الحرب السيبرانية
في ضوء قواعد القانون الدولي الإنساني

الأستاذ المُساعد الدكتور
يحيى ياسين سعود

(ISSN : 2537 - 0758)

الحرب السيبرانية
في ضوء قواعد القانون الدولي الإنساني

أ. م. د. يحيى ياسين سعود

الملخص

يدور البحث حول هجمات سيبرانية أثناء النزاعات المسلحة أو أن تلك الهجمات تجري في سياق ذلك النزاع، مما انعكس في تعريف اساليب ووسائل القتال المعروفة أثناء الحروب التقليدية، وبالتالي مدى امكانية تطبيق مبادئ وقواعد القانون الدولي الإنساني على تلك الهجمات.

واذا كنا نتفق بأن قواعد القانون الدولي الإنساني لم تشير إلى الهجمات السيبرانية أثناء النزاعات المسلحة بوصفها النطاق المادي لتطبيق ذلك القانون، إلا أن شمولية العديد من قواعده يمكن أن تستوعب الكثير من التطورات ذات الصلة، دون انكار حقيقة التغيرات التي شهدتها طبيعة الحروب، ولعل الاستخدام المتزايد للفضاء السيبراني للأغراض العسكرية أحد أهم الأسباب التي تدعو إلى إعادة تنظيم قواعد واحكام النزاعات المسلحة وصياغتها بالشكل الذي يتلائم مع طبيعة هذه الاستخدامات.

وقد يبدو وضع مقاربات إنسانية متباينة بين الحروب التقليدية وحروب الفضاء الالكتروني مهمة ليست باليسيرة، إلا أنه في ضوء الظروف الواقعية للنزاعات المسلحة وما تشهده من انتهاكات جسيمة يمكن الإشارة إلى أن الاستخدام الامثل لذلك الفضاء وفي بيئة عمل سليمة تحكمها قواعد محددة قد تجعل تلك المقاربة تستحق البحث والاستقصاء.

Cyber war in Light of International Humanitarian Law

Abstract

This paper revolves around cyber attacks made during armed conflicts or taking place in the context of the same, which is reflected in defining known methods and means of fighting during traditional wars, and consequently in the possibility of implementing principles and rules of international humanitarian law to such attacks.

Although we agree that rules of international humanitarian law did not refer to cyber attacks during armed conflicts as the material domain for application of the said law, the universality of many of its rules can still accommodate many relevant developments, without denial of changes witnesses by the nature of wars. The ever-growing use of cyberspace for military purposes is probably one of the most important reasons of reorganizing rules and regulations of armed conflicts and reshaping them in a way suitable for the nature of such uses.

Drawing humanitarian comparisons between traditional wars and cyberspace wars may seem a difficult task. However, based on realistic conditions of armed conflicts and the grave violations they had faced, we can infer that the best use of cyberspace in a sound work environment restricted by specific rules, may make that comparison worthy of research and investigation.

المقدمة

أولاً: موضوع البحث

في هذه الدراسة استخدمنا مصطلح الحرب السيبرانية للإشارة إلى وسائل واساليب القتال المستخدمة في عمليات الفضاء الالكتروني بحيث ترقى إلى مستوى النزاع المسلح أو تجري في سياقه، ضمن المعنى المقصود في القانون الدولي الإنساني.

ذلك أن اللجوء المتزايد للدول في استخدام الفضاء الالكتروني لشن هجمات سيبرانية أثناء نزاعاتها المسلحة، جعل قواعد ذلك القانون أمام اختبار حقيقي ومعقد حول مدى امكانية تطبيق قواعد ومبادئ القانون الدولي الإنساني على هكذا نوع جديد من الحروب.

ثانياً: إشكالية البحث

إنَّ الاشكالية القانونية التي يثيرها موضوع البحث تتلخص في محاولة الإجابة عن أسئلة عدة منها ما يتعلق بتحديد مفهوم الحرب السيبرانية ومدى تطبيق القواعد والمبادئ

(ISSN : 2537 - 0758)

الرئيسية للقانون الدولي الإنساني بشأنها، حيث لا تزال قواعد واحكام ذلك القانون، ومنذ صياغة اتفاقيات جنيف الاربعة لعام ١٩٤٩ والبروتوكولين الملحقين بها عام ١٩٧٧، هي قواعد واجبة التطبيق على كافة الانشطة التي تقوم بها الاطراف أثناء النزاع المسلح وينبغي احترامها، مع اشكالية أن وسائل الحرب واساليبها تتطور مع مرور الوقت، كما يستلزم موضوع البحث واشكاليته وضع مقاربة قانونية وانسانية بين الحروب التقليدية والتي يكون الإنسان محورها المادي وما يكتنفها من شعور بالعداء وحب الانتقام والحفاظ على الذات في كثير من الاحيان، وبين الاستخدام الامثل للتكنلوجيا في تحديد الأهداف وامكانية امتثالها لقواعد القانون الدولي الإنساني.

ثالثاً: أهمية البحث

تبدو أهمية البحث في تسليط الضوء على التبعات الإنسانية التي من المحتمل أن تنشأ جراء اللجوء إلى العمليات السيبرانية في الفضاء الالكتروني أثناء النزاعات المسلحة بالمقارنة مع وسائل واساليب القتال في الحروب التقليدية.

واذا كنا نتحدث عن أهمية الموضوع بسبب حداثته، فأننا نعني الحرب السيبرانية التي يحكمها القانون الدولي الإنساني، كأحد القضايا الرئيسية لتحديد الظروف التي يمكن في اطارها اعتبار العمليات الالكترونية بوصفها تحدث في سياق نزاع مسلح أو تؤدي بحد ذاتها إلى نشوب نزاع مسلح، لضمان أن اللجوء للعمليات الالكترونية أثناء تلك النزاعات سيجري وفقاً للالتزامات الدولية.

رابعاً: منهجية البحث

أن طبيعة البحث وموضوعه تستدعي الاعتماد بدرجة كبيرة على المنهج التحليلي (الاستنباطي)، من اجل تحليل القواعد العامة للقانون الدولي الإنساني لمعرفة مدى امكانية تطبيقها على انشطة الدول والاطراف من غير الدول في الفضاء الالكتروني والتي تشكل أو يمكن أن توصف بأنها نزاع مسلح أو جزء منه.

خامساً: هيكلية البحث

سنتناول موضوع الحرب السيبرانية في ضوء قواعد القانون الدولي الإنساني في ثلاث مطالب يسبقها مقدمة، وسنخصص المطلب الأول لمفهوم الحرب السيبرانية من خلال فرعين نبين في الفرع الأول تعريف الحرب السيبرانية، ونوضح في الثاني طبيعتها

القانونية، إما في المطلب الثاني فسوف نتناول فيه، مدى أمكانية تطبيق قواعد القانون الدولي الإنساني بشأن العمليات السيبرانية، وذلك من خلال فرعين، نتناول في الأول، شمولية قواعد القانون الدولي الإنساني، وفي الثاني، خصوصية العمليات السيبرانية واثرها في تطبيق تلك القواعد.

وسنفرد المطلب الثالث لمقاربات متباينة بشأن الهجمات السيبرانية، حيث نكرس الفرع الأول منه للمقاربة الإنسانية بين الحرب التقليدية والحرب السيبرانية، وفي الفرع الثاني ومن وجهت نظر فلسفية سوف نحاول استخلاص بعض الجوانب الايجابية لاستخدام الفضاء الالكتروني أثناء النزاعات المسلحة.

علـى اننـا سـوف نختـم بحثنـا لاهـم مـا توصلنا إليه من استنتاجات وتوصيات.

المطلب الأول
مفهوم الحرب السيبرانية

سوف ننطلق في تحديد مفهوم الحرب السيبرانية، بالإشارة إلى أن قواعد القانون الدولي الإنساني، وهي القواعد القانونية المنظمة للنزاعات المسلحة، لا تنطيق على كافة العمليات الالكترونية أو ما يطلق عليه هجمات سيبرانية وفقاً لعمومية المصطلح، حيث يستخدم المصطلح في مجالات عدة تقع خارج نطاق النزاع المسلح وبالتالي خارج نطاق تطبيق قواعد القانون الدولي الإنساني، فهناك ميدان لتطبيق تلك الانشطة يتعلق بالشركات التجارية والحكومات وجرائم الفضاء الالكتروني والجرائم الجنائية الاخرى بالقدر نفسه الذي تهتم به الهجمات السيبرانية التي يحكمها القانون الدولي الإنساني، وبالتالي لا بد من التعريف بالمصطلح وتميزه عما يشتبه به، فضلاً عن تبيان الطبيعة القانونية لتلك الهجمات.

الفرع الأول
تعريف الحرب السيبرانية

السيبرانية في اللغة مصطلح مشتق من الكلمة اليونانية (kybernetes) بمعنى القيادة والتحكم عن بعد[١].

(ISSN : 2537 - 0758)

وفي الاصطلاح عرف (Michael N. Schmitt) الهجمات السيبرانية بأنها: (تلك الإجراءات التي تتخذها الدولة من اجل الهجوم على نظم المعلومات للعدو وبهدف التأثير والاضرار فيها، والدفاع عن نظم المعلومات الخاصة بالدولة المهاجمة)[٢].

واذا شكلت الهجمات السيبرانية وتبعاً للظروف نزاعاً مسلحاً، فنكون أمام مصطلح الحرب السيبرانية أو ما يعرف بالهجوم السيبراني وفقاً لقواعد القانون الدولي الإنساني، بوصفه عملية الكترونية سواء هجومية أو دفاعية يتوقع أن تتسبب في اصابة أو قتل أشخاص أو الأضرار بأعيان أو تدميرها، وبالتالي فأن الهجمات السيبرانية يمكن أن تكون أوسع نطاقاً من الحرب السيبرانية وقد تحدث خارج اطار الحروب وقد تكون سبباً لبدء الحرب[٣].

وتتميز الحرب السيبرانية عن الحرب التقليدية، في أن المفهوم التقليدي للحرب، ينطوي على استخدام الجيوش النظامية ويسبقها اعلان واضح لحالة الحرب وميدان قتال محدد، بينما تبدو هجمات الفضاء الالكتروني غير محددة المجال وغامضة الأهداف، كونها تتحرك عبر شبكات المعلومات والاتصالات المتعدية للحدود الدولية، إضافة إلى اعتمادها ما يمكن وصفه بأسلحة الكترونية جديدة تلائم طبيعة السباق الالكتروني لعصر المعلومات، حيث يتم توجيهها ضد المنشئات الحيوية أو دسها عن طريق عملاء لأجهزة الاستخبارات، وعليه فأن احد معايير التمييز بين الحرب السيبرانية والحرب التقليدية يمكن أن يكون بالاستناد إلى طبيعة السلاح المستخدم، وبالتالي يمكن القول أن الحرب السيبرانية، هي الحرب التي تستخدم فيها الاسلحة غير التقليدية وفقاً للآثار المترتبة على استخدام هكذا نوع من الاسلحة والمتمثلة بالتدمير واسع النطاق[٤].

فتعريف الاسلحة غير التقليدية وفقاً للجنة الاسلحة التقليدية للأمم المتحدة والصادر عام ١٩٦٨ بأنها: (اسلحة الانفجارات الذرية والاسلحة المصنوعة من مادة ذات نشاط اشعاعي واسلحة الفتك الكيميائية والبيولوجية واي نوع من الاسلحة الاخرى التي يتم تصنيعها في المستقبل والتي تتشابه خصائصها في الاثر التدميري مع القنبلة الذرية أو الاسلحة الاخرى)[٥].

ويبدو أن ايراد عبارة واي نوع من الاسلحة الاخرى التي يتم تصنيعها في المستقبل ذات اثر تدميري يتشابه أو يقترب مما تخلفه الاسلحة غير التقليدية بمعناها المتعارف عليها من اسلحة ذرية وكيميائية وبيولوجية، جاءت لتتسع حيث تشمل ما تخلفه الهجمات السيبرانية في اطار النزاع المسلح من اختراق واعاقة للحواسيب وشبكات المعلومات التابعة للدول محل الهجوم، مما يجعل المدنيين عرضة لخطر الحرمان من الاحتياجات الأساسية مثل مياه الشرب والرعاية الطبية والكهرباء، إذا ما تعطلت تلك الأنظمة عن العمل بسبب الهجوم السيبراني، حيث يمكن أن تتعرض السدود والمحطات النووية وانظمة التحكم في الطائرات مما يصعب الحد من آثار الهجوم السيبراني دون الأضرار بأجزاء أخرى مما يشكل اثر تدميري هائل.

ويثير تعريف الموضوع محل البحث مسألة على قدر من الاهمية تتعلق بوصف الهجمات السيبرانية كجزء من نزاع مسلح سواء أكان نزاعاً مسلحاً دولياً أم غير ذي طابع دولي، ذلك أن القانون الدولي الإنساني، هو مجموعة من القواعد التي تسعى للحد من آثار النزاعات المسلحة لأسباب إنسانية، وبالتالي فأن ميدان القانون الدولي الإنساني هو النزاع المسلح، وعليه يجب ابتداءً رسم خط واضح يفصل بين الحالات التي تمثل والحالات التي لا تمثل نزاعاً مسلحاً، وهي ليست بالمهمة اليسيرة لاعتبار الهجمات السيبرانية، لاسيما وان تلك الهجمات تمتاز في كونها قد ترتكب في ظل ظروف غير منتظمة بصورة أساسية[٦].

وبغض النظر عن الاشكاليات المشار إليها سابقاً، فان الهجمات السيبرانية يمكن أن تكون جزءاً من حرب سيبرانية متى ما استخدمت في اطار نزاع مسلح واستهدفت تحقيق أهداف عسكرية، وبالتالي يمكن تعريفها على انها: تلك الإجراءات التي تتخذها الاطراف في نزاع مسلح لكسب الميزة على خصومهم في فضاء السايبر باستخدام مختلف الأدوات التكنلوجية والاشخاص التقنيين، ويحصل على المزايا من جراء تلك الهجمات من خلال اتلاف أو تدمير أو تعطيل أو اغتصاب أنظمة الحاسوب للعدو أو من خلال الحصول على معلومات يرغب العدو في أن تبقى سرية، أو ما يعرف

(ISSN : 2537 - 0758)

بالتجسس السيبراني أو الاستغلال لشبكات الحاسوب، متى ما كانت في اطار نزاع مسلح يصل إلى مستوى الحرب(٧).

الفرع الثاني

الطبيعة القانونية للحرب السيبرانية

أن البحث في امكانية تطبيق قواعد القانون الدولي الإنساني على الحرب السيبرانية قد يستلزم ابتداءً التكييف القانوني لتلك المسألة من حيث شرعية وعدم شرعية الحرب السيبرانية في ضوء استخدام القوة في العلاقات الدولية، فالعلاقة بين حق اللجوء إلى الحرب وقانون الحرب تتسم بأنها علاقة توتر لا بد منه، فالقواعد المعاصرة للقانون الدولي تحظر استخدام القوة، بأستثناء حق الدول فرادى أو جماعات في الدفاع عن نفسها(٨)، أو بمقتضى استخدام تدابير انفاذ القانون التي يتخذها مجلس الأمن(٩)، إما قانون الحرب فهدفه التوفيق بين ضرورات الحرب وقوانين الإنسانية من خلال فرض قيود واضحة على سير العمليات العسكرية، وبخلاف ما تم الإشارة إليه، فأن استخدام القوة في العلاقات الدولية يعد عملاً غير مشروع وفقاً لميثاق الأمم المتحدة حيث نص على ما يلي: (يمتنع أعضاء المنظمة جميعاً في علاقاتهم الدولية عن التهديد بأستعمال القوة أو استخدامها ضد سلامة الاراضي أو الاستقلال السياسي لاية دولة أو أي وجه آخر لا يتفق ومقاصد الأمم المتحدة)(١٠).

وهنا يثار التساؤل حول تفسير مصطلح (القوة) بين المقصود بهذا المصطلح، هو استخدام القوة المسلحة في اطار عدوان أو هجوم مسلح ترتكبه الدول باستخدام قواتها المسلحة أو جماعات منظمة تابعة لها أو مسندة من قبلها(١١)، وبين من يرى انه ليس هناك سبب قانوني يدعو إلى آقتصار مفهوم القوة على القوة المسلحة فقط، بل يمكن أن يشمل الضغط الاقتصادي أو السياسي كذلك(١٢).

والحقيقة أن الأخذ بالمعيار الأول المعتمد على العنصر الحركي للقوات المسلحة لا يستقيم والكثير من الاستخدامات للقوة أثناء الحروب، وبغض النظر عن مشروعية تلك الحرب من عدمها ومنها الهجمات البايولوجية والجرثومية وكذلك الهجمات السيبرانية مدار بحثنا، كما أن الاعتماد على المعيار الثاني قد يوسع كثيراً من مفهوم استخدام القوة والتهديد بها ليشمل الاكراه الاقتصادي والسياسي، وقد يخالف المقصود بما ورد في

ميثاق الأمم المتحدة من مقاصد وفقاً لرأي اغلبية الفقهاء كونه يوسع من مفهوم العدوان بما يعطي مسوغاً لاستخدام القوة المضادة استناداً لحق الدفاع الشرعي(١٣).

على أن هناك من يذهب بخلاف الاتجاهين السابقين في تحديد المقصود بالقوة، لتشمل كافة صور استخدام القوة المسلحة، بالإضافة إلى صور أخرى يترتب عليها انتهاك أو تأثير واضح على الأمن القومي لدولة أخرى(١٤).

وفي ضوء ما تقدم، فأن هناك مجموعة من الاطر التفسيرية المرتبطة بالحرب السيبرانية، منها ما يتعلق بمفهوم القوة، حيث لعب الفضاء الالكتروني دوراً اساسياً في تعظيمها والاستحواذ على عناصرها الأساسية في العلاقات الدولية، حيث اصبح التفوق في ذلك المجال عنصراً حيوياً في تنفيذ عمليات ذات فعالية على الأرض والبحر والجو والفضاء الخارجي من خلال اعتماد القدرة القتالية في الفضاء الالكتروني على نظم التحكم والسيطرة التكنلوجية، وهذا الأمر يستدعي بالضرورة تغير في مفهوم القوة حيث بات بالإمكان تعريفها بأنها: (مجموعة الوسائل والطاقات والامكانيات المادية وغير المادية المنظورة وغير المنظورة التي بحوزة الدولة ويستخدمها صانع القرار في فعل مؤثر يحقق مصالح الدولة وتؤثر في سلوك الوحدات السياسية الاخرى)(١٥).

ومن هنا فأن عناصر القوة وفقاً للمنظور السابق يتمثل في التناغم بين القدرات التكنلوجية والسكانية والاقتصادية والصناعية والقوة العسكرية وارادة الدولة وغيرها مما يسهم في دعم امكانات الدولة على ممارسة الاكراه أو الاقناع أو ممارسة التأثير السياسي في أعمال الدول الاخرى بغرض الوصول للأهداف، سواء اكانت تلك الأهداف مشروعة متى ما توافقت مع القواعد القانونية، ومنها القواعد القانونية الدولية، أو غير مشروعة وما يستتبعه من مخالفة لقواعد القانون الدولي التي اوجبت على الجماعة الدولية من الامتناع في استخدام القوة أو التهديد بها في علاقاتهم الدولية، وبالتالي فأن التغير في مفهوم القوة يؤدي بالضرورة إلى تغير في منظور الحرب، حيث انتقلت من نسق الحروب التقليدية القائمة على تدمير الخصم أو احتلال ارضه أو الاستيلاء على موارده، إلى حروب تعمل للاستحواذ على سباق التقدم التكنلوجي وسرقة الاسرار الاقتصادية والعلمية والتحكم بالمعلومات والعمل على اختراق الأمن القومي بدون

(ISSN : 2537 - 0758)

طائرات أو متفجرات، أو حتى انتهاك الحدود وتدمير مواقع التجسس والتي قد يكون لها تأثير يفوق الحرب التقليدية لما تشكله من آثار مدمرة على الاقتصاد والبنية التحتية.

واذا تبين لنا فيما تقدم أن مفهوم القوة في اطار الحرب السيبرانية له مدلولاته عن مفهومها التقليدي وفقاً لما قصده واضعي ميثاق الأمم المتحدة[١٦]، فأن هناك اطار تفسيري آخر مرتبط في أن استخدام القوة بصورة غير مشروعة، انما يتمثل بمعيار استخدام القوة المسلحة بالإضافة إلى انتهاك الأمن القومي لدولة أخرى، وفي ضوء انماط متعددة للحروب السيبرانية في كون جميع درجاتها يمكن أن تشكل استخدام غير مشروع للقوة؟ فقد يتم استخدام الفضاء الالكتروني كساحة لصراع منخفض الشدة من خلال التأثير على النواحي الاقتصادية أو الثقافية أو الاجتماعية، وهي لا تتطور بالضرورة إلى استخدام الفضاء الالكتروني كقوة مسلحة أو شن حرب الكترونية واسعة النطاق، حيث يمكن أن تتجسد تلك الصراعات بوسائل عدة، منها الحرب النفسية والاختراقات المتعددة والتجسس وسرقة المعلومات وشن حرب الأفكار وغيرها، ومثال ذلك ما تعرضت له روسيا من اتهام بالقرصنة الالكترونية في الانتخابات الامريكية لدعم المرشح الجمهوري دونالد ترامب في مواجهة منافسته الديمقراطية هيلاري كلنتون[١٧].

وهناك نمط آخر من الحروب السيبرانية يتمثل في تحويل الصراع عبر الفضاء الالكتروني كساحة موازية أو مرافقة أو مرتبطة لحرب تقليدية دائرة على الأرض، ومنها ما تعرضت له سوريا في ٢٠٠٧/١٢/٦ لهجمة سيبرانية على دفاعاتها الجوية في إحدى المنشئات التي يشتبه في انها منشأة نووية في مدينة دير الزور من قبل اسرائيل، مما ادى إلى تعطيل هذه الدفاعات لتمكين الطائرات الاسرائيلية من قصف هذا الموقع دون أن يتم الكشف عن الهجوم[١٨].

ونمط ثالث يعبر عنه في نشوء حروب في الفضاء الالكتروني بصورة منفردة، واذا لم يشهد العالم هكذا نوع من الحروب وفقاً لآثارها المدمرة من خلال اختراق العمليات العسكرية عالية التقنية أو استهداف الحياة المدنية والبنية التحتية بالشكل الذي يمكن تصوره إلا أن هناك نماذج لتلك الحروب تتمثل على شكل رسائل تهديد مصحوبة بآثار محدودة جراء تلك الهجمات، ومنها ما تعرضت له جمهورية استونيا عام ٢٠٠٧ من هجوم

سيبراني مستقل بذاته موجه من روسيا الاتحادية وذلك عن طريق اغراق المواقع الالكترونية بسيل من البيانات غير اللازمة، حيث وجهت ما يقارب من مليون حاسبة من عدة نقاط في العالم، واستهدفت المواقع الحكومية والصحف والجامعات والمستشفيات والمصارف وخدمات الاطفاء والاسعاف وذلك بهدف اسقاط وشل الحكومة الاستونية[١٩].

ووفقاً لما تقدم فأن الهجمات السيبرانية تثير اشكالية تتعلق بالقواعد المتعلقة بحق اللجوء إلى الحرب من حيث طبيعة تلك الهجمات في امكانية وصفها استخدام للقوة وبالتالي البحث في مشروعية أو عدم مشروعيتها وفي ضوء المبادئ والقواعد القانونية، لاسيما بعد إنشاء الأمم المتحدة والتي تتعلق بضرورة عدم استخدام القوة أو التهديد بها في ميدان العلاقات الدولية، ما خلا الاستثناءات المتعلقة بحق الدفاع الشرعي أو بموجب قرار صادر عن مجلس الأمن وفقاً للفصل السابع من الميثاق، والأمر يزداد صعوبة في ظل عدم الاتفاق حول مفهوم القوة المستخدمة والتي توصف كونها غير مشروعة لتشكل ما يعرف جريمة العدوان، لاسيما وان ميدان الهجمات السيبرانية يمكن أن يأخذ أشكال عدة منها الاقتصادية والثقافية، فضلاً عن ما يمكن وصفه بأنه هجوم مسلح.

المطلب الثاني
مدى إمكانية تطبيق مبادئ وقواعد القانون الدولي الإنساني بشأن العمليات السيبرانية

إذا كنا فيما سبق تطرقنا إلى مفهوم الحرب السيبرانية، بالرغم مما يثيره ذلك المفهوم من غموض، فأننا في هذا المقام سوف نتناول استخدام (الهجمات السيبرانية) أو (العمليات السيبرانية) في اطار النزاعات المسلحة، تلك النزاعات التي لا يحتمل بشأنها الخلاف، في انها النزاعات التي يستخدم أو من المرجح أن يستخدم فيها السلاح من قبل كل الاطراف أو بعضهم، وحسبنا في ذلك أن نشير إلى النطاق المادي لتطبيق القانون الدولي الإنساني، انما هو زمن النزاعات المسلحة، سواء اكانت تلك النزاعات هي نزاعات مسلحة دولية، أو نزاعات مسلحة غير ذي طابع دولي، كل ذلك لمعرفة مدى اتساق قواعد ذلك القانون ومدى امكانية تطبيقها بشأن العمليات السيبرانية.

الفرع الأول
شمولية مبادئ وقواعد القانون الدولي الإنساني

(ISSN : 2537 - 0758)

إذا كنا نتفق بأن قواعد القانون الدولي الإنساني لم تشير على وجه الخصوص للعمليات السيبرانية، غير أن غياب اشارات محددة في ذلك القانون لا يعني عدم خضوع هذه العمليات لقواعد القانون الدولي الإنساني، وذلك من خلال قواعده العامة التي تنظم جميع اساليب الحرب ووسائلها بما فيها استخدام الاسلحة، حيث جاءت تلك القواعد لتشتمل على كافة التطورات ذات الصلة، حيث يمكن أن نشير إلى ما تضمنه البروتوكول الاضافي الأول الملحق بأتفاقيات جنيف الاربعة لعام ١٩٧٧ اذ نص على ما يلي: (يلتزم أي طرف سام متعاقد عند دراسة أو تطوير أو اقتناء سلاح جديد أو اداة للحرب أو اتباع اسلوب للحرب، بأن يتحقق مما إذا كان ذلك محظوراً في جميع الاحوال أو في بعضها بمقتضى هذا الملحق ((البروتوكول)) أو أية قاعدة أخرى من قواعد القانون الدولي التي يلتزم بها الطرف السامي المتعاقد)[٢٠].

ووفقاً للنص السابق واذا ما تم تكييف التكنلوجيا الجديدة بأنها سلاح للحرب أو اداة لها أو اسلوب من اساليب الحرب، فعلى الاطراف التحقق في مدى مشروعية استخدامها وفقاً لقواعد البروتوكول أو أية قاعدة أخرى من قواعد القانون الدولي.

ويمكن الاستناد ايضاً إلى المبادئ الأساسية للقانون الدولي الإنساني لمعرفة مدة امكانية تطبيقها بشأن ما اطلقنا عليها الحرب السيبرانية، ولعل أحد أهم تلك المبادئ ما يعرف (بشرط مارتنز)، ذلك الشرط الذي وضع اصلاً في ديباجة اتفاقية لاهاي الرابعة لعام ١٨٩٩ وعام ١٩٠٧، ودخل بعد ذلك في نص البرتوكول الاضافي الأول لعام ١٩٧٧ وفي ديباجة البروتوكول الثاني، حيث ينص ذلك الشرط على ما يلي: (في حالة عدم وجود قاعدة معينة في القانون التعاهدي، يظل المحاربون في حمى وتحت سلطة القانون العرفي ومبادئ الإنسانية وما يمليه الضمير العام).

على أن النص السابق يمكن أن يثير مسألة خلافية تتعلق بالعبارة الواردة (مبادئ الإنسانية وما يمليه الضمير العام) في كونها مقياس لقاعدة قانونية ملزمة تتعلق بالسلاح المستخدم أو أي نوع معين من السلوك، أم انها مجرد مبادئ اخلاقية غير ملزمة؟

وفي هذا الصدد نود الإشارة إلى الفتوى الصادرة عن محكمة العدل الدولية بشأن مشروعية التهديد بالأسلحة النووية أو استخدامها، حيث اكدت المحكمة على أهمية شرط

مارتنز، الذي لا يمكن الشك في استمرار وجوده وقابليته للتطبيق، وبأن هذا الشرط يعد وسيلة فعالة لمواجهة التطور السريع في التكنلوجيا العسكرية[٢١].

ويمكن الاستدلال ايضاً بما ورد في حكم محكمة الولايات المتحدة الامريكية العسكرية في قضية (كروب) عام ١٩٤٨ والتي اشارت إلى أن (شرط ماتنز) في كونه أكثر من مجرد اعلان ورع، وانه شرط عام يجعل العادات المستقرة بين الأمم المتحضرة وقوانين الإنسانية وما يمليه الضمير العام جزءاً من المقاييس القانونية التي يجب تطبيقها إذا لم وعندما لا تغطي إحكام الاتفاقيات حالات محددة[٢٢].

وهنا نود أن نشير إلى أن الظروف المصاحبة لانتهاك المعايير الإنسانية قد تكون أكثر تطوراً الآن مما كان عليه الحال عندما وضع شرط (مارتنز)، وان فلسفة واصفي هذا الشرط هو في أن ما لم يحظر صراحةً في المعاهدات أو العرف لا يمكن أن يكون مباحاً إذا كان يتعارض مع مبدأ الإنسانية وما يمليه الضمير العام، وانها بدون شك تمثل عوامل تقييدية قانونية.

كما أن أهمية (شرط ماتنز) قد تبدو جزء من الاهمية الجوهرية لمبادئ القانون الدولي الإنساني بشكل عام، ذلك أن تلك المبادئ شأنها شأن أي مجال قانوني آخر، انما تقدم الحل بالاستقراء للحالات غير المتوقعة وتسهم في سد ثغرات القانون وتساعد في تطوره مستقبلاً بتبيان المسار الذي ينبغي اتباعه، وهي تمثل في هذا القطاع القانوني ابسط الاسس الإنسانية التي يمكن أن تطبق في كل زمان ومكان وتحت جميع الظروف، وذلك انها قد تستند احياناً إلى قانون مكتوب وأخرى مستمدة من اعراف الشعوب، وبالتالي فأنها صالحة حتى بالنسبة للبلدان من غير الاطراف في الاتفاقيات التي ضمت تلك المبادئ في احكامها.

واتساقاً مع ما تم الإشارة إليه، فأن هناك اتفاق عام منعقد بين فقهاء القانون الدولي الإنساني في تفسير قواعد قانونية يستلزم مراعاتها بشأن النزاعات المسلحة مهما كانت درجتها أو اسلوب تطورها، منها ما يشير إليه البرتوكول الاضافي الأول الملحق باتفاقيات جنيف لعام ١٩٧٧، حيث نص على ما يلي: (في حالة الشك بشأن شخص ما على انه مدني أم غير مدني فيجب اعتبار ذلك الشخص مدنياً)[٢٣].

(ISSN : 2537 - 0758)

على أن جوهر القواعد القائمة لا تستهدف حماية المدنيين فحسب، بل لا بد أن يكون في اطار الاستهداف المشروع، وهو ما يعبر عنه بمبدأ التميز القائم بين من يشارك أو يستطيع المشاركة في العمليات العدائية، وكذلك التميز بين الأهداف العسكرية والاعيان المدنية، حيث تجد هذه القاعدة سندها في الفقه القانوني عندما عبر (بورتاليس)، أن الحرب هي علاقة دولة بدولة لا فرد بفرد، وانها بين امتين متحاربتين، لا يكون الافراد الذين تتكون منهم تلك الأمم اعداء إلا بصفة عرضية، ليس بوصفهم كرجال أو كمواطنين وإنما فقط بوصفهم كجنود(٢٤).

ويلحق بعمومية مبادئ القانون الدولي الإنساني، مبدأ حظر الهجمات العشوائية، تلك الهجمات التي لا توجه إلى هدف عسكري محدد، أو التي تستخدم طريقة أو وسيلة قتال لا يمكن توجيهها إلى هدف عسكري محدد، أو الهجمات التي تستخدم طريقة أو وسيلة قتال لا يمكن تحديد آثارها على النحو الذي يقتضيه القانون الدولي الإنساني، وبالتالي من شأنها في كل حالة كهذه أن تصيب اهدافاً عسكرية واعيان مدنية ومدنيين دون تمييز (٢٥).

ويرتبط بما سبق الإشارة إليه، من انه يحظر الهجوم الذي قد يتوقع منه أو يسبب بصورة عرضية خسائر في ارواح المدنيين أو اصابات بينهم أو أضرار بالأعيان المدنية، أو قد يسبب مجموعاً من هذه الخسائر والاضرار ويكون مفرطاً في تجاوزه ما ينظر إليه أو يسفر عنه من ميزة عسكرية ملموسة ومباشرة، وهذا ما يطلق عليه مبدأ التناسب، ذلك المبدأ الذي يجد اساسه ايضاً في قواعد القانون الدولي الإنساني العرفي والتي تطبق في النزاعات المسلحة الدولية وغير الدولية(٢٦).

وهناك مبدأ الضرورة العسكرية الذي يسمح فقط باستخدام النوع والدرجة من القوة غير المحظورة والتي تكون لازمة لتحقيق الهدف المقصود والمشروع من النزاع المسلح وهو اخضاع العدو بصورة كاملة أو جزئية وبأقل قدر ممكن من التضحية في الارواح والموارد، وبالتالي يمنع في هذا الخصوص تدمير ممتلكات العدو أو حجزها، إلا إذا كانت ضرورات الحرب تقضي حتماً هذا التدمير والحجز (٢٧).

ويعد مبدأ الإنسانية، وهو مبدأ عام اذ يبدو مكملاً لمبدأ الضرورة العسكرية ومتضمناً فيه، كما يحظر بموجبه الحاق الآلام أو الاصابة التي لا مبرر لها، وبالتالي فأن ذلك المبدأ يحظر اللجوء إلى وسائل أو اساليب الحرب التي لا تحظر استخدامها قاعدة أخرى من قواعد القانون الدولي الإنساني، من حيث أن حق اطراف أي نزاع مسلح اختيار اساليب ووسائل القتال ليس حقاً لا تقيده قيود[٢٨]، وكذلك حظر استخدام الاسلحة والقذائف والمواد ووسائل القتال التي من شأنها احداث اصابات أو آلالام لا مبرر لها[٢٩].

ومما تقدم يمكن القول أن المبادئ والقواعد المشار إليها لا تقتصر على وسائل واساليب القتال وفقاً للمفهوم التقني لبعض الاسلحة أو طريقة استخدامها، وإنما تقتضي تلك القواعد على وجه التحديد مفهوماً مستقبلياً ينطبق على تطوير أو اقتناء أو اعتماد سلاح جديد أو وسائل أو اساليب جديدة للحروب.

الفرع الثاني
خصوصية الهجمات السيبرانية وأثرها في تطبيق مبادئ وقواعد القانون الدولي الإنساني

إذا كنا قد تطرقنا إلى شمولية مبادئ وقواعد القانون الدولي الإنساني، إلا أن ذلك لا يعني انكار حقيقة التغيرات التي شهدتها طبيعة الحروب منذ اعتماد اتفاقية جنيف الأصلية قبل ما يقارب مائة وخمسون عاماً، حيث اصبحت وسائل واساليب الحروب متطورة إلى درجة لم يكن يتصورها واضعي تلك الاتفاقية، ولعل الاستخدام المتزايد للفضاء السيبراني للأغراض العسكرية احد أهم الأسباب التي تدعو إلى إعادة النظر في القواعد التي تنظم سير النزاعات المسلحة وصياغتها بالشكل الذي يتلائم مع طبيعة هذه الاستخدامات[٣٠].

واذا امكننا القول بأن مبدأ (مارتنز)، والذي تم الإشارة إليه فيما سبق، هو الشرط المطبق بكل تأكيد أيا كانت وسائل واساليب الحرب المستخدمة، إلا أن البعض الأخر من المبادئ والقواعد قد يستلزم بعض التطوير والاضافات وفقاً للتطبيق العملي لها في الفضاء السيبراني.

(ISSN : 2537 - 0758)

ففي اطار تطبيق مبدأ التميز على الهجمات السيبرانية اشار دليل تالين، بالرغم من عدم الزامية قواعده، بأنه لا يجوز أن تكون الاعيان المدنية هدفاً للهجمات السيبرانية، فلا يجوز على سبيل المثال توجيه الهجمات السيبرانية التي من شأنها تدمير الأنظمة المدنية والبنية التحتية، ما لم تعتبر هذه الأنظمة من قبيل الأهداف العسكرية التي يجوز استهدافها وفقاً للظروف السائدة(٣١).

وقد يثير تطبيق مبدأ التناسب على الهجمات السيبرانية بعض الصعوبات، ذلك أن الأضرار العرضية أمر لا محال بسبب عدم وجود الفاصل في كثير من الاحيان بين الفضاء السيبراني موضع استخدام المدنيين وبين ذلك الفضاء الذي يستخدم من قبل القوات والجماعات المسلحة والمدنيين المشاركين في العمل العدائي(٣٢).

وبالرغم من الصعوبة العملية المشار إليها إلا أن دليل تالين بشأن القانون المطبق على الحروب السيبرانية، تضمن وجوب الالتزام بمبدأ التناسب، من حيث حظر الهجمات السيبرانية التي من شأنها أن تسبب الخسارة في ارواح المدنيين أو أصابتهم أو الأضرار بالأعيان المدنية أو مزيجاً منهما، والتي تكون مفرطة مقارنة بالميزة العسكرية الملموسة والمباشرة التي يتوقع من الهجوم الحصول عليها(٣٣).

وفيما يتعلق بمبدأ الضرورة العسكرية، اشار دليل تالين، إلى انه في الحالات التي يكون الخيار ممكناً بين عدة أهداف عسكرية للحصول على ميزة عسكرية مماثلة، فالهدف الذي يتم اختياره للهجوم السيبراني، هو ذلك الهدف الذي يتوقع منه أن يسبب خطر اقل على المدنيين والاعيان المدنية، على أن مراعاة وتطبيق مبدأ الضرورة العسكرية، يتطلب أن يختار الهجوم الذي يتسبب بأضرار واصابات اقل، إما في حالة وجود العديد من الأهداف إلا أن احداها تحقق ميزة عسكرية أكثر من مثيلاتها، ففي هذه الحالة من حق المهاجم توجيه الهجمات السيبرانية المباشرة ضد الهدف العسكري آلذي يحقق أكثر ميزة عسكرية ممكنة في اطار النزاع المسلح، وهنا يجب أن ينظر بشأن الهجمات السيبرانية إلى الضرر الذي يلحق بالمنشئات والبنية التحتية المهمة بالنسبة للمدنيين، فضلاً عما يسببه للمدنيين من حرمان في وظائف وخدمات هذه المنشئات تطبيقاً لمبدأ الضرورة(٣٤).

وبخصوص تطبيق مبدأ الإنسانية والتي قد يكون عدم التسبب بالآلام لا مبرر لها جزء منها، فيمكن القول أن تطبيق هذا المبدأ على الهجمات السيبرانية قد لا يختلف عن جميع صور واساليب الحرب الاخرى من حيث ضرورة عدم التسبب بأضرار أو آلالام لا مبرر لها(٣٥).

ووفقاً لما تقدم فأن امكانية تطبيق مبادئ وقواعد القانون الدولي الإنساني قد تتمايز احياناً بشأن الهجمات السيبرانية عنها في الحروب التقليدية، على انه من وجهة نظرنا أن معايير هذا التباين لا تتعلق بتطبيق تلك المبادئ والاحكام فحسب، وإنما هناك الكثير من المسائل الاخرى التي تثيرها اشكالية الهجمات السيبرانية في اطار النزاعات المسلحة، منها ما يتعلق بتحمل مسؤولية الأفعال غير القانونية، تلك المسؤولية التي يمكن أن تتضمن خيارات القائد العسكري والمبرمج والمصنع، لاسيما إذا ما تعلق الأمر بالمسؤولية الجنائية الفردية، وعليه نجد من الضروري وضع قواعد تتفق وطبيعة الهجمات السيبرانية أثناء النزاعات المسلحة.

المطلب الثالث
مقاربات متباينة بشأن الهجمات السيبرانية

أن ترجمة قواعد القانون الدولي ذات الصلة في النزاعات المسلحة على ارض الواقع قد تكون مهمة ليست باليسيرة، ذلك انها تستند بشكل اساسي بين الصلاحيات المخولة للقوات أثناء العمليات بما في ذلك حماية القوات لذاتها وبين حماية المدنيين وفئات أخرى ممن لم يشتركوا في العمليات العدائية وكذلك حماية الاعيان المدنية.

وفي هذا المطلب سوف نحاول أن نتطرق إلى مقاربات متباينة بين سلوك الجنود الافراد وفي ضوء الظروف الواقعية للنزاعات المسلحة وما تشهده من انتهاكات جسيمة، وبين الاستخدام الامثل للفضاء الالكتروني أثناء النزاعات المسلحة في بيئة عمل سليمة قد تكون أكثر التزاماً بقواعد القانون الدولي الإنساني.

الفرع الأول
الجوانب السلبية للهجمات السيبرانية

يتمثل الجانب السلبي لاستخدام الهجمات السيبرانية أثناء النزاعات المسلحة، وعلى فرض برمجتها وفقاً للالتزام المفروض بقواعد القانون الدولي الإنساني، إلا أن التوقعات

(ISSN : 2537 - 0758)

يمكن أن تشير إلى امكانية استخدامها من قبل قائد عسكري لا يعرف الرحمة قادر على إعادة برمجتها، أو أن تتحول تلك البرامج إلى اسلحة مارقة نتيجةً لعيوب في المنظومة، مما يؤدي إلى اتخاذ خيارات بخلاف تلك التي يتوقعها أو يشجع عليها مبرمجي هذه الأنظمة، كما أن الضرورات العملية في تطبيق مبادئ القانون الدولي الإنساني، ومنها على سبيل المثال تطبيق مبدأ الضرورة العسكرية في معالجة الأهداف التي تستلزم احياناً اسر الأهداف المشروعة بدلاً من قتلها، قد يكون الإنسان أفضل دائماً في اتخاذ هكذا قرار والقدرة على التميز بين من يدعي الاصابة والذي قد يمثل تهديداً، وبالتالي يمكن استهدافه وقتله وفقاً لمبدأ الضرورة العسكرية، وبين من جرح جرحاً بالغاً حتى انه لم يعد يمثل تهديداً، ذلك أن مبدأ الضرورة العسكرية يستلزم أن تكون الإجراءات أو القوة المستخدمة لا تتضمن عمليات الثأر والاقتصاص[٣٦]، بالإضافة إلى عدم وجود بديل آخر للإجراءات أو التدابير المقرر استخدامها استناداً لمبدأ الضرورة[٣٧]، كما أن الفعل ذاته قد ينتهك مبدأ الآلام التي لا مبرر لها، ذلك المبدأ الذي يشتمل على أي تعد على السلامة البدنية والذهنية أو على حياة المقاتلين الذين يجوز قانوناً أن يكون عرضة لأعمال العنف المشروعة[٣٨].

كما أن المقاربة السلبية للهجمات السيبرانية، قد تتجلى في حالة الجنود في الميدان في صعوبة تطبيق مبدأ التناسب، ذلك المبدأ وكما تم الإشارة سابقاً الذي يرتبط بتقديم الأضرار التي قد تلحق، لاسيما بالسكان المدنيين والاعيان المدنية من الميزة العسكرية المنتظرة، حيث أن الميزة العسكرية الملموسة والمباشرة المنتظرة من هجوم على هدف مشروع قد تتغير باستمرار وفقاً للواقع الميداني المتعلق بخطط القادة الميدانيين وتطور العمليات العسكرية على كلا الجانبين، وبالتالي وعلى فرض استثناء الحالات التي يكون فيها تلك المتغيرات متوقعة، فأن برمجة تلك العمليات الالكترونية لا يمكن في مقدورها تطبيق مبدأ التناسب، لاسيما إذا ما علمنا أن معادلة التناسب تعد معادلة صعبة ودقيقة حتى أثناء وادارة العمليات الحربية التقليدية، فتحقيق المهمة القتالية واحراز النصر هدف اساسي للقوات العسكرية، وتنفيذ القوانين وضبط التدمير وعدم الحاق أضرار مفرطة بالخصم التزام قانوني واجب النفاذ، وبالتالي يحتاج إلى قائد ماهر شديد

المراس يسوي ميزان هذه المعادلة، والأمر بدون شك يزداد تعقيداً إذا ما تعلق الأمر بالهجمات السيبرانية[٣٩].

واذا كنا فيما سبق قد اشرنا إلى صعوبة تطبيق العديد من المبادئ الإنسانية بشأن الهجمات السيبرانية، فأننا في هذا المقام لا بد أن نشير إلى مسألة أخرى على قدر من الاهمية تتعلق بالقدرة على تقييم عملي سليم للمواقف الاجتماعية من حسن تقدير الأمور، وهي لابد من اسنادها إلى خبرة بشرية، اذ سوف يكون من الصعوبة بشكل خاص استنساخ هذه القدرة في البرامج الالكترونية، ففي الواقع العملي قد يصدر تصرف من مدني أو مجموعة من المدنيين ناتج عن خوف أو رعب أثناء العمليات العسكرية مما يوحي بأن هذا التصرف قد يشكل خطراً على القوات العسكرية، وبالتالي فأن مثل هذه الموقف يحتاج بالضرورة إلى جندي بشري قادر أن يحدد بسهولة ما يحدث في مثل هذه المواقف، فالجندي لا يجوز له اطلاق النار، إذا كان لديه الشك في أن تصرفاً ما انما يعبر عن خوف ورعب، وان ذلك التصرف لا يشكل تهديداً حقيقياً، لاسيما وان هذه المسألة لها اهميتها في تحديد المسؤولية عند تقييم القصد الجنائي لتحقق المسؤولية الجنائية والتي يتعين أن يكون الفعل الغير مشروع صادر عن ارادة أثمة مذنبة تتوفر فيها الادراك والتميز وحرية الاختيار، ولعل ما جاء به النظام الاساسي للمحكمة الجنائية الدولية كان واضحاً وصريحاً بشأن اقرار المسؤولية عندما نص على انه: (١- ما لم ينص عن غير ذلك لا يسأل الشخص جنائياً عند ارتكاب جريمة تدخل في اختصاص المحكمة ولا يكون عرضة للعقاب على هذه الجريمة إلا إذا تحققت الاركان المادية للجريمة مع توافر القصد والعلم ٢- لأغراض هذه المادة يتوافر القصد لدى الشخص عندما: أ- يتعمد هذا الشخص فيما يتعلق بسلوكه ارتكاب هذا السلوك ب- يتعمد هذا الشخص فيما يتعلق بالنتيجة التسبب في تلك النتيجة أو يدرك في انها ستحدث في اطار المسار العادي للأحداث ٣- لأغراض هذه المادة تعني لفظة ((العلم)) أن يكون الشخص مدركاً انه توجد ظروف أو ستحدث نتائج في المسار العادي للأحداث وتعتبر لفظة يعلم أو عن علم تبعاً لذلك)[٤٠].

(ISSN : 2537 - 0758)

وفي رأينا أن النص المتقدم يحاول أن يضع اسس موضوعية يمكن آخذها في الاعتبار عند تقييم القصد الجنائي تتعلق بظروف المرتكب الفعلي، وهذه المسألة نجدها غاية في الصعوبة إذا ما كان الاستهداف بواسطة البرامج الالكترونية ووفقاً للمعطيات الميدانية المتغيرة.

وبالتالي فأن عدم تحديد معايير منظمة لاستخدام التكنلوجيا أثناء الهجمات السيبرانية لاسيما للأغراض العسكرية الهجومية سوف ينشئ تحدياً واضحاً أمام تطبيق مبادئ وقواعد القانون الدولي الإنساني.

الفرع الثاني
بعض الجوانب الايجابية لاستخدام الفضاء الالكتروني أثناء النزاعات المسلحة

من المعلوم أن الدعوة إلى تطبيق قواعد القانون الدولي الإنساني أثناء النزاعات المسلحة، ومن وجهة نظر عملية، هي دعوة في جوهرها تقوم على احترام معايير موضوعية ارستها قواعد ذلك القانون، فلا يجوز لجندي على سبيل المثال، أن يقتل مدنياً حتى وان كانت لديه أسباب وجيهة لكرهه في حين يجوز له أن يقتل مقاتلاً حتى إذا كان هذا المقاتل في غاية اللطف، وعليه فأن استخدام التكنلوجيا في بيئة عملية سليمة قد يكون أكثر التزاماً بقواعد القانون الدولي الإنساني، ذلك اننا نرى الكثير من الجنود في ميدان المعركة أو في بيئة عدائية وفي ضوء مشاعر الكره أو الخوف أو الجوع أو التعب أو غريزة البقاء على قيد الحياة قد يرتكب اعمالاً وحشية قد يكون بالإمكان تجنبها بالاستخدام الامثل للتكنلوجيا المتطورة وفي اطار الهجمات السيبرانية[٤١].

كما أن بعض الجرائم التي قد ترتكب أثناء النزاعات المسلحة، لا يمكن تصور قيامها، إلا من قبل البشر، ومنها على سبيل المثال جريمة الاغتصاب[٤٢].

ومن جانب آخر، ومن وجهة النظر التي ترى أن استخدام الفضاء الالكتروني أثناء النزاعات المسلحة قد تجعل الحروب أكثر مروعة من الحروب التقليدية، وان الحروب يجب أن تكون عقلانية ومقبولة بشكل اكبر، فأن النظر لهذه المسألة من زاوية أخرى قد تتضمن مسألة ايجابية، تتعلق من وجهة نظر البعض بأن الحرب إذا ما كانت مروعة فسوف تعمل على ردع الدول والبشر من اللجوء إليها[٤٣].

ومن الشواغل المتصلة بالموضوع ما يراه البعض، أن اللجوء إلى الهجمات السيبرانية أثناء النزاعات المسلحة قد يكون تصرف غير عادل، والحقيقة أن هذا الفهم لا يمكن الاخذ به على اطلاقه، ذلك أن الحرب ومنذ زمن بعيد لم تكن عادلة بهذا المفهوم، لا احد يرى أن طرفاً ما لا يجوز له استخدام قواته الجوية أو البحرية إذا لم يكن لدى الطرف الأخر قوات جوية أو بحرية أو ليست لديه اسلحة مقاومة طائرات على سبيل المثال(٤٤).

ومن جهة أخرى وبما لا يدع مجالاً للشك، بأن استخدام التقنيات الحديثة، ومنها الهجمات السيبرانية أثناء النزاعات المسلحة قد تقلل بشكل كبير ما يمكن استخدامه من قبل البشر بشأن الالتفاف حول القواعد القانونية أو اتخاذ قرار من وجهة نظر نفعية بحتة، على الرغم مما تثيره الهجمات السيبرانية كما في بعض الاسلحة الاخرى أثناء النزاعات المسلحة من جدلية في العلاقة حول انطباق قواعد القانون الدولي الإنساني والقانون الدولي لحقوق الإنسان، ذلك أن مهاجمة هدف في اطار القانون الدولي الإنساني من موقع بعيد عن منطقة القتال الفعلي يثير مسألة السيادة لأي من القانونيين في مثل هذه الظروف(٤٥).

ووفقاً لما تقدم، فان استخدام التقنيات الالكترونية الحديثة، ومنها الهجمات السيبرانية في اطار النزاعات المسلحة، يجب أن لا تقيم مقابل فكرة مثالية افتراضية، بل يجب مقارنتها بالبشر في ضوء الظروف والالتباسات المحيطة أثناء النزاع المسلح، وحيثما نظرنا إلى القواعد الحالية للقانون الدولي الإنساني، والتي يقع في جزء كبير منها على مبدأ التدابير الاحتياطية المستطاعة، تلك الاحتياطات التي من الممكن أن تكون متاحة في الاستخدامات التقنية الحديثة(٤٦)، لاسيما اذا ما تم تطويرها لتفوق كفاءة البشر في الامتثال لقواعد القانون الدولي الإنساني من خلال وسائل تقنية بحيث تكون قادرة على الحصول على المعلومات التي تشير إلى ضرورة وقف الهجوم إذا ما تبين أن تلك الهجمات تشكل انتهاكاً لقواعد ذلك القانون وهي بذلك قد تحقق ميزة حتى على بعض الاسلحة التقليدية، ومنها على سبيل المثال عدم القدرة على الغاء أو تأجيل هجوم تم بواسطة المدفعية أو القذائف بعد اطلاقها، أي في اللحظات الاخيرة(٤٧).

(ISSN : 2537 - 0758)

واخيراً يمكن القول بأن وجود تلك التقنيات ووفرتها وقدرتها العسكرية يجب أن لا تفسر في جميع الاحوال بأن هناك ضرورة عسكرية لاستخدامها.

الخاتمة

بعد أن تطرقنا بشكل مختصر إلى العمليات السيبرانية كجزء من حدث عالمي مهم يتمثل في استحداث أجهزة الكومبيوتر كأداة لمعالجة وحفظ المعلومات رقمياً (Digital) وظهور الشبكة العنكبوتية (الانترنيت) كجزء من عملية التواصل ونقل المعلومات بسرعة فائقة عن طريق سيل من البيانات المرسلة عبر الاثير، وما يمكن أن تتجسد به الهجمات السيبرانية لتشكل جرائم داخلية، وبالتالي ضرورة معالجتها عن طريق تشريعات جزائية واخرى تنظيمية تقوم على تجريم الدخول غير المشروع إلى المواقع الالكترونية والأنظمة المعلوماتية والمملوكة للغير، ومن ثم التركيز على المستوى الدولي الذي يستلزم التعاون بين الدول لمكافحة تلك الجرائم وهي في الاغلب تطال مؤسسات مالية ومصرفية، فضلاً عن شركات متخصصة ببرمجة نظم الاتصالات.

وبعد تلك الإشارة، كان لا بد من البحث في الهجمات السيبرانية كجزء من التهديد على المستوى العسكري والسياسي أثناء النزاعات المسلحة، حيث اعطت تلك الهجمات تعريفاً مغايراً لوسائل القتال وطرائقها وهو ما كان مدار بحثنا الذي توصلنا من خلاله على النتائج والتوصيات التالية:-

١- من المبادئ المستقرة في القانون الدولي المعاصر، أن استخدام القوة أو التهديد بها في العلاقات الدولية يعد عملاً غير مشروع، إلا أن هناك مجموعة من الاطر التفسيرية المرتبطة بالهجمات السيبرانية يدور حول تفسير مصطلح القوة بين معيار يعتمد على العنصر الحركي للقوات المسلحة، واخر يشمل كافة صور استخدام القوة متى ما ترتب عليها انتهاك وتأثير واضح على الأمن القومي لدولة أخرى.

٢- أن تطبيق مبدأ التميز بين المقاتلين وغير المقاتلين على الهجمات السيبرانية للأغراض العسكرية لاسيما الهجومية، هي مسألة في غاية التعقيد بالقدر الذي يمكن تصوره أن يكون المهاجم في اغلب الاحيان بعيداً عن المكان المستهدف من الهجوم والتي قد تصل احياناً لمسافة تتجاوز الالاف الكيلومترات.

٣- أن عدم تحديد معايير ثابتة لاستخدام تكنلوجيا المعلومات والتي تشكل هجمات سيبرانية أثناء النزاعات المسلحة، سوف ينشئ تحدياً واضحاً أمام تطبيق مبدأ الضرورة العسكرية ذلك المبدأ الذي يتيح مهاجمة الأهداف العسكرية كخيار ضروري بالمرتبة الأولى، مع امكانية مهاجمة اعيان مدنية إذا كانت تسهم بطريقة غير مباشرة في تحقيق ميزة عسكرية اكيدة، الأمر الذي يكون أكثر تعقيداً بشأن الهجمات السيبرانية، حيث يكون من المرجح استهداف منشئات تقدم خدمة للجهد العسكري وفي الوقت ذاته تستهدف خدمة المدنيين.

٤- بدى لنا أن تأكيد احترام مبدأ التناسب على الهجمات السيبرانية لا يزال غامضاً، ذلك المبدأ الذي يستلزم الغاء أو تعليق آية هجوم إذا تبين أن الهدف المقصود ليس هدفاً عسكرياً أو انه مشمول بحماية خاصة، أو قد يحدث خلطاً من الخسائر أو الأضرار في المدنيين والاعيان المدنية تتجاوز ما ينتظر أو يسفر عنه ذلك الهجوم من ميزة عسكرية مباشرة.

٥- من النتائج التي توصلنا إليها وعلى الرغم مما تم الإشارة إليه سابقاً من صعوبات في تطبيق مبادئ وقواعد القانون الدولي الإنساني في شأن الهجمات السيبرانية، إلا انه في جميع الاحوال يجب أن لا تكون المقارنة وفقاً لحالة افتراضية مثالية فيما يتعلق بالحروب التقليدية، وبالتالي امكانية تطوير تلك البرامج لتتفق مع التطبيق الامثل لقواعد القانون الدولي الإنساني.

٦- اعطاء تفسير أوسع لمبادئ وقواعد القانون الدولي الإنساني، ومنها على سبيل المثال ما يعرف بشرط (مارتنز) لتشمل جميع الظروف المتغيرة، لاسيما تلك المتعلقة بوسائل واساليب القتال.

٧- اقرار مسؤولية الدولة على جميع التصرفات التي يقوم بها افراد أو مجموعات يعملون في ضوء تعليماتها أو تحت ادارتها أو سيطرتها، لتشمل جميع العناصر المساهمة في البرامج الالكترونية التي تشكل خرقاً لالتزام دولي، فضلاً عن المسؤولية الجنائية الفردية، والتمكين من الملاحقة القضائية لأشخاص يقفون وراء المرتكبين المباشرين لتلك الجرائم.

(ISSN : 2537 - 0758)

٨- ابرام اتفاقيات دولية تعمل على تقييد استخدام تكنلوجيا المعلومات بصورة هجمات سيبرانية، إذا كان من العسير برمجتها وفقاً للتطبيق الامثل لقواعد القانون الدولي الإنساني، وفي ضوء الموازنة بين المصالح القومية والدفاع عن النفس، وبين الآثار غير الإنسانية التي قد تتسبب بها تلك الهجمات.

٩- والى أن تعقد اتفاقية خاصة بشأن حظر أو تقييد الهجمات السيبرانية أثناء النزاعات المسلحة، التركيز في القياس على تصرفات أخرى حظرها القانون الدولي الإنساني.

١٠- وضع مقاربة منطقية بين الحروب التقليدية وما قد يصاحبها من مشاعر في الكره وحب الانتقام، وبين الحروب التي تكون فيها الهجمات السيبرانية وسيلة أو طريقة للقتال، لاسيما إذا ما تم تطويرها وبرمجتها وفقاً للامتثال السليم لقواعد القانون الدولي الإنساني.

الهوامش

١- د. احمد عبيس نعمة الفتلاوي، الهجمات السيبرانية: مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر، مجلة المحقق الحلي للعلوم القانونية والسياسية، جامعة بابل– كلية القانون، العدد الرابع، السنة الثامنة، ٢٠١٦، ص٦١٤.

2- Michael N. Schmitt, Computer network attack and the use of force in international law: Thoughts on a normative framework, Columbia journal of transnational law, 1998– 1999, Vol. 37, P890.

3- Philip Levitz, The law of cyber– Attack, 2012, Vol. 100, Issue 4, P833.

٤- عمرو رضا بيومي، مخاطر اسلحة الدمار الشامل الاسرائيلية على الأمن القومي العربي، ط١، دار النهضة العربية، ٢٠٠٢، ص٢٥.

٥- عمر بن عبد الله بن سعيد البلوشي، مشروعية اسلحة الدمار الشامل وفقاً لقواعد القانون الدولي، منشورات الحلبي الحقوقية، بيروت، ٢٠٠٧، ص ١٥–١٧.

٦- عمر مكي، القانون الدولي الانساني والارهاب، اللجنة الدولية للصليب الأحمر، ص٩٣.

7- Herbert Lin, Cyber conflict and international humanitarian law, International review of the red cross, 2012, Vol. 94, N886, P515.

٨- المادة (٥١) من ميثاق الأمم المتحدة.
٩- المادة (٤٢) من ميثاق الأمم المتحدة.
١٠-الفقرة (٤) من المادة (٢) من ميثاق الأمم المتحدة.
١١-علاء الدين حسين مكي خماس، استخدام القوة في القانون الدولي، المطابع العسكرية، بغداد، ١٩٨٢، ص٦٧.
١٢-المصدر السابق، ص٦٨.
١٣-المصدر السابق، نفس الصفحة.
١٤-سراب احمد ثامر، الهجمات على شبكات الحاسوب في القانون الدولي الانساني، أطروحة دكتوراه، جامعة النهرين– كلية الحقوق، بغداد، ٢٠١٥، ص١٠٧.
١٥-جوزيف ناي، المنازعات الدولية– مقدمة للنظرية والتاريخ، ترجمة احمد أمين الجمل ومجدي كامل، الجمعية المصرية لنشر المعرفة والثقافة العالمية، القاهرة، ١٩٩٧، ص٨٢.
١٦-الفقرة (٤) من المادة (٢) من ميثاق الأمم المتحدة.
١٧-افادات وكالة الاستخبارات الامريكية بتدخل روسيا في الانتخابات الرئاسية الامريكية لدعم (دونالد ترامب)، وان روسيا وراء الهجمات الالكترونية والقرصنة المعلوماتية التي طالت حسابات البريد الالكتروني لمرشحة الحزب الديمقراطي (هيلاري كلنتون)– ٢٠١٨/٨/١٠، موقع الكتروني، www.SaSapost.com .
18- Heather Harrison Dinniss, The status and use of computer network attacks in international law, Phd thesis, London school of a economics and Political science, 2008, P 33.
١٩-سراب ثامر احمد، مصدر سابق، ص٨٣– ٨٤.
٢٠-المادة (٣٦) من البروتوكول الاضافي الأول الملحق باتفاقيات جنيف لسنة ١٩٧٧.
21- Blinding weapons: Reports of the meetings of experts convened by the international committee of the red cross on battlefield laser weapons, 1989– 1991, ICRC, 1993, P 78.
22- Ibid, P22– 23.
٢٣-الفقرة (١) من المادة (٥٠) من البروتوكول الاضافي الأول الملحق باتفاقيات جنيف لسنة ١٩٧٧.

(ISSN : 2537 - 0758)

24- Hall William Edward, A Treatise on international law, Fourth edition, Oxford, London, 1895, PP 68– 69.

٢٥-الفقرة (٤) من المادة (٥١) من البروتوكول الاضافي الأول الملحق باتفاقيات جنيف لسنة ١٩٧٧.

٢٦-الفقرة الفرعية (ب) من الفقرة (٥) من المادة (٥١) وكذلك المادة (٥٧) من البروتوكول الاضافي الأول الملحق باتفاقيات جنيف لسنة ١٩٧٧.

٢٧-الفقرة (٣) من المادة (٥٧) من البروتوكول الاضافي الأول الملحق باتفاقيات جنيف لسنة ١٩٧٧.

٢٨-الفقرة (١) من المادة (٣٥) من البروتوكول الاضافي الأول الملحق باتفاقيات جنيف لسنة ١٩٧٧.

٢٩-الفقرة (٢) من المادة (٣٥) من البروتوكول الاضافي الأول الملحق باتفاقيات جنيف لسنة ١٩٧٧.

30- Jeffrey T. G Kelsey, Hacking in to international humanitarian law: The principles of distinction and neutrality in the age of cyber warfare, Michigan law review, 2008, Vol. 106, Issue7, P 1437.

٣١-مايكل شميت، الحرب بواسطة شبكات الاتصال: الهجوم على شبكات الكومبيوتر (الحاسوب) والقانون في الحرب، المجلة الدولية للصليب الأحمر، ٢٠٠٢، ص١٠٥.

٣٢-د. احمد عبيس نعمة الفتلاوي، مصدر سابق، ص٦٣٨.

٣٣-مايكل شميت، مصدر سابق، ص١٢١.

٣٤-المصدر السابق، ص١٣٠.

٣٥-المصدر السابق، ص١٣٥.

٣٦-هشام بشير، المدخل للقانون الدولي الانساني، ط١، المركز القومي للإصدارات القومية، القاهرة، ٢٠١٢، ص٨٩.

٣٧-سلوان جابر هاشم، حالة الضرورة العسكرية في القانون الدولي الانساني، ط١، المؤسسة الحديثة للكتاب، لبنان، ٢٠١٣، ص١٠٥.

٣٨-هنري ميروفيتز، مبدأ الآلام التي لا مبرر لها، دراسات في القانون الدولي الانساني، دار المستقبل العربي، القاهرة، ٢٠٠٩، ص٢٢.

٣٩-احمد الانور، قواعد وسلوك القتال، دراسات في القانون الدولي الانساني، دار المستقبل العربي، القاهرة، ٢٠٠٠، ص٣١٩.

٤٠-المادة (٣٠) من النظام الاساسي للمحكمة الجنائية الدولية.

41- Michael N. Schmitt & Jeffery S. Thumher, Autonomous weapon systems and the law of armed conflict, Harvard notional security journal, P 232.

٤٢-حدثت حالات اغتصاب جنسي في العديد من الحروب والنزاعات المسلحة، لاسيما النزاعات المسلحة غير الدولية حيث تتصارع طوائف عرقية أو دينية مختلفة مما يطغي على هذه الحروب حقد شديد ومقت كبير، ومنها ما حصل من اغتصاب واعتداء جنسي على النساء في كشمير وافغانستان ورواندا والصومال وادرفور ويوغسلافيا السابقة وكوسوفو وغيرها– رواء عطية، الاغتصاب في النزاعات المسلحة الدولية وغير الدولية كجريمة حرب وجريمة ضد الانسانية، موقع الكتروني ٢٠١٨/٨/١، www.m.ahewar.org.

٤٣-هناك سياسة في مجال الدفاع مفادها امتلاك دولة ما القوة العسكرية الكافية سوف يخيف عدداً محتملاً وتمنعه في الهجوم عليها، وهذا المفهوم يعد جوهرياً في سياسته الولايات المتحدة الامريكية، ولعل أهم وسيلة للروع هو مجرد الاسلحة النووية إلا انها لن تستعمل منذ نهاية الحرب العالمية الثانية– محمد يسري، هل يصبح السلاح النووي سبباً في تحقيق السلام، موقع الكتروني، ٢٠١٨/٨/١، http://raseef22.com.

٤٤-تعرف الحروب على انها: (مجموعة من العمليات الاجتماعية السلبية حيث تتسم بطابع الصراع التدميري العنيف، حيث تستخدم القوة المسلحة كل الوسائل لالحاق الضرر والاذى بالطرف الأخر)– موقع الكتروني، ٢٠١٨/٨/٣– www.marefa,org.

٤٥-القانون الدولي الانساني وفتوى محكمة العدل الدولية بشأن مشروعية التهديد بالأسلحة النووية أو استخدامها، اللجنة الدولية للصليب الأحمر، موقع الكتروني، ٢٠١٨/٨/١٠– www.icrc,org.

٤٦-نوال احمد بسيح، القانون الدولي الانساني وحماية المدنيين والاعيان المدنية في زمن النزاعات المسلحة، ط١، منشورات الحلبي الحقوقية، ٢٠١٠، ص٨٧.

٤٧-المصدر السابق، ص٩٨.

قائمة المصادر

أولاً: الكتب

(ISSN : 2537 - 0758)

١- عمرو رضا بيومي، مخاطر اسلحة الدمار الشامل الاسرائيلية على الأمن القومي العربي، ط١، دار النهضة العربية، ٢٠٠٢.
٢- عمر بن عبد الله بن سعيد البلوشي، مشروعية اسلحة الدمار الشامل وفقاً لقواعد القانون الدولي، منشورات الحلبي الحقوقية، بيروت، ٢٠٠٧.
٣- علاء الدين حسين مكي خماس، استخدام القوة في القانون الدولي، المطابع العسكرية، بغداد، ١٩٨٢.
٤- جوزيف ناي، المنازعات الدولية– مقدمة للنظرية والتاريخ، ترجمة احمد أمين الجمل ومجدي كامل، الجمعية المصرية لنشر المعرفة والثقافة العالمية، القاهرة، ١٩٩٧.
٥- هشام بشير، المدخل للقانون الدولي الانساني، ط١، المركز القومي للإصدارات القومية، القاهرة، ٢٠١٢.
٦- سلوان جابر هاشم، حالة الضرورة العسكرية في القانون الدولي الانساني، ط١، المؤسسة الحديثة للكتاب، لبنان، ٢٠١٣.
٧- نوال احمد بسيح، القانون الدولي الانساني وحماية المدنيين والاعيان المدنية في زمن النزاعات المسلحة، ط١، منشورات الحلبي الحقوقية، ٢٠١٠.

ثانيا: الدوريات والاطاريح والرسائل

١. د. احمد عبيس نعمة الفتلاوي، الهجمات السيبرانية: مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر، مجلة المحقق الحلي للعلوم القانونية والسياسية، جامعة بابل– كلية القانون، العدد الرابع، السنة الثامنة، ٢٠١٦.
٢. عمر مكي، القانون الدولي الانساني والارهاب، اللجنة الدولية للصليب الأحمر.
٣. مايكل شميت، الحرب بواسطة شبكات الاتصال: الهجوم على شبكات الكومبيوتر (الحاسوب) والقانون في الحرب، المجلة الدولية للصليب الأحمر، ٢٠٠٢.
٤. هنري ميروفيتز، مبدأ الآلام التي لا مبرر لها، دراسات في القانون الدولي الانساني، دار المستقبل العربي، القاهرة، ٢٠٠٩.
٥. احمد الانور، قواعد وسلوك القتال، دراسات في القانون الدولي الانساني، دار المستقبل العربي، القاهرة، ٢٠٠٠.
٦. سراب احمد ثامر، الهجمات على شبكات الحاسوب في القانون الدولي الانساني، أطروحة دكتوراه، جامعة النهرين– كلية الحقوق، بغداد، ٢٠١٥.

ثالثاً: المواثيق والاتفاقيات الدولية

١- ميثاق الأمم المتحدة لسنة ١٩٤٥.
٢- النظام الاساسي للمحكمة الجنائية الدولية لسنة ١٩٩٨.
٣- البروتوكول الاضافي الأول الملحق باتفاقيات جنيف لسنة ١٩٧٧.
رابعاً : المواقع الالكترونية .
١- www.SaSapost.com.
٢- https://raseefzz.com.
٣- www.marefa.org.
٤- www.icrc.org.

خامساً : المصادر الاجنبية .
1- Michael N. Schmitt, Computer network attack and the use of force in international law: Thoughts on a normative framework, Columbia journal of transnational law, 1998– 1999, Vol. 37.
2- Philip Levitz, The law of cyber– Attack, 2012, Vol. 100, Issue 4.
3- Herbert Lin, Cyber conflict and international humanitarian law, International review of the red cross, 2012, Vol. 94, N886.
4- Heather Harrison Dinniss, The status and use of computer network attacks in international law, Phd thesis, London school of a economics and Political science, 2008.
5- Hall William Edward, A Treatise on international law, Fourth edition, Oxford, London, 1895.
6- Jeffrey T. G Kelsey, Hacking in to international humanitarian law: The principles of distinction and neutrality in the age of cyber warfare, Michigan law review, 2008, Vol. 106, Issue7.
7- Michael N. Schmitt & Jeffery S. Thumher, Autonomous weapon systems and the law of armed conflict, Harvard notional security journal.

(ISSN : 2537 - 0758)

8- Blinding weapons: Reports of the meetings of experts convened by the international committee of the red cross on battlefield laser weapons, 1989– 1991, ICRC, 1993.