تكييف استخدام الحرب الالكترونية في النزاعات المسلحة وفقاً للقانون الدولي الانساني

أ.م.د.سلافة طارق الشعلان

نبذة عن الباحث :
استاذ مساعد القانون الدولي العام حاصلة على شهادة الدكتوراه في القانون الدولي العام سنة 2012 م . تدريسية في جامعة القادسية .

المقدمة

ربما كان يصعب التفكير في وجود الحرب الالكترونية (المعلوماتية) والآثار الناجمة عنها طالما لم تكن هنالك حرب حقيقية تدور على ارض الواقع، ولكن الواقع اليوم، تجاوز هذا الاعتقاد وامتد بخطى واسعة الى ما يشابه فترة ظهور الطائرات الحربية للمرة الاولى، في عام 1914، التي بدأت مهامها بالاستطلاع ثم تحولت لتنفيذ اغراض حربية، ولم يكن استخدام الطائرات الحربية في ذلك الوقت منظماً بقانون كما لم يكن القانون الدولي الانساني بصيغته القائمة. واليوم ظهر استخدام أطراف النزاعات المسلحة لمنظومات الأسلحة التي يتم التحكم بها عن بُعد كالطائرات بدون طيار، والأسلحة الأوتوماتيكية، والمنظومات الآلية كالرجال الآليين لأغراض القتال في ساحة المعركة ويثير استخدام كل من هذه التكنولوجيات عدداً كبيراً من المسائل القانونية1 . ويمكن ان يمثل استخدام الانترنيت كوسيلة في الحرب، جزء من حرب المعلومات، التي تشمل الحرب باستخدام سلاح المعلومة سواء كانت من خلال الانترنيت أو القنوات الفضائية أو وسائل الإعلام الأخرى المسموعة والمرئية، وغيرها2. او استخدامه لتوجيه اسلحة او لتعطيل دفاعات العدو في الميدان، او للتحكم في التوجيهات او المعلومات التي يجب ان يتم انتقالها عبر الشبكات لتنفيذ اوامر القادة، وغير ذلك من الوسائل المؤثرة على سير النزاع.

وتوالت التطورات العلمية في هذا المجال الى ان اصبح الكومبيوتر والانترنيت جزء مهم من وسائل الحرب المعاصرة. وقد فرض ظهور التكنولوجيا الجديدة باختلاف انواعها، التساؤل عن امكانية اعتبار توجيه الأسلحة والهجوم باستخدام الحاسوب أو الانترنيت هجوما مسلحا وفقا لقواعد القانون الدولي العام، اذ يثير تطبيق قواعد قانونية موجودة من قبل على تكنولوجيا جديدة ، مسألة ما إذا كانت هذه القواعد تتسم بما يكفي من الوضوح في ظل خصائص هذه التكنولوجيا، وكذلك في ما يتعلق بالآثار الإنسانية المرتقبة التي قد تنجم عنها .فقد شهدت السنوات الماضية إدخال مجموعة واسعة من التكنولوجيات الجديدة إلى ساحة المعركة الحديثة وأوجد الفضاء المعلوماتي ميداناً جديداً للقتال.

ونتناول في هذا البحث موضوع استخدام الانترنيت "كسلاح" من خلال توجيه العمليات الالكترونية لاحداث اضرار مادية في سياق النزاعات المسلحة، اذ يثير هذا الموضوع العديد من الاشكاليات، منها مدى خضوع هذه العمليات الى القانون الدولي الانساني، وهل توجد قاعدة قانونية ضمن القانون القائم قادرة على مواكبة التحديات التي يفرضها استخدام هذه "الاسلحة الجديدة"، في النزاعات المسلحة الجديدة، التي لا يتقاتل فيها جيش نظامي واضح تجاه جيش اخر او فئات مسلحة منظمة اخرى.

كما تواجهنا صعوبة الفصل بينما ماهو مدني وعسكري في عالم تتداخل فيه عمليات التكنولوجيا لخدمة الاغراض العسكرية والمدنية في ان واحد، وتمثل خدمات الاتصالات الالكترونية مثال واضح لذلك. هذا فضلا عن ان تحديد ما إذا كانت أساليب الحرب الالكترونية ووسائلها تختلف عن تلك المتعلقة بالحرب التقليدية وإلى أي نطاق تختلف، فجهل الهوية قاعدة وليس استثناء في الحروب الالكترونية التي تحصل يومياً، وفي بعض الحالات من المستحيل إقتفاء أثر المصدر المسبب للضرر. وتسمى الحروب التي تتم باستخدام الانترنيت بالحروب الالكترونية، او المعلوماتية، او الحرب السيبرانية وفقا للجنة الدولية للصليب الاحمر، وهذه التسمية مأخوذة ترجمة لاصطلاح (Cyber War) .

ولا تخفى اهمية هذا الموضوع في ظل تطور وتغير طبيعة النزاعات المسلحة التقليدية، خصوصا ان الامن الالكتروني بات يوضع في اعلى سلم التهديدات التي تواجه الدول الكبرى، في ظل صراعها المتنامي للتدخل في مناطق النزاعات المسلحة، التي تمتلك فيها مصالح ستراتيجية، دون ترك ادلة تكشف هوية الفاعل . والحرص على التدخل دون خسائر تذكر من الناحية البشرية ، وقد كان احتلال العراق في 2003 مسرحا لتجارب وصور وانواع متعددة من الحروب وكانت الحرب الالكترونية من بينها، وربما كانت دراسة مدى انطباق القانون الدولي الانساني على الحرب الالكترونية جزء من الجانب الموضوعي والجوهري لتكييف صور النزاعات الاخرى التي تستخدم في مواقع التواصل والحرب الاعلامية والاسلحة الموجهه عن بعد والمقاتليين الاليين الذي تجري التجارب لاعتمادهم في النزعات المسلحة، التي تجري كل يوم باليات

ووسائل اكثر حداثة واقل انسانية وان كان البعض يرى فيها دقة فائقة لا يمكن التغاضي عنها.

وفي هذا البحث سنعتمد تسمية الحرب الالكترونية بالمعنى المشار اليه اعلاه . وسيتم تناول الموضوع في سياق مناقشة مدى انطباق قواعد القانون الدولي الانساني على الحرب الالكترونية، وذلك في ثلاث مباحث مقسمة على النحو الاتي:

المبحث الاول: الحرب الالكترونية واستخدام القوة وفقا لميثاق منظمة الامم المتحدة 1945.

المبحث الثاني :الحرب الالكترونية كسلاح وفقا للقانون الدولي الانساني.

المبحث الثالث: تطبيق القانون الدولي الانساني على الحرب الالكترونية وفقا للضرر او الهدف المتحقق.

المبحث الاول: الحرب الالكترونية واستخدام القوة وفقا لميثاق منظمة الامم المتحدة 1945

منذ الستينيات من القرن العشرين اثبتت شبكة الانترنيت بوجه خاص انها تشكل بنية اساسية لتبادل المعلومات المتعلقة بكل نواحي الحياة بما فيها الماسة بالأمن الدولي، بشكل يتخطى الحدود المادية التقليدية للدول، مما يشكل تحديا للمفاهيم التقليدية المتعلقة بسيادة الدولة، وقد اصبح الانتقال الالكتروني للبيانات بين الدول امرا ايسر واقل كلفة واوسع انتشارا ولا يستغرق سوى بضعة ثواني او دقائق قليلة3.

وقد ادى ظهور شبكة الانترنيت في عام 1946 الى حدوث ثورة في عملية جمع وتبادل المعلومات كما ادى الى ظهور عدة جرائم مرتبطة بها لم يكن لها وجود من قبل ومن امثلة هذه الجرائم استخدام الانترنيت كوسيلة في الحرب للقيام بالاختراقات غير المشروعة، او لتوجيه الطائرات والصواريخ نحو الأهداف العسكرية والمدنية، وتعطيل أجهزة التحكم والسيطرة على موارد خطرة أو موارد حيوية..4

وسيتم تناول هذا المبحث في مطلبين، نتناول في الاول مفهوم الحرب الالكترونية التي تجري في سياق النزاعات المسلحة، اما المطلب الثاني فيناول استخدام القوة وفقا لميثاق منظمة الامم المتحدة 1945 والحرب الالكترونية.

المطلب الاول: مفهوم الحرب الالكترونية التي تجري في سياق النزاعات المسلحة

لا بد من الاشارة الى ان اهتمام المجتمع الدولي بالحرب الالكترونية او كما يطلق عليها (الحرب السيبيرية)، بدأ منذ عام 1990، وفي عام 1999 عقدت الكلية البحرية الحربية اول مؤتمر قانوني بهذا الخصوص، وقد ازداد الاهتمام الدولي بالجرب العلوماتية الى حد كبير بعد هجمات الحادي عشر من سبتمبر في 2001، ثم ازداد الاهتمام اثر هجمات 27 ابريل (نيسان) 2007، الالكترونية التي نفذت ضد استونيا وامتدت لاسابيع ، وجدير بالذكر ان قائمة المواقع التي تعرضت لهذه الهجمات ضمت موقع الرئيس الاستوني ورئيس الوزراء وموقع البرلمان على شبكة الانترنت، فضلا عن مواقع

خاصة بوزارات، إذ تعرضت هذه المواقع لسيل متواصل من الرسائل الأمر الذي ادى الى إغلاقها.

وفي عام 2010 وصفت ستراتيجية الامن الوطني للمملكة المتحدة التهديدات الالكترونية باعتبارها احد اربعة تهديدات تواجه امنها الوطني. بينما اعتبرت الولايات المتحدة الامريكية التهديدات الالكترونية بانها من اخطر التهديدات التي تواجه امنها الوطني.

وخلال هذه الفترة ايضا اطلقت كندا ستراتيجية الامن الالكتروني Cyber Security Strategy. بينما اصدرت روسيا رؤيتها المتعلقة بالنزاعات المسلحة في الفضاء الالكتروني5.

وقد توجت الجهود الدولية المتعلقة بتنظيم الحرب الالكترونية، باصدار دليل تالين حول القانون الدولي المنطبق على الحرب السيبرانية في عام 2012 الذي بدأ العمل على صياغته منذ عام 2009 ، وهو من إعداد اللجنة الدولية للخبراء وبدعوة من مركز التميز للدفاع السيبراني التعاوني التابع لحلف شمال الأطلسي (الناتو).وينطبق هذا الدليل على الحرب الدولية والحرب غير الدولية، وهو يعنى بالحرب الالكترونية بين الطرفين المتنازعين، وهو بكل الاحوال يمثل وثيقة غير ملزمة اعدها مجموعة من الخبراء. واذا كان لهذه لجرائم الحرب الالكترونية سمات محددة، فيمكن تحديدها بالاتي:

لا تقف هذه الجرائم عند الحدود الدولية للدول(لكنها ليست جرائم عابرة للحدود، اذ ان في الاخيرة يمتد الضرر الى خارج حدود الدولة دون انتقاء لمكان معين كالتلوث الكميائي الذي يحدث في دولة ما، لا تتمكن من ايقافه ويمتد ليشمل اقاليم لدول اخرى) ، بينما تعتمد الحرب الالكترونية التي تحدث في سياق نزاع مسلح، على تبادل المعلومات والتعاون عبر الحدود بين اشخاص منتشرين على مستوى العالم معتمدين وسائل التكنولوجيا والاتصالات الحديثة، لكن الضرر يكون موجها الى هدف يتم تحديده مسبقاً6.

يصعب احيانا تحديد المكان الذي تم توجيه "الهجوم" منه وبالتالي اثبات المسؤولية عنه.

يصعب في الغالب اثبات هوية ودوافع الفاعل اذ يمكن ان يكون الفاعل ارهابيا يعمل كجزء من منظومة ارهابية او بمفرده او بتوجيه من الدولة ذاتها التي انطلق العمل غير المشروع منها، او قد يتم بتوجيه من دولة معادية اخرى.

يحتاج تحديد المسؤول عن هذه الجرائم، الى منظومات الكترونية متطورة قادرة على التتبع وتحديد الاثر بشكل دقيق.

تمتاز هذه الجرائم بالقدرة الهائلة على التدمير دون ضرورة للتواجد المادي في ارض المعركة، وبالتالي دون خسائر بشرية للاطراف او الطرف الذي ينفذ الهجوم.

وتوجد تعاريف متعددة "للعمليات المعلوماتية"، بسبب عدم الاتفاق دوليا على معنى قانوني او تعريف لها، و تُستخدم العبارة في سياقات مختلفة (ولا تقتصر

دائماً على النزاعات المسلحة). وهي جميعا تشير إلى عمليات ضدّ أو بواسطة حاسوب أو نظام حاسوب من خلال التدخل في عمليات تدفق البيانات. ويجوز استخدام تكنولوجيا المعلومات في حرب ما، وفي بعض الظروف، يمكن اعتبار بعض هذه العمليات بمثابة (هجمات مسلحة) اذا تمت في سياق نزاع مسلح سواء كان دولي او داخلي. ولا يعنى القانون الدولي الانساني سوى بالحرب الالكترونية التي تتم في سياق نزاع مسلح، لان حدوثها في غير هذا السياق يخضعها لنظم قانونية اخرى..

وقد تثير العمليات الالكترونية شواغل إنسانية، لا سيما عندما لا يقتصر أثرها على بيانات نظام الحاسوب المستهدف فقط، لتؤدي إلى إحداث أثر في "العالم الحقيقي". ويستطيع المرء من خلال التلاعب بنظم الحواسيب الداعمة على سبيل المثال أن يستخدم نظم العدو لمراقبة الحركة الجوية أو نظمه لتدفق خطوط أنابيب النفط أو محطاته النووية، ونتيجة لذلك، يكون الأثر الإنساني المحتمل لبعض العمليات الالكترونية هائلاً7.

وتعتبرُ الهجمات ضد شبكةِ الحاسوب ظاهرة حديثة نسبياً. ويمكن وُصِفَ هذه الهجمات بشكل أولي، بأنها عمليات تعطيل، تزويرُ، أو خفّضُ، أو تدمير لقاعدة المعلوماتِ في شبكاتِ الحاسباتَ، أو بين الحاسبات وشبكات الانترنيت نفسها. وقدْ تشنُّ ضدّ الصناعات، البنى التحتية، الاتصالات، دوائر النفوذ السياسية، القوى الاقتصادية العالمية، أو حتى ضدّ دول بالكامل.

وتعتبر هذه الهجمات عمليات تجسس في وقت السلم، بينما تعتبر عمليات عسكرية في أوقات النزاعات المسلحة8.

و يمكن وصف العمليات الالكترونية (السيبرانية)ايضا وبوجه عام بانها عمليات تُشنّ ضد أو عبر حاسوب أو نظام حاسوبي بواسطة تيار البيانات .وقد تهدف هذه العمليات إلى تحقيق أغراض مختلفة تضم على سبيل المثال اختراق نظام معين وجمع أو نقل أو تدمير أو تغيير أو تشفير البيانات، أو إجراء أو تعديل العمليات التي يتحكم بها الجهاز الحاسوبي المخترق أو التلاعب بهذه العمليات.

ويمكن بالتالي استخدام هذه الوسائل في العالم الافتراضي، لتدمير أو تعديل أو تعطيل مجموعة متنوعة من" الاهداف "في العالم الحقيقي، كالصناعات والبُنى الأساسية والاتصالات النُظم المالية .وتثير النتائج المحتملة لهذه العمليات بالتالي مخاوف كبيرة على الصعيد الإنساني، إذ يمكن لشخص ما، على سبيل المثال، التلاعب بما يملكه العدو من نُظم مراقبة الحركة الجوية أو نُظم أنابيب نقل النفط أو منشآت نووية عن طريق العبث بالنُظم الحاسوبية المستخدمة فيها، مسبباً نتائج خطيرة تترك اثارها على المدنيين والممتلكات المدنية9.وقدْ تتضمن طرقَ جديدةً للقتال، كالنشاطات ضد قراصنة الكومبيوتر والفيروساتِ وغيرها.

و تجري هذه الهجمات مِنْ مسافات بعيدة باستخدام موجات الراديو أو شبكةِ الاتصالات الدوليةِ، بدون اصطدام أو تلاحم جسدي مباشر في حدود العدو الإقليمية

، ولا يؤدي هذا غالبا إلى النوع المعتاد من الضرر التقليدي الفوري الناجم عن تلاحم القوات المتحاربة، على سبيل المثال قَدْ يُستَعملُ الفيروس لمُهَاجَمَة نظام حاسوب لمحطة طاقة نوويةٍ مما يُسبّبُ إطلاقَ الانبعاثات الخطرةِ10.

وقد يؤدي استخدام هذه الوسائل، التي توصف بالدقة الكبيرة، الى تداعي المبادئ الاساسية للقانون الدولي الانساني، في حال حدوث خطأ غير متوقع يؤدي الى استهداف مدرسة او ملجأ بدلا من ثكنة عسكرية او معسكر او تفجيرات نووية او كيميائية...

ويفترضُ بأنّ انظمة الاتصالات والحاسوب سَيُصبحانِ أكثر تعرضا للهجمات المنظمة لتحقيق أهداف عسكرية. ويقتضي تطور التكنولوجيا بهذا الاتجاه وابتكار الوسائل التي من شأنها القضاء على الإنسانية بشتى السبل، ان يقوم المجتمع الدولي وبدون تأخير بتحديد القواعد الموضوعية الأساسية التي تحكم هذه الأخطار، ومن الضروري بالتالي بذل أقصى الجهود للتخفيف من آثارها بمختلف الطرق الممكنة، لا سيما عن طريق تعليم المقاتلين أنفسهم اذ إن القانون الدولي الإنساني يفرض قواعد أساسية من شأن مراعاتها التمييز بين الجندي والمدني، ومن شأن الإخلال بهذه القواعد إفساد أسمى القضايا وأنبلها11...

المطلب الثاني

استخدام القوة وفقا لميثاق منظمة الامم المتحدة 1945 والحرب الالكترونية

وضع ميثاق منظمة الامم المتحدة 1945 ، نظاماً محدداً لتسوية النزاعات وتحقيق السلم والأمن الدولي ، وكان تنظيم اللجوء إلى استخدام القوّة أمرا جوهريا في الميثاق ، وفي حالة استخدام الانترنيت كوسيلة في الحرب فانه قد يستخدم في أي مرحلة من مراحل النزاع او خلال فترات السلم ، ويمكن لحرب المعلومات ان تكون وسيلة دفاعية او هجومية.

بينما نظم ميثاق منظمة الامم المتحدة ، الاستخدام المشروع للقوة بين الدول(بشكل مطلق ودون تحديد لطبيعة القوة)، واعتبر ان استخدام القوة بين الدول يعد مشروعا في حالتين فقط12، فأقرت م/51 من الميثاق بالحق الطبيعي للدول فرادى أو جماعات، في الدفاع عن أنفسهم إذا اعتدت قوة مسلحة على أحد أعضاء الأمم المتحدة...

وتسمح م/39 لمجلس الأمن أن يقرر ما إذا كان قد وقع تهديد للسلم أو إخلال بها و كان ما وقع عملا من أعمال العدوان، ويقدم في ذلك توصياته أو يقرر ما يجب اتخاذه من التدابير.

ويستلزم التوصل إلى تحريم استخدام القوة لحل المنازعات الدولية وتطبيقها في حالة استخدام تكنولوجيا الاتصالات كسلاح في الحرب، تحديد معنى مصطلح "استخدام القوة"، ولتوضيح هذا المفهوم هنالك ثلاثة اتجاهات:

الاتجاه الأول: يمثل وجهة النظر الشائعة بين العسكريين وصانعي القرار السياسي اللذين يرون ان المطالبة بمنع استخدامَ القوة تعني السعي إلى إبْقاء الحوادثِ الذي تحت عتبة العنفِ دون التحول إلى حروبِ.

الاتجاه الثاني وهو النهج الاكثر انتشارا في الاوساط الأكاديمية والذي يرى بان الميثاق يسعى لحل النزاعات بالطرق السلمية والسياسية وعن طريق الوسائل غير العسكرية. وانسجاما مع هذا النهج ، فان الهجوم المسلح هو (هجوم القوات العسكرية التقليدية) وهذ ما يشكل استخداما للقوة.

الاتجاه الثالث يأخذ بهذا الاتجاه اصحاب النهج التحليلي من خلال دعوتهم الى دراسة وتحليل كل حالة من حالات العنف من كل جوانبها ليتم على اساس ذلك معرفة ان تم استخدام القوة او لم يتم ...13

ومن المعلوم أن الدولة المتورطة في نزاع تهدف منه إلى تحقيق غاية معينة فأنها تسعى بأقل الخسائر من جانبها إلى تحطيم أو إضعاف الطاقة الحربية للعدو وهذه الطاقة تتضمن عنصرين : الموارد البشرية والمعدات14.

ويختلف الانترنيت عن غيره من الوسائل التي تعد أسلحة مباشرة كاستخدام السلاح النووي أو الكيميائي أو سلاح الليزر الذي يتم توجيهه باستخدام تقنية عالية نحو هدف محدد. ورغم أن هذه الاسلحة موجهه نحو هدف محدد، إلا أن آثارها التدميرية الواسعة على البيئة والبشرية جمعاء تصعب السيطرة عليها وتفاديها.

بينما يتميز الانترنيت بمزايا واستخدامات أخرى لا يمكن من خلالها تصنيف هذه الوسيلة الإلكترونية المتطورة كسلاح إلا إذا أسيء استخدامها وتم التجاوز على حقوق وسرية المعلومات غير المتاحة للاستخدام العام من قبل الدول ..

كما ان الانترنيت لا يمكن ان يستخدم كسلاح مباشر حتى ألان ،إلا انه يمكن ان يستخدم في تدمير قواعد بيانات وعرقلة وصول او تغيير مسار المعلومات المتعلقة بمخاطبات العدو، او التأثير على أنظمة التحكم المتعلقة بمصالح العدو وموارده ومنشاته.

أي أن المهاجمة باستخدام الانترنيت قد تكون بتوجه إيعاز لتعطيل التحكم بمنشاة نووية مثلا لتسبب أضرارا خطيرة تصعب السيطرة عليها والحد من أضرارها.. ولم يظهر استخدام الانترنيت هنا كسلاح مباشر وانما كنتيجة غير مباشرة لتعطل أنظمة التحكم الخاصة بالمنشاة النووية مثلا.

ومن الجدير بالذكر ان عبارة " اسلحة ووسائل واساليب الحرب"، لم يوضع لها تعريف في قواعد القانون الدولي الانساني، ومن ثم لابد من تفسيرها تفسيرا معقولا وتحديد ما اذا كانت احدى المعدات تعتبر سلاحا ام لا، اذ يفيد التعبير ضمنيا، القدرة الهجومية التي يمكن ان تطبق على هدف عسكري او مقاتل من الاعداء.

و لتحديد مضمون تعبير "وسائل" و" اساليب الحرب" فقد رأى بعض فقهاء القانون بانها تعني الطريقة التي تستخدم بها الاسلحة، ومن المسلم به ان مصطلحات وسائل واساليب الحرب يمكن من الناحية العملية ان تقرأ معا.. وبذلك

تشمل تلك البنود المعدات اتي لا تشكل سلاحا بالمعنى المفهوم، ولكن لها اثر مباشر على القدرة الهجومية للقوات التي تملكها15.

وقد نشرت في الولايات المتحدة الأمريكية مؤخرا بعض الدراسات التي تشير إلى إمكانية استخدام العمليات المعلوماتية لمهاجمة شبكات اتصالات العدو"Information Operations "...

وتتلخص طموحات وزارة الدفاع الامريكية منذ عام 2003 باعتماد وسائل جديدة لقتال العدو تكون اقل كلفة من ناحية خسارة الارواح والمعدات وربما تمكن من تحقيق اهداف المعركة عن بعد ..واحد ابرز هذه الوسائل هي المحاربة باستخدام شبكة المعلومات (الانترنيت) وتوصي وزارة الدفاع باعتماد العمليات النفسية لنشر الدعاية في أرض العدو، فضلا عن الطائرات بدون طيار، شبكات البث، مكبرات الصوت "، أدوات لاسلكية، هواتف خلوية والإنترنت، وهي ليست فكرة مكلفة جداً أو بعيدة المنال، كما إنها بكل تأكيد ستحافظ على ارواح جنود الفئة التي تستخدم هذه التقنيات.

وتُعرّفُ الولايات المتّحدةُ الحرب الالكترونية بانها " عمليات المعلوماتِ التي توجه أثناء اوقات الأزمات أو النزاعات لإنجاز أو تحقيق اهدافِ معيّنةٍ ضد مصلحة الخصم"16

ويرى العسكريين أنصار استخدام هذه الوسيلة بان الدقة في استخدام الانترنيت قد لا تؤدي إلى نتائج عرضية كبيرة كما في الأسلحة التقليدية ..إذ أن بإمكان المهاجم أن يحدد درجة الضرر التي ستحدث نتيجة لهجومة، إن كان يريد التقيد بقواعد القانون الدولي الإنساني ومبادئه فيقرر مهاجمة نظم الحاسوب في المكان المستهدف بدلا من قصفه لتدمير المعلومات التي يحتويها...

ويمثل الاعتداء باستخدام الحاسب الآلي أية عملية تهدف إلى تعطيل،أو منع، أو إضعاف أو تدمير المعلومات الموجودة في شبكات الحاسب الآلي بشكل يؤدي إلى المساس بمصلحة الدولة وأمنها وسلامتها17.وذلك دون استخدام مباشر للعنف كما في الحروب التقليدية.

وأخطر صور الحرب (الالكترونية) او السيبرانية، هى العمليات التى تستهدف مواقع عسكرية وأمنية تمثل انتهاكا لسيادة الدول، كاختراق شبكات معلومات البنية الأساسية مثل شبكات الكهرباء ومحطات المياه والمفاعلات النووية وأنظمة البنوك وشبكات بيانات المواطنين المتصلة بالانترنت، وتستطيع أجهزة المخابرات بجيوشها الالكترونية وقراصنة الفضاء تدمير أو شل فاعلية التحكم فى هذه الخدمات وإيقافها، مثلما حدث مع إيران التى سجلت أول هجوم تدميرى عليها عام 2010 على مفاعل «بوشهر» النووى من قبل «تحالف سيبرانى»، بين إسرائيل وأمريكا على نظامها الخاص بالتحكم والمراقبة بواسطة فيروس ستكسنت (Stuxnet) الذي قام باختراق أجهزة الطرد والتفتيش، وبدأ نشاطه التخريبى فى تدمير أنظمة التحكم فى تطوير نقل النفط ومحطات توليد الكهرباء، ونظام المفاعل النووى أدى

إلى تقديم قراءات مغلوطة على شاشات المراقبة بالمفاعل وأدى إلى تعطيل أجهزة الطرد المركزى، فقامت إيران على أثرها بضخ مليارات الدولارات بقطاع تكنولوجيا المعلومات أنتج منظومة الكترونية خاصة بهم وحجب بعض التطبيقات الأمريكية بعد توفير البديل المحلى، سبقه هجوم مماثل قبلها بثلاث سنوات، قامت به إسرائيل لشل قدرة الرادارات السورية الروسية الصنع، على رصد طائراتها التى قصفت مركز تصنيع أسلحة دمار شامل كان فى مرحلة إنشائه بالتعاون مع كوريا الشمالية.

وفى نفس العام (2007)، تعرضت دولة استونيا لهجوم تخريبى مماثل، عند قيام استونيا بمحاولة نقل النصب التذكارى السوفيتى للحرب العالمية الثانية من تالين مما أثار غضب الحكومة الروسية والأقلية الروسية فيها فقامت بهجمات واسعة شلت حكومة استونيا، التى تتميز بتطورها فى تبنى واستخدام وسائل الاتصالات الالكترونية وشبكة الانترنت فى تقديم الخدمات المالية المختلفة، فتم وقف 98٪ من إجمالى معاملاتها المصرفية عبر شبكة الانترنت وذلك عبر هجمات منع الوصول إلى الخدمة. وحفلت المواقع الإخبارية الاستونية بالتعليقات المعارضة للحكومة واستهداف الخوادم والمحولات غير المعلومة للعامة مثل تلك العاملة فى قطاعات البنوك والاتصالات السلكية والمعاملات المالية مما شل قطاعات عديدة فى الدولة لعدد من الساعات واتهم وزير الخارجية الاستونى بشكل مباشر الحكومة الروسية بشن هذه الهجمات السيبرانية.

ولم تنج الولايات المتحدة نفسها، عندما قام أحد القراصنة الروس باختراق منظومة حاسبات خدمات مرافق مدينة «سبرينجفيلد» بولاية ايلينوى فى نوفمبر 2011 مما أدى إلى قطع المياه لفترة عن المدينة بالكامل18.

وقد أعربت الحكومة اليابانية عن قلقها من إمكانية اختراق أنظمة الكمبيوتر الخاصة بها بدرجة من السهولة لم تكن متوقعة بسبب تعرض موقعان تابعان للحكومة إلى التخريب والى فقدان كل البيانات المتعلقة بالسكان..

وقد تستعمل حرب المعلومات لعَرْقَلَة نقلِ المالِ من جماعة إرهابية إلى أخرى. و في بِداية نزاعِ كوسوفو، نوقشتْ خطط متعددة للضغطِ على الرّئيسِ ميلوسوفيتش و اقتِحام حساباته المصرفية وعرقلُة اتصالاته الشخصية بواسطة الانترنيت..

وقد صدر في عام 2006 كتاب عن معهد "السلام الأمريكي" للمؤلف جابريل ويمان Gabriel Weimann ، وهو يتعرض بالتحليل الوافي للزيادة المخيفة في عدد المواقع الإلكترونية التي تديرها المنظمات الإرهابية على شبكة الإنترنت العالمية، فقد قفز عدد تلك المواقع من 12 موقعا عام 1998 إلى 4.800 موقع في 2006، مما يعتبر مؤشرا خطيراً للوجود والتنامي المكثف للإرهاب على صفحات الشبكة العالمية، ويقول ويمان إن هناك حرباً ضروساً تدور على ساحة الشبكة العالمية الرهيبة، بيد أننا لا نراها، وبالتالي نجهل وجودها أساساً19.

وقد اقر مؤتمر القمة العالمي لمجتمع المعلومات الذي عقد على مرحلتين (عام 2003 في جنيف وعام 2005 في تونس)، بأهمية بناء الثقة في استخدام تكنولوجيا المعلومات والاتصالات .وينعكس هذا الأمر في شعار الاحتفال للمؤتمر، ألا وهو "تعزيز أمن الفضاء الإلكتروني على النطاق العالمي"20. ففي عالم يتزايد فيه الترابط وإقامة الشبكات، أضحى من الهام للغاية ضمان سلامة نظمنا وهياكلنا التحتية الحيوية من هجمات مجرمي الفضاء الإلكتروني، والعمل في الوقت نفسه على بث الثقة في التعاملات الإلكترونية بهدف تشجيع التجارة والصيرفة والتطبيب من بعد والحكم الإلكتروني وطائفة من التطبيقات الإلكترونية الأخرى. ولما كان هذا الأمر يتوقف على الممارسات الأمنية التي يتبعها كل من البلدان والشركات والمواطنين المرتبطين بشبكات، فإننا في حاجة إلى إرساء ثقافة عالمية لأمن الفضاء الإلكتروني21.

المبحث الثاني: الحرب الالكترونية كسلاح وفقا للقانون الدولي الانساني

لا يستطيع اكمل تقنين ان يتنبأ بكل ما يمكن ان يحدث مستقبلا. وكلما تعددت التفاصيل في تقنين معين، كلما ازدادت خطورة انطوائها على نقص معين22. وعندما يتعلق الأمر بأثر التكنولوجيا الحديثة فان التفوق التقني وحده كفيل بإتاحة المجال لحروب يمكن فيها لجيش أن يقهر خصومه دون الحاجة لان يطأ أرضاً أجنبية، بينما تقوم القواعد التقليدية للقانون الدولي الانساني على الاشتباك المادي(الهجوم المسلح)، وتدرس الهيئات الدولية المختصة اليوم اثر الحرب غير المتكافئة على تطبيق القانون الدولي الإنساني23 فبعض الدول التي تمتلك التكنولوجيا الحربية الحديثة تواجه دول لا تملك من الأسلحة التقليدية أحيانا شيئا يذكر. وسيتم تناول هذا المبحث في مطلبين، يخصص الاول لتطور تفسير مفهوم استخدام القوة استجابة لتطور تكنولوجيا الحرب، اما الثاني فيتناول تطبيق قواعد القانون الدولي الانساني على الهجمات باستخدام شبكة الحاسوب.

المطلب الاول: تطور تفسير مفهوم استخدام القوة استجابة لتطور تكنولوجيا الحرب

وقد تطور مفهوم استخدام القوة استجابة لتطور تكنولوجيا الحرب، وربما، كان يصعب في القرن الماضي الحديث عن استخدام القوة والهجوم المسلح، في اطار ما يسمى بالعالم الافتراضي، او الالكتروني، اذ لم يكن مفهوم الحرب الالكترونية Cyber War، شائعاً ومألوفاً في ثمانينيات القرن العشرين ، كما هي الان.

وقد ثبت مؤخراً بجلاء مدى تعقد النزاعات التي تتفاعل فيها عدة مصادر لتقود الى انعدام الامن والسلم.والتي تحتاج فيها الدول الى عناصر قتالية مستترة تتدخل لتطيل امد النزاع او لتساهم بحسمه لصالح احد الاطراف المتنازعة، فاذا كان بالامكان تحقيق ذلك دون ظهور واضح وبكلفة مادية اقل، فضلا عن حدوث ذلك دون خسائر بشرية، يساعد في تحقيق ذلك مصادر اخرى معقدة تمثلا بحد ذاتها اسبابا لتأجيج النزعات حول العالم، وتشمل تلك المصادر :الطائفية، الإجرام، التطرف،

الاستبعاد، الفساد، والضغوط المتصلة بالموارد والظروف السكانية والبيئة، وضعف قدرة الدولة ، وتفشي انتهاكات حقوق الإنسان وعدم استقرار البلدان المجاورة، واستخدام الأسلحة المتفجرة ضد المدنيين، والحدود غير المُحكمة التي تتيح التدفق غير المشروع للأسلحة والمخدرات والأشخاص .واقتران هذه العوامل بالابتكارات التكنولوجية التي عزّزت سطوة الجماعات المسلحة، والعناصر الإجرامية والمتطرفة، وزوّدتها بوسائل متطورة لإيقاع ضرر شديد، بطرق شتى من بينها الأساليب غير المتناظرة . وعادة ما تكون هذه الجماعات مجهزة تجهيزا جيدا وتحظى بموارد جيدة، ولديها قدرة غير مسبوقة على التواصل العابر للحدود الوطنية.

ولمقاربة التطورات الدولية على هذا الصعيد منذ ثمانينات القرن التاسع عشر، وما حدث من تغير لمفاهيم الامن والسلم خلال العقود الماضية، نشير الى حكم محكمة العدل الدولية، في القضية المتعلقة بالانشطة العسكرية وشبه العسكرية في نيكارغوا وضدها، الصادر في 27/حزيران/1986، اذ قررت بان الولايات المتحدة لامريكية بوضعها الغاما في المياه الداخلية او الاقليمية لجمهورية نيكاراغوا اثناء الاشهر الاولى من عام 1984، قد تصرفت ضد نيكاراغوا على نحو يخرق التزاماتها بموجب القانون الدولي العرفي، الذي يلزمها بعدم استخدام القوة ضد دولة اخرى وعدم التدخل في شؤنها الداخلية، وعدم انتهاك سيادتها24.

كما قررت المحكمة بان الولايات المتحدة الامريكية بانتاجها في عام 1983 كاتابا دليليا بعنوان(العمليت النفسية في حرب العصابات) وتوزيعا اياه على قوات المعارضة"الكونترا"، قد شجعت على ارتكاب اعمال منافية للقانون الدولي الانساني25.

وكانت المحكمة مقتنعة بان الولايات المتحدة قد اوجدت ونظمت جيشا من المرتزقة هو قوة المعارضة "الكونترا"، وهي مولت ودربت وجهزت وسلحت الجبهه الديمقراطية الوطنية، وهي عنصر واحد من عناصر هذه القوة.

وقد ادعت حكومة نيكاراغوا ان الولايات المتحدة صممت استراتيجية قوة المعارضة، ووجهت تكتيكاتها وقدمت دعما قتاليا مباشرا لعملياتها العسكرية. وفي ضوء ما تقدم قررت المحكمة بان الادلة المشار الها لا تبرر قرارا، بان الولايات المتحدة قدمت دعما قتاليا مباشراً اذا كان معنى ذلك، تدخلا مباشرا من قبل القوات المقاتلة للولايات المتحدة، ووفقا للمحكمة لا يوجد دليل واضح على ان الولايات المتحدة تمارس فعلا درجة من السيطرة تبرر معاملة الكونترا على انها تعمل نيابة عنها، ولكي تكون الولايات المتحدة مسؤولة قانونا، يجب اثبات ان تلك الدولة تمارس سيطرة فعلية على العمليات التي وقعت اثنائها انتهاكات القانون الدولي الانساني26.

وناقشت المحكمة في هذه القضية مدى مسؤلية الولايات المتحدة الامريكية عن اعمال المتمردين التي دعمتهم بطرق مختلفة والتي شكلت اعمالهم انتهاكا

للقانون الدولي الانساني، وعلقت مسؤولية الولايات المتحدة على شرط اثبات سيطرتها الفعلية على العمليات التي كانت قائمة.

اي ان الولايات المتحدة الامريكية في ثمانينيات القرن التاسع عشر، لم تاخذ بنظر الاعتبار المسؤولية الناجمة عن تصميم استراتيجية قوة المعارضة، وتنظيم جيش من المرتزقة، والتوجيه وتقديم الدعم القتالي المباشر من قبلها للعمليات العسكرية.وبرغم كل ذلك رأت المحكمة بان مسؤولية الولايات المتحدة الامريكية متوقفة على اثبات سيطرتها الفعلية على العمليات.

بينما تطورت مؤخرا وسائل واساليب الحرب بشكل كبير، رغم أن النتائج الرئيسية للحرب بقيت كما هي لم تتغير كثيرا، الموت والتدمير، والعنف والتخريب، لكن بوسائل جديدة، اضيفت الى الوسائل التقليدية ، يمكن من خلالها مهاجمة انظمة الكمبيوتر الموصولة بشبكة الانترنت من أي نقطة في العالم لتؤدي الى انفجارات وكوارث وفيضانات27، او تدمير انظمة هامة تتحكم في منظومات اساسية في الدولة، ترتبط باحتياجات المدنيين، او اجهزة التحكم في الاسلحة. فاصبح سائداً اقتحام المواقع وتدميرها عن بعد لتغيير محتوياتها والدخول على الشبكات والعبث بها28 ، او الاستيلاء عليها او الدخول الى شبكات التحكم بالطاقة، بهدف تعطيلها عن العمل لأطول فترة ممكنة او تدميرها نهائيا لتمثل جزءً من الوسائل الحربية الشائعة للتدمير على المستوى الدولي29. ولم تعد السيطرة الفعليه جزءاً اساسيا لاثبات المسؤولية الدولية.

وفي الوقت نفسه فان المسؤولية الدولية او الجنائية الفردية عن اعمال لافراد تشكل انتهاكا للقانون الدولي الانساني لا يمكن ان تشترط التواجد الفعلي في الميدان او السيطرة الفعلية على الارض.

وقد توصلت لجنة القانون الدولي في تقريرها لعام 2006 الى عدد من المباديء الاساسية التي استخلصتها من التطورات التي حدثت في هذا الميدان في فترة اربعين عاما تقريبا والتي تتعلق بالحق الشخصي للوصول الى البيانات والمبادىء الي يجب مراعاتها عند استخدام هذه البيانات والتي بينت فيه بان الاصل هو حرية تدفق المعلومات دون قيود الا انها بينت امكانية ورود استثناءات وفرض قيود اذا كانت ضرورية لحماية الامن القومي و النظام العام، ويبدو واضحا مدى ارتباط الحرب الالكترونية بامن الدول وسيادتها. ، وتشمل هذه المباديء ما يلي:

جمع البيانات ومعالجتها بطريقة مشروعة ونزيهه ..فيقتصر جمع البيانات الشخصية على الحد الادنى الضروري وينبغي بصورة خاصة عدم الحصول على هذه المعلومات بصورة غير مشروعة عن طريق وسائل غير نزيهه.

الدقة:مبدا نوعية المعلومات يستتبع المسؤولية عن ان تكون البيانات دقيقة وكاملة للغرض المتوخى.

تحديد الغرض المتوخى والحدود الواردة لا يجوز استخدام المعلومات لاغراض غير الاغراض المحددة الا بموافقة الشخص المعني او على النحو الذي ياذن به القانون

مشاركة الفرد وخاصة حقه في الوصول الى المعلومات

الشفافية وهي تشير الى سياسة انفتاح عامة بشان التطورات والممارسات والسياسات فيما يتعلق بحماية البيانات الشخصية

ينبغي عدم جمع البيانات التي تؤدي الى تمييز غير مشروع وتعسفي ..وهذا يشمل المعلومات المجمعة عن الاصل العرقي او الاثني او عن اللون او المعتقدات الدينية او السياسية

التناسبية التي تتطلب ان يكون التدبير الضروري المتخذ متناسبا مع المطالبات المشروع المتوخاة..

المسؤولية يتضمن هذا المبدا امن البيانات ، اذ ينبغي حماية البيانات بتدابير معقولة وملائمة لتجنب فقدانها او تدميرها او الوصول اليها على نحو غير مأذون به...كما يجب ضمان وجود سلطة مسؤولة قانونا عن انفاذ متطلبات حماية البيانات

في حالة تدفق البيانات الشخصية عبر الحدود، يجب تجنب نشوء عقبات وقيود لا مبرر لها على تدفق البيانات بحرية..

مبدأ امكانية ورود استثناءات وفرض قيود اذا كانت ضرورية لحماية الامن القومي و النظام العام .

المطلب الثاني: تطبيق قواعد القانون الدولي الانساني على الهجمات باستخدام شبكة الحاسوب

وعند تطبيق قواعد القانونِ الإنسانيِ على الهجمات باستخدام شبكةِ الحاسوب(CAN)Computer Network Attacks تواجهنا الكثير من المصاعب التي يمكن أن تتعلق بسعة هذا الموضوع، وتصنيف هذا النوع من الهجمات ، وعدم وجود أية قواعد اتفاقية ضمن إطار قواعد القانون الدولي الإنساني تسعى إلى الحد من هذا الخطر الناشئ بشكل مباشر.. فمهاجمة العدو باستخدام شبكة الحاسوب لم تنظمه قواعد القانون الدولي الإنساني بعد.

ويصب تقييم مشروعية الأسلحة الجديدة في مصلحة كافة الدول، حيث أنه يساعدها في ضمان توافق سلوك قواتها المسلحة مع الالتزامات الدولية. وتُلزم المادة 36 من البروتوكول الإضافي الأول لعام 1977 كل دولة من الدول الأطراف التحقق من امتثال أي أسلحة جديدة تقوم بنشرها أو تدرس مسألة نشرها لقواعد القانون الدولي الإنساني. وهذه نقطة أخرى استحضرها دليل "تالين" على نحو مفيد. وقد طالبت الدول الأطراف في اتفاقيات جنيف أثناء المؤتمر الدولي الثامن والعشرين للصليب الأحمر والهلال الأحمر المنعقد عام 2003 بأن تخضع جميع الأسلحة الجديدة ووسائل وأساليب الحرب الجديدة "لاستعراض دقيق ومتعدد التخصصات" وذلك لضمان ألا يتخطى تطور التكنولوجيا الحماية القانونية المكفولة.ويُعَد استخدام العمليات السيبرانية(الالكترونية)، أثناء النزاعات المسلحة مثالاً جيدًا على هذا التطور التكنولوجي السريع30.

وبالرجوع الى نص المادة 36 من البروتوكول الاول الملحق باتفاقيات جنيف تلتزم الدول بمراجعة الاسلحة ووسائل واساليب الحرب التي تستخدمها حديثاً اثناء النزاعات المسلحة، وهنالك عاملان يحددان ما اذا كان السلاح جديدا ام لا:

- بالرجوع إلى الدولة التي تنوي استخدامه، فواقع ان سلاحا ما كان موجودا في الخدمة في دولة معينة لبعض الوقت قبل بيعه لدولة اخرى، لا يمنع الدولة المتلقية من اعتبار ان السلاح "جديد" وفقا لنص المادة 36، لكن ربما يكون من قبل الحيطة للدولة ان تجري مراجعة لهذه الاسلحة التي تخضع للفحص الدولي الدقيق حتى تستطيع الدفاع عن امتلاكها واستخدامها لها بشكل اكثر قوة، وان كانت المادة 36 لا تستوجب ذلك..

على انه ربما يخضع السلاح الى ترقية قدراته خلال سنوات خدمته، وسواء كان ذلك مخططا لترقية او لاستغلال تقنية جديدة، فانه يجعل السلاح جديدا من حيث سماته الخاصة، وقد يحتاج الامر الى تحديد اثر ذلك على قدرات السلاح . فاذا كان الهدف الوحيد من الترقية هو انقاص وزن السلاح مثلا لتسهيل حركته دون ان يؤثر ذلك على قدرته، فمن المنطقي الا يعد جديدا في اطار هذا المعنى من المادة 3136.

على انه من الضروري ان نميز بين المعدات واستخدامها وبين التكتيكات، والتقنيات، والاجراءات التي تتبعها القوات المسلحة. اذ تغطي هذه الجوانب نطاقا كبيرا من المجالات لا تتعلق كلها باستخدام الاسلحة او وسائل واساليب الحرب. وهي في الواقع توفر اطارا للعمل تجري من خلاله العمليات التي صممت للعدد الهائل من الظروف التي تواجه القوات في الميدان وهي لا تقع في نطاق المادة 36. ويصدق هذا ايضا على الرقابة على استخدام السلاح في اطار قواعد الاشتباك فهي لا تشكل جزءا من عملية المراجعة القانونية بل تخص بالضرورة العمليات تحديدا، ولا يمكن التكهن بها في الاعداد للمراجعة القانونية لسلاح او لوسيلة او اسلوب للحرب.

ويعد مجال الاتصالات الالكترونية مثالا جيدا على اسلوب تطبيق نص المادة 36 في مواجهة التقنيات المستجدة، فلا شك ان نظم الاتصالات تتزايد يوما بعد يوم، وهي لا تنقل المعلومات فحسب بل لها القدرة على ترتيب المعلومات المنتجة وتحليلها ونشرها وتخزينها واستعراضها وعرضها في مراحل اعداد العمليات العسكرية وتنفيذها وادخال المعلومات الرقمية الى ساحة المعركة يعزز من قدرة الاتصال بالشبكات التي تتيحها هذه التقنية.

وعند تحديد مدى انطباق المادة 36 لا بد من فهم كيفية عمل نظم الاتصالات في الواقع من خلال فهم العلم من جهة، وفهم الاستخدام الحربي لهذا العلم من جهة اخرى لتحديد ما اذا كان النظام يمتلك قدرة هجومية ام لا؟ فان كان يمتلك فما هو الاسلوب المتوخى لاستخدام هذه القدرة؟ وهل سوف يستخدم النظام على سبيل المثال لتحليل بيانات الهدف ومن ثم تقديم حل له او صورة عنه؟

فاذا كان الامر كذلك فمن المنطقي ان يقع دور نظام الاتصال في اطار معنى "وسائل واساليب الحرب" لأنه بذلك يوفر جزءا لا يتجزأ من عملية اتخاذ قرار

الاستهداف. ومن المسلم به ان وسائل واساليب الحرب يمكن ان تشمل المعدات التي لا تشكل سلاحا بالمعنى المفهوم ولكن لها اثر مباشر على القدرة الهجومية للقوات التي تملكها. ومن امثلة ذلك عربة تطهير الالغام. فربما لا تخضع سماتها للجدل من المنظور القانوني ولكن ربما يكون من المعقول ان تدرج في نطاق "وسائل واساليب الحرب" لأنها تقدم اسهاما مباشرا في القدرة الهجومية للقوات العسكرية. اما اذا كان نظام الاتصالات يجمع البيانات ويصنفها بطريقة يضع فيها صورة بيانية لمواقع التشكيلات العسكرية دون تغيير طبيعة البيانات او فحواها او كان ببساطة ينقل البيانات من موقع الى اخر. فلا يعد واقعا في نطاق وسائل واساليب الحرب...32

هذا فضلا عن أن مهاجمة العدو باستخدام الحاسوب لا يعد "هجوم مسلح" وفقا للمفهوم الذي حددته اتفاقيات جنيف ، ففي هذه الجرائم لا وجود لأي التحام جسدي بين المتنازعين. كما ان هذه الاعتداءات لا تتضمن استخداماً مباشراً للعنف.

لكن وبتطبيق القواعد العامة للقانون الدولي الإنساني فانه عندما يكون الهدف من الاعتداء على شبكة الحاسوب هو تعريض الأشخاص المحميين أو الممتلكات المحمية للخطر ، أو المخاطرة بحدوث ذلك ، يصبح القانون الإنساني منطبقاً، وتندرج تلك الاعتداءات تحت قانون الحرب33 وذلك بغض النظر عن حدوث تلاحم مادي في الميدان من عدمه، طالما كان الضرر واقعا للمدنيين والممتلكات المدنية.

وبالعودة إلى تعريف النزاع المسلح وفقا لاتفاقية جنيف الأولى 1949 والتي لا تعرف النزاع المسلح لكنها تحدد وقت بدء الحرب كآلاتي:

" .... تنطبق هذه الاتفاقية في حالة الحرب المعلنة، أو أي اشتباك مسلح آخر ينشب بين طرفين أو اكثر من الأطراف السامية المتعاقدة حتى لو لم يعترف أحدها بحالة الحرب34

أي أن الاتفاقية تنطبق في حالة أي اشتباك مسلح (وذلك بدون تحديد واضح لمعنى الاشتباك)، حتى لو لم يعترف أحد الطرفين بحالة الحرب القائمة...فتطبيق الاتفاقية وفقا لنص المادة يستلزم وجود اشتباك مسلح...وهذا لا يتوفر في النزاع باستخدام الحاسوب.

وفي هذا النص أيضا ابتعاد عن التمسك بالإعلان الرسمي من قبل الدولة لحالة الحرب ليتم إلزامها بتطبيق قواعد القانون الدولي الإنساني سواء اعلنت او لم تعلن ذلك....

بينما ذهب البروتوكول الأول الإضافي 1977 الى ابعد من ذلك فعرف الهجمات كآلاتي:

" تعني الهجمات 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 على

كل عملية حربية في البر كانت أو في الجو أم في البحر قد تصيب السكان المدنيين أو الأفراد المدنيين أو الأعيان المدنية على البر.كما تنطبق على كافة الهجمات الموجهة من البحر أو من الجو ضد أهداف على البر ولكنها لا تمس بطريقة أخرى قواعد القانون الدولي التي تنطبق على النزاع المسلح في البحر أو الجو35 "

أي أن المهاجمة من البحر أو من الجو ضد أهداف على البر يمكن أن تعتبر نزاع مسلح بموجب هذا النص، لذا فأن قواعد القانون الدولي الإنساني تنطبق على المهاجمة باستخدام الطائرات الحربية وهي تتضمن استهدافا مباشرا ...كما تنطبق في نفس الوقت على المهاجمة باستخدام الحاسوب رغم أنها قد لا تتضمن عنف مباشر طالما لم يشترط النص أن تكون المهاجمة من البحر او الجو (عنفا مباشرا او اشتباكا مسلحا...).

ووفقا لما ورد في نص المادة /2 المشار إليها أعلاه يتضح أننا ننظر إلى نتائج هذا السلوك اكثر مما نأخذ بعين الاعتبار الوسيلة التي تم استخدامها والتي يمكن أن تكون مشروعة لكنها تستخدم لتحقيق أغراض غير مشروعة36، كالتسبب بمعاناة إنسانية خطيرة أو التسبب بتحمل المدنيين لخسائر دائمة كخسائر الأسهم التجارية والإضرار بحياة وسلامة المدنيين أو بسلامة البيئة والمنشآت المدنية كالجسور والسدود ومحطات توليد الطاقة الكهربائية ...

اما عن الحدود الجغرافية التي يمكن تطبيق قواعد القانون الدولي الانساني ضمنها على الحرب الالكترونية، فينبغي الاشارة ابتداً الى ان الفضاء الالكتروني لا يمكن ان يكون منطقة غير خاضعة للقانون، وان كان من غير الممكن وضع حدود جغرافية لهذه الانتهاكات، وقد يتداخل تطبيق القانون الدولي الانساني عند تطبيقه على الانتهاكات الناجمة عن الحرب الالكترونية مع القانون الدولي للبحار وقانون الفضاء وقانون الهواء، وينبغي تحديد الحيز الجغرافي الذي جرت فيه العمليات المعلوماتية التي ادت الى انتهاك قواعد القانون الدولي الانساني، كما ينبغي تحديد الانظمة الالكترونية المستهدفة والاضرار التي نجمت عن ذلك، وقد يثير ذلك مشاكل قانونية مع الدول التي تمر هذه العمليات عبر فضائها.

ووفقا للقواعد التقليدية للقانون الدولي الانساني، فلتطبيق 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 ان بعض الفقهاء يرون ان من الممكن ان يمتد النزاع الداخلي الى خارج حدود الدولة الاقليمية37.وبالرجوع الى دليل تالين فان قانون النزاعات المسلحة ينطبق على جميع الاثار المرتبطة بالنزاع المسلح(على سبيل المثال الاضرار العرضية)38، اينما حدثت في اراضي دولة تشارك في نزاع مسلح غير دولي، وهذا يعني انه ليست هنالك منطقة نزاع يقتصر تطبيق قانون النزاعات المسلحة (القانون الدولي الانساني) عليها، كما وافق الخبراء على ان القانون ينبق على الانشطة التي تجري في سياق نزاع مسلح، فقد تستغل بعض المجموعات المسلحة المنظمة المنشقة عن

الدولة، ضعف التشريعات المتعلقة بمعالجة انتهاكات القانون الدولي الانساني التي تحدث نتيجة لعمليات معلوماتية، فتشن هجوما الكترونيا على الدولة (من خارج اقليمها) يؤدي الى حدوث اضرار وخسائر للمدنيين او الممتلكات المدنية، وبذلك نكون ايضا امام انتهاك لقواعد القانون الدولي الانساني في نزاع مسلح غير دولي(عابر للحدود)39.

المبحث الثالث: تطبيق القانون الدولي الانساني على الحرب الالكترونية وفقا للضرر او الهدف المتحقق

في إطار الأخذ بنظر الاعتبار، الهدف والضرر المتوقع (إن لم تكن الوسيلة محرمة قانونا) بسبب حداثتها ، فان محكمة العدل الدولية في فتواها بشان مشروعية استخدام الأسلحة النووية قدمت دراسة تحليلية لمبادئ القانون الدولي الإنساني في ضوء التغيرات الحديثة المتعلقة باستحداث أنواع مختلفة من الأسلحة الفتاكة، وقد أقام معظم القضاة قرارهم النهائي بشأن شرعية استخدام أو التهديد باستخدام الأسلحة النووية على أساس أن الحق في الدفاع عن النفس هو أهم قيمة أساسية كما أن بقاء الحضارة والكوكب ككل له الأهمية القصوى40.

ففسرت المحكمة وحللت واستنتجت تحريم استخدام السلاح النووي بسبب طبيعته التدميرية، ونظرت إلى نتائج استخدام هذا السلاح والأضرار التي يمكن أن يسببها للبشرية.. بغض النظر عن الوسيلة، خصوصا وان للطاقة النووية استخدامات سلمية أيضا، وفي رأيها المشار إليه فان المحكمة وضعت تفسيرات جديدة لقواعد القانون الدولي الإنساني ومبادئه، ليتم تطبيقها على جميع الأسلحة التي لم يتمكن المجتمع الدولي من وضع قيود على استخدامها أو تحريمها بعد...لكي تمتنع الدول عن استخدام الأسلحة الفتاكه الجديدة بذريعة عدم وجود نص قانوني يحرم استخدامها.

وبشكل عام فان الأهداف المحتملة للحرب الالكترونية باستخدام شبكات الحاسوب لا تختلف عنها في الحرب التقليدية، ويُمْكِنُ أَنْ تُصنّفَ إلى ثلاثة أنواع، ، وهي الاضرار التي تصيب:1) المدنيون والأهداف المدنية وسيتم تناوله في المطلب الاول، والمقاتلون والأهداف عسكرية التي سيتم تناولها في المطلب الثاني من هذا المبحث.

المطلب الاول: المدنيون الأهداف المدنية

بموجب القانون الدولي الإنساني المطبق في النزاعات المسلحة ، "يتمتع المدنيون بحصانة من الهجمات ما لم يقوموا بدور مباشر في الأعمال العدائية وعلى مدى الوقت الذي يقومون خلاله بهذا الدور"41. ويلاحظ من خلال هذا النص بانه لا يوجد نص في المعاهدات او القانون الدولي العرفي تمنع المدنيين من المشاركة في العمليات العدائية، كما لا يوجد نص قانوني يعرف المشاركة المباشرة في العمليات العدائية،

لكن ان قام المدنيين بذلك فانهم يفقدون حصانتهم على مدى الوقت الذي استغرقته هذه المشاركة المباشرة.

ويثير هذا المفهوم اشكالية كبيرة، اذ قد يتدخل المدني في العمليات العدائية، من خلال قيامه بهجوم الكتروني، قد يستغرق منه دقيقة او خمس دقائق، ووفقا للنص المشار اليه اعلاه فان المدني يفقد حصانته خلال المدة التي استغرقها قيامه بالعمل العدائي، فكيف يطبق النص في حال ان اثار هذا العمل العدائي لم تظهر فورا، وانما استغرق ساعات او ايام لظهور اثاره التدميرية.....

ووفقا لفقهاء القانون الدولي فانه يجب الاحتفاظ بالصفة المدنية للمدني، حتى لو شارك في العمليات العدائية لان استهدافه قد يؤدي الى هدم مبدأ التمييز كاحد اهم الركائز التي قام عليها القانون الدولي الانساني، ويمكن التعامل مع كل حالة مشاركة المدنيين في الهجمات المعلوماتية، وفقا لنوع المشاركة المباشرة ودرجة خطورتها في كل حالة، وما سببته من ضرر 42.

وهذا يعني أن الأهداف المسموحة بموجب القانون الدولي الإنساني في تخطيط العمليات المعلوماتية وتنفيذها هي فقط الأهداف العسكرية، من قبيل الحواسيب أو نظم الحواسيب المُستخدمة لدعم البنية التحتية العسكرية أو البنية التحتية المستخدمة على وجه خاص لأغراض عسكرية. ويعقب ذلك أن الهجمات عبر الفضاء المعلوماتي قد لا تكون موجهة ضدّ نظم الحواسيب المستخدمة في المرافق الطبية والمدارس وغيرها من المنشآت المدنية البحتة. وتكمن مسألة القلق الإنساني في هذا الصدد في أن الفضاء المعلوماتي يتميّز بالتوصيل بين نظم الحواسيب. ويتألف هذا الفضاء من عدد لا يُحصى من نظم الحواسيب المتصلة ببعضها البعض في أرجاء العالم. وغالباً ما يبدو أن نظم الحواسيب العسكرية تتصل بالنظم التجارية والمدنية وتعتمد عليها كلياً أو جزئياً. وبالتالي، قد يكون فعلاً من الصعب شنّ هجوم (معلوماتي) على بنية تحتية عسكرية وجعل الآثار تقتصر على هدف عسكري فحسب43.

وتلزم اتفاقية جنيف أطراف النزاع على التمييز بين السكان المدنيين والمقاتلين وبين الأعيان المدنية والأهداف العسكرية ، هذا فضلا عن إلزامها بتوجيه عملياتها ضد الأهداف العسكرية دون غيرها، وذلك من اجل تامين احترام وحماية السكان المدنيين والأعيان المدنية"44، وقد تم التاكيد على الالتزام بهذا المبدأ في البروتوكولين الاضافيين 1977 لاتفاقيات جنيف45.

كما نص البروتوكول الاضافي الاول الملحق باتفاقيات جنيف على مبدأ المعاناة غير الضرورية ووضع قيودا على اساليب ووسائل القتال46، 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 تحليل 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 النصر47.

وتشمل هذه الاحكام أية عملية عسكرية وبضمنها عمليات الهجوم باستخدام الحاسوب طالما أنها تسبب ضررا بالمدنيين والأعيان المدنية إذ لا ينبغي ان تتعرض هذه الفئات للهجوم مهما كان نوع الوسيلة المستخدمة في الحرب،لان القانون يحرم إيقاع الضرر ابتداءً قبل ان يبحث في الوسيلة المستخدمة لإيقاع هذا الضرر.

وقد رأت محكمة العدل الدولية بأنه أيا كانت طبيعة الصراع وايا كان حجم التباين بين القوى المتنازعة فان على جميع القوى احترام المبادئ التي تحظر المعاناة دون داع48، 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 اتخاذ 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 مستقبلا ويمثل شرط مارتنز النص المثالي الذي يضمن هذه الحماية للمدنين49.

كما بينت المحكمة أن المبادئ الأساسية للقانون الإنساني تظل منطبقة على جميع الأسلحة الجديدة، وذكرت أنه لا توجد دولة تجادل في ذلك50.ولا يمكن بناء على ما تقدم وفقا لقواعد القانون الدولي الإنساني القول بأن ما لم يحظر صراحة في المعاهدات أو العرف يكون مباحاً، لأن مبدأ الإنسانية وما يمليه الضمير العام يمثلان عوامل تقييدية قانونية. ولاشك أن هذه العوامل هي التي منعت الدول في الواقع من استخدام الأسلحة النووية منذ عام 1945،لأنه ما من شك في أن هناك وصمة قوية مرتبطة باستخدامها.51

فذريعة استخدام الدول لسلاح جديد لم يتم تحريمه مباشرة بموجب قواعد القانون الدولي لم تعد مقبولة مطلقا، وبنفس هذه المقاييس فان استخدام الحرب الالكترونية للتسبب بمعاناة إنسانية غير ضرورية أو لاستهداف السكان المدنيين هي أمر غير جائز بموجب قواعد القانون الدولي الإنساني52.

المطلب الثاني:المقاتلون والأهداف العسكرية

يعد استهداف المدنيين في النزاعات المسلحة في الحروب الالكترونية، انتهاكا لقواعد القانون الدولي الانساني، بينما يكون الاستهداف مشروعا لافراد القوات المسلحة واعضاء الجماعات المسلحة المنظمة، والمدنيون الذين يشاركون مشاركة

مباشرة في العمليات العدائية، والافراد الذين يقاومون المحتل في الهبة الجماهيرية او الشعبية. وهذه القاعدة تطبق في النزاعات المسلحة الدولية والداخلية53.

وفي الحرب الالكترونية تتغير في لحظات، صفات من يقومون بالاعمال الالكترونية التي تسبب اضرارا في اوقات النزاعات المسلحة، اذ قد يكون من تدخل في نظام الملاحة البحرية الالكتروني، مدنيا، ولا ينتمي الى القوات المسلحة، وقد يكون قد قام بفعل يسبب ضررا خطيرا، وهو يقصد هذه النتيجة، او انه لم يقصدها، وقد يطول العمل الالكتروني الذي قام به لساعات او لدقائق، كل هذه التساؤولات وغيرها الكثير مرتبطة بتكييف الحرب الالكترونية ونطاق الحماية الذي يمكن توفيره للمقاتلين في هذه الحروب، ومدى الحماية التي يمكن منحها للمدني الذي يشارك مباشرة في العمليات العدائية، وما نقصده من هذا البحث هو معرفة ان كانت قواعد القانون الدولي الانساني القائمة تسعفنا لحل هذه الاشكالات العملية والقانونية.

ولا يقصد بذلك القول بان القانون الدولي الإنساني يخلو من اية فجوات او انه ينطبق على كافة العمليات الالكترونية أو كل ما يطلق عليه "هجمات سيبرانية" في اللغة الشائعة: فالقانون الدولي الإنساني لا ينظم العمليات المعلوماتية التي تقع خارج سياق النزاع المسلح. وتهتم الشركات التجارية والحكومات بالتجسس الإلكتروني وجرائم الفضاء الإلكتروني والأنشطة الإلكترونية الجنائية الأخرى بالقدر نفسه الذي تهتم به بالهجمات الالكترونية التي يحكمها القانون الدولي الإنساني. وقد تتشابه الوسائل التقنية المستخدمة في حماية البنية التحتية الإلكترونية من التجسس أو من الهجوم، ولكن القانون الذي يحكم هذه العمليات لا يختلف. ومن ثم فإن إحدى القضايا الرئيسية هي تحديد الظروف التي يمكن في إطارها اعتبار العمليات الإلكترونية بوصفها تحدث في سياق نزاع مسلح أو تؤدي في حد ذاتها إلى نشوب نزاع مسلح بحيث ينطبق عليها القانون الدولي الإنساني.

وبالعودة الى القواعد التقليدية للقانون الدولي الانساني نجد إن الوجه المتغير للحرب والذي يعود إلى عوامل عديدة من بينها التطورات الدائمة في التقنيات العسكرية ساهم في ظهور قراءات جديدة للأحكام ذات الصلة54.

ووفق لهذه القواعد، يعتبر المقاتلون والأهداف العسكرية أهدافاً مشروعة بطبيعتها وفقا لقوانين الحرب ويمكن أن يتم أستهدفهم مباشرةً بالوسائل المتاحة على أن لا تتعارض هذه الوسائل مع قواعد ومبادئ القانون الدولي الإنساني.أي انه لا يجوز أثناء العمليات العسكرية توجيه الهجوم المباشر إلا إلى الأهداف العسكرية دون سواها، ويعد توجيه الهجماتِ باستخدام شبكةِ الحاسوبِ ضدّ المقاتلين، على سبيل المثال للتسبّب بفقدان سيطرة الملاحة الجوّية العسكرية على نظام إرْسال المعلوماتِ الملاحيةِ ليتم إرسال معلومات خاطئةٍ تتُسبّبَ في نقل قوّاتِ جيشِ لتدَميرها(بعيدا عن المدنيين) جائزٌ ومشروع بموجب هذا المفهوم55.

وبشكل عام يعد تعريف الأهداف العسكرية الوارد في البروتوكول الإضافي الأول انعكاسا للقانون الدولي العرفي. وتنص م/52(2) من البروتوكول على أن الأهداف

العسكرية تنحصر فيما يتعلق بالأعيان، على تلك التي تساهم مساهمه فعالة في العمل العسكري سواء كان ذلك بطبيعتها أم بموقعها أم بغايتها أم باستخدامها، والتي يحقق تدميرها التام أو الجزئي أو الاستيلاء عليها أو تعطيلها في الظروف السائدة حينذاك ميزة عسكرية أكيدة"

أي انه يشترط في الهدف المشروع وفقا لنص المادة :

يجب ان يساهم تدمير الهدف مساهمة فاعلة في العمل العسكري سواء كان ذلك بطبيعتها أو بموقعها أم بغايتها أم باستخدامها، أي انه يجب ان يسهم إسهاما فعالا في القدرات العسكرية المعادية.

يجب أن يحقق تدميرها أو الاستيلاء عليها أو تعطيلها ميزة عسكرية أكيدة أو قطعية في ظروف الصراع56. وتتضمن الأغراض العسكرية المشروعة قوات العدو وأسلحته وقوافله ومنشآته وإمداداته.

ونظرا لان البروتوكول الأول يتضمن تعريفا عاما وليس قائمة محدده بالأهداف العسكرية فعلى أطراف النزاع المسلح الالتزام الصارم بالشروط الواردة في المادة 52.

وتصف قوانين الحرب كل المنشآت بأنها مدنية ما لم تستوفِ الشرطين المشار إليهما. فالمنشآت التي تخصص عادة للاستخدامات المدنية كالمنازل والمساجد والكنائس والمدارس يفترض أنها ليست أغراضا عسكرية، أما إذا استخدمت فعلا لمساعدة المجهود الحربي للعدو فقد تفقد حصانتها ضد الهجوم المباشر. ويسري هذا الافتراض فقط على المنشآت التي ليست لها استخدامات أو أغراض عسكرية مهمة في الأحوال العادية، فعلى سبيل المثال، لا يتضمن هذا الافتراض منشآت من قبيل نظم النقل والاتصالات، التي لا تعتبر أغراضا عسكرية إلا إذا استوفت المعايير التي تميز تلك الأغراض.

وتطبيق الشرطين المذكورين على وسائل الاتصالات(باعتبار الانترنيت احد أهم وسائل الاتصالات المعاصرة) هو الذي يحسم موضوع استهدافها إن كان باعتبارها هدف عسكري او مدني، ونظرا إلى استخدامات هذه الوسيلة المتعددة فان التكييف القانوني باعتبارها أحد وسائل الحرب او خلاف ذلك يختلف من حالة إلى أخرى ..

وهكذا أراد القائمون بصياغة مشروع البروتوكول استثناء المساهمة غير المباشرة والحالات التي تكون الميزة المتحققة فيها غير أكيدة. ودون هذين القيدين كان يمكن بسهولة تقويض قصر الهجمات المشروعة على الأهداف العسكرية وبالتالي إبطال مبدا التمييز ، وفي كل الحالات يجب ان يلتزم المهاجم باتخاذ كافة الاحتياطات الممكنة للتحقق من أن الأغراض التي سيهاجمها عسكرية وليست مدنية. ويعني مصطلح "ممكنة" "كل ما هو عملي أو ممكن من الناحية العملية، مع الأخذ في الاعتبار كل الظروف في ذلك الوقت، بما فيها الظروف المتعلقة بنجاح العمليات العسكرية". وفي الوقت نفسه يجب على المدافعين اتخاذ كل الاحتياطات الممكنة لحماية المدنيين الواقعين تحت سيطرتهم من آثار الهجمات57. ويجب على كافة الأطراف في أثناء الصراعات الدولية المسلحة، وفي الصراعات الداخلية أيضا ،

تجنب اقتراب العمليات العسكرية من المناطق ذات الكثافة السكانية المرتفعة، كما يجب عليها قدر الإمكان إبعاد المدنيين والمنشآت المدنية عن نطاق الأغراض العسكرية.

بينما تنشا مشكلة خاصة فيما يطلق عليه الأهداف المزدوجة الاستخدام وهي التي تخدم أغراضا مدنية وعسكرية في أن واحد كالمطاراتَ، خطوط سكة حديدية، الأنظمة الكهربائية، أنظمة الاتصالات، المصانع التي تُنتجُ الموادَ لكلا الجيش والسكان المدنيين، والأقمار الصناعية مثل Intelsat، Eurosat وArabsat..... وينبغي التأكيد على ان تعبير الاستخدام المزدوج ليس مصطلحا قانونيا وترى اللجنة الدولية للصليب الاحمر ان طبيعة أي هدف يجب تقديرها على ضوء تعريف الاهداف العسكرية الوارد في البروتوكول الإضافي الأول، وعلى ذلك فربما يمكن القول انه حتى الاستخدام العسكري الثانوي يمكن ان يحول مثل هذا الهدف الى هدف عسكري على ان الهجوم على هدف كهذا يمكن ان يكون غير مشروعا اذا كانت الاثار على الاستخدام المدني للهدف تنتهك مبدا التناسب، أي اذا كان من المتوقع ان يسبب تلفا او خسائر مدنية عرضية مفرطة او إذا كان اسلوب أو وسيلة الهجوم لم يتم اختيارهما بغرض تجنب الخسائر والأضرار العرضية بين المدنيين أو على الأقل تقييدها58.. ويكون الهجوم عشوائياً عندما لا يتم تحديد الهدف العسكري بسبب الإهمال أو استعمال الأسلحةِ التي بطبيعتها لَيست قادرة على أنْ تُوجّهَ بهذه الدقة ، أَو لأن تأثيراتَ الهجومِ على الهدف العسكري يمكن أن تكون خارج السّيطرة وغير متوقع النتائج59.

وبعد مناقشات مكثفة للخبراء المسؤولين عن اعداد دليل تالين حول القانون الدولي المنطبق على الحرب السيبرانية ، اتفق أغلب الخبراء على أنه علاوة على الضرر المادي فإن توقف أحد الأعيان عن العمل قد يشكل ضرراً أيضاً.

وإذا تعطل أحد الأعيان، لا يكون من المهم كيفية حدوث ذلك سواء بوسائل حركية أو عملية إلكترونية، وهذه القضية مهمة للغاية في الممارسة العملية حيث أن أي عملية إلكترونية تستهدف تعطيل شبكة مدنية خلاف ذلك، لن يشملها الحظر الذي يفرضه القانون الدولي الإنساني على الاستهداف المباشر للأشخاص المدنيين والأعيان المدنية.

يتضح مما تقدم إنّ المشكلةَ في استخدام الحاسوب والانترنيت في الحرب هي مشكلة عملية، ولَيست قانونية فقط، فقد يَعتمدُ الجيشَ على الأهداف المزدوجة الاستعمال كشبكة الاتصالات والطرق والجسور .. معرضا بذلك المدنيين إلى ضرر حتمي ولكن ينبغي ملاحظة ان 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 المحدد60، وينبغي اثناء الحرب الالكترونية الالتزام بمبادىء القانون الدولي الانساني المتعلقة بالتمييز والتناسب واتخاذ الحيطة اللازمة.

وعندما يكون الهدف من الاعتداء على شبكة بيانات هو تعريض الأشخاص المحميين أو الممتلكات المحمية للخطر، أو المخاطرة بحدوث ذلك، يصبح القانون الإنساني منطبقاً، وتندرج تلك الاعتداءات تحت قانون الحرب.

الخاتمة والاستنتاجات

يبدو جلياً من خلال هذا البحث بانه لا يجوز شَنّ العمليات الالكترونية في النزاعات المسلحة إلا بالطريقة وبالقدر الذي يكفل احترام القانون الساري، على الرغم من عدم نصّ القانون الدولي الإنساني على حظر هذه العمليات نصاً صريحاً61. فالقواعد المتعلقة بالحرب الالكترونية والمستمدة من مصادر القانون الدولي الانساني، تسري على النزاعات المسلحة الدولية والداخلية.

وتعد الحرب الالكترونية بمثابة ثورة في الوسائل المستخدمة في النزاعات المسلحة التقليدية، ولا بد من الاعتراف بان العالم يسير في طريق تكون الحرب التقليدية فيه جزءً من الماضي . فالهجوم يمكن ان يشن الان من اي مكان في العالم ودون امكانية حتمية لتحديد هوية ودوافع الفاعل، كما ان التجسس(الالكتروني) او السيبراني أصبح أكثر فاعلية ودقة من نظيره الكلاسيكي التقليدي، وبهذا يتم المساس بمعلومات استخبارية وامنية وعسكرية لها مساس بسيادة الدولة وقد تؤثر على وجودها. وكل هذا يحدث دون اشتباك مادي بين الطرفين المتنازعين، بل ان احدهما، ربما يجهل هوية الاخر، ورغم الدقة الفائقة التي تتمتع بهاالاسلحة الالكترونية، فقد لا يراعي (المهاجم) مباديء القانون الدولي الانساني المتعلقة بالتمييز والضرورة العسكرية والتناسب.

وسوف لن تتمكن الدول التي لم تطور قواعدها التكنولوجية الحربية الالكترونية من الرد على الهجمات الالكترونية، وان تمكنت فالقانون الدولي الانساني لم يحدد بعد ماهي الحدود المشروعة للرد، وكيف للدول ان تتعامل مع قضايا المرتزقة والجواسيس وكيف لها تحديد وقت بدء وانتهاء العمل غير المشروع او حتى كيف بامكانها تحديد هوية المهاجم.

وتظهر كل هذه الفجوات وغيرها الكثير مما يتعلق بالحرب الالكترونية، الحاجة إلى تطوير قواعد القانون الدولي الانساني ودراسة جوانب كثيرة في الحرب الالكترونية (السيبرانية) لم تغطها قواعد القانون الدولي الانساني القائمة ، لضمان توفيره الحماية الكافية للسكان المدنيين ولمواكبة تطور التكنولوجيا الحديثة وجعل تأثيرها منصبا على النزاعات المسلحة فقط وليس على المدنيين والاعيان المدنية.

وقد عالج دليل تالين للحرب السيبرانية والذي سبقت الاشارة اليه في هذا البحث بعضا من هذه الفجوات، لكن لازل هنالك الكثير مما لم يعالج بعد، لذلك تعمل لجنة الخبراء في دليل تالين للحرب السيبرانية على انجاز الجزء الثاني من الدليل بحلول عام 2016.

وذلك يظهر ان الدول سوف تستمر في نوع جديد من السباق العلمي والالكتروني لتطوير وسائل الحرب الالكترونية، ليماثل ما يحدث من تطوير مستمر لترسانات

الدول العسكرية. ومن غير المرجح أن تمتنع الدول عن الانخراط في الحرب السيبرانية، لذا يجب ان تتطور مبادئ القانون الدولي الانساني لاستيعاب هذا النوع من الحروب لضمان حماية حياة المدنيين في عصرالحرب السيبرانية.

المصـــــادر:

ا. المصادر باللغة العربية

اولا. الكتب

1.جان بكتيه ، مبادئ القانون الدولي الإنساني، محاضرات في القانون الدولي الإنساني، اللجنة الدولية للصليب الأحمر ، القاهرة ، الطبعة الخامسة ، 2005.

2.جون ماري هنكرتس، لويز دوزوالد بك، القانون الدولي الانساني العرفي، المجلد الاول:القواعد،منشورات اللجنة الدولية للصليب الاحمر، مصر، القاهرة، 2007.

3.محمد خالد، الحرب الالكترونية، موسوعة علوم سلسلة الكتاب العلمي العسكري ،المكتبة العالمية،بغداد 1986 .

4.منير محمد الجيهني، جرائم الانترنيت والحاسب الالي ووسائل مكافحتها، دار الفكر الجامعي، الاسكندرية ،2005

5.يونس عرب ، قانون الكمبيوتر ، منشورات اتحاد المصارف العربية ، 2001

ثانياً: التقارير الدولية باللغة العربية

6.المؤتمر الدولي الحادي والثلاثون للصليب الاحمر والهلال الاحمر، اللجنة الدولية للصليب الاحمر، جنيف ، سويسرا، تشرين الثاني 2011.

7.القانون الدولي الإنساني وتحديات النزاعات المسلحة المعاصرة – تقرير اللجنة الدولية للصليب الاحمر للمؤتمر الدولي الثامن والعشرين للصليب الاحمر والهلال الاحمر – جنيف– 2003

8. اعمال لجنة القانون الدولي، الدورة الحادي والستون، الوثائق الرسمية، الملحق رقم /10 الوثيقة: A/61/109

9. منظمة الامم المتحدة، محكمة العدل الدولية، موجز الاحكام والفتاوى الصادرة عن محكمة العدل الدولية 1948–1991

10.بول روجرز، حماية امريكا ضد الارهاب على الأنترنيت، المركز القومي لحماية البنية التحتية، مكتب التحقيقات الفدرالي،2004

arab.htm http://usinfo.state.gov/journals/

ثالثا: الدوريات والمقالات باللغة العربية

11.إيف ساندوز، حظر وتقييد استعمال أسلحة معينة، ثلاثة أسئلة جوهرية ، المجلة الدولية للصليب الأحمر العدد37 ، 1994

12.جان لوك بلونديل ،العولمة مدخل الى الظاهرة وتاثيرها على العمل الانساني، المجلة الدولية للصليب الاحمر، مختارات من اعداد عام 2004،اللجنة الدولية للصليب الاحمر، القاهرة، 2005

13.جستن ماك كليلاند ، استعراض الاسلحة وفقا للمادة 36 من البروتوكول من البروتوكول الاضافي الاول، منشورات اللجنة الدولية للصليب الاحمر، العدد 850، 2003

14.ستانيسلاف ا. نهليك، عرض موجز للقانون الدولي الانساني، الترجمة العربية لمقال نشر في المجلة الدولية للصليب الاحمر ، 1984.

15.كوردولا دروغيه، ما من فراغ في الفضاء السيبراني، مقابلة منشورة على موقع اللجنة الدولية للصليب، الاحمر،2011، اخر زيارة للموقع: 2014/10/5
https://www.icrc.org/ara/resources/documents/interview/2011/cyber-warfare-interview-2011-08-16.htm

17. روبن م. كوبلاند، وبيتر هيربي، استعراض لمشروعية الأسلحة: مدخل جديد لمشروع "الإصابات المفرطة أو الآلام التي لا مبرر لها، المجلة الدولية للصليب الأحمر العدد 835 ، 1999

18.لوران جيزيل، ما هي القيود التي يفرضها قانون الحرب على الهجمات السيبرانية، مقالة منشورة على على الموقع الرسمي للجنة الدولية للصليب الاحمر،2013.

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

اخر زيارة للموقع: 2015/10/5

19.لويز دوسوالد بيك، القانون الدولي الإنساني وفتوى محكمة العدل الدولية بشأن مشروعية التهديد بالأسلحة النووية أو استخدامها، المجلة الدولية للصليب الأحمر العدد 1997،316

2. البحوث باللغة الانكليزية:

20.Knut Dörmann, Computer network attack and international humanitarian law, 19/5/2001
https://www.icrc.org/eng/resources/documents/misc/5p2alj.htm

21. 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

22.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.

23. Thomas C. Wingfield-When is a Cyber Attack an "Armed Attack?" Legal Thresholds for Distinguishing Military Activities in Cyberspace-The Potomac Institute for Policy Studies-2004

24 .Michael N.Schmitt, Tallinn Manual on the International Law Applicale to Cyber Warfare, Prepared by the International Group of Experts at the Invitationof the NATO cooperative cyber defence Center of excellence, Cambridge University press, 2013, first published.

25 .Michael N. Schmitt -Wired warfare: Computer network attack and jus in bello-RICR Juin IRRC Vol. 84 No 846, June 2002

26. 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/

الهوامش

[1] القانون الدولي الإنساني وتحديات النزاعات المسلحة المعاصرة،المؤتمر الدولي الحادي والثلاثون للصليب الاحمر والهلال الاحمر، اللجنة الدولية للصليب الاحمر، جنيف ، سويسرا، تشرين الثاني 2011، ص 41.
الوثيقة: 31IC/11\5.1.2

[2] يعد استخدام التجهيزات الالكترونية على نطاق واسع في الحروب من ابرز التطورات التي تشهدها ساحة المعركة في الوقت الحاضر، اذ يتم في الوقت الحاضر استخدام التجهيزات الالكترونية والحرب الاعلامية على نطاق واسع في نظم التسليح والقتال وفي الحرب النفسية ... ويمكن القول بان اول تطبيق للحرب الالكترونية جرى في العام 1905 عندما رصدت قيادة الاسطول الروسي عن طريق استراق المكالمات اللاسلكية، لتحركات القوات اليابانية، وفي بداية الحرب العالمية الاولى ازدادت تقنية الحرب الالكترونية، حيث قامت السفن الالمانية بالتشويش على العديد من الامواج اللاسلكية التي كانت البحرية البريطانية تتداولها... وفي حرب فيتنام انتج الأمريكيون اول طائرة متخصصة في الحرب الالكترونية، احتوت على انواع مختلفة من اجهزة التشوش والتوجيه والانذار.
محمد خالد، الحرب الالكترونية، موسوعة علوم سلسلة الكتاب العلمي العسكري ،المكتبة العالمية، بغداد،1986، ص36.

[3] اعمال لجنة القانون الدولي، الدورة الحادي والستون، الوثائق الرسمية، الملحق رقم /10
A/61/10، ص 460

[4] المصدر السابق، ص461

[5] Michael N.Schmitt, Tallinn Manual on the International Law Applicale to Cyber Warfare, Prepared by the International Group of Experts at the Invitationof the NATO cooperative cyber defence Center of excellence, Cambridge University press, 2013, first published, p.2-3.

[6] جان لوك بلوندیل ،العولمة مدخل الى الظاهرة وتاثيرها على العمل الانساني، المجلة الدولية للصليب الاحمر، مختارات من اعداد عام 2004،اللجنة الدولية للصليب الاحمر، القاهرة، 2005، ص184.

[7] كوردولا دروغيه، ما من فراغ في الفضاء السيبراني، مقابلة منشورة على موقع اللجنة الدولية للصليب، الاحمر،2011، ص1
اخر زيارة للموقع: 2014/10/5
https://www.icrc.org/ara/resources/documents/interview/2011/cyber-warfare-interview-2011-08-16.

[8] Michael N. Schmitt -Wired warfare: Computer network attack and jus in bello, RICR Juin IRRC Vol. 84 No 846, June 2002, p367

[9] المؤتمر الدولي الحادي والثلاثون للصليب الاحمر والهلال الاحمر، مصدر سابق، ص 42.
الوثيقة: 31IC/11l5.1.2

[10] Knut Dörmann, Computer network attack and international humanitarian law-

[11] إيف ساندوز، حظر وتقييد استعمال أسلحة معينة، ثلاثة أسئلة جوهرية ، المجلة الدولية للصليب الأحمر العدد37 ، 1994، ص2

[12] " يمتنع أعضاء الهيئة جميعا في علاقاتهم الدولية عن التهديد باستعمال القوة أو استخدامها ضد سلامة الأراضي أو الاستقلال السياسي لأية دولة أو على أي وجه آخر لا يتفق ومقاصد الأمم المتحدة"
م/2 ف4 من ميثاق منظمة الامم المتحدة 1945

[13] 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- p.3

[14] جان بكتيه ، مبادئ القانون الدولي الإنساني، محاضرات في القانون الدولي الإنساني، اللجنة الدولية للصليب الأحمر ، القاهرة ، الطبعة الخامسة ، 2005،ص53

[15] جستن ماك كليلاند ، استعراض الاسلحة وفقا للمادة 36 من البروتوكول من البروتوكول الاضافي الاول، منشورات اللجنة الدولية للصليب الاحمر، العدد 850، 2003، ص 9.

[16] Thomas C. Wingfield-When is a Cyber Attack an "Armed Attack?" Legal Thresholds for Distinguishing Military Activities in Cyberspace-The Potomac Institute for Policy Studies-2004- p.3

[17] Michael N. Schmitt -Wired warfare: Computer network…- Op.cit- p368

[18] ومن ضمن هذه الحروب نشر برمجيات خبيثة مثل wiper التى تقوم بمحو البيانات، وتشمل أيضا: القنابل المنطقية وديدان الحواسب، وصناعة "رقائق" الكترونية بها نقاط ضعف عند تصميمها تمكنها من تدمير نفسها ذاتيا حال استقبالها لإشارات محددة، وأيضا الرقائق "المكونات" التى يعتمد في تصميمها أن تشكل أبوابا سرية يمكن من خلالها فك الرسائل المشفرة وإعادة إرسالها لأجهزة المخابرات التى صنعتها. وأيضا اشعاعات "فان آيك" التى تعيد بث المعلومات و(الخداع) الذى يتم به إرسال معلومات مزيفة على نظم الاتصالات الخاصة بالقوات في الجيوش بحيث تبدو كإحدى الرسائل المتبادلة بينها مما يحدث إرباكا يترتب عليه اتخاذ قرارات هامة، فقد وصلت القدرة إلى تزييف المرئيات بطريقة مماثلة لـ (السينما) اذ يمكن ان يظهر قائد ما يتحدث في أشياء أو يلقى أوامر لم تحدث بالفعل ولم يقلها حقيقة.
ايمن السيسي، هدفها تفكيك الدولة وتقسيم المنطقة، حروب المعلومات؟ من يواجهها، 13/ حزيران/2015 ، ص2-3.
http://www.ahram.org.eg/News/121599/135/NewsPrint/414060.aspx
اخر زيارة للموقع: 2013/10/26

[19] www.taqrir.org

[20] الوثيقة WSIS-03/GENEVA/DOC/4-A - 2003

[21] http://www.un.org/arabic/news/sg/searchstr.asp?newsID=537

[22] ستانيسلاف ا. كليك، عرض موجز للقانون الدولي الانساني، الترجمة العربية لمقال نشر في المجلة الدولية للصليب الاحمر ، 1984، ص 39.

[23] القانون الدولي الإنساني وتحديات النزاعات المسلحة المعاصرة ، التقرير الذي أعدته اللجنة الدولية للصليب الأحمر للمؤتمر الدولي الثامن والعشرين للصليب الأحمر والهلال الأحمر، جنيف ، 2003

[24] منظمة الامم المتحدة، محكمة العدل الدولية، موجز الاحكام والفتاوى الصادرة عن محكمة العدل الدولية 1948-1991، ص213

[25] منظمة الامم المتحدة، محكمة العدل الدولية، موجز الاحكام والفتاوى .....، المصدر سابق، ص214

[26] المصدر نفسه، ص 215

[27] بول روجرز، حماية امريكا ضد الارهاب على الأنترنيت، المركز القومي لحماية البنية التحتية، مكتب التحقيقات الفدرالي،2004

http://usinfo.state.gov/journals/ arab.htm

[28] منير محمد الجيهني، جرائم الانترنيت والحاسب الالي ووسائل مكافحتها، دار الفكر الجامعي، الاسكندرية ،2005، ص 111.

[29] اما على الصعيد الداخلي فقد ظهرت مؤخرا جرائم مختلفة تقوم بها مجموعات معينة باستخدام أساليب مختلفة لتدمير أجهزة الحاسوب والبيانات والمعلومات لجهات معينة باستخدام طرق غير قانونية. مثل جرائم المساس بالمعلومات ذات القيمة المالية أو جرائم الكمبيوتر ذات الطبيعة الاقتصادية، وكذلك الجرائم المتعلقة باختراق حماية برامج الحاسوب من مخاطر القرصنة المتمثلة بالنسخ غير المصرح به وإعادة الإنتاج والتقليد وهو ما يقع ضمن دراسات الملكية الفكرية وتحديدا حق حماية حق المؤلف... وكذلك الجرائم المتعلقة باختراق حماية برامج الحاسوب من مخاطر القرصنة المتمثلة بالنسخ غير المصرح به وإعادة الإنتاج والتقليد
يونس عرب ، قانون الكمبيوتر ، منشورات اتحاد المصارف العربية ، 2001

[30] لوران جيزيل، ما هي القيود التي يفرضها قانون الحرب على الهجمات السيبرانية، مقالة منشورة على على الموقع الرسمي للجنة الدولية للصليب الاحمر،2013،ص1.

https://www.icrc.org/ara/resources/documents/faq/130628-cyber-warfare-q-and-a-eng.htm
اخر زيارة للموقع: 2015/10/5

[31] جستن ماك كليلاند ، مصدر سابق ، ص 10

[32] المصدر نفسه – ص 10.

[33] Michael N. Schmitt -Wired warfare: Computer network….Op.cit – p.367

[34] م/2 من اتفاقية جنيف الأولى 1949

[35] م/49ملحق البروتوكول الأول الإضافي إلى اتفاقيات جنيف المعقودة في 12/آب /1949 المتعلق بحماية ضحايا المنازعات الدولية المسلحة

[36] Michael N. Schmitt, Wired warfare: Computer network….Op.cit , 377

[37]Michael N. Schmitt, Tallinn Manual on the International Law Applicale to Cyber Warfare…., Op.Cit, p.145

[38] يعد الضرر جانبيا او عرضيا اذا كان قد يتوقع من الهجوم ان يسبب عرضياً اضراراً مفرطة، وهذه احدى القواعد العرفية في القانون الدولي الانساني، وقد شملت هذه القاعدة دولا ليست اطرافا في البرتوكول الاضافي الاول1977، الذي قنن هذه القاعدة العرفية فيما بعد في م57(2)(ب)، وعندما ناشدت اللجنة الدولية للصليب الاحمر اطراف النزاع في الشرق الاوسط في عام 1973، بالقيام بكل ما هو مستطاع لالغاء او تعليق هجوم اذا تبين ان الهدف ليس عسكرياً او اذا كان يتوقع من الهجوم ان يسبب اضرار عرضية مفرطة، جاءت ردود فعل الدول المعنية بذلك(مصر، العراق، اسرائيل، سوريا) ايجابية.
جون ماري هنكرتس، لويز دوزوالد بك، القانون الدولي الانساني العرفي، المجلد الاول:القواعد،منشورات اللجنة الدولية للصليب الاحمر، مصر، القاهرة، 2007، ص55.

[39]Ibid , p 106

[40] لويز دوسوالد بيك، القانون الدولي الإنساني وفتوى محكمة العدل الدولية بشأن مشروعية التهديد بالأسلحة النووية أو استخدامها- المجلة الدولية للصليب الأحمر العدد 316،1997-ص35

[41]بموجب م/43(2) من البروتوكول الإضافي الأول 1977

[42] Michael N. Schmitt, Tallinn Manual on the International Law Applicale to Cyber Warfare…., Op.Cit, p.125

[43] كوردولا دروغيه، مصدر سابق، ص3

[44] البروتوكول الاضافي الاول 1977، م/48

[45] البروتوكل الاضافي الاول 1977، م/51(2)، والبروتوكول الثاني، المادة 13(2).

[46] نصت المادة 35 من البروتوكول الاضافي الاول 1977 على الاتي:

1- إن حق أطراف أي نزاع مسلح في اختيار أساليب ووسائل القتال ليس حقاً لا تقيده قيود.

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

3- يحظر استخدام وسائل أو أساليب للقتال، يقصد بها أو قد يتوقع منها أن تلحق بالبيئة الطبيعية أضراراً بالغة واسعة الانتشار وطويلة الأمد.

[47] إيف ساندوز، حظر وتقييد استعمال أسلحة معينة، ثلاثة أسئلة جوهرية، المجلة الدولية للصليب الأحمر العدد 37، 1994، ص 2

[48] المصدر نفسه، ص 2

[49] ويعد هذا الشرط على جانب كبير من الأهمية، لكن تفسيره الدقيق يخضع لتباين كبير. وقد وضع هذا الشرط أصلاً في ديباجة اتفاقية لاهاي الرابعة لعام 1899 وعام 1907، ودخل بعد ذلك في صلب نص البروتوكول الإضافي الأول لعام 1977 وفي ديباجة البروتوكول الثاني

لويز دوسوالد بيك، القانون الدولي الإنساني وفتوى محكمة العدل الدولية بشأن مشروعية التهديد بالأسلحة النووية أو استخدامها، المجلة الدولية للصليب الأحمر العدد 316،1997، ص35

[49] وقد أثارت اللجنة الدولية للصليب الأحمر تساؤلا حول حقيقة وجود الآلام

[50] 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

[51] Ibid.p.3

[52] 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

[53] Michael N. Schmitt, Tallinn Manual on the International Law Applicale to Cyber Warfare…., Op.Cit, p.145

[54] لوران جيزيل، ما هي القيود التي يفرضها قانون الحرب على الهجمات السيبرانية؟، منشورات اللجنة الدولية للصليب الاحمر، 2013، ص1

https://www.icrc.org/ara/resources/documents/faq/130628-cyber-warfare-q-and-a-eng.htm
اخر زيارة للموقع 2015/10/16

[55] 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

[56]، قاعدة 8، البروتوكول الأول، مادة 52(2).

[57] البروتوكول الأول مادة 57(2)(أ)، البروتوكول الأول، مادة 58(ج).

[58] القانون الدولي الإنساني وتحديات النزاعات المسلحة المعاصرة ، تقرير اللجنة الدولية للصليب الاحمر للمؤتمر الدولي الثامن والعشرين للصليب الاحمر والهلال الاحمر ، جنيف، 2003، ص10

[59] يَمنعُ القانون الدولي الإنساني الهجمات عشوائية. بموجب م/ 51 (4) /1

[60] 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 – p.14
www.hsph.harvard.edu/

[61] القانون الدولي الإنساني وتحديات النزاعات المسلحة المعاصرة، مصدر سايق، 2011. ص44.