مجلة العلوم القانونية و الاجتماعية

Journal of legal and social studies

Issn: 2507-7333

Eissn: 2676-1742

الحرب الإلكترونية والقانون الدولي الإنساني

Electronic warfare and international humanitarian law

عليوة صبرينا *

جامعة زيان عاشور الجلفة ، (الجزائر)، alioua.sab@gmail.com

تاريخ ارسال المقال: 2022/06/01	تاريخ القبول: 2022/08/13	تاريخ النشر: 2022/09/01

*المؤلف المرسل

الملخص:

الحرب الإلكترونية من أهم المواضيع المطروحة على الساحة الدولية، لما تثيره من جدل حول إمكانية خضوعها لقواعد القانون الدولي الإنساني في ظل الخصوصية التي تتميز بها عن الحرب التقليدية، وفي هذه الدراسة سنحاول إلقاء الضوء على مفهوم الحرب الإلكترونية من جهة، وإمكانية شمولية قواعد القانون الدولي الإنساني واستيعابها لهذا النوع من الحروب من جهة أخرى، كون الحرب الإلكترونية لا تقل شراسة عن الحروب التقليدية من ناحية الآثار، وستكون أبرز الحروب المستقبلية في ظل التطور التكنولوجي المستمر .

الكلمات المفتاحية: الحرب الإلكترونية ؛ القانون الدولي الإنساني ؛ العمليات الإلكترونية

Abstract :

Electronic warfare is one of the most important topics on the international scene, because of the controversy it raises about the possibility of being subject to the rules of international humanitarian law in light of the privacy that it enjoys over conventional war،

In this study, we will try to shed light on the concept of electronic warfare on the one hand, and the possibility of comprehensiveness of the rules of international humanitarian law for this type of war on the other hand, because electronic warfare is no less fierce than conventional wars in terms of effects and will be the most prominent future wars in light of the continuous technological development.

Keywords: Electronic warfare ; International humanitarian law ؛ Electronic operations

مقدّمة:

يحظى موضوع الحرب الإلكترونية باهتمام متزايد من قبل فقهاء القانون الدولي وخبرائه، على اعتبار أن الواقع الدولي يثبت اللجوء إلى هذا الشكل الجديد من الحروب في الوقت الراهن، وسيكون أكثر استخداما في المستقبل.

ومنذ نهاية الحرب العالمية الأولى، حدثت تطورات تقنية كبيرة أدت إلى ظهور معدات وأنظمة الكترونية متطورة تم استخدامها استخداما واسعا في المجالات العسكرية خاصة في أنظمة القيادة والسيطرة وتوجيه الأسلحة والاتصالات ذات التقنية العالية .

وقد أدى استخدام الأسلحة المتطورة ذات الدقة العالية إلى تقصير فترات الحروب التقليدية، وتحطيم قدرات الأطراف المتحاربة وفعاليتها منذ المراحل الأولى للقتال، وكان للتطورات الإلكترونية الدور الكبير في إحداث هذه التغييرات، وهكذا فقد برز دور الحرب الإلكترونية وما انجر عنها من عمليات الكترونية تطبق في كافة الأعمال القتالية، لمختلف أنواع القوات المسلحة، سواء في الهجوم أو الدفاع. (1)

إن العمليات الإلكترونية في حالات النزاع المسلح، قد يكون لها عواقب وخيمة للغاية، خاصة وأن تأثيرها لا يقتصر على بيانات النظام الحاسوبي، أو أجهزة الكمبيوتر المستهدفة، فالعمليات الإلكترونية تهدف عادة إلى إحداث تأثير في العالم الواقعي، حيث تخلف بعض العمليات الإلكترونية تأثيرا هائلا على السكان المدنيين. (2)

من هذا المنطلق تتجلى الأهمية البالغة لهذا الموضوع إذ أنه من الضروري تحليل قواعد القانون الدولي الإنساني ومدى مواءمتها للحرب الإلكترونية.

إن الهدف من هذه الدراسة يتعلق بمعرفة إن كان من الممكن أن تنظم قواعد القانون الدولي الإنساني بشكلها الحالي، الحرب الإلكترونية في ظل الخصوصية التي تتمتع بها هذه الأخيرة .

وعليه يمكن طرح الإشكالية التالية :

ما مدى خضوع الحرب الإلكترونية لقواعد القانون الدولي الإنساني؟ .

إن طبيعة الموضوع تفترض إتباع منهج استقرائي تحليلي، كما أن الإجابة عن الإشكالية ستكون من خلال تقسيم الدراسة إلى مبحثين، يتعلق الأول بمفهوم الحرب الإلكترونية ويتم التركيز فيه على تعريفها وخصائصها، فيما يرتبط المبحث الثاني بإمكانية تطبيق قواعد القانون الدولي الإنساني على الحرب الإلكترونية بالتعرض إلى الجدل الفقهي المثار حول هذه النقطة تحديدا، ثم القيام بعملية إسقاط مبادئ القانون الدولي الإنساني على الحرب الإلكترونية .

المبحث الأول: مفهوم الحرب الإلكترونية :

تكمن خطورة حروب الانترنيت والشبكات في كون العالم أصبح يعتمد أكثر فأكثر على الفضاء الإلكتروني لاسيما في البنى التحتية المعلوماتية العسكرية والمصرفية والحكومية إضافة إلى المؤسسات والشركات العامة والخاصة، ولاشك أن ازدياد الهجمات الإلكترونية يرتبط أيضا بازدياد هذا الاعتماد على شبكات الكمبيوتر والانترنيت في البنية التحتية الوطنية الأساسية، وهو ما يعني إمكانية تطور الهجمات الإلكترونية اليوم لتصبح سلاحا حاسما في النزاعات بين الدول في المستقبل، علما أن أبعاد مفهوم الحرب الإلكترونية لا تزال غير مفهومة.(3)

سنحاول من خلال هذا المبحث تسليط الضوء على تعريف الحرب الإلكترونية في المطلب الأول ثم التطرق إلى الخصائص التي تميزها عن الحروب التقليدية في المطلب الثاني .

المطلب الأول: تعريف الحرب الإلكترونية :

ليس هناك إجماع على تعريف محدد ودقيق لمفهوم الحرب الإلكترونية، وعلى الرغم من ذلك ، فقد اجتهد عدد من الخبراء على اختلاف اختصاصاتهم في تقديم تعريف يحيط بهذا المفهوم، فعرف " ريتشارد كلارك " الحرب الإلكترونية على أنها " أعمال تقوم بها دولة تحاول من خلالها اختراق أجهزة الكمبيوتر والشبكات التابعة لدولة أخرى بهدف تحقيق أضرار بالغة أو تعطيلها " .

فيما يعرف آخرون مصطلح الحرب الإلكترونية بأنها " مفهوم يشير إلى أي نزاع يحدث في الفضاء الإلكتروني ويكون له طابع دولي ".(4)

أما من الناحية العملية فتعرف الحرب الإلكترونية بأنها " مجموعة الإجراءات الإلكترونية المتضمنة استخدام بعض النظم والوسائل الإلكترونية في استطلاع الإشعاع الكهرومغناطيسي الصادر من نظم العدو ووسائله ومعداته الإلكترونية المختلفة مع الاستخدام المتعمد للطاقة الكهرومغناطيسية في التأثير على هذه النظم والوسائل لمنع العدو أو حرمانه، أو تقليل استغلاله للمجال الكهرومغناطيسي، فضلا عن حماية الموجات الكهرومغناطيسية المستخدمة من استطلاع العدو لها، أو التأثير عليها ".(5)

تبدو هذه التعريفات عامة وواسعة، لذلك لابد من الوصول إلى تعريف يتماشى مع القانون الدولي الإنساني، على اعتبار أن الهدف في هذا الإطار هو تحديد مفهوم الحرب الإلكترونية التي يمكن أن تكون موضوعا للقانون الدولي الإنساني .

في هذا السياق أوضحت اللجنة الدولية للصليب الأحمر أن تعبير الحرب الإلكترونية يستخدم 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.

كما تعتبر اللجنة أن تعرض 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 ما تعطلت أنظمة تحديد المواقع GPS عن العمل، قد تحدث إصابات في صفوف المدنيين من خلال تعطيل عمليات

إقلاع مروحيات الإنقاذ على سبيل المثال، ويمكن أن تتعرض السدود والمحطات النووية وأنظمة التحكم في الطائرات لهجمات الكترونية نظرا لاعتمادها على الحواسيب .[6]

وقد عرف دليل تالين[7] الهجمات السيبرانية بأنها " عمليات سيبرانية، سواء كانت هجومية أو دفاعية، والتي يهدف من خلالها بصورة معقولة التسبب بالإصابة أو وفاة الأشخاص أو الإضرار أو تدمير الأعيان ".[8]

وفي هذا الإطار تجدر الإشارة إلى أن الحرب الإلكترونية هي نوع أو جزء من الهجمات السيبرانية التي تحدث في أثناء نزاع مسلح حركي أو التي تنتج آثارا مادية تشبه وتعادل آثار الهجمات المسلحة التقليدية، بينما الهجمات السيبرانية هي كل نشاط سيبراني ضار بالدول الأخرى سواء كان في وقت السلم أو في سياق نزاع مسلح حركي وسواء نتجت عنه آثار مادية جسيمة في الأرواح أو الممتلكات أو لم يؤد إلا إلى تشويش أنظمة الكمبيوتر فيها ما دام كان ذلك لأغراض أمنية وعسكرية.[9]

المطلب الثاني: خصائص الحرب الإلكترونية :

يقر الكثير من المراقبين بوجود اختلافات واضحة بين الفضاء الإلكتروني والمادي التقليدي – ومن ثم بين الحرب الإلكترونية والحرب التقليدية – والتي يمكن إجمالها في ما يلي[10]:

- مكان النزاع : في النزاع الحركي التقليدي (أي النزاع الذي تخوضه قوات منظمة تسيطر عليها الحكومة باستخدام أسلحة حركية)، يجري الكثير من الأنشطة العسكرية (لاسيما تلك التي تحدث في الجو وعلى المحيط أو تحته) في مجال منفصل إلى حد كبير عن الحيز الذي توجد فيه أعداد كبيرة من المدنيين، أما في الحرب الإلكترونية فإن الحيز الذي يجري فيه الكثير من الأنشطة العسكرية يتسم بأن المدنيين ينتشرون فيه في كل مكان.
- التوازن بين الهجوم والدفاع : في النزاع الحركي التقليدي تكون التقنيات الهجومية والتقنيات الدفاعية في الغالب في حالة توازن تقريبي، أما في الحرب الإلكترونية (وعلى الأقل قبل اندلاع العمليات العدائية المكشوفة) فإن الهجوم يتفوق بطبيعته على الدفاع ، لأن الهجوم يتطلب أن يكون ناجحا مرة واحدة فقط، لكن الدفاع يتطلب أن ينجح في كل مرة، ولأنه لا سبيل لضمان أن مدخلات المعلومات الضارة أو المغلوطة أو المعيبة (سواء كانت برامج أو بيانات) لن يتم إدخالها في نظام قائم على تكنولوجيا المعلومات .
- إسناد المسؤولية : النزاع الحركي التقليدي تخوضه قوات عسكرية يفترض أنها تحت سيطرة حكومات وطنية، ولا تصدق مثل هذه الافتراضات على الفاعلين المشاركين في الحرب الإلكترونية، ونسبة الأفعال التي تجري في الفضاء الإلكتروني بشكل قاطع إلى حكومات وطنية أمر صعب للغاية أو مستحيل .
- قدرات الفاعلين من غير الدول : في النزاع الحركي التقليدي، تكون الآثار التي تتحقق بوجه عام مرهونة بعدد القوات العسكرية التي يمكن أن تشارك في القتال، وحيث إن مثل هذه الأعداد تكون في العادة أصغر لدى الفاعلين من غير الدول عما هو متاح للدول، فإن الآثار التي يمكن للفاعلين من غير الدول إحداثها تكون صغيرة نسبيا بالمقارنة بما يمكن أن يحدثه فاعلون تابعون للدول مجهزون تجهيزا جيدا، أما في الحرب

الإلكترونية فإن الفاعلين من غير الدول يمكنهم استخدام قدرات تكنولوجيا المعلومات لإحداث بعض الآثار واسعة النطاق التي يستطيع تحقيقها فاعلون كبار .

- أهمية بعد المسافات والحدود الوطنية : في النزاع الحركي التقليدي، تبدو المسافات كبيرة وانتهاكات الحدود الوطنية مهمة، أما في الحرب الإلكترونية فإن المسافات ليست ذات أهمية، واختراقات الحدود الوطنية للهجوم أو بغرض الاستغلال تحدث بشكل روتيني دون أن يلحظها أحد .
- الحرب الإلكترونية حرب لا تناظرية : فالتكلفة المتدنية نسبيا للأدوات اللازمة لشن هكذا حروب يعني أنه ليس هناك حاجة لأن تقوم دولة ما بتصنيع أسلحة مكلفة جدا كحاملات الطائرات والمقاتلات المتطورة لتفرض تهديدا خطيرا أو حقيقيا على دولة أخرى .(11)
- فشل نماذج " الردع " المعروفة : فالردع بالانتقام أو العقاب لا ينطبق على الحرب الإلكترونية، فعلى عكس الحروب التقليدية حيث ينطلق الصاروخ من أماكن يتم رصدها والرد عليها ، فإنه من الصعوبة بمكان بل ومن المستحيل في كثير من الأحيان تحديد مصدر الهجمات الإلكترونية، فبعض الحالات قد تتطلب أشهرا لرصدها وهو ما يلغي مفعول الردع بالانتقام، وكثير من الحالات لا يمكن تتبع مصدرها في المقابل، وحتى إذا تم تتبع مصدرها وتبين أنها تعود لفاعلين غير حكوميين ، فإنه في هذه الحالة لن يكون لديهم أصول أو قواعد حتى يتم الرد عليها.(12)

المبحث الثاني : إمكانية تطبيق قواعد القانون الدولي الإنساني على الحرب الإلكترونية :

لا تشير أحكام القانون الدولي الإنساني على وجه التحديد إلى العمليات الإلكترونية ، ولهذا السبب ولما كان استغلال التكنولوجيا الإلكترونية ظاهرة جديدة نسبيا ويبدو أنها تؤدي في بعض الأحيان إلى استحداث تغيير نوعي كامل في وسائل وأساليب القتال، يدفع البعض من حين لآخر بأن القانون الدولي الإنساني غير متوائم مع العالم الإلكتروني ولا يمكن تطبيقه على الحرب الإلكترونية، وبالمقابل فإن عدم وجود إشارات محددة في القانون الدولي الإنساني إلى العمليات الإلكترونية لا يعني أن هذه العمليات غير خاضعة لقواعد القانون الدولي الإنساني،فالتكنولوجيات الجديدة بجميع أنواعها تتطور طوال الوقت، ويتسع القانون الدولي الإنساني بما فيه الكفاية لاستيعاب هذه التطورات الجديدة. (13)

إن مسألة خضوع الحرب الإلكترونية لقواعد القانون الدولي الإنساني أثارت الكثير من الجدل الفقهي وهو ما سنتناوله في المطلب الأول من هذا المبحث، في حين يتعلق المطلب الثاني بدراسة مدى توافق مبادئ القانون الدولي الإنساني مع الحرب الإلكترونية.

المطلب الأول:الجدل الفقهي حول إمكانية خضوع الحرب الإلكترونية لقواعد القانون الدولي الإنساني:

استند جانب من الفقه إلى أن الحرب الإلكترونية لا تخضع لقواعد القانون الدولي الإنساني مستندين في ذلك إلى ثلاث حجج،تتعلق الأولى بأنه لا توجد أحكام في أي وثيقة من مواثيق القانون الدولي الإنساني تتناول بشكل مباشر موضوع الحرب الإلكترونية أو العمليات الإلكترونية، وتتعلق الثانية بأن تطوير واستخدام الهجمات الإلكترونية يرجع تاريخهما إلى ما بعد اعتماد المعاهدات القائمة، ولذلك لم تدخل في مجال تفكير الأطراف المشتركة في هذه

الصكوك، وبالتالي لم تعطيها تلك المعاهدات، أما الحجة الثالثة فتتمثل في أن القانون الدولي مصمم للتعامل مع الأساليب والوسائل الحركية بطبيعتها حيث أن الهجوم على شبكات الحاسوب لا يتضمن إلا القليل مما هو "مادي"، لذلك فإن الهجمات عن طريق الحاسوب تقع خارج نطاق القانون الدولي الإنساني.

وقد عمد الرأي المؤيد لخضوع الحرب الإلكترونية لقواعد القانون الدولي الإنساني إلى دحض الحجج السالفة الذكر، حيث يمكن استبعاد الحجة الأولى بسهولة، فحقيقة أن الاتفاقيات القائمة صامتة بشأن الهجوم على شبكات الحاسوب ليست ذات أهمية تذكر، فأولا: لأن شرط مارتينز – وهو مبدأ من القانون الدولي الإنساني مقبول بشكل جيد – ينص على أنه " عند وجود حالة لا تغطيها اتفاقية دولية يظل المدنيون والمقاتلون تحت حماية وسلطة مبادئ القانون الدولي المستمد من التقاليد الراسخة ومن مبادئ الإنسانية وما يمليه الضمير العام."، كما أن قبول العرف الدولي كمصدر للقانون في المادة 38 من النظام الأساسي لمحكمة العدل الدولية يوضح أيضا المغالطة في أي جدال بعدم الانطباق اعتمادا على غياب نص قانوني معين.(14)

وبالمثل، فالحجة التي تركز على حقيقة أن الهجوم على شبكات الحاسوب يرجع تاريخه إلى ما بعد اعتماد المواثيق الحالية تنطوي على مغالطة أيضا، وقد قدم هذا التعليل على وجه التحديد إلى محكمة العدل الدولية لترى مدى " مشروعية التهديد بالأسلحة النووية أو استخدامها"، ورفضت المحكمة – في رأيها الاستشاري – القول بأنه نظرا لأن " المبادئ والقواعد الإنسانية قد وضعت قبل اختراع الأسلحة النووية، فإن القانون الإنساني يكون غير منطبق عليها"، وكما قالت المحكمة فإنه " في رأي الأغلبية العظمى من الدول والكتاب أيضا لا يوجد شك بالنسبة لانطباق القانون الإنساني على الأسلحة النووية."

ولأنه ليس هناك ما يدعو للتمييز بين الأسلحة النووية وأسلحة الحاسوب – على الأقل من حيث التوقيت الذي استحدثت فيه بالنسبة لدخول المعايير الإنسانية ذات الصلة حيز التنفيذ – فإن نفس النتيجة تنطبق على الهجوم على شبكات الحاسوب، وفضلا عن ذلك فإن مراجعة الأسلحة الجديدة ونظمها لمعرفة خضوعها للقانون الدولي الإنساني تعتبر من الضرورات القانونية، بل والمنهجية أيضا، حيث تنص المادة 36 من البروتوكول الإضافي الأول لعام 1977 – المتعلق بالنزاعات المسلحة الدولية – على أنه " عند دراسة أو تطوير أو امتلاك أو تبني أسلحة جديدة أو وسائل للحرب تكون الأطراف المتعاقدة خاضعة للالتزام بتحديد هل سيكون استخدامها- في بعض أو كل الظروف – محظورا بموجب هذا البروتوكول أو بأي قاعدة من القانون الدولي المطبق على الأطراف المتعاقدة ".

وبعد هذا التحليل تظل الحجة الثالثة فقط لعدم انطباق القانون الدولي الإنساني على الهجوم على شبكات الحاسوب وهي أنه ليس نزاعا مسلحا، على الأقل في حالة غياب الأعمال العدائية التقليدية، وفي الواقع فإن النزاع المسلح هو الشرط الذي يفعل القانون المطبق في الحرب، و تنص المادة الثانية المشتركة من اتفاقيات جنيف لعام 1949 على أنه يطبق – بغض النظر عن الشروط المحددة التي تتعلق بوقت السلم – على جميع حالات الحرب المعلنة أو أي نزاع مسلح آخر ينشب بين طرفين أو أكثر من الأطراف المتعاقدة، حتى لو لم يعترف أحدها بحالة الحرب، كما أن البروتوكول الإضافي الأول – مثله مثل الاتفاقيات – يتبنى نفس معيار " النزاع المسلح " وهو ما أصبح قانونا عرفيا مقبولا للقانون الإنساني، وواقع أن البروتوكول الإضافي الثاني لعام 1977 ينص أيضا على تعبير

" نزاع مسلح " وإن كان في سياق النزاع المسلح غير الدولي، يوضح أن النزاع المسلح شرط تحدده طبيعته وليس المشاركون فيه أو موقعه .

وفي الشرح الذي نشرته اللجنة الدولية للصليب الأحمر لاتفاقيات جنيف لعام 1949 والبروتوكولين الإضافيين لعام 1977 نجد نهجا موسعا بشأن معنى هذا التعبير، فشرح الاتفاقيات يعرف النزاع المسلح بأنه " أي خلاف نشأ بين دولتين ويؤدي إلى تدخل القوات المسلحة حتى إذا أنكر أحد الأطراف وجود حالة الحرب، ولا يختلف الأمر بالنسبة لطول فترة النزاع، أو عدد المذابح التي وقعت".

وبالمثل، فإن شرح البروتوكول الإضافي الأول يحدد " أن القانون الدولي الإنساني يغطي أي نزاع بين دولتين يشتمل على استخدام قواتها المسلحة، ولا تلعب فترة استمرار النزاع أو كثافته دورا "، كما يصف شرح البروتوكول الإضافي الثاني النزاع المسلح بأنه " وجود أعمال عدائية صريحة بين القوات المسلحة تكون منظمة بدرجة أو بأخرى "، والشرط الضروري في الحالات الثلاث هو مشاركة القوات المسلحة.[15]

وينبغي توضيح أنه نظرا للتقدم في وسائل وطرق الحرب، ولاسيما الحرب الإلكترونية، فلا يكفي لتطبيق القانون الدولي الإنساني وضع أساس يعتمد على الفاعل (القوات المسلحة)، بل إنه من الملائم بدرجة أكبر اعتماد أساس يقوم على آثار العمل، وهذا ليس تجليا فقهيا، فلا أحد ينكر على سبيل المثال أن الحرب البيولوجية والكيميائية تخضع للقانون الدولي الإنساني على الرغم من أنها لا تتضمن أسلحة حركية.

إن النهج القائم على العواقب تؤيده أيضا حقيقة أنه ما دام النزاع المسلح قد بدأ (باستثناء حالة حظر أسلحة معينة)، فإن الوسائل التي تستخدم لإحداث الأذى أو الموت أو إحداث التلف أو الدمار لا علاقة لها بمشروعية العمل، فتعمد استهداف أحد المدنيين أو غيره من الأشخاص المحميين عمل غير أخلاقي بغض النظر عن الوسيلة أو الطريقة التي استخدمت، فالتجويع والضرب والرمي بالرصاص وإلقاء القنابل وحتى الهجوم الإلكتروني، كلها خاضعة للقانون الدولي الإنساني بسبب واقع حدوث نتائج معينة، وهذا ضد أي قول بأن الهجمات الإلكترونية – بصفة عامة والحرب الإلكترونية بصفة خاصة – لا تخضع للقانون الدولي لأنها ليست قوة مسلحة فعلى العكس من ذلك، فإن خضوعها أو عدم خضوعها إنما يعتمد على طبيعتها وعلى النتائج المتوقعة .[16]

المطلب الثاني : مبادئ القانون الدولي الإنساني والحرب الإلكترونية :

جاء في تقرير اللجنة الدولية للصليب الأحمر عام 2011 أنه يجب أن يتوافق توظيف الهجمات السيبرانية في إطار النزاع المسلح مع جميع مبادئ القانون الدولي الإنساني وقواعده، كما هو الحال مع أي سلاح أو وسيلة أو أسلوب حرب آخر، جديدا كان أم قديما، وما يؤيد ذلك ما أشارت إليه محكمة العدل الدولية بأن " مبادئ وقواعد القانون الدولي الإنساني المطبق في النزاع المسلح، تنطبق على جميع أشكال الحروب وعلى جميع أنواع الأسلحة بما في ذلك تلك المستقبلية "، لذا فإن نقل مبادئ القانون الدولي الإنساني إلى استخدامها في الهجمات السيبرانية على الرغم من كونها سلاحا جديدا للحرب، ليس ممكنا فحسب بل مناسبا أيضا.[17]

وعليه سنتطرق في هذا المطلب إلى أهم المبادئ التي ينبغي مراعاتها عند شن حرب إلكترونية .

الفرع الأول : مبدأ الضرورة العسكرية :

يتيح مبدأ الضرورة العسكرية، مهاجمة الأهداف العسكرية كخيار ضروري في المرتبة الأولى، إلا أن ذلك لا يمنع من مهاجمة أعيان مدنية إذا كانت تسهم بطريقة غير مباشرة في تحقيق ميزة عسكرية أكيدة، وقد تم تحديد شروط معينة في القانون الدولي الإنساني يمكن بموجبها اللجوء لمبدأ الضرورة العسكرية وهي ما يلي :

- أن يكون هذا التجاوز مؤقتا ومرتبطا بمدة قيام هذه الضرورة .
- أن يكون على أهداف محددة .
- أن يكون الغرض منها تحقيق ميزة عسكرية أكيدة .
- أن يتم مراعاة القانون الدولي الإنساني .

وبالنسبة لدليل تالين الذي استوحى قواعده من القانون الدولي الإنساني أشار إلى أنه في الحالات التي يكون الخيار ممكنا بين عدة أهداف عسكرية للحصول على ميزة عسكرية مماثلة، فالهدف الذي يتم اختياره للهجوم السيبراني، هو ذلك الهدف الذي يتوقع منه أن يسبب خطر أقل على المدنيين والأعيان المدنية، أما في حالة وجود العديد من الأهداف إلا أن أحداها تحقق ميزة عسكرية أكثر من مثيلاتها، ففي هذه الحالة من حق المهاجم توجيه الهجمات السيبرانية المباشرة ضد الهدف العسكري الذي يحقق أكثر ميزة عسكرية ممكنة في إطار النزاع المسلح، وهنا يجب أن ينظر بشأن الهجمات السيبرانية إلى الضرر الذي يلحق بالمنشآت والبنية التحتية المهمة بالنسبة للمدنيين، فضلا عما يسببه للمدنيين من حرمان في وظائف وخدمات هذه المنشآت تطبيقا لمبدأ الضرورة العسكرية .

واستنادا إلى ما سبق يمكن القول إن اللجوء إلى الهجمات السيبرانية يجب أن يكون ضروريا لتحقيق الهدف العسكري المشروع، وأما مسألة تحديد الأهداف والمنشآت العسكرية في الفضاء السيبراني فتثير تحديا واسعا أمام المجتمع الدولي، وذلك لأن المنشآت التي تقدم خدمة للجهد العسكري هي في الوقت نفسه تخدم القطاع المدني، فيجب إذا على المقاتل السيبراني تحديد كل حالة على حدة، أي أنه في كل حالة، يجب على المقاتل السيبراني أن يقرر بشكل قاطع أن الهجوم السيبراني يوفر ميزة عسكرية لتحقيق هدف عسكري، وقد أشار إلى هذا التحدي ريكس هيوز مدير شبكة الابتكار السايبري في جامعة كامبردج بالقول: " إن الهجمات الرقمية تنشئ تحديا واضحا أمام تطبيق مبدأ الضرورة العسكرية ولحل هذه المعضلة لابد من تضافر الجهود بين خبراء القانون الدولي ومهندسي الصناعات الإلكترونية لتحديد ما يمكن أن يوصف بهدف ...". (18)

الفرع الثاني : مبدأ التناسب :

تبنى دليل تالين هذا المبدأ في القاعدة 51 منه، وتناول المواقف التي يتعرض فيها المدنيون أو العيان المدنية للأذى العرضي، أي أنهم ليسو أهدافا مقصودة للهجوم. كما وضح، بأن حقيقة تعرض المدنيين أو الأعيان المدنية للأذى أثناء هجوم سيبراني على هدف عسكري مشروع لا تجعل بالضرورة الهجوم المذكور غير قانوني في حد ذاته. بدلا من ذلك، تعتمد مشروعية الهجوم الذي ينتج عنه أضرار جانبية، على العلاقة بين الضرر الذي يتوقع المهاجم بشكل معقول أن يتسبب فيه بشكل عرضي للمدنيين والأعيان المدنية والميزة العسكرية التي يتوقعها نتيجة للهجوم.

ومن ناحية أخرى قد تتسبب الهجمات السيبرانية في حدوث إزعاج أو تهيج أو توتر أو خوف، فلا تعتبر مثل هذه العواقب أضرارا جانبية لأنها لا ترقى إلى "خسارة في أرواح المدنيين، أو إصابة المدنيين، أو الإضرار التي تلحق بالأعيان المدنية"، فلا ينبغي أخذ هذه الآثار في الاعتبار عند تطبيق هذه القاعدة.

وبالنظر إلى مخاطر الهجمات السيبرانية من المرجح جدا أن يتم انتهاك مبدأ التناسب في تفسيره التقليدي بسبب الترابط بين الأنظمة المدنية والعسكرية والآثار التي لا يمكن السيطرة عليها على البنى التحتية المدنية، وفي سبيل الحد من هذه المخاطر والانتهاكات، قد نرى تغييرات في الأنظمة والشبكات من أجل فصل الشبكات المدنية عن الشبكات العسكرية من أجل تسهيل الوصول إلى مثل هذه الفروق في أوقات الحرب أو الأزمات.[19]

الفرع الثالث :مبدأ التمييز :

يجب أن يكون مبدأ التمييز في قلب النزاعات المسلحة الحديثة، لأنه أساس المبادئ الرئيسية المتعلقة بمسألة الاستهداف القانوني، وقد تم النص عليه في البروتوكول الإضافي الأول لعام 1977، والقانون الدولي الإنساني العرفي، وبالتالي ينطبق مبدأ التمييز في صياغته وتفسيره على نطاق واسع ولا يقتصر على أنواع معينة من الأسلحة أو وسائل الحرب، فهو قابل للتطبيق على الهجمات الإلكترونية ويقتضي ضمان احترام هذا المبدأ أثناء التحضير لاستخدام الهجمات الإلكترونية التمييز بين المقاتلين وغير المقاتلين من جهة، وبين الأعيان العسكرية وتلك المدنية من جهة أخرى .[20]

وبذلك يمكن اعتبار الحرب الإلكترونية أحد أهم أشكال النزاعات التي يمكن أن تستند إلى مبادئ القانون الدولي الإنساني، والذي يجب ألا يقتصر فقط على النزاعات المسلحة التقليدية.[21]

الخاتمة :

تحتل أعمال الحرب الإلكترونية، في الوقت الحاضر، مكانا بارزا بين الأنشطة العسكرية الأخرى، ويولي كافة الأطراف من الشرق إلى الغرب، الكثير من الاهتمام لتطوير وسائلها وأساليب استخدامها بعد أن أثبتت خبرات الحروب المحدودة التي تلت الحرب العالمية الثانية أهميتها سواء في الدفاع أو الهجوم .

وقد أحدث استخدام معدات الحرب الإلكترونية في الحروب الحديثة تطورا هائلا في مجالات هذه الحروب ومراحلها،وأصبح الحسم في المعارك الحديثة لصالح الجيوش والقوات التي تستخدم الحديث منها.

وانطلاقا من الأهمية التي يكتسيها موضوع الحرب الإلكترونية حاولنا معالجته بالمرور على مجموعة من النقاط حيث ناقشنا مفهوم الحرب الإلكترونية من خلال تعريفها ورصد أهم خصائصها، ثم درسنا إمكانية خضوعها لقواعد القانون الدولي الإنساني من خلال التطرق إلى الجدل الفقهي الذي أثاره الموضوع ومحاولة وضع عملية إسقاط لمبادئ القانون الدولي الإنساني على الحرب الإلكترونية.

ومن خلال هذه الدراسة توصلنا إلى النتائج التالية :

- ليس هناك تعريف جامع مانع للحرب الإلكترونية، مع وضوح معالمها من الناحية العملية والتقنية.تخضع الحرب الإلكترونية لقواعد القانون الدولي الإنساني إذا كانت في سياق نزاع مسلح،

- وتخضع لقواعده كذلك إذا كانت خارج سياق نزاع مسلح ولكن مع ضرورة توافر شرط التداعيات أو النتائج، أو بمعنى آخر بالنظر إلى الآثار التي يمكن أن ترتبها خاصة إذا أمكن نسبة هذه الآثار إلى الدولة.
- تطبق مبادئ القانون الدولي الإنساني على الحرب الإلكترونية شأنها في ذلك شأن الحرب التقليدية، ولكن نظرا لخصوصية الحرب الإلكترونية فإنه من الصعب بل من المستحيل في بعض الأحيان تطبيق جميع مبادئ القانون الدولي الإنساني وخاصة منها مبدأ التمييز.

وعلى ضوء ما سبق يمكن تقديم المقترح الآتي :

- توسيع النقاش بشأن الحرب الإلكترونية بين مختلف مكونات المجتمع الدولي وبمساهمة الفقهاء والخبراء الدوليين – على اختلاف تخصصاتهم وخاصة منهم القانونيين – بغية الوصول إلى إطار قانوني واضح وملزم ينظم ويضبط الحرب الإلكترونية.

المراجع :

أولا : الكتب .

1- صلاح الدين الأشرم،الحرب الإلكترونية من الحرب العالمية الأولى إلى حرب النجوم،الطبعة الثانية،دمشق:دار طلاس،1993.

2- عادل عبد الصادق، أسلحة الفضاء الإلكتروني في ضوء القانون الدولي الإنساني، الإسكندرية:مكتبة الإسكندرية، 2016.

3- فيصل محمد عبد الغفار ، الحرب الإلكترونية، الطبعة الأولى، عمان: الجنادرية، 2016.

ثانيا : المقالات .

1- اللجنة الدولية للصليب الأحمر، ما هي القيود التي يفرضها قانون الحرب على الهجمات السيبرانية؟، مقال منشور بتاريخ : 28-06-2013على الرابط الإلكتروني:

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

2- كوردولا دوريجي، لا تقترب من حدود فضائي الإلكتروني، الحرب الإلكترونية والقانون الدولي الإنساني وحماية المدنيين، المجلة الدولية للصليب الأحمر،مجلد 94(886)،2012.

3- مايكل ن.شميث، الحرب بواسطة شبكات الاتصال: الهجوم على شبكات الكمبيوتر(الحاسوب) والقانون في الحرب، المجلة الدولية للصليب الأحمر، مختارات من أعداد 2002.

4- هربرت لين،النزاع السيبراني والقانون الدولي الإنساني،المجلة الدولية للصليب الأحمر، المجلد94 (886)،2012.

ثالثا: المذكرات :

- نور أمير الموصلي، الهجمات السيبرانية في ضوء القانون الدولي الإنساني، مذكرة ماجستير، الجامعة الافتراضية السورية،2021.

رابعا : الوثائق .

- دليل تالين حول القانون الدولي المطبق على الحرب السيبرانية، من إعداد مجموعة من الخبراء الدوليين بدعوة من مركز التميز للدفاع السيبراني التعاوني التابع لحلف شمال الأطلسي(الناتو)،2013.

خامسا : المواقع الإلكترونية .

https://www.icrc.org-

الهوامش:

(1) - صلاح الدين الأشرم، الحرب الإلكترونية من الحرب العالمية الأولى إلى حرب النجوم، الطبعة الثانية، دمشق:دار طلاس، 1993، ص ص11-13 .

(2) - كوردولا دوريجي، لا تقترب من حدود فضائي الإلكتروني، الحرب الإلكترونية والقانون الدولي الإنساني وحماية المدنيين، المجلة الدولية للصليب الأحمر،مجلد 94(886)،2012،ص 540-541،مقال تاريخ الإطلاع 30-05-2022، 21:13. https://international-review.icrc.org/ منشور على الموقع الإلكتروني:

(3)- فيصل محمد عبد الغفار ، الحرب الإلكترونية، الطبعة الأولى، عمان: الجنادرية، 2016، ص 9.

(4)- المرجع السابق، ص 10.

(5)- المرجع السابق، ص 26.

(6)- اللجنة الدولية للصليب الأحمر، ما هي القيود التي يفرضها قانون الحرب على الهجمات السيبرانية؟، مقال منشور بتاريخ : 28-06-2013على الرابط الإلكتروني:

https://www.icrc.org/data/rx/ar/resources/documents/faq/130628-cyber-warfare-q-and-a-eng.htm تاريخ الإطلاع : 2022/08/13، 15:37.

(7)- دليل تالين حول القانون الدولي المطبق على الحرب السيبرانية، من إعداد مجموعة من الخبراء الدوليين بدعوة من مركز التميز للدفاع السيبراني التعاوني التابع لحلف شمال الأطلسي(الناتو)،2013.

(8)- القاعدة 30 من دليل تالين .

(9)- نور أمير الموصلي، الهجمات السيبرانية في ضوء القانون الدولي الإنساني، مذكرة ماجستير، الجامعة الافتراضية السورية،2021،ص15.

(10)- هربرت لين، النزاع السيبراني والقانون الدولي الإنساني، المجلة الدولية للصليب الأحمر، المجلد94(886)،2012ص 521، مقال منشور على الموقع الإلكتروني:

https://international-review.icrc.org/ar/articles/cyber-conflict-and-international-humanitarian-law تاريخ الإطلاع : 2022/08/11،19:05.

(11) - فيصل محمد عبد الغفار، مرجع سابق، ص 11.

(12)- المرجع السابق، ص 12.

(13) - كوردولا دوريجي، مرجع سابق، ص540-541.

(14)- مايكل ن.شميث، الحرب بواسطة شبكات الاتصال: الهجوم على شبكات الكمبيوتر(الحاسوب) والقانون في الحرب، المجلة الدولية للصليب الأحمر، مختارات من أعداد 2002،ص89-90 مقال منشور على الرابط الإلكتروني : icrc.org/ar/doc/resources/documents/misc/5x6lSP.htm تاريخ الإطلاع: 2022/08/11،18:37.

(15) - المرجع السابق، ص91-92.

(16)- المرجع السابق، ص94-95

(17) - نور أمير الموصلي، مرجع سابق، ص44.

)- المرجع السابق، ص18.53(

(19)- المرجع السابق، ص51-52

(20)- المرجع السابق، ص44-45.

)- عادل عبد الصادق، أسلحة الفضاء الإلكتروني في ضوء القانون الدولي الإنساني، الإسكندرية: مكتبة الإسكندرية، 2016،ص86. 21(