع لمبدأ الضرورة العسكرية كما أن العمليات الإلكترونية التي تقوم بها الدولة في ممارسة حقها في الدفاع عن النفس يجب أن تكون ضرورية ومتناسبة.

واشترط "كوه" على أطراف النزاع أن تراعي عدة شروط قبل تنفيذ الهجمة الإلكترونية وهي[١]:

١. دراسة آثار الأسلحة السيبرانية على البنية التحتية للمستخدمين العسكريين والمدنيين على حد سواء، بما في ذلك تقاسم البنية التحتية المادية المشتركة مثل شبكة السدود وشبكات الماء والكهرباء التي من شأنها أن تؤثر على المدنيين.

٢. دراسة الأضرار المادية المحتملة التي قد تسببها الهجمات عبر الإنترنت مثل الوفاة، أو الإصابة التي قد تنجم من أثر الهجوم على البنية التحتية الحيوية.

٣. دراسة الآثار المحتملة لهجوم عبر الإنترنت على الأهداف المدنية التي لا تشكل أهدافًا عسكرية مثل أجهزة المدنيين ولكن قد تكون مرتبطة مع أجهزة الكمبيوتر التي هي أهداف عسكرية.

٤. قيام الدول بتقييم أسلحتها الإلكترونية، بمعنى أن يكون استخدام هذه الأسلحة ليس محظوراً، ولا يتنافى مع قانون الحرب أو أنه لا يمكن استخدام هذه الأسلحة بطريقة مغايرة لمبدأي التمييز والتناسب.

٢. مدى ملائمة مبدأ التمييز والتناسب للتطبيق على الحرب الإلكترونية

جاء في إعلان سان بطرسبورغ لعام (١٨٦٨م) يجب أن يكون الغرض الشرعي الوحيد الذي تستهدفه الدول أثناء الحرب هو إضعاف قوات العدو العسكرية، ويكفي لهذا الغرض عزل أكبر عدد ممكن من الرجال عن القتال[٢].

ونص دليل تالين على إمكانية تطبيق مبدأ التمييز على الهجمات الإلكترونية، وبين الدليل أن المدنيين أفرادًا أو جماعات يجب ألا يكونوا هدفًا للهجمات الإلكترونية، وفي حالة الشك في حالة الشخص فيما إذا كان عسكريًا أو مدنيًا فإنه يعد مدنيًا، وقد حددت المادة (٩٦) من الدليل بأن الفئات التالية هي الأهداف التي يمكن مهاجمتها خلال النزاع وهي:

١. أفراد القوات المسلحة.

٢. أعضاء الجماعات المسلحة المنظمة.

٣. المدنيون الذين يشاركون مباشرة في الأعمال الحربية.

٤. المشاركون في الانتفاضة الشعبية، في النزاع المسلح الدولي.

واعتبرت المادة (٩٦) أن المدنيين يتمتعون بالحماية خلال الفترة التي لا يشاركون فيها بالعمليات العدائية، ونصت المادة (٩٨) على حظر توجه هجمات تبث الذعر بين المدنيين، وفي المادة (٩٩) نصت على أنه لا يجوز استهداف الأعيان المدنية بالهجمات الإلكترونية التي تشمل أجهزة الكمبيوتر وشبكاته والبنية التحتية الحاسوبية.

(1) Koh, H., International Law in Cyberspace,Op.cit. p 5.

(٢) إعلان سان بطرسبورغ بغية حظر استعمال قذائف معينة في زمن الحرب، ١٨٦٨.

ونظرًا للطبيعة المترابطة للشبكات الحاسوبية، فإنه من غير المتصور استهداف جزء من الشبكة دون التأثير على باقي الأجزاء سواءً أكانت الهجمة إلكترونية أو هجمة بالمفهوم التقليدي، ففي شروحات دليل تالين نجد في شرح المادة (٩٩) بأن مجموعة الخبراء الدوليين ترى بأن دراسة تحديد طبيعة الشبكة فيما إذا كانت عسكرية أو مدنية يتم من خلال دراسة كل حالة على حده، لعدم وجود معيار يحدد طبيعة الشبكة المستهدفة.

وتنص المادة (١٠٢) من الدليل على أنه في حالة الشك فيما إذا كانت الأعيان التي تكرس عادة لأغراض مدنية وتستخدم التقديم مساهمة فعاله في العمل العسكري لا يجوز استهدافها إلا بعد تقييم دقيق لإثبات الاستخدام العسكري، ويجب على المهاجم مراعاة جميع المعلومات المتاحة في هذا الوقت لإتمام التقييم والمعايير المهمة في تأسيس معقولية الاستنتاج ووضوح المعلومات بما في ذلك مصداقية المصدر، أو أجهزة الرصد والاستشعار، وتاريخ المعلومات واحتمالية التعرض للخداع، وإمكانية سوء تفسير البيانات، وأن اليقين المطلق بأن العين المنوي استهدافها تستخدم عسكريًا غير ضروري، فمجرد وصول معلومات مؤكدة للقيادة العسكرية بأن العين المحددة تستخدم لغرض عسكري يرى الدليل بأن "أي مهاجم يفكر بشكل منطقي لن يتردد في الاستهداف على الرغم من وجود شك"(١).

كما يرى الدليل بأنه على الطرف الذي يقوم بالدفاع واجب تحديد طبيعة هذه العين فيما إذا كانت تستخدم لغرض طبي أو تعليمي أو غيرهما من الأغراض المدنية(٢).

ولكن هل يمكن تحديد طبيعة استخدام كل جهاز حاسوب أو شبكة حاسوبية موجودة في البنية التحتية الإلكترونية للدولة؟

الواقع من غير المتصور تطبيقه في البنية التحتية الإلكترونية، حيث إنه عالم افتراضي لا تنطبق عليه بعض المعايير المادية للتمييز، كوضع إشارات مميزه على الأعيان الطبية والأثرية كما في العالم المادي(٣)، حيث يتم تعريف كل حاسوب بواسطة عنوان (IP) وهو رمز لكل جهاز حاسوب، وهذا الرقم متغير بشكل دوري (٩١)(٤)، فلن تستطيع أي جهة تحديد هذا الجهاز وطبيعة استخدامه بسبب التغيير الدائم لعنوان ال(IP).

ويرى "شميت" أن استخدام العين المدنية لأغراض عسكرية يحولها إلى هدف عسكري وتكون عرضة للهجوم بما في ذلك الهجوم على شبكة الكمبيوتر، وينطبق هذا الوصف حتى لو أن

---

(1) A Reasonable Attacker Would Not Hesitate Before Conducting The Strike Despite The "Doubt.

(٢) أيضا وكذلك؛ ١٩٠٧، من الاتفاقية الخاصة باحترام قوانين وأعراف الحرب البرية لعام المادة (٢٧).
Kolb, R:, Military Objectives in International Humanitarian Law, Leiden Journal of International Law, 2015, 28, P. 691 700, P. 699.

(3) Schmitt, M., (2002), Wired warfare: Computer network attack and jus in Bello. International Review of the Red Cross, 84(846), P. 365-399, P. 390.

(4) Green, J., Cyber warfare: a multidisciplinary analysis, P. 37.

الاستخدام العسكري للشبكة كان ثانويًا مقارنة بالاستخدامات المدنية، وبما أن الإنترنت يستخدم للأغراض المدنية والعسكرية على السواء، ففي أوقات النزاع المسلح قد تكون كل عناصر شبكة الإنترنت هدفًا عسكريًا إذا كان تدميرها يوفر ميزة عسكرية(١).

وكذلك فإن الاستخدام المزدوج للشبكة يجعلها هدفًا عسكريًا حسب تعريف الأعيان المدنية الوارد في البروتوكول الإضافي الأول الذي عرف الأعيان المدنية بشكل سلبي، حيث عرفها بمفهوم المخالفة بأنها الأعيان التي ليست أعيانة عسكرية(٢)، فبمجرد أي استخدم عسكري للعين المدنية يفقدها حمايتها الدولية، ولهذا نجد بأن مبدأ التمييز قد تم تقييده إلى درجة عدم الوجود وأن جميع الشبكات أصبحت أهدفًا مباحة، لأنه لا يمكن التمييز فيها بين الأهداف العسكرية والمدنية.

٣. مدى ملائمة مبدأ الإنسانية للتطبيق على الحرب الإلكترونية

مبدأ الإنسانية من أقوى وأصلب مرتكزات التنظير والتقنين لكل مستجدات الحياة المعاصرة ومنها الحرب الإلكترونية، وهو مبدأ ورد في أغلب الصكوك الدولية، بحيث يعتبر ميثاق الأمم المتحدة من أبرز المواثيق الدولية التي تضمنت هذا المبدأ في ديباجته.

كما تضمن الإعلان العالمي لحقوق الإنسان (١٩٤٨م) في ديباجته (الإقرار لجميع أعضاء الأسرة البشرية من كرامة أصيلة فيهم.

ويقول بعض الفقهاء: "ويبدو لنا أن الإعلان العالمي يتمتع بقيمة قانونية تفوق تلك التي تتمتع بها التوصيات الصادرة عن الجمعية العامة وأنه يصلح أساسًا قانونيًا ترتكز عليه أجهزة الأمم المتحدة عند مباشرتها لوظائفها المؤسسية في الحالات التي لا يمكن فيها إعمال نصوص تعاهديه أخرى، كما أن عدم الاعتراف بالقيمة القانونية للإعلان يعني بالضرورة إفراغ كافة قرارات الأمم المتحدة المتعلقة بحقوق الإنسان من مضمونها وحيدتها عن أهدافها الأمر الذي سيؤثر بالسلب على نظام حماية حقوق الإنسان الذي يعتمد في تطوره على أعمال وقرارات المنظمات الدولية"(٣).

---

(1) Gill, T., McCormack, T., Geiß. R., Krieger, H., and Paulussen, C., (2016), Yearbook of International Humanitarian Law 2016, Springer Nature, Berlin, P. 298.

(2)Schmitt, M., International Law In Cyberspace: The Koh Speech And Tallinn Manual Juxtaposed, HARVARD INTERNATIONAL LAW JOURNAL, Online Volume 54. December 2012, p27.

(٣) د. عصام محمد أحمد زناتي، الإعلان العالمي لحقوق الإنسان، مجلة دراسات في حقوق الإنسان، مركز دراسات وبحوث حقوق الإنسان- جامعة أسيوط، السنة الأولى، العدد الأول، يوليو ٢٠٠٧م، ص ٣٥، ٣٦. عصام محمد أحمد زناتي، الحماية الدولية لحقوق الإنسان، الأساس القاعدي والإطار المؤسسي، الجزء الأول، دار النهضة العربية، القاهرة، بدون عام نشر، ص ٦١ونظراً لافتقار نصوص الإعلان العالمي لحقوق الإنسان للقوة الملزمة فقد شرعت لجنة حقوق الإنسان التي أنشأتها الأمم المتحدة ١٩٤٧م في صياغة هاتين الوثيقتين ثم تم مناقشتها في اللجنة الثالثة للجمعية العامة والتي تعالج المسائل الاجتماعية والإنسانية والثقافية وفي ١٦ ديسمبر سنه ١٩٦٦م اعتمدت الجمعية العامة هذين العهدين والبروتوكول الاختياري المكمل وقد دخلاً حيز التنفيذ سنة ١٩٧٦م. ود. عصام محمد أحمد زناتي، التنظيم الدولي، دار النهضة العربية، مصر، ٢٠٠٨م، ص ٣١٩. ود. معمر رتيب محمد، الحماية الإقليمية لحقوق الإنسان، مجلة مركز حقوق الإنسان جامعة أسيوط العدد الأول، ص ١٦٦.

وعليه يمكن القول بأن هذا المبدأ من المرتكزات التي يدعم بها المدى النظري والعملي ليكون محلاً صالحًا للتطبيق على الحرب الإلكترونية، والإحالة عليه في كل مشكلاتها وآثارها.

المطلب الثاني

مدى تطبيق القواعد التقليدية على الحرب الإلكترونية

تنفرد الحرب المعلوماتية بخصوصيات فارقة عن القواعد التقليدية للقانون؛ وذلك بسبب خصائصها المميزة لها، والحديث عن النوعين في هذا السياق لبيان إمكانية تطبيق القواعد التقليدية على الحروب الإلكترونية، وهو ما نقدم له بالحديث عن تطويع مفهوم الحرب الإلكترونية ليناسب مفهوم الحروب التقليدية.

تطويع مفهوم الحرب الإلكترونية ليناسب مفهوم الحرب التقليدية

إن مصطلح "حرب الإنترنت أو الحرب المعلوماتية" يشير بشكل عام إلى مجموعة من الأعمال غير الودية تمارس ضد دولة ما باستخدام السلاح الإلكتروني، وتسبب لها أضرار مباشرة تصيبها أو تصيب رعاياها(١).

ولكن هل نستطيع في ظل انتشار ظاهرة الإرهاب والجريمة المنظمة(٢)، أن نقول بأن مرونة مصطلح "الحرب"، يمكن أن يشمل أيضا "الحرب المعلوماتية"، سواء من حيث تحديد مجال تطبيق القواعد القانونية في الحرب أم من حيث ما يسمى بالحرب العادلة؟

في الحقيقة، لا يوجد في القانون الوضعي ما يسمح بتوسيع مصطلح "الحرب" بما فيه الكفاية ليشمل جميع وقائع الأفعال "التكنولوجية"، بل إن استخدام مصطلح "الحرب" في عمليات الفضاء الإلكتروني لا ينسجم من حيث الإطار القانوني مع مصطلح "الحرب" و "استخدام القوة في القانون الوضعي"(٣).

---

(١) يعتبر الأستاذ (Joshua E. Kasterberg) أن الهجمات التي تمت ضد جورجيا عام ٢٠٠٨ التي عادة ما توصف بأنها من أعمال الحرب المعلوماتية، يمكن أن تعد جرائم وفقا لاتفاقية مجلس أوربا حول الجرائم الإلكترونية. أنظر:
E. Kastenberg, «Non-Intervention and Neutrality in Cyberspace, An Emerging Principle in the National Practice of International Law», Air Force Law Review, Y..9, vol. 76, p. ٥٨.
انظر:
W. Adhami, «The Strategic Importance of the Internet for Armed Insurgent Groups in Modern Warfare», RICR, vol. ٨٩, n°٨٤٨, ٢٠٠٧, p. 864.

(٢) حول هذا الموضوع، انظر:
S. Vité, «La lutte contre la criminalité organisée: peut-on parler de conflit armé au sens où l'entend le droit international humanitaire?», Conflits armés, parties aux conflits armés et droit international humanitaire: les catégories juridiques face aux réalités contemporaines, Actes du colloque de Bruges, ٢٣-٢٢ octobre ٢٠٠٩, Collegium, n° 40, ٢٠١٠, pp. ٧٧-١٩.

(٣) أنظر: فيدا أنتولين جينكينز:
V.M. Antolin-Jenkins, «Defining the Parameters of Cyberwar Operations: Looking for Law in All the wrong Places?», Naval Law Review, .٢٠5, p. ١٣٤.

وإذا كان مصطلح "الحرب" يؤكد على خطورة الأفعال وعواقبها، فإنه لا يمكننا غالبا تحديد حالات الهجمات الإلكترونية التي تدخل ضمن هذا المصطلح، فهدف هذه الهجمات إحداث أضرار متفاوتة الخطورة تترك آثارا في الجوانب الاقتصادية أو السياسية أو العسكرية أو حتى الإنسانية، علاوة على ذلك، فإنه من خلال رصد بعض الحقائق تبين أن هجمات الحاسوب تشكل أحيانا تصرفا معزولاً(١).

وترى الباحثة أنه في خضم هذه المصطلحات، يبدو أن مصطلح "النزاع المسلح" هو أقرب المصطلحات التي تستطيع تحديد مفهوم "الحرب المعلوماتية"، أما بقية المصطلحات فيمكن أن تؤدي إلى مفاهيم غامضة، وقد لا تفي بالغرض المطلوب، وهناك رأي يدعو لوضع مصطلح يسمح بوصف جميع أنواع التصرفات الضارة عبر شبكة الإنترنت، سواء أكانت هذه التصرفات موجهه ضد دولة ما أو ضد مصالح هذه الدولة.

وإذا كانت العمليات الإلكترونية هي التي يمكن وصفها على نطاق واسع، بأنها مجموعة عمليات موجهة ضد جهاز حاسوب أو شبكة معلوماتية أو من خلال تدفق البيانات بين هذه الأجهزة والشبكات(٢)؛ فإن الهجوم الإلكتروني هو أحد مشتقاتها، فهو يقع في حال كون الدولة هي أصل العمل العدواني الموجه ضد الأهداف السياسية أو العسكرية أو الاقتصادية أو التجارية أو الاجتماعية لدولة أخرى.

إمكانية تطبيق القواعد التقليدية على الحرب الإلكترونية

تكمن صعوبة تطبيق القواعد التقليدية على الحرب الإلكترونية في الخصائص التي تفرق بين النوعين، ومع تلك الفوارق فرض سؤال التطبيق نفسه على فقهاء القانون الدولي، وكل ما قدموه في هذا الباب يعد بمثابة اللبنات الأولى لتأسيس فقه قانوني مقارن سيفضي حتماً للترجيح ويرفع الخلاف أو يقلل من حدته على الأقل(٣).

(١) أنظر: فيدا أنتولين جينكينز، مرجع سابق، ص. ١٢٧.

M. Dunn Cavelty, «Cyberwar: Concept, Status Quo, and Limitations», CSS Analysis in Security Policy, n°٧١, avril ٢٠١٠.

(٢) اللجنة الدولية للصليب الأحمر:

Comité international de la Croix-Rouge, Le droit international humanitaire et les defies posés par les conflits armés contemporains. Rapport, XXXIème Conférence de la Croix-Rouge et du Croissant-Rouge, Genève, Suisse, 28 novembre-1er décembre 2001, 31 IC/11/ 5,1,2, p.42.

(٣) انظر على سبيل المثال:

A.-T. Norodom, «Propos introductifs. Internet et le droit international: défi ou opportunité?», dans: Colloque de la S.F.D.I., Rouen, Internet et le droit international, Paris, Pedone, ٢٠١٦, pp. ١١ et suiv.

ولابد من التأكيد على أن الهجمات الإلكترونية تحتاج إلى معالجة خاصة تتكيف مع الخصوصية التي تنتج عن استخدام شبكة الإنترنت التي تتصف بالفورية والآنية بالإضافة إلى الصعوبات التي تواجه تحديد مكان وزمان هذه التصرفات(١).

وعندما ينطوي الهجوم الإلكتروني على تورط سلطات الدولة التي تحمل المسؤولية عن هذه الأعمال أو يؤدي هذا الهجوم إلى الإضرار بمصالح إحدى الدول، فإن القواعد الأساسية تعتمد على سياق الوقائع المحددة لكل حالة على حدة.

وعندما يكون النزاع المسلح موجود بالفعل، فإن القانون الدولي الإنساني يسعى إلى تطبيق قواعد هذا النزاع على الهجوم الإلكتروني نفسه(٢)؛ أي يصبح هذا الهجوم الإلكتروني مسألة فرعية أو جزء من كل، ولكن باعتبار أن الحرب تتضمن "قيام بأفعال " كشرط لتطبيق قواعد لاهاي وجنيف(٣)، والحرب المعلوماتية فقط هي التي يمكن أن يطبق عليها القانون الدولي الإنساني دون بقية الحالات أو الممارسات الإلكترونية، وكذلك فإن الحرب المعلوماتية يجب أن تحترم القواعد الآمرة في قانون الحرب، وخاصة فيما يتعلق بمبدأ الضرورة العسكرية ومبدأ التناسب ومبدأ الحياد(٤).

وعلاوة على ذلك عندما تكون قواعد الحرب قابلة للتطبيق، فإنها تواجه صعوبات جمة منها: عدم وجود قواعد محددة خاصة بالحرب المعلوماتية، وصعوبة تحديد مكان الهجوم، بالإضافة إلى تجنب السلطات الحكومية توريط نفسها بشكل مباشر في هذه الأعمال.

وهكذا على الرغم من أن القواعد التقليدية للقانون الدولي الإنساني قد تكون مفيدة في فهم الهجمات الإلكترونية، إلا أنها تبدو غير كافية.

من ناحيته، فإن القانون الدولي العام يقدم أيضا بعض الحلول، ولكنه لم يستطع الإجابة على كثير من الأسئلة، فالهجوم الإلكتروني يجب أن يحتوي على استخدام القوة بموجب القانون الدولي، وتحديدًا وفق ميثاق الأمم المتحدة؛ وبالتالي فإنه يمكن جزئيا على الأقل أن يوصف على هذا الأساس، بأنه عدوان(٥).

---

(١) أنظر:

M.N. Schmidt (dir.), Tallinn Manual on the International Law Applicable to Cyber Warfare. Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defense Centre of Excellence, Cambridge UP, ٢٠١٣, p. ١٠.

(٢) انظر:

K. Dörmann, « Applicability of the Additional Protocols to Computer Network Attacks», International Expert Conference on Computer Network Attacks and the Applicability of International Humanitarian Law, Stockholm, 17/9 novembre 2004, http://www.icrc.org/eng/resources/documents/misc/1xlgar.htm.

(٣) أنظر:

E. David, Principes de droit des conflits armés, oème éd., Bruxelles, Bruylant, P.11, p.va.

(٤) كثيرا ما يتم اختراق مبدأ الحياد في الحرب المعلوماتية بسبب ان الفاعلين قد يستخدمون أراضي الدول المحايدة.

(٥) انظر علي سبيل المثال:

M.N. Schmitt, « Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework », Columbia Journal of Transnational Law, 1974, pp.

كذلك فإن الهجوم الإلكتروني عندما يأتي كإجراء انتقامي أو كإجراء مضاد، فإنه يمكن أن يخضع للنظام القانوني ذي الصلة؛ وبالتالي عندما يكون الهجوم الإلكتروني نوعا من الإجراءات الانتقامية، فإنه يجب ألا يسبب إلا أضرارا محدودة، لأنه يخضع لمبدأ التناسب وهو السبيل الوحيد لرد العدوان(١).

ويجب التنويه أيضًا إلى أنه في كثير من الأحيان يتم اللجوء إلى مبدأي الإقليمية والشخصية بالنسبة للقوانين التي تسمح عادة بتحديد اختصاصات الدولة، وذلك لتطبيق القواعد القانونية المناسبة على جرائم الشبكة العنكبوتية(٢).

المطلب الثالث

إمكانية تطبيق القانون الدولي لحقوق الإنسان على الحرب الإلكترونية

تعرف حقوق الإنسان بأنها: فرع من فروع العلوم الاجتماعية ويختص بتحديد الحقوق والرخص الضرورية التي تتيح ازدهار شخصية كل فرد في المجتمع استنادا إلى كرامته الإنسانية(٣).

وبفضل صفتي العموم والشمول التي يتمتع بها هذا القانون يعتبر أوسع مجالاً من القانون الدولي الإنساني كما يتميز بالدوام(٤) مما يجعله أقدر على احتواء وفهم أغلب ظواهر الحرب الإلكترونية وعواقبها ضد الأفراد، خاصة أن الحالات التي يعالجها القانون الدولي لحقوق الإنسان ليس من الضروري أن تكون محكومة بقواعد القانون الدولي الإنساني وبالتالي فإن قواعد القانون الدولي لحقوق الإنسان يمكن أن تكون قابلة للتطبيق على الهجمات الإلكترونية بصورة مرنة وعملية.

---

٨٨٥ - ٩٣٦; M. Roscini, World Wide Warfare - Jus ad bellum and the Use of Cyber Force», Max Planck UNYB, ٢٠١٠, pp. ٨٥ -١٣٠.

(١) انظر:

Tribunal arbitral germano-portugais, Affaire de Lysne (Responsabilité de l'Allemagne à raison des actes commis postérieurement au ri juillet 1918 et avant que le Portugal ne participat a la guerre), RSA II, p. 1.56.

(٢) انظر علي سبيل المثال:

Ph. Lagrange, «Internet et l'évolution normative du droit international: d'un droit international applicable à l'Internet à un droit international du cyberespace?», dans: Colloque de la S.F.D.I., Rouen, Internet et le droit international, Paris, Pedone, P. 11, p. 28.

(٣) د. أحمد عبد الكريم سلامة وآخرون حقوق الإنسان وأخلاقيات المهنة، دراسة في بعض القوانين المصرية والمواثيق الدولية، جهاز نشر وتوزيع الكتاب الجامعي جامعة حلوان ٢٠٠٥م ص ١١. و د. عزت سعد السيد البرعي، حماية حقوق الإنسان في ظل التنظيم الدولي الإقليمي دار النهضة العربية القاهرة ١٩٨٥م ص ٤. ود. محمد كمال القاضي، حقوق الإنسان، جامعة حلوان، كلية الآداب، القاهرة، ٢٠٠٦م، ص ١٤. ود. أحمد الرشيدي حقوق الإنسان دراسة مقارنة في النظرية والتطبيق مكتبة الشروق الدولية ٢٠٠٣ ط ١ ص ٣٥. ود. الشافعي محمد بشير، قانون حقوق الإنسان، مصادره وتطبيقاته الوطنية والدولية، منشأة المعارف، الإسكندرية، ٢٠٠٧، ص ٣٥.

(٤) من المعروف أن القانون الدولي لحقوق الإنسان يطبق في جميع الاوقات (السلم والحرب)، بعكس القانون الدولي الإنساني أو ما يسمى (بقانون الحرب الذي لا يطبق إلا في وقت الحرب.

كما أن القانون الدولي لحقوق الإنسان يقدم إطارًا جديدًا قد يساعد على حل اثنتين من الصعوبات القانونية الرئيسة التي تثيرها الحرب المعلوماتية، الأولى: إسناد الهجوم الإلكتروني إلى دولة معينة، والثانية: تحديد قواعد القانون التي يجوز أن تحكم آثار هذا الهجوم على الأفراد.

ففي قضية العراقيين الذين قتلتهم القوات البريطانية والتي عرضت على المحكمة الأوروبية لحقوق الإنسان عام (٢٠٠٧م) المتعلقة بانتهاكات حقوق الإنسان، أثيرت عدة نقاشات حول إمكانية الولاية القضائية خارج الحدود دون وجود أي علاقة بين الأفعال المجرمة وبين هذا القضاء الأجنبي، وتتلخص وقائع هذه القضية[١] بتقديم مجموعة من المواطنين العراقيين شكاوي فردية إلى المحكمة الأوروبية لحقوق الإنسان بخصوص مقتل أقاربهم من قبل القوات البريطانية في مدينة البصرة، وقد دفعوا بأن أقاربهم قتلوا وهم يخضعون لقضاء المملكة المتحدة وولايتها، حسب ما تنص عليه المادة الأولى من الاتفاقية الأوروبية لحقوق الإنسان[٢].

كما تشملهم حماية حق الحياة التي تقررها المادة الثانية من هذه الاتفاقية، وحظر التعذيب والعقوبات والمعاملات غير الإنسانية أو المهينة التي تنص عليها المادة الثالثة من الاتفاقية.

وقد بينت المحكمة الأوروبية أن المملكة المتحدة كانت تملك الولاية القضائية التي تنص عليها المادة الأولى من الاتفاقية الأوروبية لحقوق الإنسان فيما يخص المدنيين الذين قتلوا خلال الأعمال الأمنية التي قامت بها القوات البريطانية في البصرة وذلك أثناء الظروف الاستثنائية المرتبطة بمسؤولية المملكة المتحدة المكلفة بسلامة جنوب شرق العراق خلال الفترة ما بين الأول من الشهر الخامس من عام (٢٠٠٣م) وحتى (٢٠٠٤/٦/٢٨م).

وحكمت المحكمة الأوروبية بمقتضى المادة (٤١) من الاتفاقية الأوروبية[٣]، بترضية عادلة للمدعين، وطلبت من حكومة المملكة المتحدة أن تدفع لكل مدع مبلغ (١٧) ألف يورو كتعويض معنوي، ومبلغ (٥٠) ألف يورو بالتضامن بينهم كنفقات دعوى[٤].

نخلص مما سبق إلى أن القانون الدولي لحقوق الإنسان، يحتوي على خصائص وميزات تجعله أكثر مرونة وسعة وشمولاً من القانون الدولي الإنساني، وبهذه الخلاصة نختتم مسار هذا البحث.

---

(١) للمزيد من التفاصيل حول هذه القضية، راجع د. محمد أمين الميداني، دراسات في الحماية الإقليمية لحقوق الإنسان، مركز المعلومات والتأهيل لحقوق الإنسان، تعز، طبعة ثانية معدلة ومزيدة، ٢٠١٢، صفحة ٣٧٠ وما بعدها.

(٢) تنص المادة الأولى من الاتفاقية الأوروبية لحقوق الإنسان على أن "تعترف كل الأطراف السامية المتعاقدة لجميع الأشخاص الخاضعين لولايتها القانونية بالحقوق والحريات الواردة في القسم الأول".

(٣) تنص المادة ٤١ من هذه الاتفاقية الأوروبية، وعنوانها ترضية عادلة، على ما يلي: "إذا قررت المحكمة بأن هناك مخالفة للاتفاقية أو لبروتوكولاتها، وإذا كان القانون الداخلي للطرف السامي المتعاقد لا يسمح بإزالة نتائج هذه المخالفة بشكل تام، تمنح المحكمة للطرف المتضرر، إذا استدعى الأمر، ترضية عادلة".

(٤)الدكتور محمد أمين الميداني، مرجع سابق، ص. ص. ٣٧٢-٣٧٣.

خاتمة:

عالج هذا البحث إمكانية ومدى تطبيق قواعد القانون الدولي الإنساني والمبادئ الأساسية والقواعد التقليدية وقانون حقوق الإنسان على الحرب الإلكترونية، وهو ما عبر عنه بأنسنة الحرب الإلكترونية، ومن أهم نتائجه وتوصياته ما يلي:

أولاً النتائج:

١. يرى الفقه الدولي أن الحرب الإلكترونية حربًا حقيقية؛ لما لها من آثار مدمرة على العالم المادي وتسمح بالرد من خلال الآلية الحديثة للدفاع.

٢. ذهب جانب من الفقه القانوني الأوروبي والأمريكي إلى اعتبار منطقة الفضاء الإلكتروني منطقة خاليه من القانون، لعدم وجود نص قانوني يعالج الهجوم على شبكات الحاسوب، أو حرب المعلومات أو العمليات المعلوماتية، كما لم يتم وضع قواعد للهجوم على شبكات الحاسوب أثناء النزاعات المسلحة.

٣. أكدت اللجنة الدولية للصليب الأحمر شرعية وضرورة تطبيق القانون الدولي الإنساني على الهجمات الإلكترونية، وأكدت المواثيق الدولية الأخرى المعنية بتنظيم السلاح والنزاعات المسلحة أن على المتحاربين احترام وحماية المرافق المدنية الضرورية والمواد التي لا غني عنها لبقاء السكان المدنيين وأن الاعتداء عليها من خلال الهجمات الإلكترونية يشكل انتهاكا للقانون الدولي الإنساني.

٤. غياب أي إشارات في القانون الدولي الإنساني إلى الاستهداف المباشر للأشخاص المدنيين والأعيان المدنية للعمليات التي تدور في الفضاء الإلكتروني، لا يعني أن قواعد القانون الدولي الإنساني لا تغطي وسائل وأساليب الحرب الإلكترونية.

٥. أشارت محكمة العدل الدولية إلى مجموعة من المبادئ التي تكفل حماية المدنيين من جميع الأخطار التي تسببها الأسلحة الحديثة التي لم تنظمها اتفاقيات دولية للحد من أخطارها.

٦. المشكلة في استخدام الحاسوب والانترنت في الحرب هي مشكلة عملية، وليست قانونية فقط، فقد يعتمد الجيش على الأهداف المزدوجة الاستعمال كشبكة الاتصالات والطرق والجسور، معرضًا بذلك المدنيين إلى ضرر حتمي.

٧. بفضل صفة العمومية التي يتمتع بها القانون الدولي لحقوق الإنسان وشموليته وقدرته على الدوام والاستمرار فهو يعد أعم وأشمل من القانون الدولي الإنساني؛ وكذلك يتميز بالدوام، مما يجعله شبه قادر على احتواء وفهم أغلب ظواهر الحرب الإلكترونية وعواقبها.

ثانيًا – التوصيات

١. يوصي البحث بضرورة تحليل مختلف العناصر والظروف لتحديد إمكانية تطبيق القانون الدولي الحالي على النزاعات الإلكترونية، وفقاً لواقع يقول إن القانون القائم يواجه إشكالات في التطبيق يمكن تجاوزها من خلال إبرام اتفاقية دولية جديدة بشأن الحرب الإلكترونية.

٢. ضرورة تكاتف الجهود الدولية والإقليمية، من أجل وضع تنظيم دولي ملزم للدول ينظم النزاعات الدولية المسلحة التي يتم فيها استخدام الأسلحة الإلكترونية، وتمنع التسلح السيبراني خلافًا لمبادئ القانون الدولي الإنساني.

٣. الاهتمام بالشروط التي وضعها دليل تالين الذي نص على "أن أطراف النزاع ملزمة بمراعاة عدة أحكام قبل تنفيذ الهجمة الإلكترونية منها دراسة آثار الأسلحة السيبرانية على البنية التحتية للمستخدمين العسكريين والمدنيين على حد سواء".

مراجع البحث:

أولاً: المراجع باللغة العربية:

أ-الكتب:

مجمع اللغة العربية بالقاهرة، المعجم الوسيط، (إبراهيم مصطفى/ أحمد الزيات/ حامد عبد القادر/ محمد النجار)، الناشر: دار الدعوة، ط.د، ت.د.

أحمد عبيس نعمة، الهجمات السيبرانية، ط١، منشورات زين الحقوقية، بيروت، ٢٠١٨م.

د. أحمد عبد الكريم سلامة وآخرون حقوق الإنسان وأخلاقيات المهنة، دراسة في بعض القوانين المصرية والمواثيق الدولية، جهاز نشر وتوزيع الكتاب الجامعي جامعة حلوان ٢٠٠٥م.

د. أحمد فتحي سرور، القانون الدولي الإنساني دليل للتطبيق على الصعيد الدولي، ط١، القاهرة، ٢٠٠٣م.

د. أحمد الرشيدي حقوق الإنسان دراسة مقارنة في النظرية والتطبيق مكتبة الشروق الدولية ٢٠٠٣ط١.

د. الشافعي محمد بشير، قانون حقوق الإنسان، مصادره وتطبيقاته الوطنية والدولية، منشأة المعارف، الإسكندرية، ٢٠٠٧م.

جان بكتيه، مبادئ القانون الدولي الإنساني، بحث منشور في كتاب محاضرات في القانون الدولي الإنساني، خرير شريف غتلم، منشورات اللجنة الدولية للصليب الأحمر.

صفات أمين سلامة، أسلحة حروب المستقبل بين الخيال والواقع، أبو ظبي، مركز الامارات للدراسات والبحوث الاستراتيجية، ٢٠١١.

د. عزت سعد السيد البرعي، حماية حقوق الإنسان في ظل التنظيم الدولي الإقليمي دار النهضة العربية القاهرة، ١٩٨٥م.

د. عصام محمد أحمد زناتي، الإعلان العالمي لحقوق الإنسان، مجلة دراسات في حقوق الإنسان، مركز دراسات وبحوث حقوق الإنسان- جامعة أسيوط، السنة الأولى، العدد الأول، يوليو ٢٠٠٧م.

د. عصام محمد أحمد زناتي، الحماية الدولية لحقوق الإنسان، الأساس القاعدي والإطار المؤسسي، الجزء الأول، دار النهضة العربية، القاهرة، بدون عام نشر.

د. عصام محمد أحمد زناتي، التنظيم الدولي، دار النهضة العربية، مصر، ٢٠٠٨م.
د. محمد أمين الميداني، دراسات في الحماية الإقليمية لحقوق الإنسان، مركز المعلومات والتأهيل لحقوق الإنسان، تعز، طبعة ثانية معدلة ومزيدة، ٢٠١٢م.
محمد الطراونة: القانون الدولي الإنساني– النص وآليات التطبيق على الصعيد الوطني الأردني، مركز عمان لدراسات حقوق الإنسان، عمان– الأردن (٢٠٠٣).
د. محمد كمال القاضي، حقوق الإنسان، جامعة حلوان، كلية الآداب، القاهرة، ٢٠٠٦م.
فيصل محمد الغفار، الحرب الإلكترونية، ط١، الجنادرية للنشر والتوزيع، الاردن، لبنان، ٢٠١٦م
هينين ويجنر، مفهوم بشأن السلام السيبراني، البحث عن السلام السيبراني، البحث عن السلام السيبراني، الناشر الاتحاد الدولي.
وليام، بارليتا، النزاع السيبراني والاستقرار الجيوسيبراني، ط١، الاتحاد الدولي للاتصالات والاتحاد العالمي للعلماء، ٢٠١١م.

ب–الأبحاث

شيماء جمال محمد، الحرب الإلكترونية واستراتيجية الدول لمواجهتها، مجلة كلية القانون والعلوم السياسية، جامعة كركوك، مج ١٠، ع ٣٦، ٢٠٢١م.
إيف ساندوز، حظر وتشييد استعمال أسلحة معينة، ثلاثة أسئلة جوهرية، المجلة الدولية للصليب الأحمر العدد ٣٧، ١٩٩٤م.
شافان دي يونس، تقرير اجتماع خبراء اللجنة الدولية للصليب الأحمر، الأسلحة المتفجرة في المناطق المأهولة، الجوانب الإنسانية والقانونية والتقنية والعسكري، سويسرا، ٢٠١٣.
شريف نسيم قلته، دليل تالين والهجمات الإلكترونية وحظر استخدام القوة في القانون الدولي، بحث منشور في مركز الفضاء العربي للأبحاث الفضاء الإلكتروني، ع ١٦٤، ٢٠١٧م.
شميت، مايكل.، الحرب بواسطة شبكات الاتصال: الهجوم على شبكات الكمبيوتر (الحاسوب) والقانون في الحرب، المجلة الدولية الصليب الأحمر، (٢٠٠٢).
عبدالله بن عبدالعزيز العجلان، الإرهاب الإلكتروني في عصر المعلومات، بحث مقدم إلى المؤتمر الدولي الأول حول "حماية أمن المعلومات والخصوصية في قانون الإنترنت"، والمنعقد بالقاهرة، يونيو ٢٠٠٨م.
عمر محمود عمر، الحرب الإلكترونية في ضوء القانون الدولي الإنساني، بحث منشور في مجلة دراسات علوم الشريعة والقانون، مج ٤٦، ع٣، ٢٠١٩م
د. طالب حسن موسى، ود. عمر محمود أعمر، الإنترنت قانونا، مجلة الشريعة والقانون، جامعة الإمارات العربية المتحدة، العدد السابع والستين، ص٣٣٩، (١٦) (٢٠١٦م).

د. عصام محمد أحمد زناتي، الإعلان العالمي لحقوق الإنسان، مجلة دراسات في حقوق الإنسان، مركز دراسات وبحوث حقوق الإنسان– جامعة أسيوط، السنة الأولى، العدد الأول، يوليو ٢٠٠٧م.

د. علي عبد المعطي الحمدان، الحرب المعلوماتية وإمكانية تطبيق قواعد حقوق الإنسان، مجلة العلوم الشرعية، جامعة القصيم، مج ١٢، ع١، ٢٠١٨م.

د. عمر محمود أعمر، الحرب الإلكترونية في القانون الدولي الإنساني، الجامعة الأردنية، مج ٦٦، ع ٣، ٢٠١٩م.

د. محمد كمال القاضي، حقوق الإنسان، جامعة حلوان، كلية الآداب، القاهرة، ٢٠٠٦م.

د. معمر رتيب محمد، الحماية الإقليمية لحقوق الإنسان، مجلة مركز حقوق الإنسان جامعة أسيوط العدد الأول.

فرونيك كريستوري، القانون الدولي الإنساني توفر طبقة إضافية من الحماية، تقرير عن الحد من التسلح في اللجنة الدولية للفريق العامل المفتوح العضوية المعني بالتطورات في ميدان المعلومات والاتصالات في سياق الأمن الدولي، ١٠ أيلول، ٢٠١٩.

لويز دوسوالد بيت، القانون الدولي الإنساني وفتوى محكمة العدل الدولية بشأن مشروعية التهديد بالأسلحة النووية أو استخدامها المجلة الدولية للصليب الأحمر العدد ٣١٦، ١٩٩٧.

هينين ويجنر، مفهوم بشأن السلام السيبراني، البحث عن السلام السيبراني، البحث عن السلام السيبراني، الناشر الاتحاد الدولي.

وليام، بارليتا، النزاع السيبراني والاستقرار الجيوسيبراني، ط١، الاتحاد الدولي للاتصالات والاتحاد العالمي للعلماء، ٢٠١١م.

ثانيًا المراجع باللغة الأجنبية:

أ–المراجع باللغة الفرنسية:

Cordula Droege, conseillere juridique au CICR.Pas de vide juridique dans le cyberspace, CICR Comité international de la Croix-Rouge: https://www.icrc.org/.../interview/.... cyber-warfare-interview-2011-0.

E. David, Principes de droit des conflits armés, oème éd., Bruxelles, Bruylant.

Joseph S. Nye, Cyber War and Peace, project syndicate, 10 April 2012, http//:www.project-syndicate.org/commentary/cyber-war-and-peace http://ar.wikipedia.org/wiki/%D8%AD%D8%B.

Lavenue, J., Cyberspace ET Droit International: pour UN nouveau Jus Communications: Revue de la Recherche, (1996) .

Lovan, M., Vittor, F., intervention militaire en Iraq et le droit international, La doctrine europeenne, Annuaire francais de droit international, Volume (2003).

Ph. Lagrange, « Internet et l'évolution normative du droit international: d'un droit international applicable à l'Internet à un droit international du cyberespace? », dans: Colloque de la S.F.D.I., Rouen, Internet et le droit international, Paris, Pedone, Roscini, M., (, Cyber Operations and the Use of Force in International Law. Oxford:Oxford University Press, 2014).

S. Vité, «La lutte contre la criminalité organisée: peut-on parler de conflit armé au sens où l'entend le droit international humanitaire? », Conflits armés, parties aux conflits armés et droit international humanitaire: les catégories juridiques face aux réalités contemporaines, Actes du colloque de Bruges, 22-23 octobre 2009, Collegium, n° 40, 2010.

ب-المراجع باللغة الإنجليزية

Brown, D., Proposal for an international convention to regulate the use of information System in Armed Conflict, Harvard International Law review, Vol (2006).

E. Kastenberg, « Non-Intervention and Neutrality in Cyberspace, An Emerging Principle in the National Practice of International Law», Air Force Law Review.

Gill, T., McCormack, T., Geiß. R., Krieger, H., and Paulussen, C., Yearbook of International Humanitarian Law 2016, Springer Nature, Berlin, (2016).

Hoisington, M., Cyberwarfare and the Use of Force Giving Rise to the Right of Self-Defense, 32(2), Boston College International and Comparative Law Review, 2009.

John Arquilla and David Ronfeldt, Cyberwar Is Coming, Comparative Strategy, Vol.12, No.2, Spring 1993.

Joseph S. Nye, Cyber War and Peace, project syndicate, 10 April 2012, http//:www.project-syndicate.org/commentary/cyber-war-and-peace http://ar.wikipedia.org/wiki/%D8%AD%D8%B

K. Dörmann, «Applicability of the Additional Protocols to Computer Network Attacks», International Expert Conference on Computer Network Attacks and the Applicability of International Humanitarian Law, Stockholm, 17/9 novembre 2004, http://www.icrc.org/eng/resources/documents/misc/1xlgar.htm .

Kelsey, J., (2008) Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare, Michigan Law Review, Volume 106, Issue 7.

Koh, H, International Law in Cyberspace, Harvard International Law Journal, Online, volume., (2012).

Kolb, R:, Military Objectives in International Humanitarian Law, Leiden Journal of International Law, 2015.

Lesley Swanson, The Era of Cyber Warfare: Applying International Humanitarian Law to the 2008 Russian-Georgian Cyber Conflict,

Loyola of Los Angeles International and Comparative Law Review Law Reviews, 2010.

Lieber, Francis, Instructions for the Government of Armies of the United States in the field, 1898.

Lieber, Francis, Instructions for the Government of Armies of the United States in the field, 1898 .

M. Dunn Cavelty, «Cyberwar: Concept, Status Quo, and Limitations», CSS Analysis in Security Policy, n° 71، avril 2010.

M.N. Schmidt (dir.), Tallinn Manual on the International Law Applicable to Cyber Warfare. Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defense Centre of Excellence, Cambridge UP, 2013.

M.N. Schmitt, « Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework », Columbia Journal of Transnational Law, 1974.

M. Roscini, World Wide Warfare - Jus ad bellum and the Use of Cyber Force», Max Planck UNYB, 2010.

Michael N. Schmitt, Heather A. Harrison Dinniss, Thomas C. Wingfield, Background Paper prepared for Informal High-Level Expert Meeting on Current Challenges to International Humanitarian Law, Cambridge, June 25-27, 2004 www.hsph.harvard.edu/

Nicolo Bussolati, The Rise of Non-State Actors in Cyberwarfare, in Jens David Ohlin, Kevin Govern and Claire Finkelstein (eds.), Cyberwar: Law and Ethics For Virtual Conflicts, (Oxford: Oxford University Press, 2015).

Schmitt, M., Wired warfare: Computer network attack and jus in Bello. International Review of the Red Cross, 84(846). (2002)

Schmitt, M., International Law in Cyberspace The Koh Speech and. Tallinn Manual Juxtaposed. Harvard International Law Journal, December, 2012, Volume 54.... www.harvardilj.org/wp-content/.../12/HILJ-Online_54_Schmitt.pdf.

Schindler, D. International Humanitarian Law and Internationalized Internal Armed Conflicts, International. (1982).

V.M. Antolin-Jenkins, « Defining the Parameters of Cyberwar Operations: Looking for Law in All the wrong Places? », Naval Law Review.

W. Adhami, « The Strategic Importance of the Internet for Armed Insurgent Groups in Modern Warfare », RICR, vol. 89, n°848, 2007,

Wingfield, T.,The Law of information Conflict: National Security Law in Cyberspace, Aegis ResearchCorp., Falls Church, VA, 2000; The Law of Armed Conflict: Basic Knowledge, international Committee of the Red Cross, June 2002. http:/www.icrc.org.