دراسات، علوم الشريعة والقانون، المجلّد 46، عدد 3، 2019

الحرب الإلكترونية في القانون الدولي الإنساني*

عمر محمود أعمر**

ملخص

يهدف هذا البحث إلى تسليط الضوء على أهم المبادئ المعمول بها في القانون الدولي الإنساني ومدى إمكانية تطبيقها على الحرب الإلكترونية، خاصة أن استخدام الفضاء الإلكتروني في الحرب قلب قوانين النزاع المسلح رأساً على عقب، لأن الأهداف في أي نزاع إلكتروني ستكون على الأرجح مدنية لا عسكريه، وستؤثر على السكان المدنيين لا على القوات العسكرية. كما يتطرق هذا البحث إلى تكييف الهجمات الإلكترونية من حيث اعتبارها نزاعا مسلحا أم لا، ويناقش البحث اختلاف وجهات النظر الفقهية حول إمكانية تطويع المبادئ الراسخة في القانون الدولي الإنساني وتطبيقها على الحرب الإلكترونية كما هي.

لقد تم تقسيم هذه الدراسة إلى مبحثين: الأول يتناول مدى خضوع الحرب الإلكترونية للقانون الدولي الإنساني، والآخر يتناول مدى مواءمة المبادئ العامة المتعلقة بقواعد القتال وسلوكه مع الحرب الإلكترونية.

الكلمات الدالة: القانون الدولي الإنساني، نزاع إلكتروني، الحرب الإلكترونية.

المقدمة

يمكن تعريف الحرب الإلكترونية بأنها عبارة عن هجمات تتم بواسطة استخدام الكمبيوتر أو الشبكات أو الأنظمة ذات الصلة، وتهدف إلى تعطيل أو تدمير أنظمة الإنترنت، أو الممتلكات أو الوظائف الحاسوبية الخاصة بالخصم[1] .كما ويستخدم هذا المصطلح للإشارة إلى وسائل وأساليب القتال التي تتألف من عمليات في الفضاء الإلكتروني ترقى إلى مستوى النزاع المسلح، أو تجري في سياقه ضمن المعنى المقصود في القانون الدولي الإنساني[2].

ويعرف الهجوم الإلكتروني" على أنه أي تصرف دفاعيا كان أم هجوميا، يتوقع منه وعلى نحو معقول التسبب بجرح أو قتل شخص أو الحاق أضرار مادية أو دمار بالهدف المهاجم، ويشكل تهديدا أو استخداما للقوة ضد سلامة الأراضي أو الاستقلال السياسي لأية دولة، أو التي لا تتفق بأي وجه مع مقاصد الأمم المتحدة"[3].

ويمكن استخدام أسلحة الفضاء الإلكتروني في الصراع بين الدول بشكل متواز أو غير متواز مع حرب عسكرية تقليدية، ويمثل كلا النمطين خطرا متصاعدا في العالم مما ينذر بتحوله إلى أكبر تهديد أمني دولي[4].

وتعرف القوة الإلكترونية" بأنها كافة القضايا التي تندرج تحت إطار الصراع الإلكتروني، ولكن بشكل مختلف عن مسمى الحرب الإلكترونية الذي يشير إلى التطبيقات العسكرية للفضاء الإلكتروني، ويعدّ هجوما الكترونيا عندما يتم اعتباره نمطا من الهجوم يتم شنه من قبل الدولة أو الفاعلين من غير الدول التي يكون لها تداعيات على الأمن القومي للدول والأمن العالمي"[5].

الهجمات ضد شبكة الإنترنت متعددة ومتنوعة، وما يهمنا في هذا الموضوع هو الهجمات الموجهة ضد شبكات الإنترنت والذي يمكن أن توصف بأنها نزاع مسلح، ومن الممكن أن تنفذ بعدة وسائل مثل الفيروسات والديدان الحاسوبية وعمليات جمع البيانات وأجهزة تشويش الاتصالات والبيانات اللاسلكية وسرقة المعلومات، وبرمجيات الحاسوبية المزيفة المشبوهة وأسلحة النبض الكهرومغنطيسي، وأدوات استطلاعات الحاسوب، والشبكات والقنابل الزمنية الطرودية المدمجة[6].

ويمكن لعمليات الإنترنت أن تثير المخاوف الإنسانية خاصة عندما لا تقتصر آثارها على البيانات في أجهزة الكمبيوتر، أو أنظمة الكمبيوتر بل تهدف إلى خلق تأثير في العالم الحقيقي، على سبيل المثال اختراق أنظمة الكمبيوتر للسيطرة على الحركة الجوية وخطوط أنابيب النفط ومحطات الطاقة النووية ومراقبة الحركة الجوية والبرية والبحرية والسدود، ولذلك فإن الأثر المحتمل

* هذا البحث مدعوم من جامعة العلوم التطبيقية الخاصة

** كلية البلقاء، جامعة البلقاء التطبيقية، الأردن. تاريخ استلام البحث 2018/6/14، وتاريخ قبوله 2019/3/6.

لمثل هذه العمليات سيكون على درجة عالية من الخطورة والذي قد يؤدي إلى وقوع أحداث كارثيه مثل التصادم بين الطائرات، واطلاق المواد السامة من المصانع الكيماوية أو انقطاع تشغيل البنية التحتية والحيوية مثل شبكات إمدادات المياه والكهرباء ويكون المدنيون هم الضحايا الرئيسيون لهذه العمليات.

أصبحت الدول تدرك أن الخطر في الوقت الحاضر قد يأتي من الفضاء الإلكتروني، وعليها أن تعمل على حماية مصالحها. فقد يعدّ الهجوم" السيبراني "عمل إرهابي أو يكافئ هجوما مسلحا إذا كان واسع النطاق، وأن الواقع يثبت أن عدداً من الدول كانوا ضحايا لهجمات الكترونية وبدرجات متفاوتة من حيث الشدة والضرر. ففي عام 2007، تعرضت إستوانيا إلى هجمات الكترونية كبيرة، واستمرت هذه الهجمات لعدة أيام [7]، وكذلك النزاع بين روسيا وجورجيا عام 2008، حيث لجأت روسيا إلى الحرب الإلكترونية بهدف تعطيل أنظمة الاتصالات للقوات الجورجية[8]، وكذلك الغارات الإسرائيلية عام 2007 على مشروع المفاعل النووي السوري في دير الزور، حيث قامت بهجوم الكتروني على الدفاعات الجوية السورية بغرض تعطيلها والتشويش عليها قبل دخول الطائرات[9] .وفي عام 2010 قامت الولايات المتحدة الأمريكية وإسرائيل باستخدام فيروس ستوكسنت Stuxnet، للهجوم على البرنامج الإيراني النووي للتأثير على عمليات تخصيب اليورانيوم وأجهزة الطرد المركزي، ونجم عن الهجوم إتلاف أكثر من 1000 جهاز طرد مركزي، فقد نجحت من خلال هذه الهجمة بالتسبب في تعطيل نظام التحكم الخاص بسرعة دوران أجهزة الطرد المركزي المستخدمة في تخصيب اليورانيوم وأصبحت تدور بسرعة فائقة ما أدى لتكسيرها، وفي نفس الوقت كانت ترسل معلومات خاطئة إلى غرفة التحكم، لجعلها تبدو وكأنها تعمل بشكل طبيعي[10]، وأصبح هذا السلاح الجديد قادرا على ضرب أي منطقة في العالم، وأخذت كل دولة تعمل على تطوير قدراتها العسكرية في الفضاء الإلكتروني سواء الهجومية أو الدفاعية.

لقد أصبح الفضاء السيبراني[11] ميدانا لخوض الحروب مثله مثل الجو، والفضاء، والبر، والبحر بواسطة أسلحة لها القدرة على الحاق أضرار مادية واسعة، كما أن هذه التكنولوجيا تستخدم الشبكة الإلكترونية كوسيلة يمكن الانطلاق منها وعبرها لتنفيذ العمليات العسكرية.

الدول اليوم معنيه بتحديد القانون الواجب التطبيق على الحرب الإلكترونية، فقد تبنت عدة دول مبادرات على المستوى الوطني والدولي، فعلى سبيل المثال، الاتحاد الأوروبي ركز جهوده على جرائم الإنترنت عندما تبنى في عام 2013، "استراتيجية الأمن السيبراني ومشروع التوجيه "الذي ركز على البعد الخاص للأمن" السيبراني ."والمبادرة الأكثر نجاحا هو ما ورد في دليل تالين الذي يشير إلى أن القانون الدولي الإنساني ينطبق على الحرب الإلكترونية، ويحدد الدور الذي ستلعبه قواعد القانون الدولي الإنساني في هذا المجال. فقد نشر حلف شمال الأطلسي الناتو في عام 2013 دليلا باسم تالين مكون من 282 صفحة، ويحتوي على 95 مادة للقوانين الدولية المطبقة في حال نشوب حروب الكترونية وتنظيم قواعد الاشتباك عبر الإنترنت. ويقسم هذا الدليل إلى قسمين: الأول يعالج قانون الأمن الإلكتروني والثاني قانون النزاعات الإلكترونية. ويقر قانون تالين بأن العمليات الإلكترونية قد تشكل نزاعات مسلحة تبعا للظروف، لا سيما الأثار المدمرة لتلك العمليات[12].

وتتميز عملية استخدام الأسلحة عبر الفضاء الإلكتروني بسهولة الانتشار، والقدرة على التأثير على الأهداف الجاهزة الكترونيا كالبنية التحتية الحيوية ومؤسسات اقتصادية ومالية وسياسية وعسكرية، وقد تنشأ الحروب الإلكترونية بالوساطة، كأن تبيع المنظمات المتخصصة في الأعمال العسكرية خدماتها المعلوماتية والأمنية لبعض الجهات[13].

إن استخدام الفضاء الإلكتروني في الحرب قلب قوانين النزاع المسلح رأساً على عقب، لأن الأهداف في أي نزاع إلكتروني ستكون على الأرجح مدنية لا عسكريه، وستؤثر على السكان المدنيين لا على القوات العسكرية[14]، كما أن شبكة الإنترنت لا تعترف بالحدود التقليدية، فالفضاء الإلكتروني جعل الحدود الوطنية وهمية، لأن التداخلات بين الشبكات جعلت الحدود غير ملموسة، ويعمل عموماً خارج سيطرة الدول ويمثل ذلك شكلاً جديداً من أشكال الأسلحة التي تعرض المدنيين لأخطار جسيمة، لذا فإنه ليس من المستغرب أن تفقد الدولة سيطرتها عندما يتعلق الامر بالأمور التنظيمية في الفضاء الافتراضي.

على امتداد التاريخ الحديث تم تحديث القوانين الدولية للنزاع المسلح، استجابة لفظائع الحروب والوسائل الجديدة لخوضها، وثمة حاجة ملحة للقيام بذلك لأن أعمال الحرب الإلكترونية ستسفر على الأرجح عن خرق أحكام عديدة في القوانين الحالية للنزاعات المسلحة، أو أنها ستكون خارج نطاق هذه القوانين تماماً.

ولذلك سوف نقصر دراستنا على النزاعات المسلحة الدولية من خلال الإجابة عن سؤالين: الأول هل يوجد قانون دولي معترف به يطبق على النزاعات المسلحة الإلكترونية؟ وهذا ما سيتم الإجابة عنه في المبحث الأول، تحت عنوان مدى خضوع الحرب الإلكترونية للقانون الدولي الإنساني. والثاني هل من الممكن تطبيق المبادئ الرئيسة للقانون الدولي الإنساني على الحرب

الإلكترونية الدولية؟ وهذا ما سيتم الإجابة عنه في المبحث الثاني، تحت عنوان مدى مواءمة المبادئ العامة المتعلقة بقواعد القتال وسلوكه مع الحرب الإلكترونية.

المبحث الأول
مدى خضوع الحرب الإلكترونية للقانون الدولي الإنساني.

تكمن خصوصية الفضاء الإلكتروني في عدم وجود دولة بإمكانها فرض سيطرتها وسيادتها الأحادية عليه، وهذا يؤدي إلى استخدامه بشكل قد يضر الإنسانية. الاتجاه الدولي في مجال تطبيق القواعد القانونية على الفضاء الإلكتروني أو الافتراضي أو المعلوماتي يتجه نحو تطبيق القواعد والمبادئ العامة التقليدية المعروفة في القانون الدولي العام، وذلك لصعوبة الوصول إلى اتفاق دولي جديد خاص وملزم للفضاء الإلكتروني.

وبعيدا عن المواجهات الأيدلوجية فإن النقاش الحالي سيكون حول طبيعة حكم السلوك الإنساني في الفضاء الإلكتروني، والذي يتمحور حول طبيعة القواعد التي ستسود الفضاء الإلكتروني، وكيفية إنشاء هذه القواعد وتطبيقها في نطاق القانون الدولي الإنساني، حيث يثار الجدل الفقهي في مدى إمكانية خضوع أو عدم خضوع الحرب الإلكترونية إلى أحكام القانون الدولي الإنساني القائم، وعلى هذا النحو يوجد اتجاهان: الأول يعدّ أن الفضاء الإلكتروني منطقه بلا قانون أي يقر بوجود فراغ قانوني، بمعنى عدم خضوع الحرب الإلكترونية لأي قانون، وهذا ما سوف نتناوله في المطلب الأول. والثاني يقضي بالعكس بأن الفضاء الإلكتروني يجب أن يكون منطقه خاضعة للقانون، ويجب تطبيق أحكام القانون الدولي الإنساني على الحرب الإلكترونية وهذا سيكون موضوع دراستنا في المطلب الثاني.

المطلب الأول. عدم خضوع الحرب الإلكترونية لأحكام القانون الدولي الإنساني.

الفضاء الإلكتروني هو مكان أو قارة أو فضاء مستقل في حد ذاته عن كل الفضاءات الأخرى، بما فيها فضائنا المادي الملموس. وعرف الفضاء بأنه كل مكان أو حيز أو مجال يمكن من قيام الحياة فيه بمختلف تشعباتها وعلاقاتها[15].

لذلك ذهب جانب من الفقه القانوني الأوروبي والأمريكي إلى اعتبار منطقة الفضاء الإلكتروني منطقة خاليه من القانون وكل شيء مباح، حيث يمكن لأي شخص القيام بأنشطة معاديه من دون قواعد أو ضبط النفس. فقد قيل بأن كلمات المرور وألواح المفاتيح وأجهزة الحواسيب هي التي تشكل حدودا وفواصل بين العالمين، ولا بد من الولوج إلى هذا العالم من خلالها، فهذا العالم لا يمكن أن يتحدد بدولة معينة، وبالتالي لا يمكن إخضاعه حتى للقانون الدولي العام التقليدي، فهذا القانون لم ينجح حتى الآن بحكم الفضاء البحري أو الجوي الخارجيين[16].

لذلك فإن أنصار الاتجاه الحر وهو مذهب يرفض التعامل القانوني مع الإنترنت، ويتزعمه بعض السياسيين الأمريكيين وعلماء التقنية، وتساندهم فئة قليلة من فقهاء القانون، يذهبون إلى القول: إن الإنترنت لا يخضع لقانون، وحجتهم أن الإنترنت عالم جديد لا يتفق والواقع المادي التقليدي[17].

وفيما يتعلق بتطبيق أحكام القانون الدولي الإنساني على الحرب الإلكترونية، يرى مؤيدو هذا المذهب بأنه لا يوجد نص قانوني بأي وثيقة من مواثيق القانون الدولي الإنساني تعالج الهجوم على شبكات الحاسوب أو تتحدث عن حرب المعلومات أو العمليات المعلوماتية، كما لم يتم وضع قواعد للهجوم على شبكات الحاسوب أثناء النزاعات المسلحة، كون استخدام تكنولوجيا الإنترنت هو حديث نسبياً، والقانون الدولي الإنساني القائم لا يتلاءم مع وسائل وأساليب الحرب الإلكترونية. بالإضافة إلى أن المعاهدات القائمة حالياً يرجع تاريخها إلى ما قبل وجود أو ظهور الهجمات عبر شبكات الحاسوب[18].

ويؤيد أصحاب هذا الرأي حجتهم من أن عبارة الحرب الإلكترونية لم ترد في ميثاق الأمم المتحدة واتفاقيات جنيف ولاهاي، ومعاهدة حلف شمال الأطلسي. ويستخدم ميثاق الأمم المتحدة ومعاهدة حلف شمال الأطلسي على حد سواء مصطلحات من قبيل "السلامة الإقليمية"، و"استخدام القوة المسلحة"، و"عمل من جانب القوات الجوية أو البرية أو البحرية "و"هجوم مسلح"، وهي مصطلحات لا تنسجم مع مفهوم الحرب الإلكترونية مما يضعها ظاهرياً خارج نطاق القانون الدولي[19] .وكما يبين النزاعان الإستواني والجورجي بصورة مثيرة عواقب النزاع الإلكتروني والتشويش المحيط بجهود الرد الناجم عن عدم اليقين بشأن قواعد القانون التي من الممكن أن تطبق عليه، فعلى الرغم من جسامة الأضرار المادية التي لحقت بالبنية التحتية لهاتين الدولتين واستمرار الهجمات الإلكترونية لعدة أيام إلا أنها لم تعدّ بمثابة نزاع مسلح[20] .بالإضافة إلى أن المادة 51 من ميثاق الأمم المتحدة

بينت انه"ليس في هذا الميثاق ما يضعف أو ينتقص الحق الطبيعي للدول، فرادى أو جماعات في الدفاع عن أنفسهم إذا اعتدت قوة مسلحة على أحد أعضاء الأمم المتحدة.... "هذا النص يعطي للدولة الحق في الدفاع عن نفسها، عندما تواجه هجوما من قبل قوة مسلحة. أما في سياق الحرب السيبرانية فلا يعدّ الهجوم السيبراني نزاعا مسلحا لأنه لا يتضمن استعمالا للقوة المسلحة ضد إقليم الدولة[21]، ولا يوجد في معظم الحالات ما يثبت الأدوار التي قامت بها الدول في هذه النزاعات، وقد لا يصل الهجوم الإلكتروني من القوة لكي يمكن اعتباره هجوما مسلحا[22].

ويبين أصحاب هذا الرأي أنه وعلى الرغم من أن مسمى الحرب يطلق على هجمات الكمبيوتر، فهو أيضا بحاجة إلى نظر كون الحرب مفهوما يرتكز بالأساس على استخدام الجيوش النظامية، وكان يسبقها إعلان واضح لحالة الحرب وميدان قتال محدد. أما في هجمات الفضاء الإلكتروني، فإنها غير محددة المجال أو الأهداف كونها تتحرك عبر شبكات المعلومات والاتصال المتعدية للحدود الدولية، أو اعتمادها على أسلحة الكترونية جديدة تلائم السياق التكنولوجي لعصر المعلومات، التي يتم توجيهها ضد المنشآت الحيوية أو وضعها عن طريق العملاء لأجهزة الاستخبارات، وتجعل عملية استخدام هجمات الكمبيوتر من الناحية السياسية في أي صراع أقرب إلى توصيفها بالإرهاب عن كونها حرب، كما أن تحديد وتعريف الأسلحة المعلوماتية يثير مشكله كبيره في كيفية التعامل معها[23].

ويضيف أصحاب هذا الرأي أن تطبيق المبادئ العامة في القانون الدولي الإنساني على الفضاء الإلكتروني تبدو غير واقعية، لأن وسائل وأساليب الحرب الإلكترونية غير واضحة ومفهومة بشكل كاف، ولأنها تتم في سرية تامه ولا يزال فهم الاستخدامات المحتملة لهذه التكنولوجيا وأثارها المتمثلة في الصراع المسلح غير جلي والذي تختلف جذريا عن تلك الحرب التقليدية، وتتسم كذلك هجمات الفضاء الإلكتروني بأنها استباقية ومن دون سابق إنذار، وأنها غير محددة المجال أو المدى وتكون أهدافها غير مأمونة بخلاف الحرب التقليدية التي تكون أهدافها ومكانها محددين وتكون قوات الحرب الإلكترونية غير معروفه وليست محددة في دولة سواء أكانت هدفا للحرب أو مشاركا فيها، حيث لا تصبح بالضرورة الدولة هي الهدف، وتكون الحرب الإلكترونية متعددة الأوجه ومتشابكة مع غيرها، ومن تم تكون تفاعلاتها كبيرة فهي تتشابك مع الحرب الإعلامية وحرب الشبكات والاتصالات والحرب السياسية والسيكولوجية والحرب التكنولوجية والإرهاب[24] .وبعكس المقاتلين التقليديين، فان المقاتلين" السيبرانيون "ليس لهم مكان ثابت ولا يحتاج المهاجمون" السيبرانيون "إلى التواجد في المكان الذي يحدث فيه الهجوم، أو حتى في المكان الذي يظهر أن الهجوم ينشأ فيه[25] .ويمكن للمهاجمين استعمال تكنولوجيا اتصال مجهول الهوية والتشفير لإخفاء هويتهم[26]. كما أن هناك صعوبة تكمن في تحديد مصدر هذه الهجمات، والذي تتم عادة من غير ذكر أسماء أو من خلال برنامج تسلل" روبوتي "آلي وصعوبة تتبع أصحابها لإسناد المسؤولية إلى دولة من الدول أو منظمه أو فرد، وإيجاد رابطة ما بين تلك العمليات والصراع المسلح الذي يعقد للغاية تحديد ما إذا كان القانون الدولي الإنساني ينطبق أم لا على هذا الوضع. بالإضافة إلى أن الترابط بين أنظمة الكمبيوتر المدنية والعسكرية يعقد تطبيق القواعد الأساسية للقانون الدولي الإنساني[27].

وحسب هذا الاتجاه يمكن القول: إن القانون المعمول به حالياً لا يتماشى مع مستجدات العصر، لأنه وضع أساسا للتعامل مع النزاعات المسلحة التقليدية ولا ينطبق على الهجمات الإلكترونية، لأنه لا يعدّ نزاعاً مسلحاً لغياب الأعمال العدائية التقليدية.

على الرغم من الحجج الواردة ضمن هذا الاتجاه، فإنه لا يمكن التسليم بوجود فراغ قانوني، فعند ظهور الثورة الصناعية الأولى لم يقل أحد بوجوب التخلي عن القوانين النافذة، وكذلك عند ظهور الطائرة كوسيلة نقل للبضائع والركاب، حيث كانت ظاهرة لا يربطها أي شيء بالماضي، فهي تفقد اتصالها بالأرض وتكون محلقة في الجو بين السماء والأرض، وتحليقها يكون في الأجواء الإقليمية وأحيانا فيما وراءها، حيث لا سيادة ولا سيطرة لدولة على هذا الفضاء الخارجي. ومحكمة العدل الدولية في رأيها الاستشاري المتعلق بالتهديد باستخدام الأسلحة النووية ذهبت إلى القول: إن "المبادئ والقواعد الإنسانية قد وضعت قبل اختراع الأسلحة النووية"، ولكن هذا لا يمنع من تطبيق القانون الدولي الإنساني عليها، ولا يمكن التمسك بعدم انطباق القانون الإنساني على هذه الأسلحة بحجة أنها لم تكن معروفة عند وضع قواعده وهذا ما لا يمنع من تطبيقه على الأسلحة النووية[28].

المطلب الثاني. خضوع الحرب الإلكترونية لأحكام القانون الدولي الإنساني.

يذهب أنصار هذا الاتجاه إلى عدم الاعتراف بوجود فراغ قانوني في الفضاء الافتراضي "Cyberspace is not a "law-free zoneواعتبار القواعد القانونية القائمة كافية لتنظيم الفضاء الإلكتروني، وانه يمكن تطبيقها على الفضائيات الحديثة وسمي هذا الرأي بالمذهب القانوني. وإنه يمكن التعامل مع الإنترنت قانونا، خاصة سبق وأن تم تنظيم وسائل اتصال تشبهها مثل الهاتف

والمانتال في فرنسا والفاكس وغيرها من الوسائل الإلكترونية. وما على القانونيين سوى التعاون مع التقنين وخاصة أن العديد من النصوص القانونية الموجودة قابلة للتطبيق عليها[29].

بهذا الخصوص بين المستشار القانوني للجنة الدولية للصليب الأحمر Cordula Droege أن الإطار القانوني الدولي الإنساني القائم يطبق على النزاعات" السيبرانية "ويجب احترامه، وقد تم تفنيد مزاعم من يعدّون خلو الفضاء الإلكتروني من القوانين وعدم انطباق القانون الدولي الإنساني على الحرب الإلكترونية بقولهم: إن هذه ليست المرة الأولى التي يحدث فيها تطوير وتغير في التكنولوجيا المستخدمة، وقد تعامل معها القانون الدولي الإنساني أو قانون النزاعات المسلحة، بمعنى أن القانون القائم قادر على التعامل مع هذه التطورات الجديدة دون الحاجة إلى إشعار أو وضع قواعد قانونية خاصة بالفضاء الإلكتروني[30].

وأما القول: إن الميثاق قد اشترط استخدام القوة وعدم اعتبار الهجوم" السيبراني "نزاعا مسلحا لأنه لا يتضمن استعمالا للقوة المسلحة، فميثاق الأمم المتحدة في المادة 2 فقره (4) حظر على الدول اللجوء إلى الحرب، أو التهديد باستعمال القوة أو استخدامها ضد سلامة الأراضي، أو الاستقلال السياسي لأي دولة أو على أي وجه آخر لا يتفق ومقاصد الأمم المتحدة، لكن الميثاق ترك تحديد المعنى الحقيقي لهذه القاعدة القانونية لمجلس الأمن الذي يقررها تبعا للظروف المحيطة بكل حالة على حدة، وهذا واضح من نص المادة 39 من الميثاق التي تمنح مجلس الأمن سلطة تقرير الإجراءات القهرية، حيث إنّ هذا النص ورد بصورة غير ملزمة وذلك بسبب تمتع مجلس الأمن بصلاحيات تقرير ما إذا وقع تهديد للأمن والسلم الدوليين، أو إخلال به أو كان وقع عملا من أعمال العدوان[31]، وقد يلجأ مجلس الأمن إلى اتخاذ هذه الإجراءات بصرف النظر عن نص المادة 2 فقرة 4 في حال رأى المجلس في موقف معين تهديدا للسلم، وذلك لعدم مخالفة هذا الإجراء لأحكام الميثاق أو لقواعد ومبادئ القانون الدولي[32]، كل هذا يعني أن الفقرة الرابعة من المادة الثانية من ميثاق الأمم المتحدة والمواد ذات الصلة من الميثاق تنطبق على الهجمات الإلكترونية، بغض النظر عن نوع الأسلحة المستخدمة ويعدّ ذلك استخداما للقوة بالمعنى المقصود في المادة 4/2 من الميثاق.

وفي حال العمليات الإلكترونية ضد دولة، فعلى مجلس الأمن التابع للأمم المتحدة أن يحدد إذا كانت الهجمة الإلكترونية تشكل تهديدا للسلم أو خرقا له أو عمل من أعمال العدوان، ويجوز له بان يأذن بأخذ التدابير غير القسرية بما في ذلك العمليات الإلكترونية، وإذا كانت هذه التدابير غير كافية فله أن يصدر قرارا بالتدابير القسرية بما في ذلك العمليات الكترونية، ويجوز لأي دولة أن ترد على هجوم مسلح ناجم عن أنشطة شبكة الإنترنت، أو تهديد وشيك به من خلال ممارسة حق الدفاع عن النفس المنصوص عليه في المادة 51 من الميثاق وباستخدامها وسائل الكترونيةأو تقليدية، كما فعلت الولايات المتحدة في استراتيجيتها الدولية للفضاء السيبراني لعام 2011[33]، خاصة وأن المادة 51 من ميثاق الأمم المتحدة لا تشير إلى استخدام نوع محدد من الأسلحة في الرد على الهجمات التي تتعرض لها لدول، مما يعني أن نوع السلاح المستخدم في الهجمات ليس له تأثير في نفي استخدام القوة، وأن ما يعتد به هو الأثار المادية لهذا السلاح على أرض الواقع. فالهجوم" السيبراني "يعدّ استخدما للقوة تبعا لنتائجه المادية ويشكل تهديدا للأمن والسلم الدوليين، ويعطي الحق للدولة التي تعرضت للهجوم بأن تطلب التعاون من دول أخرى لمواجهة هذه الهجمة.

لقد أجمع الفقه الدولي على أن الحرب الإلكترونية تعدّ حرب بالمعنى الصحيح عندما تكون أثارها على العالم المادي أثار مدمرة[34]، وإن استخدام القوة من خلال هذه الآلية الحديثة ضد دوله يشكل حق وطني للدولة المعتدى عليها للدفاع عن نفسها[35].

وفي قضية نيكاراغوا ضد الولايات المتحدة الأمريكية والمتعلقة بالأنشطة العسكرية وشبه العسكرية في عام1986 ، بينت محكمة العدل الدولية أن المادة 51 لا تشير إلى أسلحة محددة وأن مفهوم الأسلحة ينطبق على" أي استخدام للقوة[36]، وبغض النظر عن حقيقة أن الهجمات" السيبرانية "لا تستخدم الأسلحة الحركية التقليدية، فإن ذلك لا يعني بالضرورة أنها لا يمكن أن تكون" مسلحة"، ويمكن اعتبار استخدام أي جهاز ينتج عنه خسائر كبيرة في الأرواح أو تدمير واسع للممتلكات مستوف لشروط الهجوم" المسلح"، ويدعم هذا الاستنتاج تأكيد مجلس الأمن على ذلك الحق في الدفاع عن النفس ردا على هجمات 11 سبتمبر 2001 على الولايات المتحدة [37].

وهناك من حاول تحديد مفهوم الهجوم المسلح بأنه" فعل"، أو بداية سلسلة من أعمال القوة المسلحة ذات الحجم الكبير، التي تؤدي إلى إلحاق دمار كبير في الركائز الأساسية داخل الدولة ويؤثر على شعبها والبنية الاقتصادية والأمنية الطبيعية الخاصة بها، ويفقد الدولة جزء من سلطتها الإقليمية، أي الاستقلالية الكاملة. كما أن" استخدام الهجمات الإلكترونية بهدف التأثير على الموارد الصناعية والاقتصادية الرئيسية للدولة، قد تصل إلى هجمات مسلحة إذا كانت واسعة النطاق وتسببت بفقدان السيطرة على أنظمة التحكم التي تمر عبر أجهزة الحواسيب، مثل: انقطاع التيار الكهربائي، وإغلاق أجهزة الكمبيوتر التي تتحكم في محطات المياه

والسدود التي ينتج عنها الفيضانات في المناطق المأهولة بالسكان، وكذلك الحوادث الهندسية المميتة والمتعمدة، مثل :المعلومات الخاطئة التي تغذيها أجهزة الكمبيوتر للطائرات" و "انهيار في محطات الطاقة النووية وانطلاق المواد المشعة في المناطق ذات الكثافة السكانية العالية"[38] .وقد اعتبر أن الهجمات الإلكترونية الخطرة تمثل هجوما مسلحا، حتى ولو لم يكن هناك إصابات بالأشخاص حالها حال الهجمات التقليدية التي لا ينتج عنها إصابات أو خسائر في الممتلكات، ولا يوجد أي سبب للوصول إلى استنتاج مختلف فيما يتعلق بالهجمات" السيبرانية "ضد النظم المدنية[39].

كما يعطي دليل تالين الحق للدولة التي تتعرض لهجوم الكتروني شن حرب هجومية الكترونية مضادة على الدولة الأخرى، كما ذكر دليل تالين إنه يمكن استخدام القوة العسكرية الحقيقية في حالة تم شن هجوم الكتروني على دولة وأدى هذا الهجوم لخسائر بالأرواح البشرية[40].

اللجنة الدولية التابعة لحلف شمال الأطلسي والمكونة من خبراء قانونيين وعسكريين نشرت في عام 2013 بما يعرف" بدليل تالين "الذي يشير إلى إمكانية تطبيق القانون الدولي الإنساني كما هو على الحرب الإلكترونية. ويتمسك هذا الدليل بالتقسيم التقليدي للنزاعات المسلحة الدولية والنزاعات المسلحة غير الدولية، ويقر بأن العمليات الإلكترونية وحدها قد تشكل نزاعات مسلحة تبعا للظروف، وقد اعتبر الهجوم الإلكتروني بمثابة استخدام للقوة إذا كان أثر هذا الهجوم عند مقارنته بالاستخدام الفعلي للقوة مساويا له، أو قريبا منه"[41]، ففي هذه الحالة يجب إخضاع هذا النوع من الهجمات لقانون النزاعات المسلحة، بحيث يتم إخضاع أطراف النزاع للاتفاقيات الدولية التي تنظم هذه النزاعات، لاسيما الآثار المدمرة لتلك العمليات[42]، ويقدم الدليل في هذا الصدد تعريفاً" للهجوم السيبراني "بموجب القانون الدولي الإنساني بوصفه" عملية الكترونية سواء هجومية أو دفاعية يتوقع أن تتسبب في إصابة أو قتل أشخاص أو الأضرار بأعيان أو تدميرها كما يعدّ توقف أحد الأعيان عن العمل قد يشكل ضرراً ماديا"[43]، وتتمثل وجهة نظر اللجنة الدولية في أنه إذا تعطل أحد الأعيان فليس من المهم كيفية حدوث ذلك، سواء بوسائل حركية أو عملية الكترونية، وهذه القضية مهمة للغاية في الممارسة العملية، حيث إنّ أي عملية الكترونية تستهدف تعطيل شبكة مدنية خلاف ذلك لن يشملها الحظر الذي يفرضه القانون الدولي[44].

إن غياب أي إشارات في القانون الدولي الإنساني على الاستهداف المباشر للأشخاص المدنيين والأعيان المدنية للعمليات التي تدور في الفضاء الإلكتروني، لا يعني أن قواعد القانون الدولي الإنساني لا تغطي وسائل وأساليب الحرب الإلكترونية ما دامت هذه الوسائل تنتج نفس الآثار الذي يمكن أن ينتج عن الأسلحة التقليدية من دمار وانقطاع الخدمات الحيوية والضرر أو الإصابة أو الوفاة. ويخضع استخدام هذه الوسائل لنفس قواعد الأسلحة التقليدية، باعتبار أن القانون الدولي الإنساني واسع بما فيه الكفاية لاحتضان التقدم الحاصل في التكنولوجيا، بالإضافة إلى أنه يمكن الرجوع إلى شرط مارتينز[45].كأساس لتفسير معاهدات القانون الدولي الإنساني كلما وجدت الشكوك حول معنى بعض الأحكام الواردة فيها[46].

واستناداً إلى هذه القاعدة، فإن كل ما يقع أثناء المنازعات يخضع لمبادئ القانون الدولي الإنساني، مما يعني عدم خلو الهجوم على شبكات الحاسوب من القانون أثناء النزاع المسلح. ويوضح الرأي الاستشاري لمحكمة العدل الدولية في مشروعية التهديد بالأسلحة النووية أو استخدامها، أن المادة 2) 4 (والمادة 51 من ميثاق الأمم المتحدة تحظر استخدام القوة بغض النظر عن الأسلحة المستخدمة، فالمبادئ والقواعد الإنسانية قد وضعت قبل الأسلحة النووية، ومع ذلك فإنه لا يوجد شك بانطباق القانون الدولي الإنساني على الأسلحة النووية، وليس هناك ما يدعو للتمييز بين الأسلحة النووية وأسلحة الحاسوب، من حيث الزمن الذي استحدثت فيه مما يعني إمكانية تطبيق القانون الدولي الإنساني عليها[47].

إن البروتوكول الإضافي الأول لعام 1977 الملحق إلى اتفاقية جنيف المؤرخة في 12 آب 1949 تنص في المادة 36 تحت بند الأسلحة الجديدة" ، بأنه عند دراسة أو تطوير أو اقتناء سلاح جديد أو أداة للحرب أو اتباع أسلوب للحرب، بأن يتحقق مما إذا كان ذلك محظورا في جميع الأحوال أو في بعضها بمقتضى هذا اللحق" البروتوكول "أو أية قاعدة أخرى من قواعد القانون الدولي التي يلتزم بها الطرف السامي المتعاقد. وهذا النص يدل على قابلية القانون الدولي الإنساني على أن يطبق على الحرب الفضائية.

فيما يتعلق باعتبار أن الهجوم على شبكات الحاسوب ليس نزاعاً مسلحاً لغياب الأعمال العدائية التقليدية، ولأن وجود النزاع المسلح هو شرط لتطبيق القانون الدولي الإنساني، لم يتبن القانون الدولي الإنساني تعريفا موحدا لفكرة النزاع المسلح، وإنما فرق فقط بين النزاعات المسلحة الدولية والداخلية. فقد نصت المادة الثانية المشتركة من اتفاقية جنيف لعام 1949، بانطباق هذه الاتفاقية بغض النظر عن الشروط المحددة التي تتعلق بوقت السلم على جميع حالات الحرب المعلنة، أو أي نزاع مسلح أخر ينشب بين طرفين أو أكثر من الأطراف السامية المتعاقدة، حتى لو لم يعترف أحدها بحالة الحرب... وأصبحت الحرب المعلنة

شكل من أشكال النزاعات المسلحة[48] .المفهوم الموضوعي لهذه المادة أخذ بالحالة الواقعية للحرب لكي يطبق عليها قانون النزاعات المسلحة بصرف النظر عن أي معيار شكلي أخر يفرض متطلبات إضافية[49].

ويرى بعض الفقهاء أن النزاع يكون دوليا في حالة اللجوء إلى العنف المسلح بين دولتين أو أكثر سواء كان ذلك بإعلان سابق للحرب أو بدونه، ويفرض على الأطراف المتحاربة تطبيق القانون الدولي الإنساني، سواء اعترفت بقيام النزاع أو لم تعترف به، وهذا ما عبر عنه البعض أيضا بقولهم: إن النزاع المسلح الدولي هو نزاع مسلح بين دولتين أو أكثر. ونفس الحال عندما تقوم بعض الجهات الفاعلة من غير الدول التي تكون تحت" سيطرة شاملة "لدولة أخرى بهجوم مسلح ضد دولة اخرى من داخل أو خارج أراضي الدولة الأخيرة، سواءً تم إعلان الحرب أم لم تعلن[50] .والمحكمة الجنائية الدولية الخاصة ليوغوسلافيا سابقا، وفي حكمها في قضية" تاديتش "قضت، بأن النزاع المسلح يكون دولياً إذا وقع بين دولتين أو أكثر وكذلك يمتد ليشمل حالة النزاع المسلح غير الدولي إذا تدخلت دولة أخرى بقوة عسكرية، أو إذا كانت مشاركة أحد الفصائل المحلية المتنازعة تدخلاً بالنيابة عن دولة أخرى[51]، حيث أصبحت النزاعات المسلحة الداخلية ذات الطابع الدولي السمة الغالبة على النزاعات في الوقت الحالي[52].

إن الهجوم على شبكات الحاسوب إذا لم يحدث في سياق نزاع مسلح أو كانت أثاره لا تصل إلى نفس تأثير الهجوم العسكري الفعلي، لا ينطبق عليه القانون الدولي الإنساني، بل يخضع للقوانين الجنائية الوطنية[53]. فحسب هذا الرأي فإن القانون الدولي الإنساني ينطبق على الحرب الإلكترونية على الرغم من عدم استخدام القوات المسلحة التقليدية ذلك عندما ينسب الفعل إلى دولة، وكانت نتائج هذا الهجوم على درجة عالية من الخطورة، بمعنى الأخذ بالنتائج المادية على ارض الواقع وليس بالأفعال العنيفة، مثل العمل الذي قد يستهدف التحكم بمركز الحاسوب والشبكات الوطنية لتوليد الطاقة، ومحولات الكهرباء ومرافق الأسلحة النووية بحيث تجعلها تُدمر نفسها من الناحية العملية، وكذلك التحكم بحركة الملاحة الجوية مما يؤدي إلى تصادم الطائرات[54]، وينتج عن ذلك الأذى أو الوفاة أو إحداث التلف أو الدمار أو تكون هذه النتائج متوقعة، فإنه يعدّ هجوما مسلحا بالمعنى المقصود في القرار رقم 3314 والصادر عن الجمعية العامة للأمم المتحدة[55] .وعليه يمكن القول: إن أي هجوم"سيبراني "على دولة أو له عواقب في دولة أخرى هو بمثابة" هجوم مسلح "أو معادل له، على الأقل عندما يستتبع دماراً كبيراً، أو خسائر في الأرواح البشرية وهذا ينسجم مع المعنى الوارد في ميثاق الأمم المتحدة ومعاهدة الناتو والقانون الدولي العام، وذلك لتمكين الدول من الدفاع الفردي والجماعي المشروع بواسطة الوسائل العسكرية[56].

وهذا تجاه كل من Harold Hongju Koh و Michael N. Schmitt حيث يعدّان أن الأنشطة التي تؤدي إلى الموت تقريبا أو الإصابة أو التدمير الكبير من المرجح أن ينظر إليها على أنها استخدام للقوة وينطبق عليها القانون الدولي الإنساني[57].فالفكرة الرئيسة تقوم على وضع معيار يعتمد على أثار العمل والنتائج المتوقعة منه[58].

كما أن التهديد بالعملية الالكترونية يعطي الدولة حق الدفاع عن النفس من خلال اللجوء إلى الهجمات الوقائية أي قبل وقوع عمل من أعمال العدوان[59]، في حين أن بعض الدول يعارض مثل هذه الفكرة على سبيل المثال فرنسا وألمانيا وكذلك غالبية الدول، وهذا يوضح الفارق بين الممارسة الأمريكية والأوروبية للقانون الدولي. وكما يمكن استخدام القوة في الفضاء الإلكتروني من قبل مجلس الأمن التابع للأمم المتحدة كجزء من مهمته في الحفاظ على السلم والأمن الدوليين. فبعد أحداث 11 أيلول 2001 والحرب على العراق أخذت مشاكل الأمن أوجها جديدة منها: الحرب على الإرهاب، والحروب الدفاعية الوقائية من خلال إعطاء مفهوم آخر لحق الدفاع الشرعي عن النفس المنصوص عليه في ميثاق الامم المتحدة، التي حاولت الولايات المتحدة الأمريكية أن تجعل منه قاعدة عرفية جديدة لتتوافق مع نهجها في حماية أمنها القومي كما حدث في العراق وأفغانستان[60].

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

في الحقيقة من الصعب تحديد ما إذا كانت الهجمات" السيبرانية "تصل إلى حد استخدام القوة في العلاقات الدولية، ومن المعروف أن الفقرة 4 من المادة 2 من ميثاق الأمم المتحدة تحتوي على اثنين من المحظورات: التهديد واستخدام القوة. الفقرة 4 من المادة 2 لا تحدد الطرق التي يجب من خلالها تنفيذ التهديد. التهديد عبر الإنترنت سيكون على نفس المستوى النظري المساوي للطرق التقليدية، والذي يحذر من هجوم الكتروني محتمل من قبل الدولة المهددة، وفي الرأي الاستشاري حول مشروعية استخدام الأسلحة النووية ربطت محكمة العدل الدولية قانونية التهديدات الموجهة إلى مشروعية استخدام القوة إلى نفس الظروف التقليدية.

أما إذا كان يمكن اعتبار القوة" السيبرانية "نوعًا من" القوة "بالمعنى المنصوص عليه في الفقرة 4 من المادة2 ، فالمعايير العامة

لتفسير المعاهدات والمنصوص عليها في اتفاقية فيينا لعام 1969 بشأن قانون المعاهدات تضمنت في فقرتها الأولى من المادة 31 المبادئ الواجب اتباعها عند تفسير معاهدة ما، فقررت تفسير المعاهدة بحسن نية طبقا للمعنى العادي لألفاظ المعاهدة في الإطار الخاص بها وفي ضوء موضوعها والغرض منها. والمعنى العادي" للقوة "هو العنف أو الضغط الموجه ضد دولة، وهو بالتالي واسع بما يكفي لتغطية ليس فقط القوة المسلحة التقليدية، ولكن أيضا أنواع أخرى من الإكراه بقدر ما يتعلق بالسياق. وتعبير" القوة "يظهر أيضا في ديباجة الميثاق وفي المواد 41 و46 حيث يسبقها صفة" مسلح"، بينما في المادة 44 فقد تمت الإشارة إلى القوة العسكرية. والميثاق يشير صراحة في مواده عندما يريد واضعوه إلى الإشارة إلى" القوة المسلحة"، وبما أن الأمر لم يكن كذلك في الفقرة 2 من المادة4 ، فربما أراد واضعوه الرجوع إلى نطاق أوسع في تفسيره ليتماشى مع الهدف العام للميثاق هو" إنقاذ الأجيال من ويلات الحرب"[61].

في نهاية هذا المطلب لا بد من الإشارة إلى الوثيقة التي وضعتها وزارة الدفاع الأمريكية في عام 1999 وتشمل دراسة مجموعة من المعاهدات التي تتعلق بسلوك الحرب الإلكترونية وخلصتإلى الاتي[62]:

أولا–أن المجتمع الدولي من غير المحتمل أن ينتج على الفور قانونا حول سلوك الحرب الإلكترونية.

ثانيا– لا توجد سبل قانونية واضحة للتصدي لهذا النوع من عمليات الحرب الإلكترونية

ثالثًا– أوصت الوثيقة بتحليل مختلف لعناصر وظروف أي عملية معينة مخطط لها، أو أي نشاط لتحديد إمكانية تطبيق القانون الدولي الحالي عليها. هذه الدراسة تؤكد على عدم اليقين من أن القانون القائم قادر على احتواء هذا النوع الجديد من الحروب.

المبحث الثاني

مدى ملائمة المبادئ الأساسية التي تحكم النزاعات المسلحة على الحرب الإلكترونية.

سعى القانون الدولي الإنساني منذ نشوئه لتنظيم القواعد والضوابط التي تحكم سير العمليات العسكرية خلال النزاعات المسلحة بنوعيها الدولي وغير الدولي، وعلى الرغم من عدم قدرة هذا القانون على منع الحرب إلا انه يسعى للحد من آثار النزاع المسلح فيما بين الأطراف المتنازعة وبشكل خاص لحماية المدنيين الذين لا يشاركون في القتال، والأشخاص الذين أصبحوا عاجزين عن المشاركة في القتال والسعي لتحييد الأعيان المدنية عن سير الأعمال العدائية خلال سير العمليات القتالية التقليدية، ظهرت هذه المبادئ في ضوء الحروب التقليدية ومع التطور التقني ودخول مفهوم الحرب الإلكترونية إلى النزاعات المسلحة كان من المفترض وجود ضوابط لحماية الفئات المحمية في سياق هذه النزاعات.

الفضاء الإلكتروني يتميز بالترابط وهو يتألف من عدد كبير من أنظمة الكمبيوتر المتعلقة مع بعضها البعض في جميع أنحاء العالم، وتكون أنظمة الكمبيوتر عسكرية في كثير من الأحيان مترابطة مع الأنظمة المدنية، لذلك فانه ليس من السهل إطلاق هجوم الكتروني ضد البنية التحتية العسكرية، والحد من آثاره دون تقوض البنية التحتية المدنية والذي من شأنه أن يكون مثالا لانتهاك القانون الدولي الإنساني من خلال ضرب الأهداف العسكرية والمدنية والمدنيين على حد سواء.

جميع قواعد القانون الدولي الإنساني من الممكن أن تنطبق على نزاع مسلح دولي، ولكن ما مدى إمكانية تطبيقها على النزاع الإلكتروني، هذا ما سنحاول بيانه من خلال مطلبين وعلى النحو التالي :المطلب الأول :مبدأ الضرورة العسكرية والمطلب الثاني مبدا التمييز والتناسب.

المطلب الأول. مبدأ الضرورة العسكرية.

ورد أول تعريف لمبدأ الضرورة العسكرية في قانون ليبر عام 1863 التي عرفها بأنها التدابير التي لا غنى عنها لتأمين انتهاء الحرب[63]. وتم الإشارة لهذا المبدأ في اتفاقية لاهاي الخاصة باحترام قوانين وأعراف الحرب البرية لعام 1907 وفي المواد(43 و54) من ذات الاتفاقية. وحدد البروتوكول الإضافي الأول لاتفاقيات جنيف لعام 1949 الضرورة العسكرية كحالة استثنائية في النزاعات المسلحة، فقد نصت المادة 2/52 بأن الأهداف العسكرية هي التي" تقصر الهجمات على الأهداف العسكرية فحسب"[64].

إن الأهداف العسكرية هي الأهداف التي تسهم بحكم طبيعتها، أو موقعها أو غرضها أو استخدامها إسهاما فعالاً في قدرة العدو العسكرية، التي يؤدي تدميرها أو تحييدها بصورة كاملة أو جزئية وقت الهجوم إلى دعم الغايات العسكرية الشرعية. فالمعدات والمنشآت تشكل أهدافا عسكرية ويمكن مهاجمتها مباشره بواسطة شبكات الحاسوب، ولكن يصعب غالباً تحديد الأهداف التي يمكن

اعتبارها عسكرية وتساهم في العمليات العسكرية[65]. أما الأهداف المحمية فهي الأهداف التي تحميها اتفاقيات جنيف، مثل المستشفيات، ووسائل نقل الجرحى أو المرضى، والمواقع الدينية أو الثقافية، ومناطق السلامة. غير انه في حال استخدام أي من هذه المواقع لأغراض عسكرية فإن من الجائز مهاجمتها، وعلى سبيل المثال فإذا ما استخدمت الهيئات العسكرية كنيسة كقاعدة للعمليات، فإنها يمكن أن تصبح هدفاً عسكريا مشروعا[66].

وبين البروتوكول الإضافي الأول حالات الضرورة، بأن تكون ضرورة عسكرية ملحة في حالات اتباع سياسة "الأرض المحروقة "في الأراضي الواقعة تحت سيطرة الخصم[67]، وحالات احترام وحماية الأجهزة المدنية للدفاع المدني وأفرادها[68]، وحالات احترام وحماية لوازم ومباني الوحدات العسكرية التي تخصص بصفة دائمة لأجهزة الدفاع المدني، وتكرس لأداء مهام الدفاع المدني للخصم[69]، توضح هذه الحالات متى يجوز اللجوء لمبدأ الضرورة العسكرية في القانون الإنساني الدولي، كما وحددت شروط الضرورة:

- أن يكون هذا التجاوز مؤقتاً ومرتبطاً بمدة قيام هذه الضرورة.
- أن يكون على أهداف محددة.
- أن يكون الغرض منها يحقق ميزة عسكرية أكيده.
- أن يتم مراعاة القانون الدولي الإنساني.

فقانون النزاعات المسلحة ينطبق نظرياً على الوسائل الإلكترونية المستخدمة في الأعمال العدائية وبالتالي يتم تطبيق المبادئ الأساسية الراسخة في القانون الدولي الإنساني، ويمكن الدفاع عن النفس والرد بوسائل الكترونية أو تقليدية، حيث يتم اللجوء لمعايير الهجوم العسكري التقليدي لتقييم الهجمة الإلكترونية[70]، فقد اعتبر" شميث "و"كوه "ومجموعة من الخبراء في حلف شمال الأطلسي ممن وضعوا ما يسمى بدليل تالين أن الهجوم الإلكتروني هو بمثابة استخدام للقوة، إذا كان أثر الهجوم عند مقارنته بالاستخدام الفعلي للقوة مساويا له أو قريبا منه[71] .فعند وقوع هجمة الكترونية على الدولة ترقى إلى الاستخدام الفعلي للقوة فان هذه الهجمة تخضع لمبدأ الضرورة العسكرية كما أن العمليات الإلكترونية التي تقوم بها الدولة في ممارسة حقها في الدفاع عن النفس يجب أن تكون ضرورية ومتناسبة.

في الحرب الإلكترونية لا يوجد معايير محدده لاستخدام تكنولوجيا المعلومات للأغراض العسكرية الهجومية، مما يعني إمكانية استخدام هذه التكنولوجيا بداعي الضرورة العسكرية[72] .وفي دليل تالين نصت المادة (113) على أن الهجمة الإلكترونية التي يتوقع منها أن تسبب خسائر عرضية في أرواح المدنيين أو إصابات في صفوف المدنيين، والإضرار بالأعيان المدنية أو كلها مجتمعة، التي من شأنها أن تكون مفرطة بالنسبة إلى ميزه عسكرية ملموسة ومباشرة محظورة. واشترط" كوه "على أطراف النزاع أن تراعي عدة شروط قبل تنفيذ الهجمة الإلكترونية وهي[73]:

1. دراسة آثار الأسلحة السيبرانية على البنية التحتية للمستخدمين العسكريين والمدنيين على حد سواء، بما في ذلك تقاسم البنية التحتية المادية المشتركة مثل شبكة السدود وشبكات الماء والكهرباء التي من شأنها أن تؤثر على المدنيين.
2. دراسة الأضرار المادية المحتملة التي قد تسببها الهجمات عبر الإنترنت مثل الوفاة، أو الإصابة التي قد تنجم من آثر الهجوم على البنية التحتية الحيوية.
3. دراسة الأثار المحتملة لهجوم عبر الإنترنت على الأهداف المدنية التي لا تشكل أهدافاً عسكرية مثل أجهزة المدنيين ولكن قد تكون مرتبطة مع أجهزة الكمبيوتر التي هي أهداف عسكرية.
4. قيام الدول بتقييم أسلحتها الإلكترونية، بمعنى أن يكون استخدام هذه الأسلحة ليس محظوراً ولا يتنافى مع قانون الحرب أو أنه لا يمكن استخدام هذه الأسلحة بطريقة مغايرة لمبدأي التمييز والتناسب.

رد الفعل في الدفاع عن النفس ضد الهجمات" السيبرانية "التي تصل إلى هجمة مسلحة يجب أن تتناسب مع متطلبات الضرورة، التي تعني أن استخدام القوة هي الوسيلة الأخيرة التي يتم اللجوء إليها، وأن الوسائل الأخرى المتاحة قد فشلت أو من المحتمل أن تفشل، وكذلك ضرورة التحقق من أن الهجوم الإلكتروني ليس من قبيل الصدفة، وأن الأمر لا يمكن أن يستقر بوسائل أقل تدخلا مثل منع المتسللين من الوصول إلى الشبكات ومواقع الويب التي تتعرض للهجوم من خلال استخدام الدفاعات السيبرانية.

في الحقيقة المشكلة الرئيسة في استخدام حق الدفاع عن النفس للرد ضد هجوم" سيبراني "هو تحديد المعتدي، ومن اجل تجاوز هذه الصعوبة اقترح بعض المعلقين أن الرد في الدفاع عن النفس عن هجوم الكتروني ضد البنى التحتية الحيوية الوطنية ينبغي

السماح بها، حتى من دون تحديد صفة المهاجم[74]، ووفقا لوجهة النظر هذه، يجب أن يسمح القانون بالرد على أساس الهدف من الهجوم، بغض النظر عن هوية المهاجم. هذا الموقف لا يمكن أن يكون مقبولا، ليس فقط لمخالفته قانون المسؤولية الدولية، وإنما لكونه غير منطقي بطبيعته.

في الفضاء الإلكتروني لا يوجد آلية واضحة لتحديد طريقة الرد على هذه الهجمات سواء إذا كانت عن طريق اللجوء لأعمال القوة بما فيها الهجمات الإلكترونية، أو الرد دون اللجوء لأعمال القوة مثل قطع العلاقات الدبلوماسية، أو الحصار الاقتصادي. ويبين دليل تالين بأن المفتاح الرئيس في تحديد حالة الضرورة العسكرية هو قلة البدائل المتاحة للتصدي لهذه الهجمة أو الحد من آثارها. ففي حال ما إذا كانت هذه الهجمات الإلكترونية ترقى لمستوى النزاع المسلح، فإنها تخضع لقانون النزاعات المسلحة[75].

ولكن السؤال المطروح في حال وجود خادم (Server) يستخدم بشكل مشترك بين المدنيين والعسكريين هل يتم استهدافه لتحقيق ميزة عسكرية؟ مع العلم بأن الضرر الذي سيلحق بالمدنيين سيكون تأثيره أكثر بكثير من الميزة العسكرية، فعلى سبيل المثال تعدّ شبكات اتصالات القطاع الخاص الأمريكي هدفاً عسكرياً مشروعاً وضمن الضرورة العسكرية بالنظر إلى أن نسبة 90% من الاتصالات الحكومية الأمريكية تستخدم الشبكات المدنية، بما في ذلك الإنترنت، والاتصالات، والهواتف الخلوية، كذلك المستشفيات التي تعتمد اعتماداً كلياً على الشبكات المذكورة، وفي حالة شن هجوم على خادم مخصص للاستخدام العسكري، ولكن يستخدم من قبل الوحدات الطبية العسكرية المحمية، على الأرجح سينظر إلى هذه الهجمات على أنها ضد هدف محمي بموجب الاتفاقيات الدولية [76]. وفي هذا الخصوص أشار دليل تالين على أن الأعيان التي تستعمل لأغراض مدنية وعسكرية مثل: أجهزة الكمبيوتر وشبكات الكمبيوتر والبنية التحتية الإلكترونية هي أهداف عسكرية، فما مدى توافق هذه القاعدة مع مبدأ الضرورة العسكرية وتحقيق الميزة العسكرية[77].

أما في حالة التهديد بشن هجوم الكتروني وكان الضرر المتوقع منه يعادل استخدام القوة، فإنها قد تعدّ من الحالات التي تبيح استخدام القوة، فنعود لمبدأ الضرورة العسكرية وقوانين النزاع المسلح التي تمكن الدولة من استهداف كل شيء بمقتضى الضرورة العسكرية.

على الرغم من الجهود التي بذلت في إعداد هذا الدليل فإن مبدأ الضرورة العسكرية قد أصبح مجرد تسمية في ظل هذا الدليل دون أي وجود فعلي له في حالة الحرب" السيبرانية"، حيث تم التوسع في حالات اللجوء الى مبدأ الضرورة العسكرية.

المطلب الثاني. مبدا التمييز والتناسب.

في الفضاء الإلكتروني عدة أسئلة بحاجة إلى الإجابة ومنها :كيف يمكن التمييز بين المدنيين والعسكريين؟ ما هي العلامات المميزة للجنود السيبرانيين؟ كيف يمكن التمييز بين الشبكات المدنية والعسكرية؟ ما القوة المفرطة في الفضاء السيبراني؟ كيف يمكن لأطراف النزاع التفريق بين الأهداف العسكرية والأهداف المحمية؟

جاء في إعلان سان بطرسبورغ لعام 1868" يجب أن يكون الغرض الشرعي الوحيد الذي تستهدفه الدول أثناء الحرب هو إضعاف قوات العدو العسكرية، ويكفي لهذا الغرض عزل اكبر عدد ممكن من الرجال عن القتال[78]"، وعالجت القواعد العرفية في القانون الدولي الإنساني في المواد من (1 إلى 10) ضرورة التمييز بين المدنيين والعسكريين، ونص البروتوكول الإضافي الأول لاتفاقيات جنيف على أن تعمل اطراف النزاع على التمييز بين السكان المدنيين والمقاتلين، وبين الأعيان المدنية والأهداف العسكرية، ومن ثم توجه عملياتها ضد الأهداف العسكرية دون غيرها، وذلك من أجل تأمين احترام وحماية السكان المدنيين والأعيان المدنية، وقد عالجت المواد (51 و52) من البرتوكول الإضافي الأول مبدأ التمييز للمدنيين والأعيان المدنية وهو ما أكدته محكمة العدل الدولية في الرأي الاستشاري المتعلق بالأسلحة النووية، وهو وجوب ألا تجعل الدول المدنيين هدفاً للهجوم، وبالتالي يجب ألا تستخدم أبداً أسلحة غير قادرة على التمييز بين الأهداف المدنية والعسكرية[79].

المراحل الأولى من أي هجوم الكتروني ستكون في بدايتها أقرب إلى الهجمة العشوائية العمياء، وهذا يعني أن استغلال شبكة الكمبيوتر في سياق النزاعات المسلحة نسيكون تحدياً لمبدأ التمييز مما يجعل مسألة الهجوم الإلكتروني أمراً غير أخلاقي[80].

مبدأ وجوب التمييز[81] بين المقاتلين والمدنيين، وبين الأهداف العسكرية وغير العسكرية ينطبق على الأنشطة" السيبرانية"، التي ترقى إلى مستوى هجوم ضمن مفهوم قانون الحرب في سياق نزاع مسلح[82]، ولهذا يجب أن تكون الأعمال العسكرية موجهة ضد الأعيان التي تسهم مساهمة فعالة في الأعمال العسكرية، التي يعطي تدميرها ميزة عسكرية، والابتعاد عن الأعيان المدنية المحمية بموجب القانون الدولي من أن تكون هدفا لهجوم عسكري. بالإضافة إلى ذلك فلا تعدّ كل هجمة الكترونية تستهدف المدنيين فعلاً

يخالف قواعد النزاعات المسلحة، مثل اختراق الشبكة المدنية بغرض إرسال رسائل الكترونية للمدنيين تحثهم على الاستسلام[83]، وفي المقابل تعدّ هجمة عشوائية إذا كان مصدر الهجمة لا يستطيع التحكم بها وتعدّ هذه الهجمة فعلا يخالف قواعد النزاعات المسلحة.

ونص دليل تالين على إمكانية تطبيق مبدأ التمييز على الهجمات الإلكترونية، وبين الدليل أن المدنيين أفرادا أو جماعات يجب ألا يكونوا هدفاً للهجمات الإلكترونية، وفي حالة الشك في حالة الشخص فيما إذا كان عسكرياً أو مدنياً فإنه يعدّ مدنياً، وقد حددت المادة (96) من الدليل بأن الفئات التالية هي الأهداف التي يمكن مهاجمتها خلال النزاع وهي:

1. أفراد القوات المسلحة.
2. أعضاء الجماعات المسلحة المنظمة.
3. المدنيون الذين يشاركون مباشرة في الأعمال الحربية.
4. المشاركون في الانتفاضة الشعبية، في النزاع المسلح الدولي.

واعتبرت المادة (96) أن المدنيين يتمتعون بالحماية خلال الفترة التي لا يشاركون فيها بالعمليات العدائية، ونصت المادة (98) على حظر توجه هجمات تبث الذعر بين المدنيين. وفي المادة (99) نصت على إنه لا يجوز استهداف الأعيان المدنية بالهجمات الإلكترونية التي تشمل أجهزة الكمبيوتر وشبكات الكمبيوتر والبينة التحتية الحاسوبية.

إن ما ورد في هذا الدليل يعدّ تطبيقاً نظرياً لمبدأ التمييز، فالقوانين الدولية للنزاع المسلح تسمح باستخدام القوات غير النظامية، فالحكومات تستطيع التعاقد مع شركات لها القدرة الاختراقية واستخدام شبكاتهم كمقاتلين شرعيين في النزاعات" السيبرانية"، ومن الجائز تخويل القوات غير النظامية المشاركة في الأعمال العدائية، ولكن هذه الشبكات الاختراقية ليست مميزة كما أن أسلحتها غير ظاهرة للعيان ولا تحمل شعاراً أو علامة.

وقد يكون الحاسوب الشخصي المشارك في هجوم يشن بأمر من دولة مملوكا لمدني بريء غير مدرك بأن حاسوبه قد تم اختراقه، وفي حال القبض على من يدير الشبكات المخترقة فهل يمكن محاكمتهم كمجرمي حرب؟ وماذا عن مالكي الحواسيب؟[84]

بالإضافة إلى أن الترابط ما بين الشبكات المدنية والعسكرية يجعل من الصعب بل من المستحيل الفصل ما بين الشبكات، كما أن موضوع التمييز بين السكان المدنيين والمقاتلين، وبين الأعيان المدنية والأهداف العسكرية مسألة في غاية التعقيد على عكس الهجمات التقليدية لوجود المهاجم في مكان بعيد عن المكان المستهدف من الهجوم، مما يؤدي إلى استحالة التمييز بين المقاتلين والمدنيين، ومثال على ذلك تعرض الدول إلى هجمات غير معروفة المصدر مثل هجمات الطائرات بدون طيار[85]، وكذلك عند تطبيق التعريف القانوني للأهداف العسكرية في المجال الإلكتروني سيجعل كل كيان إلكتروني هدفاً عسكرياً مشروعاً، فكل عنصر من عناصر البنية التحتية الإلكترونية هو عين ثنائية الاستخدام، بالإضافة إلى أن الجيش يستخدم إلى حد كبير نفس البنية التحتية الإلكترونية التي تستخدم في الأغراض المدنية[86].

ونظراً للطبيعة المترابطة للشبكات الحاسوبية، فإنه من غير المتصور استهداف جزء من الشبكة دون التأثير على باقي الأجزاء سواء أكانت الهجمة الكترونية أو هجمة بالمفهوم التقليدي، ففي شروحات دليل تالين نجد في شرح المادة (99) بأن مجموعة الخبراء الدوليين ترى بأن دراسة تحديد طبيعة الشبكة فيما إذا كانت عسكرية أو مدنية يتم من خلال دراسة كل حالة على حده، لعدم وجود معيار يحدد طبيعة الشبكة المستهدفة. في الحقيقة هذا المعيار فضفاض وغير موضوعي بالنسبة للطرف المهاجم، لإمكانيته شل البنية التحتية لدولة ما بسبب معاييره الخاصة، باعتبار أن البنية التحتية المستهدفة تعدّ هدفاً عسكرياً مشروعاً من وجهة نظره. فقد اعتبرت المادة (100) من دليل تالين أن الأعيان المدنية هي كافة الأعيان التي ليست أهدافاً عسكرية، والأهداف العسكرية هي تلك الأشياء التي بحكم طبيعتها وموقعها وغرضها أو استخدامها تقدم مساهمة فعالة في العمل العسكري، التي يشكل تدميرها التام أو الجزئي أو الاستيلاء عليها أو تعطيلها في الظروف السائدة حينذاك ميزة عسكرية أكيدة، ويمكن أن تشمل الأهداف العسكرية: أجهزة الكمبيوتر وشبكات الكمبيوتر والبنية التحتية الحاسوبية، فمن المؤكد أن البنية التحتية التي تحمل الاستخدام المزدوج هي الأداة الأولى في الحرب الإلكترونية ومن خلال تدميرها بشكل تام أو جزئي سيؤدي إلى ميزة عسكرية أكيدة بنفس المعايير التي استخدمت ضد العراق خلال الحصار، حيث تم منع العراق من استيراد أقلام الرصاص بحجة الاستخدام المزدوج[87].

إن الأعيان التي تستخدم لأغراض مدنية وعسكرية وأجهزة الكمبيوتر وشبكات الكمبيوتر والبنية التحتية الإلكترونية تتحول بشكل تلقائي لهدف عسكري مشروع، فعلى سبيل المثال نظام الرادار المستخدم لمراقبة السفن والطائرات المدنية يدخل حيز الاستهداف إذا استخدم لرصد أي طائره أو سفينة عسكرية مع العلم بأن وظيفة هذا الجهاز هي رصد هذه المركبات بغض النظر عن تصنيفها ما

إذا كان مدنياً أو عسكرياً فبمجرد رصدها لهذه المركبات فإنها تصبح هدفا مشروعاً، وحتى شبكة الاتصالات المدنية في حال استخدامها تصبح هدفاً مشروعاً لكونها مزدوجة الاستخدام.

والمادة (102) من الدليل نصت على أنه"في حالة الشك فيما إذا كانت الأعيان التي تكرس عادة لأغراض مدنية وتستخدم لتقديم مساهمة فعاله في العمل العسكري لا يجوز استهدافها إلا بعد تقييم دقيق لإثبات الاستخدام العسكري، ويجب على المهاجم مراعاة جميع المعلومات المتاحة في هذا الوقت لإتمام التقييم والمعايير المهمة في تأسيس معقولية الاستنتاج ووضوح المعلومات بما في ذلك مصداقية المصدر، أو أجهزة الرصد والاستشعار، وتاريخ المعلومات واحتمالية التعرض للخداع، وإمكانية سوء تفسير البيانات. وأن اليقين المطلق بأن العين المنوي استهدافها تستخدم استخداماً عسكرياً غير ضروري، فمجرد وصول معلومات مؤكدة للقيادة العسكرية بأن العين المحددة تستخدم لغرض عسكري يرى الدليل بأن " أي مهاجم يفكر بشكل منطقي لن يتردد في الاستهداف على الرغم من وجود شك"[88].

كما يرى الدليل بأن على الطرف الذي يقوم بالدفاع، عليه واجب تحديد طبيعة هذه العين فيما إذا كانت تستخدم لغرض طبي أو تعليمي أو غيرهما من الأغراض المدنية[89] .ولكن هل يمكن تحديد طبيعة استخدام كل جهاز حاسوب أو شبكة حاسوبية موجوده في البنية التحتية الإلكترونية للدولة؟، الواقع من غير المتصور تطبيقه في البنية التحتية الإلكترونية، حيث إنّه عالم افتراضي لا تنطبق عليه بعض المعايير المادية للتمييز، كوضع إشارات مميزه على الأعيان الطبية والأثرية كما في العالم المادي[90]، حيث يتم تعريف كل حاسوب بواسطة عنوان (IP) يرمز لكل جهاز حاسوب، وهذا الرقم عبارة عن رقم متغير بشكل دوري[91]، فلن تستطيع أي جهة تحديد هذا الجهاز وطبيعة استخدامه بسبب التغيير الدائم لعنوان الـ(IP) .

في الواقع، تعدّ الهجمات المجهولة واحدة من أكبر مزايا حرب الإنترنت، على الرغم من أن الهجمات قد تنشأ من دولة معينه، لكن هذا لا يعني بالضرورة أن هذه الدولة معنية بالهجوم، أو حتى أصحاب أجهزة الكمبيوتر المعنية، على سبيل المثال الهجوم الإلكتروني الذي حدث عام 2007 على إستونيا، فإن المشكلة الرئيسية تنشأ عندما لا يمكن أن يعزى الهجوم إلى دولة لتحديد المسؤولية الدولية وتطبيق قواعد قانون الحرب، على عكس الحرب التقليدية، والهجمات" السيبرانية "يمكن تنفيذها بسهولة ليس فقط من قبل الدول، ولكن أيضا من قبل الجماعات وحتى الأفراد، كل ما يتطلبه الأمر هو الكمبيوتر والبرامج والاتصال بالإنترنت[92].

ويرى" شميت "أن استخدام العين المدنية لأغراض عسكرية يحولها إلى هدف عسكري وتكون عرضة للهجوم بما في ذلك الهجوم على شبكة الكمبيوتر، وينطبق هذا الوصف حتى لو أن الاستخدام العسكري للشبكة كان ثانوياً مقارنة بالاستخدامات المدنية[93]، وبما أن الإنترنت يستخدم للأغراض المدنية والعسكرية على السواء، ففي أوقات النزاع المسلح قد تكون كل عناصر شبكة الإنترنت هدفًا عسكريًا إذا كان تدميرها يوفر ميزة عسكرية[94]، وكذلك فإن الاستخدام المزدوج للشبكة يجعلها هدفاً عسكرياً حسب تعريف الأعيان المدنية الوارد في البروتوكول الإضافي الأول الذي عرف الأعيان المدنية بشكل سلبي، حيث عرفها بمفهوم المخالفة بأنها الأعيان التي ليست أعياناً عسكرية[95]، فبمجرد أي استخدم عسكري للعين المدنية يفقدها حمايتها الدولية، ولهذا نجد بأن مبدأ التمييز قد تم تقييده إلى درجة عدم الوجود وأن جميع الشبكات أصبحت اهدفا مباحه، لأنه لا يمكن التمييز فيها بين الأهداف العسكرية والمدنية.

وكذلك فإن مبدأ التناسب قد حظر الهجمات على شبكات الكمبيوتر في سياق نزاع مسلح، التي يمكن أن يتوقع منها أن تسبب خسائر عرضية في المدنيين وإلحاق الضرر بالأعيان المدنية بشكل مفرط بالنسبة إلى الميزة العسكرية الملموسة والمباشرة المتوقعة[96]، ويجب على أطراف أي نزاع مسلح تقييم الضرر المتوقع للمدنيين ومدى مخاطر مثل هذه الأضرار الجانبية والميزة العسكرية المتوقعة التي يمكن الحصول عليها[97]، وفي هذا الخصوص يرى" شميث "أن المادة (48) من الملحق الإضافي الأول لاتفاقيات جنيف تحظر عمليات الهجوم على شبكات الحاسوب الموجهة ضد أهداف غير عسكرية، وتؤدي إلى الأذى أو الوفاة أو التلف أو الدمار لكن إذا كانت هذه الهجمات لا تؤدي إلى هذه النتائج فانه مسموح بها ضد الأهداف غير العسكرية، مثل السكان المدنيين، ولذا يلزم إجراء تقييم دقيق للعمليات العسكرية لاعتبارها هجوما أم لا وتقييم هذه العملية يعتمد على نتائجها[98]، وفي حال الرد على الهجمات الإلكترونية، فقد لا تملك الدولة الضحية التكنولوجيا الكافية لإجراء الهجوم الإلكتروني، أو لأن المعتدي ليس لديه شبكة كمبيوتر لمهاجمته من خلالها، ومن المشكوك فيه أيضا ما إذا كانت سلسلة من الهجمات السيبرانية صغيرة النطاق، ولكنها تراكمية ستجعل ردة الفعل وتطبيق مبدأ التناسب محدد وواضح للرد على الهجمة بصورة متزامنة[99].

كما أن تطبيق واحترام مبدأ التناسب يطرح مشكلة في غاية الأهمية، عندما يتم توجيه هجمات" سيبرانية "ضد بنى تحتية مزدوجة الاستخدام مدنية وعسكرية، فلا يبدو أن المنفعة العسكرية ستكون واضحة ما يجعل من تطبيق مبدأ التناسب في أثناء

الهجمات" السيبرانية"أمرا في غاية التعقيد، وكذلك الرد على الهجمات" السيبرانية"[100].

وتحدد اتفاقيتا لاهاي الخامسة والثالثة عشره حقوق وواجبات البلدان المحايدة، فيما يتعلق بالحرب في البر والبحر، لكهنا لا تشير إلى الفضاء الالكتروني، ولا يجوز لبلد ما تحريك أو نقل قواته عبر إقليم دولة محايدة أو ارتكاب أي عمل من الأعمال العدائية في المياه الإقليمية لبلد محايد، ولكن ماذا عن عبور شبكات البلدان المحايدة؟ وهل ينبغي على البلدان أن تطلب الاذن من البلدان المحايدة لشن هجوم سيبراني عبر شبكاتها؟ ومع تبديل الرزم كيف يمكن للبلدان أن تعرف حتى ما هي الشبكات التي تستخدم؟ وهل يمكن لبلد ما استخدام شبكة اختراقية كقوة غير نظامية إذا ما كانت تشتمل على حواسيب في دولة محايده؟

وعن سوء السلوك ومسؤولية الدول على الصعيد الدولي، فان هذا الموضوع يثير مشكلة تحديد المسؤولية الدولية. ففي هذا السياق يمكن تحديد عدة سيناريوهات يمكن إيجازها في الحالات التالية :الأولى حالة المتسللين" بالزي الرسمي "عدة دول أنشأت وحدات إنترنت عسكرية (جنود سبرانيين) مثل الصين، ويمكن كذلك أن يكون المتسللون أعضاء في الوكالات الحكومية أو المؤسسات شبه الحكومية، ووفقا للمادة 4 من مواد لجنة القانون الدولي لعام 2001 المتعلقة بمسؤولية الدولة، فإنه يعدّ تصرف أي جهاز من أجهزة الدولة عملاً من أعمال تلك الدولة[101].

والحالة الثانية، يمكن أن يكون المتسللون أيضًا من أجهزة الدولة مثل :الأفراد أو الشركات التي تستأجرها الدول من أجل إجراء عمليات الكترونية، ومن الأمثلة المعروفة على ذلك شبكة الأعمال الروسية (RBN) وهي شركة جرائم متخصصة في الأعمال الاحتيالية التي يشتبه في قيامها بتنفيذ الهجمات" السيبرانية "ضد جورجيا. وتنص المادة 8 من مواد لجنة القانون الدولي على أن هذه الأفعال، تعدّ عملاً من أعمال الدولة إذا كان الشخص أو مجموعة الأشخاص يتصرفون في الواقع بتعليمات، أو تحت توجيه وسيطرة تلك الدولة)[102]).

والحالة الثالثة وهي عندما لا يكون المتسللون قانونيين ولا بحكم الواقع تابعين لأجهزة الدولة، فلا تكون الدولة هنا مسؤولة إلا بحالة وجود تحريض من قبل الدولة، وهكذا يستتبع التحريض مسؤولية الدولة عن الإجراءات المحرضة فقط بالقدر الذي تتحمله عن التوجيه والتحكم، المادة 11 من مواد لجنة القانون الدولي. ومع ذلك فإن الدولة بموجب المواد السابقة تعدّ مسؤوله في حالة التحريض على ذلك صراحة يمكن أن يكون التحريض عملاً غير قانوني لكل شخص يعترف ويعتمد السلوك المعني على أنه خاص به انظر على سبيل المثال المادة الثالثة من اتفاقية الإبادة الجماعية لعام 1948[103].

ومع ذلك، فإن الاعتراف بالهجمات السيبرانية من قبل عملاء الدولة أمر غير محتمل أن يحدث، فإن التقنيات" السيبرانية "هي الأداة المثالية لعمليات سرية. وأخيراً، يمكن أن تكون الهجمات" السيبرانية "مصدرها أجهزة كمبيوتر تقع في دولة معينة دون أي تدخل للدولة. في هذه الحالة فإن سلوك المتسللين لا يمكن أن ينسب إلى دولة، ومع ذلك، تتحمل الدولة المسؤولية عن عدم اتخاذ تدابير قادرة على منع أو وقف الهجوم.

الخاتمة

يتضح من خلال هذه الدراسة التحليلية لهذا الموضوع الحديث في القانون الدولي العام والقانون الدولي الانساني أن الرؤية ما زالت غير واضحة حول الضوابط القانونية التي تحكم الحرب الالكترونية، وما زالت الأبعاد السياسية تلعب دورا هاما في تعديل أو اضافة قواعد قانونية جديدة تحكم هذا النوع من الحروب الحديثة. ونعرض في هذه الخاتمة أهم النتائج والتوصيات التي توصلنا إليها في هذه الدراسة وهي على النحو التالي:

أولاً: النتائج:

1- أن القانون الدولي الإنساني القائم قد ينطبق على جزء من العمليات الإلكترونية التي تقع في سياق النزاع المسلح ولكن لا ينظم كافة العمليات الإلكترونية لصعوبة تحديد هوية الفاعل أو المكان التي تنطلق منه الهجمات الإلكترونية وصعوبة التمييز بين المدنيين والعسكريين بسبب الاستخدام المزدوج لشبكة الإنترنت وان التوسع في تفسير النصوص القانونية القائمة سيؤدي إلى خروجها من مضمونها ومحتواها.

2- ظهور مستجدات في أساليب ووسائل الحرب لم تكن معروفة في الماضي لكن يجب أن لا تعد عقبة أو عثرة أمام القانون، ومن ثم فإن احدى القضايا الرئيسية هي تحديد الظروف التي يمكن في إطارها اعتبار العمليات الإلكترونية تحدث في سياق نزاع مسلح أو تؤدي في حد ذاتها إلى نشوب نزاع مسلح بحيث ينطبق عليها القانون الدولي الإنساني.

3- ومع كل ما تقدم تبقى الحاجة ماسة لتطوير قواعد القانون الدولي الإنساني، لكن كيف يمكن إيجاد توافق في الآراء بين

أكثر 198 دولة من الدول بشأن تعريف مفهوم الهجمات" السيبرانية "ووضع قانون شامل أو إبرام معاهدة بشأن الفضاء" السيبراني " والذي يمثل ضرب من ضروب الخيال وذلك بسبب تباين الآراء بين الدول وعزوف الدول من الانضمام إلى المعاهدات الدولية الملزمة.

ثانياً: التوصيات:

على مر السنين تمكنت القوانين الدولية للنزاع المسلح من أن تتكيف مع هذه التطورات وظلت تشكل مجموعة متسقه تنسجم مع هذه التطورات. أن معظم الاتفاقيات الدولية مثل ميثاق الأمم المتحدة، ومعاهدة حلف شمال الأطلسي، واتفاقية جنيف، واتفاقية لاهاي تتمتع جميعاً بقابلية التعديل ولهذا يجب إدخال بعض التعديلات على الاتفاقيات القائمة ومنها:

1. تعديل اتفاقيات جنيف لعام 1949 والبرتوكولين المضافين اليها في عام 1977بغرض تحريم الهجمات على البنية التحتية الحيوية التي يمكن أن تعطل الاتصالات الأساسية الدنيا وتعرض السكان المدنيين للخطر.
2. تعديل ميثاق الأمم المتحدة لاستيعاب النزاع الإلكتروني وتحديد مفهوم النزاع المسلح وحالات الدفاع عن النفس ضد الهجمات الإلكترونية. وعلى وجه الخصوص تعديل المادة 42 من ميثاق الأمم المتحدة بما يسمح لمجلس الأمن باتخاذ التدابير اللازمة من خلال الوسائل الإلكترونية.
3. تعديل اتفاقيات لاهاي لعام 1907بغرض تحريم استخدام القوات غير النظامية في القتال" السيبراني "وحظر نقل الهجمات "السيبرانية "عبر شبكات البلدان المحايدة، وتقديم المساعدة في التحقيقات المتعلقة بالأنشطة" السيبرانية "التي يعتقد أنها مرت عبر شبكاتها.

الهوامش

(1) Kittichaisaree, K., (2017), Public International Law of Cyberspace, Law, Governanceand Technology, Series 32, P.154.

(2) ما هي القيود التي يفرضها قانون الحرب على الهجمات السيبرانية؟ اللجنة الدولية للصليب الأحمر، 28-6-2013 https://www.icrc.org/ara/resources/documents/faq/130628-cyber-warfare-q-and-a-eng.htm

(3) Schmitt, M., (2013), Tallinn Manual on the International Law Applicable to Cyber Warfare, (1st Edition) Cambridge University press, first publishes, p.92.

(4) عبد الصادق، عادل، (2009)، الإرهاب الإلكترونيالقوة في العلاقات الدولية:نمط جديد وتحديات مختلفة، مركز الدراسات السياسية والاستراتيجية بالأهرام، القاهرة، ص130-140.

(5) عبد الصادق، عادل، مؤتمر حروب الفضاء السيبراني، الفضاء الإلكتروني وأسلحة الانتشار الشامل بين الردع وسباق التسلح، 2015/05/15، متاح على الرابط التالي/https://seconf.wordpress.com/2015/05/15:

(6) إن تحديد وتعريف الأسلحة المعلوماتية تعدّ نقطة خلاف من حيث تحديد السمات المميزة للأسلحة المعلوماتية كما انه ليس من السهل عزل الأسلحة المعلوماتية عن الطائفة الكاملة للأسلحة :جانكارلو أ. بارليتا أ. ووليام. ا وفيتالي تسجيشكو، (2011)النزاع السيبراني والاستقرار الجيوسيبراني، البحث عن الامن السيبراني، الناشر الاتحاد الدولي للاتصالات والاتحاد العالمي للعلماء.

(7) Collier, J., (2017), Strategies of Cyber Crisis Management: Lessons from the Approaches of Estonia and the United Kingdom. In: Mariarosaria, Taddeo and Glorioso, Ludovica (Volume 134), Ethics and Policies for Cyber Operations. (pp.186-212), Switzerland, A NATO Cooperative Cyber Defence Centre of Excellence Initiative, P 191.

(8) Baylon, C.,(2015), Russia's Information Warfare Capabilities. In: Lemieux, Frederic, Current and Emerging Trends in Cyber Operations: Policy, Strategy, and Practice. (pp.65-83), U.K, PALGRAVE MACMILLAN.

(9) Applegate, S.(2015), Cyber Conflict: Disruption and Exploitation in the Digital Age. In: Lemieux, Frederic, Current, and Emerging Trends in Cyber Operations: Policy, Strategy, and Practice (pp.19-36), Switzerland, A NATO Cooperative Cyber Defence Centre of Excellence Initiative, P 27.

(10) Baylon, C.,(2017), Lessons from Stuxnet and the Realm of Cyberand Nuclear Security: Implications for Ethicsin Cyber Warfare. In: Mariarosaria, Taddeo and Glorioso, Ludovica (Volume 134), Ethics and Policies for Cyber Operations. (pp.213-230), Switzerland, A NATO Cooperative Cyber Defence Centre of Excellence Initiative.

الفتلاوي، احمد عبيس نعمة،)2018(، الهجمات السيبرانية، منشورات زين الحقوقية، بيروت، ط.1، ص35-36. يعد فيروس Stuxnet ستوكسن جزء من برنامج ذاتي الاستنساخ ينتشر من كمبيوتر إلى أخر واستخدم في ضرب منشأت نووية في إيران، وهو الذي دفع روسيا

للتحذير من خطر وقوع كارثة نووية في منطقة الخليج العربي مشابهة لكارثة محطة تشرنوبيل عام 1980.

(11) يقصد بالفضاء الإلكتروني" البيئة أو الفضاء المصنوع من قبل الإنسان حيث يشكل المكان الذي تحدث فيه الاتصالات الإلكترونية عبر الشبكات المترابطة للبنية التحتية للمعلومات والاتصالات، بما في ذلك الإنترنت وشبكات الاتصالات وأنظمة الكمبيوتر:"

Kittichaisaree (2017), Public International Law of Cyberspace, Law, Governanceand Technology, Op. Cit. P.2.

(12) Barrett, E. (2017), On the Relationship between the Ethics and the Law of War: Cyber Operations and Sublethal Harm, Ethics & International Affairs, 31(4), Pp. 467-477.

دليل تالين تمت كتابته من قبل مجموعة من الخبراء برئاسة مايكل سميث بتكليف من منظمة حلف شمال الأطلسي، والذي يقترح تطبيق القانون الدولي على النزاعات الإلكترونية. ظهر هذا المشروع في عام 2013، وتم تعديل الدليل ونشره في فبراير 2017 تحت اسم Tallinn 2.0، وتتناول الدراسة الجديدة الخيارات التي يقدمها القانون الدولي للدول ضحايا الهجمات الإلكترونية. ويعد هذا الدليل وثيقة غير ملزمه أعدتها مجموعة من الخبراء الدوليين، كما أن هذه الوثيقة لا تعكس الموقف الرسمي لحلف شمال الأطلسيأو موقف كل دولة من الدول الأعضاء في الحلف. ولكن من الممكن أن تكون لهذه الوثيقة تأثير في المفاوضات المستقبلية بين الدول، وتجدر الإشارةإلىأن هذه الوثيقة تعكس رؤية أمريكية بحته كانت محل انتقاد من قبل الدول الأوروبية.

(13) Libicki, M., (2007), "Conquest in Cyberspace: National Security and Information Warfare", Cambridge University Press, New York, P. 13-323.

(14) وستبي، جودي ر.، 2011، دعوة إلىالاستقرار الجيوسيبراني، البحث عن السلام السيبراني، الناشر الاتحاد الدولي للاتصالات والاتحاد العالمي للعلماء، ص68.

(15) موسى، طالب حسن، أعمر، عمر محمود، (2016)، الإنترنت قانونا، مجلة الشريعة والقانون، جامعة الإمارات العربية المتحدة، العدد السابع والستين، ص.339.

(16) نفس المرجع، ص. 340.

(17) Lavenue,J., (1996), Cyberspace ET Droit International: pour UN nouveau Jus Communications:Revue de la Recherche Juridique–droit prospectif, p. 830-832.

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

(19) وستبي، جودي ر.،)2011(، دعوة إلىالاستقرار الجيوسيبراني، مرجع سابق. ص.64.

(20) أن الهجوم الإلكتروني الذي تعرضت له البنية التحتية في إستونيا العضو في حلف شمال الأطلسي والذي شمل تعطيل المواقع الحكومية واستهدف الخدمات المصرفية المالية للقطاع الخاص تجاوز السلوك الإجرامي المجرد، وقد أثار هذا الموضوع نقاشا في مدى اعتباره هجوما مسلحا يهدد دول الحلف وذلك بالاستناد إلىالمادة 5 من اتفاقية حلف شمال الأطلسى لعام 1949، التى تنص على أن" يتفق الأطراف، على أن أى هجوم، أو عدوان مسلح، ضد طرف منهم، أو عدة أطرافففى أوروبا أو أمريكا الشمالية يعد عدوانا عليهم جميعا، وبناء عليه فانهم متفقون على انه فى حالة وقوع مثل هذا العدوان المسلح، فان على كل طرف منهم، تنفيذا لما جاء فى المادة 51 من ميثاق الأمم المتحدة عن حق الدفاع الذاتى عن انفسهم بشكل فردي أو جماعى، تقديم المساندة والعون للطرف أوالأطراف التي تتعرض للهجوم، ..: جانكارلو أ. بارليتا أ. ووليام. ا وفيتالي تسجيشكو، (2011)النزاع السيبراني والاستقرار الجيوسيبراني، عن الاتحاد الدولي للاتصالات وبرنامج الأمن السيبرانى العالمى، الناشر الاتحاد الدولي للاتصالات والاتحاد العالمي للعلماء ص51−52.

(21) توريه، حمدون إ.،)2011(، الاستجابة الدولية للحرب السيبرانية، البحث عن الامن السيبراني، الناشر الاتحاد الدولي للاتصالات والاتحاد العالمي للعلماء، ص.89.

Declaration on Principles of International Law Concerning Friendly Relations and Co-operation among States in Accordance with the Charter of the United Nations, UN Doc. A/8028, General Assembly Resolution 2625, UN GAROS 25 TH Session Supplement 28, 121 (1970).

(22) هناك من يدعي أن نص المادة 2 فقره 4 من ميثاق الأمم المتحدة ينطبق فقط على التهديد أو الاستخدام الفعلي للقوة المسلحة:

Stahn, C., (2007),"Jus ad bellum', jus in Bello" jus post bellum"? – Rrthing the Conception of the Law of Armed Force", The European Journal of International of International Law, 17(5) , p. 923,footnot,8.

(23) لمزيد من العلومات انظر عبد الصادق،)2009(، الإرهاب الإلكترونيالقوة في العلاقات الدولية:نمط جديد وتحديات مختلفة، مرجع سابق، ص. 155−229.

(24) Glenny, M., (2011), The cyber arms race is on, as nations large and small mobilize to protect themselves and their enemies if provoked, post-gazette.com, October 23, 2011: http://www.post-gazette.com/pg/11296/1183849-109-0stm#ixzz10MYTghXE

(25) توريه، حمدون، الفضاء السيبراني وتهديد الحرب السيبرانية، البحث عن السلام السيبراني، المرجع السابق. ص، 11.

(26) نفس المرجع، ص11.

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

(28) la licéitéde la menace ou de l'emploi d'armes nucleaires, Rec. 1996, 241-242.

(29) Koh, H., (2012), International Law in Cyberspace, Harvard International Law Journal, Online, volume 54, p.3.

حمودي، ناصر، (2012)، العقد الدولي الإلكتروني المبرم عبر الإنترنت، بدون دار نشر، ص. 54.

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

خلقت الثورة الرقمية شكلا جديدا من أشكال التهديدات مما دفع مركز الدفاع في حلف شمال الأطلسي مناقشة مسألة انطباق القانون الدولي ما في ذلك قانون النزاعات المسلحة والقانون الدولي الإنساني) على الهجمات الإلكترونية وتم التأكيد على عدم وجود فراغ قانوني. والواقع أن بعض المنظمات الدولية مثل اللجنة الدولية للصليب الأحمر وبعض الدول مثل الولايات المتحدة الأمريكية وأستراليا تعدّ أن القانون الدولي القائم كافي لتنظيم الهجمات الإلكترونية.

(31) الفتلاوي، احمد عبيس نعمة، الهجمات السيبرانية، المرجع السابق. ص.49

(32) علوان، عبد الكريم،)2006(، الوسيط في القانون الدولي العام، دار الثقافة، عمان، ص34.

(33) See, e.g., Schmitt,M., (1999), Computer Network Attack, and the Use of Force in International Law: Thoughts on a Normative Framework, 37 COLUM. J. TRANSNAT'L L. 885, 913

(34) وضع مايكل سميث عدة معايير لاعتبار العمليات الإلكترونية بمثابة استخدام للقوة ومنها شدة الإصابة والفورية وتقييم الأثار وتورط الدولة والقرينة القانونية:

Schmitt,M., (2012), Classification of Cyber Conflict. Journal of Conflict & Security Law, 17(2), P. 245–260

وكذلك:

Shi Beomchul, The Cyber and The Right of Self – Defense: Legal Perspectives and the Case of the United States, IFANS, Vol, 19. 1, June 2011,p.111:اعتبر أن الهجمات السيبرانية الناتج عنها أثار مادية ملموسة في الأعيان المدنية أو العسكرية هي استخدام للقوة وفقا للمادة 4/2 من ميثاق الأمم المتحدة، وفي نفس الاتجاه:

Roscini, M., (2010), World Wide Warfare –Jus ad bellum and Use of Cyber Force, Max Planck Yearbook of United Nations Law, Volume 14, 2010, p. 130.

(35) في حال وقوع هجمات الكترونية من دولة فان الدولة المعتدى عليها الحق في الدفاع عن نفسها استناداً لنص المادة 51 من ميثاق الأمم المتحدة سواء كان ذلك ناتج عن عدوان مسلح في العالم الحقيقي أو في الفضاء الإلكتروني وهنا يكون الرد فرادي أو جماعي ويكون من حق الدولة الضحية اتخاذ تدابير للدفاع عن النفس في الفضاء الإلكترونيأو في العالم الحقيقي ولكنها يجب أن تكون ضرورية ومتناسبة لمواجهة الهجوم المفاجئ:

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

شميت، مايكل ن.، (2002) الحرب بواسطة شبكات الاتصال :الهجوم عى شبكات الكمبيوتر (الحاسوب) والقانون في الحرب، المجلة الدولية للصليب الأحمر، ص87.

(36) ICJ Reports 1986, see note 64, 94 para. 176

(37) Roscini, M., World Wide Warfare –Jus ad bellum and Use of Cyber Force, p. Cit. p. *115*

(38) Idem.

(39) Idem.

(40). الفصل 14 من دليل تالين.

(41) . المادة 69 من دليل تالين.

(42) . المادة 80 من دليل تالين.

(43. المادة 92من دليل تالين

(44) Decision on the Defence motion for interlocutory appeal, paras. 120, 124.

(45) حتى تصدر مدونة بقوانين الحرب أكثر اكتمالا ترى الأطراف السامية المتعاقدة من أن تعلن انه في الحالة التي تشملها اللائحة التي اعتمدتها يظل السكان والمقاتلون تحت حماية قاعدة مبادئ قانون الأمم الناتج عن العادات الراسخة بين الشعوب المتحضرة وعن قواعد

الإنسانية وعما يمليه الضمير العام.

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

(47) International Court of Justice. Reports, 1996. Legality of the threat or use of nuclear weapons p. 226 at para. 39.

انظر كذلك: سميث، مايكل، (2002)، الحرب بواسطة شبكات الاتصال: الهجوم على شبكات الكمبيوتر (الحاسوب والقانون الدولي)، مرجع سابق ص. 93.

(48) لقد ورد في التعليق الرسمي للجنة الدولية للصليب الأحمر وفي الشرح لاتفاقيات جنيف لعام 1949، والبروتوكولين الإضافيين لعام 1977، تعريف النزاع المسلح الذي يتسم بطابع دولي، بأنه هو" أي خلاف ينشأ بين دولتين ويؤدي إلى تدخل القوات المسلحة حتى اذا انكر احد الأطراف وجود حالة الحرب ولا يختلف الأمر لطول فترة النزاع أو عدد المذابح التي وقعت:"

Pictet, Jean S. (1952), the Geneva Conventions of 12 August 1949. Commentary Volume I: For the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, International Committee Of The Red Cross, P. 27-37.

(49) للمزيد من المعلومات انظر. العنبكي، نزار، تصنيف النزاعات المسلحة، ورقة عمل قدمت لمؤتمر التطبيق الأمين للقانون الدولي الإنساني وذلك بتاريخ 6–7 نيسان 2016 في جامعة العلوم التطبيقية الخاصة / قصر المؤتمرات.

ان البروتوكول الإضافيالأول لعام 1977، المتعلق بالنزاعات المسلحة الدولية اخذ بمعيار النزاع المسلح واستخدم هذا المصطلح أيضا فى النزاعات الداخلية، انظر المادتينالأولى والثانية من البروتوكول الإضافي الثاني لعام 1977 المتعلق بحماية ضحايا المنازعات المسلحة غير الدولية والملحق باتفاقيات جنيف المؤرخة في 12 آب 1949

(50) Kittichaisaree, Op. Cit. P.208.

(51) International Criminal Tribunal for the former Yugoslavia (ICTY), Prosecutor v. Tadic, Case No. IT-94- 1-A, Judgment (Appeals Chamber), 15 July 1999, para 84

(52) Schindler, D. (1982). International Humanitarian Law and Internationalized Internal Armed Conflicts, International Review of the Red Cross, 22(230), P. 255-264.

(53) Green, J., (2015), Cyber warfare: a multidisciplinary analysis, (1st Edition), Routledge Studies in Conflict, Security and Technology, P. 126.

(54) Messmer, E.,(2010), "Cyberattack Seen as Top Threat to Zap U.S. Power Grid," NetworkWorld, 2 June 2010, www.networkworld.com/news/2010/060210-nerc-cyberattack-power-grid.html

(55) قرار الجمعية العامة 3314 مع تعريف العدوان المرفق به، في 14 كانون الأول /ديسمبر 1974

(56) هينين ويجنر، مفهوم بشأن السلام السيبراني، البحث عن السلام السيبراني، البحث عن السلام السيبراني، الناشر الاتحاد الدولي للاتصالات والاتحاد العالمي للعلماء، ص.76.

(57) Koh, H., (2012), International Law in Cyberspace, Harvard International Law Journal, Online, volume54.

هارولد هونغجو كوه محامي أمريكي وعمل مستشارا قانونيا لوزارة الخارجيةفي الولايات المتحدة الامريكية تم ترشيحه لهذا المنصب من قبل الرئيس باراك أوباما في 23 مارس 2009، وعاد إلى جامعة ييل كأستاذ قانون،

(58) سميث، مايكل، (2002) الحرب بواسطة شبكات الاتصال: الهجوم على شبكات الكنبيوتر (الحاسوب والقانون الدولي)، مرجع سابق. ص. 94.

(59) انظر المواد 70 و73 من دليل تالين

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

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

(62) Hoisington, M., (2009), Cyberwarfare and the Use of Force Giving Rise to the Right of Self-Defense, 32(2), Boston College International and Comparative Law Review, P. 439-454.

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

(64) لقد تم الإشارة لمبدأ الضرورة العسكرية في المواد 2/54 و1/62 و3/71 و4/67 فيالبروتوكول الإضافي الاول الملحقباتفاقيات جنيف المؤرخة في 12 أغسطس/ آب 1949 والمتعلق بحماية ضحايا النزاعات المسلّحة الدولية.

(65) وتعرف المادة 52 من البروتوكول الإضافي الاول الملحقباتفاقيات جنيف المؤرخة في 12 أغسطس/ آب 1949 والمتعلق بحماية ضحايا النزاعات المسلّحة الدولية الأهداف العسكرية بأنها الأهداف" التي تسهم مساهمة فعالة في العمل العسكري، سواء كان ذلك بطبيعتها أو بموقعها أو بغايتها أو باستخدامها، التي يحقق تدميرها التام أو الجزئي أو الاستيلاء عليها أو تعطيلها في الظروف السائدة حينذاك ميزة عسكرية مؤكدة.

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

(67) البروتوكول الإضافي الأول، المادة 2/54

(68) البروتوكول الإضافي الأول، المادة 1/62 والمادة 3/71

(69) البروتوكول الإضافي الأول: المادة 4/67

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

(71) Koh, H., International Law in Cyberspace, Harvard International Law Journal, Online Volume54, December 2012, p 4; See also Rules 93–94, in Tallinn Manual, pp 420, 422; Schmitt, M., (2002), wired warfare: Computer network attack and jus in Bello, OP. Cit. p.387.

(72) احمد عبيس نعمة الفتلاوي، الهجمات السيبرانية، منشورات زين الحقوقية، بيروت 2018، ص 56

(73) Koh, H.,International Law in Cyberspace,Op.Cit, p 5.

(74) Roscini, M.,World Wide Warfare –Jus ad bellum and Use of Cyber Force, Op.Cit, p. 119

(75) دليل تالين :المادة 80

(76) The Insider Threat to U.S. Government Information Systems, National Security Telecommunications and Information Systems Security Committee, NSTISSAM INFOSEC/1-99,www.cnss.gov/Assets/pdf/nstissam/infosec 1-99.pdf.

(77) المادة 101 من دليل تالين

(78) إعلان سان بطرسبورغ بغية حظر استعمال قذائف معينة في زمن الحرب، 1868.

(79) International Court of Justice. Reports, 1996. Legality of the threat or use of nuclear weapons para. 78.

(80) McDonald,J., (2017), Blind Justice? The Role of Distinction in Electronic Attacks (Volume 134), Ethics and Policies for Cyber Operations. (pp.17-32), Switzerland, A NATO Cooperative Cyber Defence Centre of Excellence Initiative, P 20.

(81) المادة 48 من البروتوكول الإضافي الأول لعام 1977 تنص بأن" تعمل أطراف النزاع على التمييز بين السكان المدنيين والمقاتلين وبين الأعيان المدنية والأهداف العسكرية، ومن ثم توجه عملياتها ضد الأهداف العسكرية دون غيرها، وذلك من أجل تأمين احترام وحماية السكان المدنيين والأعيان المدنية."

والفقرة 4 من المادة 51 من ذات البرتوكول نصت على حظر الهجمات العشوائية وتعدّ هجمات عشوائية:

أ. تلك التي لا توجه إلى هدف عسكري محدد.

ب. أو تلك التي تستخدم طريقة أو وسيله للقتال لا يمكن أن توجه إلى هدف عسكري محدد

ج. أو تلك التي تستخدم طريقة أو وسيلة للقتال لا يمكن حصر أثارها على النحو الذي يتطلبه هذا الملحق" البروتوكول "ومن ثم فان من شأنها أن تصيب في كل حالة كهذه لأهداف العسكرية والأشخاص المدنيين أو الأعيان المدنية دون تمييز.

والفقرة الفرعية (أ) تشير إلى الاستخدام غير التمييزي بينما تصف الفقرتان (ب) و(ج) الأسلحة أو التكتيكات غير التمييزية ويشمل جانب الاستخدام غير التمييزي ثلاثة عناصر مرتبطة هي: التمييز، والتناسب، وتقليل الدمار الملازم والأذى العرضي.

(82) Green, J., (2015), Cyber warfare: a multidisciplinary analysis, (1st Edition), Routledge Studies in Conflict, Security and Technology, P. 127.

(83)Clarke, R. and Knake, R., (2010) Cyberwarfare: The Next Threat to National Security and What to Do about It, p.9–10.

(84) هناك من يعدّ اشتراك المدنيون في هجوم على شبكات الحاسوب يعتمد على نتائجه، فاذا كانت نتائج الهجوم أو النتائج المتوقعة حدوثها تؤدي إلى الوفاة أو الأذى أو الدمار يكون المقترفون مقاتلين غير قانونيين لأنهم قاموا بدور مباشر في أعمال عدائية دون استيفاء معايير التصنيف كمقاتلين؛

Boothby, M., (2014),Conflict Law: The Influence of New Weapons Technology, Human Rights and Emerging Actors, T.M.C. Asser Press,Pp. 257 - 259.

(85) Marco Roscini,World Wide Warfare –Jus ad bellum and Use of Cyber Force, Op.Cit. p. 88

(86) Jensen,E., (2010), Cyber Warfare and Precautions against the Effects of Attacks, Texas LawReview, Volume 88, P 1533- 1569, P. 1542.

(87) Arnove, A., (2003), Iraq under Siege: The Deadly Impact of Sanctions and War, P. 24-25.

(88) دليل تالين المادة 102، A Reasonable Attacker Would Not Hesitate Before Conducting The Strike Despite The" Doubt "

أيضاً وكذلك ؛1907 ، من الاتفاقية الخاصة باحترام قوانين وأعراف الحرب البرية لعام(27) المادة (89)

Kolb, R., (2015), Military Objectives in InternationalHumanitarian Law, Leiden Journal of International Law, 28, P. 691-700, P. 699.

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

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

(92) Marco Roscini, World Wide Warfare –Jus ad bellum and Use of Cyber Force, Op.Cit., p. 96.

(93) Schmitt, M., (2002), wired warfare: Computer network attack and jus in Bello, OP. Cit. p.390.

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

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

(96) لقد تمت الإشارة إلى مبدأ التناسب في البروتوكول الإضافيالأوللاتفاقيات جنيف لعام 1949في المادتين 15/5 ب و57/5/2 أوب، كما ذكر هذا المبدأ في القانون الدولي الإنساني العرفي: ماري–هنكرتس–جون ولويز دوزوالد–بك، القانون الدولي الإنساني العرفي، المجلد الأول، القواعد، 2007، ص. 41. وعلى الرغم من عدم وجود نص صريح يعرف مبدأ التناسب إلا انه يعدّ من اهم المبادئ في النزاعات المسلحة، ويهدف مبدأ التناسب إلى الحد أو التقليل من الخسائر وأوجه المعاناة المترتبة على العمليات العسكرية سواء بالنسبة للأشخاص أو الأشياء. ويقصد بالهجوم غير المتناسب، بأنه الهجوم الذي يتوقع منه أن يسبب خسائر في أرواح المدنيين أو أصابتهم، أو يلحق أضرارا بالأعيان المدنية، أو أن يجمع بين هذه الخسائر والأضرار بشكل يفرط في تجاوز ما ينتظر أن يسفر عنه ذلك الهجوم من ميزة عسكرية ملموسة ومباشرة.

(97) المادة 5 /ب من المادة 51 من البروتوكول الإضافي لعام 1997 وكذلك الفقرة ب/2 من المادة 57 من البروتوكول الإضافي لعام 1997.

(98) مايكل ن شميت، الحرب بواسطة شبكات الاتصال: الهجوم عى شبكات الكمبيوتر (الحاسوب) والقانون في الحرب، المجلة الدولية للصليب الأحمر، 2002، ص97.

(99) Marco Roscini, World Wide Warfare –Jus ad bellum and Use of Cyber Force, Op.Cit., p. 120.

(100) Shine, Beomchul, p. 118

(101) Cheng, D., (2017), Cyber Dragon: Inside China's Information Warfare and Cyber Operations, California: Praeger, P. 27.

(102) Roscini, M., (2014), Cyber Operations and the Use of Force in International Law, Oxford:Oxford University Press, P. 36.

(103) عرفت المادة 3 من اتفاقية منع ومعاقبة جريمة الإبادة الجماعية.الجرائم التى يمكن أن يعاقب عليها:

1. الإبادة الجماعية.
2. التآمر على ارتكاب الإبادة الجماعية.
3. التحريض المباشر والعلنى على ارتكاب الإبادة الجماعية.
4. محاولة ارتكاب الإبادة الجماعية.
5. الاشتراك فى الإبادة الجماعية.

المصادر والمراجع

اولا. المراجع باللغة العربية

توريه، حمدون إ.، (2011)، الاستجابة الدولية للحرب السيبرانية، البحث عن الامن السيبراني، الناشر الاتحاد الدولي للاتصالات والاتحاد العالمي للعلماء.

جانكارلو أ. باريتا أ. ووليام. ا وفيتالي تسجيشكو، (2011)النزاع السيبراني والاستقرار الجيوسيبراني، البحث عن الأمن السيبراني، الناشر الاتحاد الدولي للاتصالات والاتحاد العالمي للعلماء.

حمودي، ناصر، (2012)، العقد الدولي الإلكتروني المبرم عبر الإنترنت، بدون دار نشر.

شميت، مايكل ن.، (2002) الحرب بواسطة شبكات الاتصال: الهجوم عى شبكات الكمبيوتر (الحاسوب) والقانون في الحرب، المجلة الدولية للصليب الأحمر.

عبد الصادق، عادل، (2009)، الإرهاب الإلكتروني، مركز الدراسات السياسية والاستراتيجية بالأهرام، القاهرة، 2009.

عبد الصادق، عادل، مؤتمر حروب الفضاء السيبراني، الفضاء الإلكتروني وأسلحة الانتشار الشامل بين الردع وسباق التسلح، 2015/05/15، متاح على الرابط التالي :https://seconf.wordpress.com/2015/05/15/

علوان، عبد الكريم،)2006(، الوسيط في القانون الدولي العام، دار الثقافة، عمان.

العنبكي، نزار، تصنيف النزاعات المسلحة، ورقة عمل قدمت لمؤتمر التطبيق الأمين للقانون الدولي الإنساني وذلك بتاريخ 6-7 نيسان 2016 في جامعة العلوم التطبيقية الخاصة / قصر المؤتمرات.

الفتلاوي، أحمد عبيس نعمة، (2018)، الهجمات السيبرانية، منشورات زين الحقوقية، بيروت، ط.1.

قرار الجمعية العامة 3314 مع تعريف العدوان المرفق به، في 14 كانون الأول /ديسمبر 1974

ما هي القيود التي يفرضها قانون الحرب على الهجمات السيبرانية؟ اللجنة الدولية للصليب الأحمر، 28-6-2013 : https://www.icrc.org/ara/resources/documents/faq/130628-cyber-warfare-q-and-a-eng.htm

موسى، طالب حسن، أعمر، عمر محمود، (2016)، الإنترنت قانونا، مجلة الشريعة والقانون، جامعة الإمارات العربية المتحدة، العدد السابع والستين.

هينين ويجنر، (2011)، مفهوم بشأن السلام السيبراني، البحث عن السلام السيبراني، الناشر الاتحاد الدولي للاتصالات والاتحاد العالمي للعلماء.

وستبي، جودي ر. (2011)، دعوة إلى الاستقرار الجيوسيبراني، عن الاتحاد الدولي للاتصالات وبرنامج الأمن السيبراني العالمي، الناشر الاتحاد الدولي للاتصالات والاتحاد العالمي للعلماء.

ثانيا. المراجع باللغة الإنجليزية والفرنسية:

Applegate, S.(2015), Cyber Conflict: Disruption and Exploitation in the Digital Age. In: Lemieux, Frederic, *Current, and Emerging Trends in Cyber Operations: Policy, Strategy, and Practice* (pp.186-212), Switzerland, A NATO Cooperative Cyber Defence Centre of Excellence Initiative.

Arnove, A., (2003), *Iraq under Siege: The Deadly Impact of Sanctions and War.*

Barrett, E. (2017), On the Relationship between the Ethics and the Law of War: Cyber Operations and Sublethal Harm, *Ethics & International Affairs*, 31(4).

Baylon, C.,(2015), Russia's Information Warfare Capabilities. In: Lemieux, Frederic, *Current and Emerging Trends in Cyber Operations: Policy, Strategy, and Practice*. (pp.65-83), U.K, PALGRAVE MACMILLAN.

Baylon, C., (2017), Lessons from Stuxnet and the Realm of Cyberand Nuclear Security: Implications for Ethicsin Cyber Warfare. In: Mariarosaria, Taddeo and Glorioso, Ludovica (Volume 134), *Ethics and Policies for Cyber Operations*. (pp.213-230), Switzerland, A NATO Cooperative Cyber Defence Centre of Excellence Initiative.

Boothby, M., (2014), *Conflict Law: The Influence of New Weapons Technology, Human Rights, and Emerging Actors*, T.M.C. Asser Press.

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

Cheng, D., (2017), *Cyber Dragon: Inside China's Information Warfare and Cyber Operations*, California: Praeger.

Clarke, R. and Knake, R., (2010) Cyberwarfare: The Next Threat to National Security and What to Do about It.

Collier, Jamie(2017), Strategies of Cyber Crisis Management: Lessons from the Approaches of Estonia and the United Kingdom. In: Mariarosaria, Taddeo and Glorioso, Ludovica (Volume 134), Ethics and Policies for Cyber Operations. (pp.186-212), Switzerland, A NATO Cooperative Cyber Defence Centre of Excellence Initiative.

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

Declaration on Principles of International Law Concerning Friendly Relations and Co-operation among States in Accordance with the Charter of the United Nations, UN Doc. A/8028, General Assembly Resolution 2625, UN GAROS 25 TH Session Supplement 28, 121 (1970).

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

Glenny, M., (2011), The cyber arms race is on, as nations large and small mobilize to protect themselves and their enemies if provoked, post-gazette.com,:http://www.post-gazette.com/pg/11296/1183849-1090stm#ixzz10MYTghXE

Green, J., (2015), Cyber warfare: a multidisciplinary analysis, (1st Edition), Routledge Studies in Conflict, Security and Technology.

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

ICJ Reports 1986, see note 64, 94 para. 176

International Court of Justice. Reports, 1996. Legality of the threat or use of nuclear weapons.

International Criminal Tribunal for the former Yugoslavia (ICTY), Prosecutor v. Tadic, Case No. IT-94- 1-A, Judgment (Appeals Chamber), 15 July 1999, para 84

Jensen,E., (2010), Cyber Warfare and Precautions against the Effects of Attacks, Texas LawReview, Volume 88.

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

Kittichaisaree, K., (2017), Public International Law of Cyberspace, Law, Governanceand Technology, Series 32.

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

Kolb, R., (2015), Military Objectives in InternationalHumanitarian Law, Leiden Journal of International Law, 28.

la licéitéde la menace ou de l'emploi d'armes nucleaires, Rec. 1996, 241-242.

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

Libicki, M., (2007), "Conquest in Cyberspace: National Security and Information Warfare", Cambridge University Press, New York.

LIEBER, Francis, Instructions for the Government of Armies of the United States in the Field, 1898, Article14, 15, 16.

Lovan, M., Vittor, F., (2003) intervention military en Iraq et le droit international, La doctrine europeenne, Annuaire Français de droit international, Volume 49.

McDonald,J., (2017), Blind Justice? The Role of Distinction in Electronic Attacks (Volume 134), Ethics and Policies for Cyber Operations, Switzerland, A NATO Cooperative Cyber Defence Centre of Excellence Initiative.

Messmer, E.,(2010), "Cyberattack Seen as Top Threat to Zap U.S. Power Grid," Network World, 2 June 2010, www.networkworld.com/news/2010/060210-nerc-cyberattack-power-grid.html

Pictet, Jean S. (1952), the Geneva Conventions of 12 August 1949. Commentary Volume I: For the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, International Committee Of The Red Cross.

Roscini, M., (2010) World Wide Warfare –Jus ad bellum and Use of Cyber Force, Max Planck Yearbook of United Nations Law, Volume 14.

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

Schindler, D. (1982). International Humanitarian Law and Internationalized Internal Armed Conflicts, International Review of the Red Cross, 22(230).

Schmitt, M., (1999), Computer Network Attack, and the Use of Force in International Law: Thoughts on a Normative Framework, 37 COLUM. J. TRANSNAT'L L.

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

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

Schmitt, M., (2012), Classification of Cyber Conflict. Journal of Conflict & Security Law, 17(2).

Schmitt, M., (2013), Tallinn Manual on the International Law Applicable to Cyber Warfare, (1st Edition) Cambridge

University press, first publishes.

Shi, B., (2011), the Cyber and the Right of Self – Defense: Legal Perspectives and the Case of the United States, IFANS, 19(1).

Stahn, C., (2007),"Jus ad bellum', jus in Bello" jus post bellum"? – Rrthing the Conception of the Law of Armed Force", the European Journal of International of International Law, 17(5).

The Insider Threat to U.S. Government Information Systems, National Security Telecommunications and Information Systems Security Committee, NSTISSAM INFOSEC/1-99,www.cnss.gov/Assets/pdf/nstissam/infosec 1-99.pdf.

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

ثالثا. الاتفاقيات الدولية:

اتفاقيات جنيف المؤرخة في 12 أغسطس/ آب 1949 المتعلقة بحماية ضحايا النزاعات المسلّحة الدولية.

الاتفاقية الخاصة باحترام قوانين وأعراف الحرب البرية لعام1907 .

اتفاقية لاهاي الخاصة باحترام قوانين وأعراف الحرب البرية لعام 1907.

إعلان سان بطرسبورغ بغية حظر استعمال قذائف معينة في زمن الحرب، 1868.

ميثاق الأمم المتحدة.

Cyber Warfare Under International Humanitarian Law

Omar Mahmoud Amar*

Abstract

This research sheds light on the most important principles of international humanitarian law and the extent to which it is possible to upgrade to cyber warfare, the ability to deal with it anywhere and will affect the civilian population and not the military. This research also deals with cyber warfare as an armed conflict or not. The research discusses the differences of jurisprudential views on the possibility of adapting the established principles of international humanitarian law and applying them to electronic warfare as it is.

The study deals with the extent to which the general principles relating to the rules of warfare and its behavior are compatible with cyber warfare.

This study divided into the following topics: The first topic deals with the extent to which electronic warfare is subject to international humanitarian law, and the second deals with the compatibility of general principles related to the rules of warfare and their behavior with cyber warfare

Keywords: International Humanitarian Law, Cyber Warfare.

* School of Law, AL-Balqa', Applied University, Jordan. Received on 14/6/2018 and Accepted for Publication on 6/3/2019.