

الهجمات السيبرانية في ضوء أحكام قواعد القانون الدولي الإنساني والاتفاقيات الدولية Cyber attacks in light of the provisions of the rules of international humanitarian law and international conventions

سنوسي علي *

مخبر الدراسات القانونية، كلية الحقوق، جامعة بن خلدون- تيارت

Ali.snouci@univ-tiaret.dz

تاريخ القبول: 2023/02/01

تاريخ المراجعة: 2023/02/01

تاريخ الإيداع: 2022/11/29

ملخص:

تهدف هذه الورقة البحثية إلى معالجة الإشكاليات ذات الصلة بالحروب والهجمات الإلكترونية التي تنفذها الدول، أو تلك التي تقوم بها جهات فاعلة من دون الدول، وكذا مفهوم النزاع المسلح في إطار الحرب الإلكترونية، بالإضافة إلى مفهوم الهجمات الإلكترونية وكيفية إدارة الحرب الإلكترونية، من خلال التطرق لقواعد الاشتباك الإلكتروني فضلا عن صفة المقاتل الإلكتروني، وأخيرا ضرورة مراعاة مبادئ القانون الدولي الإنساني والاتفاقيات الدولية، ومسألة المقاتل الإلكتروني بالوسائل العسكرية الإلكترونية.

ومن أهم نتائج البحث: أن الحرب الإلكترونية تنطوي على أعمال عنف، وتندرج هذه الأعمال في تعريف القانون الدولي الإنساني. كما أنها الحرب الإلكترونية وسيلة من وسائل القتال المعاصرة، بدأت الدول تلجأ إليها في النزاعات الحديثة، وبالتالي تخضع للمادة 36 من البروتوكول الإضافي الأول.

كما أن الأشخاص الذين يساهمون في الحرب الإلكترونية يعدون مدنيين فاقدن للحماية طيلة مشاركتهم في تلك الهجمات، حيث تبقى الحرب الإلكترونية مفتوحة لكثير من المناقشات القانونية.

الكلمات المفتاحية: الهجمات الإلكترونية؛ القانون الدولي الإنساني؛ المقاتل الإلكتروني؛ الاتفاقيات الدولية؛ النزاعات الحديثة.

Abstract:

This research paper aims to address the problems related to wars and electronic attacks carried out by states, or those carried out by non-state actors, as well as the concept of armed conflict within the framework of electronic warfare, in addition to the concept of electronic attacks and how to manage electronic warfare, by addressing the rules Electronic engagement as well as the character of the electronic combatant, and finally the need to observe the principles of international humanitarian law and international conventions, and the issue of the electronic combatant by electronic military means. Among the most important results of the research: that electronic warfare involves acts of violence, and these acts fall within the definition of international humanitarian law. Electronic warfare is one of the contemporary means of warfare, which states have begun to resort to in modern conflicts, and is therefore subject to Article 36 of Additional Protocol I. People who participate in electronic warfare are considered unprotected civilians as long as they participate in these attacks, and electronic warfare remains open to many legal debates.

Keywords : cyber attacks; International humanitarian law; electronic fighter; international agreements; modern conflicts

* المؤلف المراسل.

مقدمة:

تثير الحرب الإلكترونية العديد من المسائل القانونية الشائكة ، والتي تحتاج إلى المزيد من البحث القانوني، شأنها شأن الأسلحة الحديثة التي تعتمد على التكنولوجيا، سواء كانت تدار عن بعد كالمطائرات المسيّرة أو تلك التي تنتقل عبر الفضاء السيبراني، كما هو الحال في الحرب الإلكترونية .

وعلى هذا، فإن الحرب الإلكترونية دفعت فقهاء القانون الدولي إلى دراسة تلك الحرب، من خلال مقاربتها مع القواعد القابلة للتطبيق في النزاعات المسلحة، تلك القواعد المتعلقة بمفهوم الحرب وموقف القانون الدولي الإنساني من الأسلحة الحديثة، ومدى تطابق مفهوم المقاتل على المهاجم الإلكتروني والمدنيين المساهمين في الحرب الإلكترونية. إن هذا البحث محاولة بحثية متواضعة لدراسة الحرب الإلكترونية، في ضوء المستجدات الفقهية في هذا المجال، بالرغم من أن موضوع الحرب الإلكترونية تم التطرق إليه بعمومية، في بدايات القرن الماضي.

حيث يركز البحث على العلاقة بين مبدأ التمييز والحرب الإلكترونية لبيان مدى تطابق متطلبات هذا المبدأ مع تلك الحرب، مبدأ التمييز الذي يحتل مكان الصدارة في القانون الدولي الإنساني ومنه تتفرع المبادئ الأخرى حيث تكمن أهمية مبدأ التمييز في أن احترام هذا المبدأ من قبل المقاتلين، ويترتب عليه منحهم امتيازات المقاتلين المتمثلة بنظام أسرى الحرب عند القبض عليهم، وعدم محاكمتهم عن المشاركة في القتال .

علاوة على ما تقدم تبرز أهمية مبدأ التمييز في جانب آخر يتمثل بالأسلحة الحديثة ، حيث أن القانون الدولي الإنساني يحظر على الدول تصنيع أو استيراد أسلحة من شأنها أن تخل بمبدأ التمييز، ويؤدي استعمالها إلى حدوث الهجمات العشوائية، أو التسبب بالألام غير المبررة.

إن الحرب الإلكترونية وما تتضمنه من تكنولوجيا، أصبحت وسيلة قتالية تلجأ إليها بعض الدول في النزاعات المسلحة، مبررة بأن تلك الوسائل كفيلة بتجنب الخسائر العرضية في الممتلكات والأرواح، لأن التكنولوجيا أصبحت وسيلة قتالية في النزاعات الحديثة، فأصبح من الضروري البحث في مدى استيفاء تلك الوسائل لمتطلبات القانون الدولي الإنساني في مسألة الأسلحة الحديثة.

ويأتي هذا البحث كمحاولة قانونية متواضعة لاستكشاف التحديات التي تواجه القانون الدولي الإنساني في زمن النزاعات المسلحة المعاصرة، تلك التحديات التي بدأت تثير العديد من الاسئلة حول مدى فعالية القواعد الحالية لتستجيب لمتطلبات تلك النزاعات، ولأن من وضع تلك القواعد لم يكن يتوقع المستجدات في النزاعات المسلحة، والوسائل الجديدة التي تلجأ إليها الدول، ومع ذلك تبقى تلك القواعد الحارس الأمين لحماية الفئات الضعيفة التي تجد نفسها تكوى بويلات النزاعات المسلحة.

والإشكال الذي يطرح هنا: هل تعد تلك الحروب هجمات دفاعية أم هجومية تنذر بوجود نزاع مسلح ؟ وهل يحق للدول التصدي لها بالمثل، وموقف القانون الدولي الإنساني والاتفاقيات الدولية من هذه المسألة.

بناء على هذا، قسمنا البحث وفق خطة وصفية تحليلية كالآتي:

مبحث أول: الإطار المفاهيمي للحرب الإلكترونية والنطاق القانوني الحاكم لها.

مبحث ثان: النطاق القانوني للحرب الإلكترونية على ضوء قواعد القانون الدولي الإنساني والاتفاقيات الدولية ذات

الصلة.

1- الإطار المفاهيمي للحرب الإلكترونية والنطاق القانوني الحاكم لها.

حظيت المسائل القانونية التي أثارها احتمال شن عمليات عدائية في الفضاء الإلكتروني وعبره باهتمام كبير للغاية خلال السنوات الماضية، فقد أوجد هذا الفضاء على ما يبدو ميدانا جديدا للقتال وساحة جديدة للحرب من صنع الإنسان تضاف إلى ساحاتها الطبيعية المتمثلة في الأرض والجو والبحر والفضاء الخارجي وترتبط بجميع هذه الساحات الطبيعية. ومنه سنعالج إشكالية مفاهيم الحرب الباردة، وأهم تعريفاتها مع بيان النطاق القانوني الذي يحكمها.

1.1- مفهوم الحرب الإلكترونية فقها وقانونا.

نتناول في هذا المطلب التعريف بالحرب الإلكترونية بينما يتناول المطلب الثاني موقف القانون الدولي الإنساني من الأسلحة الجديدة، وذلك لتحديد العلاقة بين الحرب الإلكترونية كسلاح جديد واليات القانون الدولي الإنساني لتقييم مدى مطابقة الأسلحة الجديدة للقانون الدولي الإنساني.

1.1.1- تعريف الحرب الإلكترونية.

إن المشكلة الأساسية في إيجاد تعريف مقبول لا يتأتى من غياب الإجماع بين فقهاء القانون الدولي على تعريف موحد للحرب الإلكترونية، بل كذلك من الطبيعة القانونية المتغيرة لمصطلحات متطورة ظهرت في الآونة الأخيرة في سياق النزاعات المسلحة مثل الهجمات الإلكترونية عن طريق الشبكة العنكبوتية، ويرجع السبب في ذلك أن الهجمات على شبكات الحواسيب هي ظاهرة حديثة نسبيا، وقد تم وصفها بأنها عمليات تهدف إلى تعطيل، أو منع أو تحليل أو تدمير المعلومات في أجهزة الكمبيوتر، وشبكات الإنترنت وقد تكون الحرب موجهة ضد صناعات وبنى تحتية و شبكات اتصالات، أو ضد بلدان بأكملها.

وجدير بالقول أنه ليس هناك إجماع على تعريف محدد ودقيق لمفهوم الحرب الإلكترونية، وعلى الرغم من ذلك، فقد اجتهد عدد من الخبراء حسب اختصاصاتهم في تقديم تعريف يحيط بهذا المفهوم، فعرف كل من "ريتشارد كلارك" و"روبرت كناكي" الحرب الإلكترونية على أنها "أعمال تقوم بها دولة تحاول من خلالها اختراق أجهزة الكمبيوتر والشبكات التابعة لدولة أخرى بهدف تحقيق أضرار بالغة أو تعطيلها"⁽¹⁾

فيما يعرف آخرون مصطلح الحرب الإلكترونية بأنها "مفهوم يشير إلى أي نزاع يحدث في الفضاء الإلكتروني ويكون له طابع دولي". ولأن مثل هذه التعريفات فضفاضة ولا تعبر بدقة عن فحوى الموضوع، يقترح آخرون أن يتم التركيز بدلا من ذلك على أنواع وأشكال النزاع التي تحصل في الفضاء الإلكتروني، ومنها⁽²⁾.

(1) : Richard A. Clarke & Robert knake, Cyber War, HarperCollins (2010), p:6.

(2) . Myriam Dunn Cavelty, Cyberwar: Concept, Status, Quo, And Limitations, CSS Analysis In Security Policy, CSS ETH Zurich, No.71, April 2010, At This Link: www.Sta.Ethz.Ch/Content/Download/906/6864/Version/1/File/CSS_Analysis_71.Pdf

- القرصنة الإلكترونية: أو التخريب الإلكتروني، وتقع في المستوى الأول من النزاع في الفضاء الإلكتروني، وتتضمن هذه العمليات القيام بتعديل أو تخريب أو إلغاء المحتوى. ومن أمثلته القيام بعمليات قرصنة المواقع الإلكترونية أو تعطيل الحواسيب الخادمة أو ما يعرف باسم الملقّات (Servers) من خلال إغراقها بالبيانات.

- الإرهاب الإلكتروني: ويقع في المستوى الرابع من النزاع في الفضاء الإلكتروني. ويستخدم هذا المصطلح لوصف الهجمات غير الشرعية التي تنفذها مجموعات أو فاعلون غير حكوميين ضد أجهزة الكمبيوتر والشبكات والمعلومات المخزنة. ولا يمكن تعريف أي هجوم إلكتروني بأنه إرهاب إلكتروني إلا إذا انطوى على نتائج تؤدي إلى أذى مادي للأشخاص أو الممتلكات وإلى خراب قدر كبير من الخوف.

بينما يعرف شايفكفورد حرب المعلومات بقوله: "حرب المعلومات يقصد بها توظيف أجهزة الحاسب وكل ما يتعلق بتكنولوجيا المعلومات لمهاجمة شبكات الإنترنت ذات الصلة بمصادر المعلومات المدنية أو العسكرية أو الحكومية للخصم".⁽¹⁾

2.1.1. خصائص الحرب الإلكترونية.

إن الحرب الإلكترونية هي المستوى الأخطر للنزاع في الفضاء الإلكتروني، وتعتبر جزءا من الحرب المعلوماتية بمعناها الأوسع، وتهدف إلى التأثير على إرادة الطرف المستهدف السياسية وعلى قدرته في عملية صنع القرار، وكذلك التأثير فيما يتعلق بالقيادة العسكرية و/أو توجهات المدنيين في مسرح العمليات الإلكتروني، ومن المتوقع أن تصبح الحرب الإلكترونية نموذجا تسعى إليه العديد من الجهات نظرا للخصائص العديدة التي تنطوي عليها، ومنها:

- حروب الإنترنت هي حروب لا تناظرية (Asymmetric): فالتكلفة المتدنية نسبيا للأدوات اللازمة لشن هكذا حروب يعني أنه ليس هناك حاجة لدولة ما مثلا أن تقوم بتصنيع أسلحة مكلفة جدا كحاملات الطائرات والمقاتلات المتطورة لتفرض تهديدا خطيرا وحقيقيا على دولة مثل الولايات المتحدة الأمريكية على سبيل المثال.⁽²⁾

- تتمتع المهاجم بأفضلية واضحة: في حروب الإنترنت يتمتع المهاجم بأفضلية واضحة وكبيرة على المدافع، فهذه الحروب تتميز بالسرعة والمرونة والمراوغة، وفي بيئة مماثلة يتمتع بها المهاجم بأفضلية، من الصعب جدا على عقلية التحصن لوحدها أن تتجح، فالتحصين بهذا المعنى سيجعل من هذا الطرف عرضة لمزيد من محاولات الاختراق وبالتالي المزيد من الضغط.

- فشل نماذج "الردع" المعروفة: يعد مفهوم الردع الذي تم تطبيقه بشكل أساسي في الحرب الباردة غير ذي جدوى في حروب الإنترنت. فالردع بالانتقام أو العقاب لا ينطبق على سبيل المثال على هذه الحروب. فعلى عكس الحروب التقليدية حيث ينطلق الصاروخ من أماكن يتم رصدها والرد عليها، فإنه من الصعوبة بمكان بل ومن المستحيل في كثير من الأحيان تحديد الهجمات الإلكترونية ذات الزخم العالي. بعض الحالات قد تتطلب أشهرا لرصدها وهو ما يلغي مفعول

(1) : باباناستاسيون أفروديتي ، تطبيق القانون الدولي في عمليات الحرب السيبرانية ، كلية الحقوق بجامعة ليستر ، 2010 ، ص. 7.

(2) : William J. Lynn III, Defending a New Domain: The Pentagon's Cyberstrategy, Foreign Affairs, September-October 2010, p:98.

الردع بالانتقام وكثير من الحالات لا يمكن تتبع مصدرها في المقابل، وحتى إذا تم تتبع مصدرها وتبين أنها تعود لفاعلين غير حكوميين، فانه في هذه الحالة لن يكون لديهم أصول أو قواعد حتى يتم الرد عليها.⁽¹⁾

- المخاطر تتعدى استهداف المواقع العسكرية: لا ينحصر إطار حروب الإنترنت باستهداف المواقع العسكرية، فهناك جهود متزايدة لاستهداف البنى التحتية المدنية والحساسة في البلدان المستهدفة، وهو أمر أصبح واقعياً في ظل القدرة على استهداف شبكات الكهرباء والطاقة وشبكات النقل والنظام المالي والمنشآت الحساسة النفطية أو المائية أو الصناعية بواسطة فيروس يمكنه إحداث أضرار مادية حقيقية تؤدي إلى انفجارات أو دمار هائل.

وتشير العديد من التقارير إلى تزايد أعداد الهجمات الإلكترونية التي تتم في العالم اليوم والتي تقوم بها مجموعات أو حكومات تندرج في الاستهداف من أبسط المستويات إلى أكثرها تعقيداً وخطورة.

ويجمع الخبراء على أنّ الهجوم الإلكتروني الذي استهدف أستونيا في العام 2007، يكاد يكون الهجوم الإلكتروني الأول الذي يتم على هذا المستوى ويستخدم لتعطيل المواقع الإلكترونية الحكومية والتجارية والمصرفية والإعلامية مسبباً خسائر بعشرات الملايين من الدولارات إضافة إلى شلل البلاد. وعلى الرغم من أنّ الشكوك كانت تحوم حول موسكو على اعتبار أنّ الهجوم جاء بعد فترة قصيرة من خلاف أستونيا-روسيا، إلا أنّ أحداً لم يستطع تحديد هوية الفاعل الحقيقي أو مصدر الهجوم الذي تم، وهي من المصاعب والمشاكل التي ترتبط بحروب الإنترنت إلى الآن.⁽²⁾

وفي عام 2007 قامت إسرائيل بتوجيه هجمات الكترونية ضد سوريا تمكنت من خلالها تعطيل منظومة الصواريخ المضادة للطائرات مما مكّنها من توجيه ضربات إلى المفاعل النووي السوري السري⁽³⁾، كما تعرضت شبكات الإنترنت الحكومية والبنكية الاستونية في 2007، وفي سنة 2008 شنت روسيا هجوماً الكترونياً ضد جورجيا⁽⁴⁾، وما تعرضت إليه المنشآت النووية الإيرانية عن طريق توجيه فيروس أطلق عليه (Stuxnet) في 2010 والذي يعتبر أول فايروس يصيب أجهزة السيطرة في معدات التصنيع المسؤولة عن السيطرة الحساسة في تلك الأجهزة.⁽⁵⁾

ولا بد من التمييز بين حرب المعلومات وعمليات المعلومات، حيث تعرف العمليات المعلوماتية بأنها: "الاعمال التي تنفذ للتأثير على معلومات العدو ونظم معلوماته، في نفس الوقت حماية المعلومات ونظم المعلومات الخاصة بالمهاجم، وتشمل هذه العمليات في الواقع أي إجراءات تتخذ بغير رضا متبادل هدف اكتشاف العمليات المخزنة في أحد أجهزة الحاسوب أو تغييرها أو تدميرها أو تشويهها أو تحويلها أو البيانات التي تستخدم أو تنقل عن طريق أحد الأجهزة. ويمكن ان يحدث ذلك في أوقات السلم أو في الأزمات على حد سواء، أو على المستويات الإستراتيجية أو العملياتية أو التكتيكية في

(1): مارتن سي ليبكي، الردع الإلكتروني والحرب الإلكترونية، راند، 2009، ص: 39-64.

(2): جريج برونو، The Evolution of Cyber Warfare، مجلس العلاقات الخارجية، 27 فبراير 2008، نقلاً عن: W w w .cfr.org

evolution_of_cyber_warfare.html/15577/

(3): Max Blumenthal، international humanitarian law for cyber-warfare، School of international Service the American university، 2011، p2.

(4): يوهان Christoph Woltag -، عمليات شبكات الكمبيوتر تحت مستوى القوة المسلحة، الجمعية الأوروبية للقانون الدولي، سلسلة أوراق المؤتمرات، ورقة المؤتمر رقم 1/2011، 2011، P3-5.

(5): حادث جورجيا يعد الأول من نوعه يحدث خلال عمليات عسكرية، حيث حدث أثناء النزاع الروسي الجورجي عام 2008، العمليات المستخدمة كانت تضم تشويه شبكات الانترنت الذي استخدم في الهجمات على إستونيا.

نزاع مسلح". أما حرب المعلومات فأضيق من ذلك، فهي عمليات معلوماتية تجري أثناء الأزمات أو النزاع لتحقيق أو تعزيز أهداف معينة إزاء عدد أو أعداد محددين، لذلك تختلف حرب المعلومات عن العمليات المعلوماتية الأخرى من حيث السياق الذي تجري فيه، وهي الأزمات أو المنازعات⁽¹⁾، كما تميز عن الهجمات الحركية، حيث تهدف الأخيرة إلى تحقيق أهداف مادية كالسيطرة على أرض الخصم، بينما الهجمات الإلكترونية لا تؤدي حتماً إلى نتائج مادية ملموسة على أرض الدولة المستهدفة.

كما أن الهجمات الإلكترونية تدار عن بعد ولها أهداف متعددة، فقد يكون الهدف من الهجوم أو سلسلة الهجمات تحقيق أهداف بسيطة للمهاجم كإيقاف شبكة المعلومات المستهدفة لوقت قصير، وذلك لمنع الدولة المستهدفة من الاستفادة من هذه الشبكة، وبالتالي تفويض نظام الأمن فيها⁽²⁾.

وعرف التقرير الحادي والثلاثين للجنة الدولية للصليب الأحمر العمليات السيبرانية "المعلوماتية" بأنها: "عمليات تشن ضد أو عبر حاسوب أو نظام حاسوبي بواسطة بيانات اخراق مخصصة للغرض وقد تهدف هذه العمليات إلى تحقيق أغراض مختلفة تضم على سبيل المثال اختراق نظام معين وجمع أو نقل أو تدمير أو تغيير أو تشفير البيانات، أو إجراء أو تعديل العمليات التي يتحكم بها الجهاز الحاسوبي المخترق أو التلاعب بهذه العمليات، ويمكن بالتالي استخدام هذه الوسائل لتدمير أو تعديل أو تعطيل مجموعة متنوعة من الأهداف في العالم الحقيقي، كالصناعات والبنى الأساسية والاتصالات المالية"⁽³⁾. مع العلم أن الاتفاقية الوحيدة التي عرفت هجمات المعلومات هي اتفاقية جرائم الإنترنت⁽⁴⁾، إلا أن عدم تبني الاتفاقية من عدد كبير من الدول لم يجعلها ملزمة بموجب القانون الدولي العرفي، علاوة على أنها لا تتعلق بهجمات الإنترنت بقدر تعلقها بكيفية مواءمة التشريعات الوطنية للدول الموقعة للاتفاقية، وتشريع قوانين مناسبة لتجريم الأعمال المتعلقة بأساء استخدام الإنترنت⁽⁵⁾.

ونتيجة للتطور المطرد لتكنولوجيا المعلومات، وغياب القواعد القانونية التي تحظر حرب المعلومات في القانون الدولي، هذا الغياب يشير إلى وجود تصريح ضمني بها، مما يدفعنا إلى البحث عن وثائق قانونية دولية يمكن ان تساعد في إيجاد قواعد تحظر تلك الحرب ومحاولة لإيجاد نطاق قانوني أدرجت هجمات الإنترنت في معاهدة الاتصالات الدولية، والتي تطبق على الاتصالات السلكية واللاسلكية الدولية، إلا انه يمكن تطبيق بعض القواعد الواردة في الاتفاقية الدولية

(1) : أسامة صبري محمد، الحرب الإلكترونية ومبدأ التمييز في القانون الدولي الإنساني، مقال منشور على شبكة النت،

10.10.2021 ، 3265966www.assrn.com/abstract=1

(2) : John Richardson , Stuxnet as cyberwarfare : Applying the law of war to the Virtual attlefield ,JMR Portfolio Intelligence,2011,p9. Available at www.assrn.com/abstract=1892888

(3) : الهجمات على شبكات الحاسوب، سواء التي قد تصل الى مستوى حرب المعلومات او التي تكون مجرد عمليات معلوماتية عبارة عن عمليات لا يقاع الفوضى في المعلومات الموجودة في اجهزة الحاسوب او شبكات الحاسوب او الاجهزة او الشبكات نفسها او نفخها او الانتقاص من شأنها او تدميرها وجوهر الهجمات على شبكات الحاسوب بغض النظر عن الاطار الذي تجري فيه ، انها تعتمد على تيار من البيانات لتنفيذ الهجوم.

(4) : مايكل ن . شميث ، الحرب بواسطة شبكات الاتصال الهجوم على شبكات الكمبيوتر (الحاسوب) والقانون في الحرب ، المجلة الدولية للصليب الاحمر ، مختارات من اعداد 2002.

(5) : القانون الدولي الانساني وتحديات النزاعات المسلحة المعاصرة ، التقرير الحادي ، والثلاثين ، 2011 لاتفاقية هي أول معاهدة دولية بشأن الجرائم التي ترتكب عبر شبكة الانترنت وشبكات الكمبيوتر الأخرى، والتعامل بشكل خاص مع التعدي على حق المؤلف، ذات الصلة بالحاسوب الاحتيال، و المواد الإباحية، جرائم الكراهية وانتهاكات أمن الشبكة. نقلا عن : Michael Geraiis,cyber attacks and the law of war, yale university law school ,October 1,2011,p7.

على هجمات الإنترنت كتلك المتعلقة بمحطات الاذاعة وعدم جواز تداخل ارساليها مع ارسالات الدول الأخرى دون موافقة الأخيرة، بالإضافة إلى واجب الدول في حماية خصوصية أجهزة الإرسال الدولية الإرسال الـ لا يجوز لتلك الدول إيقاف العمل بتلك الإذاعات لأ سباب أمنية.

2.1- أصناف ومسارح الحروب الإلكترونية ضمن قواعد القانون الدولي الإنساني .

لا جدال أن حق المقاتلين في اختيار وسائلهم القتالية وأساليبهم في المعركة ليست مطلقة بل هي مقيدة بالعديد من قواعد القانون الدولي الإنساني المتعلقة بأسلوب القتال، العديد منها يتضمنه البروتوكول الإضافي الأول الملحق باتفاقيات جنيف لعام 1977 ، وهناك عدد من الاتفاقيات التي تحظر أو تقيد استخدام نوع معين من الأسلحة مثل الأسلحة الكيميائية والبيولوجية والأسلحة الليزر التي تسبب العى⁽¹⁾، كما توجد العديد من القواعد العرفية في القانون الدولي التي تحظر أو تمنع بعض اساليب ووسائل القتال⁽²⁾ .

1.2.1- أصناف الحرب الإلكترونية.

- الهجوم الإلكتروني: وهو استخدام الطاقة الكهرومغناطيسية، أو الطاقة الموجبة لمهاجمة الأفراد أو المعدات؛ لغرض إضعاف قدرتها.

- الحماية الإلكترونية: وهي اتخاذ تدابير لحماية الأفراد والمعدات والمرافق من أي تأثير ناشئ من جراء استخدام الحرب الإلكترونية؛ سواء كان من قبل قوات صديقة، أو معادية.

- الإسناد الإلكتروني: وهي عمليات بحث عن مصادر الطاقة الكهرومغناطيسية، وتتبع مصادرها؛ سواء كان انبعاثها متعمداً، أم لا.

2.2.1- مسارح الحرب الإلكترونية.

تعتمد الحرب الإلكترونية على استخدام وسائل ونظم إلكترونية تُتيح استغلال الحيز الكهرومغناطيسي لصالح طرف، وجرمان أو خداع الطرف الآخر، وتختلف هذه الوسائل باختلاف مسرح العمليات كالآتي:

- مسرح العمليات البرية: استخدام نظم تقدير المسافة بالليزر وبواعث الأشعة؛ لتحديد الأهداف بدقة، وتوجيه وإدارة نيران الأسلحة بدقة عالية، فضلاً عن استخدام نظم الذخيرة الموجهة بالليزر أو التليفزيون أو الأشعة، كما تتطلب معركة الأسلحة الحديثة كذلك استخدام مستشعرات تضم شبكة حاسبات إلكترونية ترصد المعلومات للأهداف، وتحللها ثم توجه نيران الأسلحة المختلفة نحوها لتدميرها، وهذه المستشعرات ذات تأثير مغناطيسي أو حراري، أو صوتي أو ضوئي؛ للكشف عن تحركات الأسلحة والمعدات في ميدان القتال البري.

(1) : اتفاقية لاهي لعام 1907 واتفاقية حظر استحداث وانتاج وتخزين الأسلحة البكتريولوجية وتدمير تلك الأسلحة 1972 واتفاقية حظر استخدام تقنيات التغيير في البيئة لأغراض عسكرية أو لاية اغراض عدائية أخرى 1976 واتفاقية حظر أو تقييد استعمال اسلحة تقليدية معينة يمكن اعتبارها مفرطة الضرر أو عشوائية الاثر والبروتوكول الخامس الملحق باتفاقية حظر أو تقييد استعمال اسلحة تقليدية معينة يمكن اعتبارها مفرطة الضرر أو عشوائية الاثر. 2003.

(2) : دليل قانون الأسلحة والوسائل والأساليب الجديدة للحرب ؛ تدابير تنفيذ المادة 36 من البروتوكول الإضافي لعام 1977 ، اللجنة الدولية للصليب الأحمر، جنيف، يناير 2006، تقارير ووثائق، المراجعة الدولية للصليب الأحمر، المجلد 88 ، العدد 864 ديسمبر 2008 ، الصفحة 932.

- مسرح العمليات البحرية: تقوم نظم الاستطلاع الإلكتروني المحمولة جواً، وفي الفضاء الخارجي، والمتصلة بوحدات الأسطول بمعاونة السفن الحربية والغوّاصات؛ لإصابة أهدافها فوق الأفق (horizon over the)، كما أنه بمقدور وحدات مكافحة الغواصات - من طائرات، وسفن، وغوّاصات - مسح قاع البحار باستخدام الأجهزة الإلكترونية - موجات السونار الردارية - للكشف عن الغوّاصات والألغام البحرية المعادية في الأعماق.

- مسرح العمليات الجوية: باستخدام نظم الإنذار المبكر، ونظم التوجيه الأرضية والمحمولة جواً وفي الأقمار الصناعية بالإبلاغ الفوري عن أيّ اختراقات جوية معادية لأجواء الدولة، وتوجيه المقاتلات الصديقة لإصابة أهدافها في الجو، وكذلك رغبة النظم الاستطلاعية الإلكترونية المحمولة جواً للتحركات المعادية في مسرح العمليات، وإخطار عُرف العمليات الرئيسية بها في حينه.

- مسرح العمليات الفضائية: إنّ للفضاء القريب الذي فرض نفسه بُعداً إستراتيجياً رابعاً، ليس مجرد مجال لعبور السفن الفضائية أو الصواريخ الباليستية، إنما هو أساساً مجالاً رحباً غير محدود، يمنح لمن يملكه قدرة عالية، تتمثل في جمع المعلومات باستخدام أجهزة المراقبة في الأقمار الصناعية والسفن الفضائية، والتي يُمكنها أن ترصد فعلياً كلّ ما يحدث في منطقة ما من العالم، وكذلك معالجة المعلومات والسيطرة على وسائل الاتصال، وهو ما يجعل من البيانات شيئاً مفهوماً ومفيداً تعرضه على شاشة تحدّد أهدافاً للصواريخ والمقذوفات، مثل: الأهداف الصغيرة كالدبابات، أو التصرف وفقاً لأهمية وحجم المعلومات في شتى الغارات الجوية بعيدة المدى وبالغة الدقة؛ لتدمير الأهداف بأقمار صناعية تصل دقتها إلى حدٍّ أن تُدمّر مبنى صغيراً على بُعد مئات الأميال، كما حدث أخيراً في العراق وأفغانستان

2- النطاق القانوني للحرب الإلكترونية على ضوء قواعد القانون الدولي الإنساني والاتفاقيات الدولية ذات الصلة.

ابتداء لا توجد قواعد قانونية في اتفاقيات القانون الدولي الإنساني تتعامل بشكل مباشر مع الهجمات الإلكترونية، لأن هذه الأخيرة - الهجمات الإلكترونية- والعمليات الإلكترونية غير منظمة في النزاعات المسلحة، إضافة إلى أن تطوير الهجمات الإلكترونية حصل في فترة لاحقة على إعداد صكوك القانون الدولي الإنساني، كما أن هذا القانون وضعت قواعده لتنظيم وسائل وأساليب القتال ذات الطبيعة المتحركة التي تنتج عنها آثار مادية غير متوفرة في الهجمات الإلكترونية، وبالتالي فإن الهجمات الإلكترونية تكون خارج نطاق القانون الدولي الإنساني، أي بعبارة أخرى أن القانون الدولي الإنساني يطبق أثناء النزاعات المسلحة، والهجمات الإلكترونية ليست مسلحة، ولكن يمكن تطبيق شرط مارتنز على الهجمات الإلكترونية⁽¹⁾. مع ذلك فإن غياب القواعد المتعلقة بصورة خاصة بالهجمات الإلكترونية لا يعني أن مثل هذه الهجمات لا تخضع لقواعد القانون الدولي الإنساني لأن وسائل وأساليب الحرب الإلكترونية تنتج نفس الآثار التي تنتجها الأسلحة التقليدية كأحداث الدمار أو إصابة الأفراد بجروح أو التسبب بالموت، فأنها تخضع لنفس القواعد التي تحكم الأسلحة التقليدية، إلا أنه مازالت هناك صعوبة في تطبيق تلك القواعد على الحرب الإلكترونية.

معلى هذا سنتطرق إلى التكييف القانوني للهجمات الإلكترونية، تم نبين موقف المعاهدات الدولية من هذه الهجمات.

(1) : Marco Roscint , World Wide Warfare – Jus ad bellum and the use of cyber Force , Max Planck Yearbook of United Nations Law , VOL.14,2010,p95.

1.2- التكييف القانوني للهجمات الإلكترونية في القانون الدولي الإنساني؟

إن القواعد القانونية الخاصة بالهجمات الإلكترونية لا تشتق من القانون الدولي الإنساني، بل من المبادئ والقواعد المشتقة من القانون الدولي وقت السلم، ومن قواعد حقوق الإنسان التي لا تلزم الدول فقط بل الجماعات المسلحة أيضاً⁽¹⁾ والسؤال القابل للطرح هنا، هل تعد الهجمات الإلكترونية هجمات مسلحة؟

عرفت المادة 49 فقرة 1 وفقرة 2 من البروتوكول الإضافي الأول الملحق باتفاقيات جنيف الهجوم بأنه: "1..-وتعني الهجمات أعمال العنف الهجومية والدفاعية ضد الخصم، 2-تنطبق أحكام هذا الحق البروتوكول المتعلقة بالهجمات على كافة الهجمات في أي إقليم تشن منه بما في ذلك الإقليم الوطني لأحد أطراف النزاع والواقع تحت سيطرة الخصم".

استناداً إلى هذا التعريف، أن الهجمات لا تقتصر على استعمال السلاح بل يمكن أن تمتد إلى الوسائل التي يشكل اللجوء إليها عمل عدائياً.

وتجيب الأستاذة Ziolkowski⁽²⁾ على ذلك التساؤل الذي طرحناه سلفاً بالقول: "تعد الهجمات الإلكترونية شبه هجمات عسكرية، إذا تأثر أفراد أو الممتلكات"، وتضيف: "بالرغم من النقص في القواعد المنظمة للهجمات الإلكترونية، يلاحظ أن البروتوكول الإضافي يشير إلى أنه قابل للتطبيق في الظروف التي لم تؤخذ بنظر الاعتبار في المؤتمر الدبلوماسي 1977، فعلى سبيل المثال المادتين 38 و 39 من البروتوكول الإضافي الأول والمادة 12 من البروتوكول الإضافي الثاني، التي تحظر إساءة استعمال الشارة المميزة أو إخفاء العلامات الإلكترونية، مع ذلك يمكن أن نعد الهجمات الإلكترونية خاضعة لحظر الغدر، الذي ورد في المواد 37 و 48 من البروتوكول الإضافي الثاني والمادة 13 من البروتوكول الإضافي الثاني⁽³⁾،

ويذهب الأستاذ Zemanek⁽⁴⁾ إلى القول: "ليس تصميم الآلة أو الاستخدام الطبيعي لها تجعل منه سلاحاً، بل نية المستخدم في توظيف تلك الآلة في إحداث أضرار، وعليه فإن استخدام الآلات استخداماً من شأنه تدمير الممتلكات أو إحداث أضرار بالأنفس، عندها تستوفي متطلبات النزاع المسلح، ذلك الاستنتاج تم تأييده عند إعادة مجلس الأمن التأكيد على حق الدفاع عن النفس بعد أحداث 11 سبتمبر 2001. فإذا أمكن التوصل إلى مثل هذا التوافق بين الدول، فإن تطبيق الاتفاقية سيواجه بتحديات تقنية سلبية، أي فرض لتلك البنود يحتاج مشاركة عامة وخاصة، وجهود تبذل للتمييز بين الدول والجماعات المسلحة، والحاجة إلى تشريعات لتفعيل بنود الاتفاقية⁽⁵⁾."

2.2- الحرب الإلكترونية ونصوص اتفاقيات الدولية.

(1) :Dieter Fleck , technological challenges in armed conflicts and areas of regulation ,p5.

(2) : أستاذة في جامعة كولومبيا.

(3) : نقلا عن : Konstantin Meljnik and Stefan Weiss, conference report 30 years additional protocols to the 1949 Geneva Conventions, past, present and future, German Law Journal, VOL.09 NO.10, 2008.p1363 .

(4) : هاينز زيمانيك (Heinz Zemanek): أستاذ جامعة و عالم كومبيوتر من النمسا. ولد في 1920/01/01 بمدينة فيينا وتوفي في 2014/06/16. من أشهر مؤلفاته: معرف الشبكات الاجتماعية وسياق الأرشيف، معرف ملف المرجع للتحكم بالسلطة في WorldCat ... نقلا عن الموقع: <https://snaccooperative.org/ark:/99166/w69g8nr6> بتاريخ 11/01/2022.

(5) : منظمة الأمم المتحدة للاتصالات والمعلومات، 1875، op.cit.

كانت أول وثيقة دولية دعت إلى ضرورة إجراء المراجعة القانونية للأسلحة الحديثة هي اعلان سان بطرسبورغ عام 1868 . وسبق الاعلان جهود الفقيه كروسيوس في كتابه De iure belli ac pacis المنشور في 1925 الذي اشار إلى ضرورة فرض قيود على القوة المدمرة للأسلحة وقد واجه هذا المبدأ اعتراضا بين عامين 1907 و 1925 ، وأعيد التأكيد على هذا المبدأ في اتفاقية لاهاي 1907 في المادة 22 التي تنص على ⁽¹⁾ " ليس للمتحاربين حق مطلق في اختيار وسائل الحاق الضرر بالعدو" وفي عام 1965 وخلال المؤتمر العشرين للجنة الدولية للصليب الأحمر تبني المشاركون المبدأ الذي يقضي بان حق المحاربين في استخدام الأسلحة التي تلحق ضرر بالخصم ليس مطلقا، وهذا الاتجاه تبنته الجمعية العامة للأمم المتحدة في عام 1969 ⁽¹⁾.

إن العلاقة بين القانون الدولي الإنساني والأسلحة الحديثة تتجسد في المادة 36 من البروتوكول الإضافي الأول لعام 1977 التي تنص على ⁽²⁾ " يلتزم أي طرف سام متعاقد، 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 الحق- البروتوكول -أو اي قاعدة اخرى من قواعد القانون الدولي التي يلتزم بها الطرف السامي المتعاقد" ⁽²⁾.

إن الغرض من المادة 36 منع استخدام الأسلحة التي من المحتمل استخدامها بشكل، انتهاك للقانون الدولي في كل الظروف، وفرض قيود على استخدام الأسلحة التي تخالف القانون الدولي في بعض الظروف، من خلال تحديد الجوانب القانونية قبل تطويرها والاستحواذ عليها، وحيث أن المادة 36 تستكمل بالمادة 27 من البروتوكول الإضافي الأول التي تلزم الدول الأطراف بتوفير المستشارين القانونيين في كل وقت لتقديم المشورة القانونية للقادة، كلا المادتين تشكلان الإطار القانوني لضمان قدرة القوات المسلحة بالقيام بأعمال عسكرية متوافقة مع القانون الدولي الإنساني من خلال تقييم وسائل وأساليب القتال ⁽³⁾.

والملاحظ أن المادة 36 مثلت محاولة البروتوكول إنشاء علاقة بين نصوصه تلك الواردة في المادة ⁽⁴⁾ 35 وإنتاج الأسلحة من قبل الدول والمبدأ الاساس في هذه المادة (36) أن الدول المتعاقدة تأخذ على عاتقها بقدر الإمكان تحديد احتمالية أن تكون الأسلحة الحديثة ذات طبيعة غير قانونية وفقا لمواد البروتوكول وأية مادة قانونية قابلة للتطبيق من قواعد القانون الدولي العام، مع أن هناك عاملان يحددان ما اذا كان السلاح جديد أم لا.

- بالرجوع إلى الدولة التي تنوي استخدامه، فواقع أن سلاحا ما إذا كان موجودا في الخدمة في دولة معينة لبعض الوقت قبل بيعه لدولة أخرى لا يمنع الدولة المتلقية من اعتبار السلاح جديد ا وفقا لنص المادة 36.

- بالرجوع إلى تاريخ دخول السلاح الخدمة، فعند تصديق الدولة على البروتوكول الإضافي الأول،

⁽¹⁾: جان بيكتيه، تعليق على البروتوكولات الإضافية المؤرخة 08/06/1977 لاتفاقيات جنيف المؤرخة 12/07/1949 اللجنة الدولية للصليب الأحمر، جنيف 1987، ص 390.

⁽²⁾: دليل لشرعية الأسلحة الجديدة، مرجع سابق، ص 933-934.

⁽³⁾: أسامة صبري محمد، المرجع السابق، ص 09.

⁽⁴⁾: المادة 35: أن حق اطراف أي نزاع مسلح في اختيار اساليب ووسائل القتال ليس حقا لا تقيده قيود 2- يحظر استخدام الاسلحة والقذائف والمواد ووسائل القتال التي من شأنها احداث اصابات او الام لا مبرر لها 3- يحظر استخدام وسائل وأساليب للقتال، يقصد بها او قد يتوقع منها ان تلحق بالبيئة الطبيعية اضرار بالغة واسعة الانتشار وطويلة الامد.

لا يمكن اعتبار الأسلحة الموجودة بالفعل في الخدمة جديدة في إطار نص المادة 36 ، ولكن ربما يكون من قبيل الحيلة للدولة ان تجري مراجعة لهذه الأسلحة التي تخضع للفحص الدولي الدقيق حتى تستطيع الدفاع عن امتلاكها واستخدامها لها بشكل أكثر قوة، وإن كانت المادة 36 لا تستوجب ذلك⁽¹⁾.

ومعايير المراجعة التي تلجأ إليها الدول للتأكد من مدى توافق الأسلحة ووسائل الحرب مع الالتزامات القانونية للدول بموجب القانون الدولي، لا بد من وضع خمسة مجالات في الاعتبار وبداية، لا بد من الاقرار بالتوازن الواجب تأمينه بين الضرورة العسكرية من جانب، ومستوى المعاناة من جانب آخر وهو ما يشار إليه غالباً بمبدأ التناسب، ويتصدر هذا التوازن الأهمية عند دراسة المعايير، لأنه يؤثر على نوع الأدلة المطلوبة لأجراء المراجعة القانونية⁽²⁾.

وبذلك تشمل تلك البنود المعدات التي لا تشكل سلاحاً بالمعنى المفهوم، ولكن لها اثر مباشر على القدرة الهجومية للقوات التي تملكها، ومن الأمثلة على ذلك عربة تطهير الألغام، فربما لا تخضع سماتها للجدل من المنظور القانوني، ولكن ربما يكون من المعقول أن تدرج في نطاق وسائل وأساليب الحرب لأنها تقدم إسهاماً مباشراً في القدرة الهجومية للقوات العسكرية، مع الأخذ بنظر الاعتبار أن التكتيكات العسكرية لا تقع في نطاق المادة 36⁽³⁾.

هذه الالتزامات لا تطبق فقط على الدول المصنعة بل كذلك على الدول القائمة بالشراء أيضاً، بالرغم من أن المادة 36 لا تطالب تحديداً بالنظر في شرعية الأسلحة المصدرة، فان على الدول أن تفعل ذلك وهذا امتداد منطقي للواجب المنصوص عليه في المادة 1 المشتركة لاتفاقيات جنيف⁽⁴⁾ 1949 .

ولكن يجب أن لا تفسر المادة على أنها تحظر بيع أو استيراد الأسلحة فالملاحظ أن نطاق المادة 36 لا تعني أنها تحظر إنتاج الأسلحة التي تحاكي المستقبل وذلك لأنه ليس من المعقول أن الدول عندما تقوم بإنتاج هذه الأسلحة ستنتهك قواعد القانون الدولي التي تحظر الأسلحة التي لا تتوافق مع متطلبات القواعد العامة التي وردت في نص المادة 35 من البروتوكول الإضافي الأول⁽⁵⁾.

بالإضافة أن محكمة العدل الدولية في رأيها الاستشاري المتعلق بشرعية استخدام الأسلحة النووية، بينت المبادئ الأساسية التي تكون القواعد العرفية للقانون الدولي الإنساني كمبدأ التمييز وعدم استخدام الأسلحة التي لا تستطيع التمييز بين الأهداف المدنية والعسكرية وحظر الأسلحة التي تسبب الألام غير المبررة للمقاتلين.

كذلك في حالة فشل الدول في إجراء التقييم بموجب قواعد القانون الدولي الاتفاقية أو العرفية، فيمكن إجراء التقييم في ضوء قواعد تتضمن المبادئ العامة التي وردت في الرأي الاستشاري والتي نجدها في المادة 35 ف 2 والمادة 48 وكذلك المادة 51 من البروتوكول الإضافي الأول.

(1) : أسامة صبري محمد، ص 11.

(2) : المجلة الدولية للصليب الأحمر، العدد 85، لسنة 2003، ص 11-10.

(3) : المجلة الدولية للصليب الأحمر، المرجع نفسه، ص 08.

(4) : اللجنة الدولية للصليب الأحمر، الأسلحة الحديثة، منشور قسم الخدمات الإستشارية للقانون الدولي الإنساني، نقلاً عن: Jean Pictet, op.cit.p426.

427 30.

(5) : إيزابيل داوست، حروب جديدة ، أسلحة جديدة؟ التزام الدول بتقييم شرعية وسائل وأساليب الحرب، مراجعة الصليب الأحمر الدولي، المجلد 84،

العدد 846، حزيران 2002، ص 350-351.

كما أن اللجنة الدولية للصليب الأحمر خلال المؤتمر السابع والعشرين والثامن والعشرين للصليب الأحمر والهلال الأحمر دعت الدول إلى تبادل المعلومات، فيما يتعلق بالياتها الخاصة بالمراجعة القانونية، كما أن الدليل ناشد الدول الأطراف بالبروتوكول الإضافي الأول، بضرورة تقاسم المعلومات وإجراءات المراجعة مع الدول الأخرى الأطراف بموجب المادة 84، التي تلزم الدول بالتشاور فيما بينها⁽¹⁾.

إن الالتزامات المتعلقة بالمراجعة القانونية للأسلحة الحديثة تتلخص في مجموعة من الإجراءات يجب أولاً على الدولة اتخاذ إجراءات دائمة أي آليات ثابتة تنشط تلقائياً لتقييم الأسلحة الحديثة، والثاني يتعلق بإنشاء هيئة تكون مسؤولة عن التطوير للأسلحة⁽²⁾. والملاحظ أن ممارسة الدول فيما يتعلق بتطبيق المادة 36 محدودة، حيث عدد قليل من الدول تبنت إجراءات للمعالجة القانونية، ومن هذه الدول استراليا، النرويج، السويد و الولايات المتحدة الأمريكية، ومعلومات تشير إلى تبني دول أخرى كبلجيكا، كندا، الدنمارك، ألمانيا و هولندا حيث تبنت هذه الدول إما آليات وطنية أو إجراءات للمراجعة القانونية⁽³⁾، وتعتبر السويد الدولة الأولى التي قامت بتشكيل هيئة مستقلة مسؤولة عن المراجعة القانونية لشرعية الأسلحة، الذي أطلقت عليه مشروع القانون الدولي الإنساني لمراقبة الأسلحة الذي تشكل في عام 1924 أي قبل تبني البروتوكول الإضافي الأول سنة 1977، والغاية من تشكيله هي التأكد من أن الأسلحة المستخدمة من قبل القوات السويدية متطابقة مع الالتزامات الدولية.

أما والولايات المتحدة الأمريكية الموقعة على البروتوكول الإضافي الأول في 12/12/1977 فقد تبنت عدة إجراءات كفيلة بضمان أن تكون الأسلحة خاضعة للمراجعة القانونية، وهذا النظام تم تأسيسه في 1974 نتيجة لحرب فيتنام الذي دعا و زارة الدفاع الأمريكية لتقييم مدى التزام الولايات المتحدة لالتزاماتها الدولية في ضوء قانون الحرب، وتعتبر المراجعة القانونية في الولايات المتحدة من الوظائف التنفيذية للوكالات المتخصصة التي تعتبر المسؤولة ابتداء في إجراء المراجعة⁽⁴⁾.

وفي ضوء التطور المطرد لتكنولوجيا التسليح في الوقت الحاضر، تبقى المادة 36 ذات أهمية من الناحية التطبيقية، ومن المؤمل أن تتضافر الجهود الدولية وتقاسم المعلومات من خلال إجراءات مراجعة وطنية، تتيح للدول الفهم الجيد لإجراءات المراجعة وتطويرها وتدعيم التعاون ما بين الدول، ولا يتأتى ذلك إلا من خلال تفعيل المادة 36 وتشجيع الدول لتبني آليات مراجعة على المستوى الوطني، بالإضافة إلى أساليب تنظيمية تشمل الخبراء القانونيين وغيرهم ممن له صلة بمجال التسليح⁽⁵⁾.

والسؤال هنا، هل تعد الهجمات الإلكترونية وسيلة قتال خاضعة لقيود القانون الدولي الإنساني؟

(1): كاثلين لاواند، المرجع السابق، ص 297.

(2): كاثلين لاواند، المرجع نفسه، ص 354.

(3): إيزابيل داوست، المرجع السابق، ص 354-356.

(4): إيزابيل داوست، المرجع نفسه، ص 362.

(5): جستين ماك كلياند، المرجع السابق، ص 10.

فمجمال القول على ذلك تتلخص في أنه، اذا وجهت الهجمات الإلكترونية بصورة مباشرة ضد الخصم، بقصد إحداث أضرار له مثل تعطيل نظام المراقبة الجوية، مما يؤدي إلى حدوث اصطدام جوي، هنا تعتبر الهجمات الإلكترونية وسيلة من وسائل القتال الخاضعة لقيود القانون الدولي الانساني⁽¹⁾.

الخاتمة:

شكلت الحرب الإلكترونية تحديا خطيرا كبيرا على السلم والأمن الدوليين، وازدادت الهجمات الإلكترونية كما ونوعا لتهدد المفاصل الحيوية المدنية وغيرها من شبكات المعلومات التي تؤدي خدمة الى المجتمع، وهذا الاندفاع من قبل الدول نحو استخدام الحرب الإلكترونية، يرجع بالدرجة الأولى إلى القيمة الرخيصة في توجيه الهجمات حيث أن هذه الهجمات غالبا ما تنتج عن فيروسات أو برامج الكترونية خبيثة، يمكن تصنيعها بقيمة رخيصة، علاوة على الاحتجاج من قبل الدول التي تملك مثل هذه القدرات، بأن استخدام الأسلحة الإلكترونية فيه ضمانات كافية لعدم انتهاك القانون الدولي الإنساني.

وفي الختام لا بد أن نذكر أن من يملك سلاح (الحرب الإلكترونية) قوي، يستطيع أن يسيطر على المعركة، ويتحكم فيها بالكلية، وهذا يستعرض لنا أهمية تكنولوجيا المعلومات، وكيف أنها دخلت في كل مناحي الحياة حتى في الحروب! والقول "بأن الحرب الإلكترونية قد ركبتنا، فسبقنا دونما استعداد منّا للعواقب الأخلاقية والمعنوية والقانونية المترتبة عليها"، قد يكون في هذا القول تلخيص للموقف كله.

وبعد هذا نصل الى استنتاجاتنا التالية.

أولاً: ظاهر جدا أن الحرب الإلكترونية تنطوي على أعمال عنف، وتندرج هذه الأعمال في تعريف القانون الدولي الإنساني للهجمات بأنها أعمال هجومية ودفاعية، والغاية من توجيه هذه الهجمات في الحرب التقليدية تحقيق الميزة العسكرية، وهذا ما يحصل في حالة قيام دولة بتوجيه فيروس الى أجهزة المراقبة الجوية، فان ذلك سيؤدي إلى تعطيل ذلك النظام، مما يسمح بتوجيه ضربات محددة إلى الأهداف التي بضررها تتحقق الميزة العسكرية، ويبقى تحديد وجود أو عدم وجود النزاع المسلح، وحتى يمكن تطبيق القانون الدولي الإنساني في الحرب الإلكترونية مسألة قابلة للنقاش خارج حدود القانون الدولي الإنساني التقليدية.

ثانياً: إن النزاع المسلح و لتحديد وجوده يجب أن لا نكتفي بتحديد الاعتماد على المعايير الموضوعية فقط ، لان من شأن ذلك خروج الكثير من النزاعات المسلحة من دائرة القانون الدولي الإنساني، ومنها الحرب الإلكترونية التي لا نجد فيها انتشار لقوات مسلحة أو تبادل لإطلاق النار عبر الحدود، والتي تعد معايير موضوعية لوجود النزاع، بل يتم الاعتماد على طبيعة الأهداف المتوخاة من الهجمات وكثافتها وما تخلفه من نتائج، أي بالاعتماد على نية المهاجم من وراء توجيه الضربة الإلكترونية، سواء كانت الخسائر مادية أو بدنية، فكلا الأثرين نتيجة لأعمال العنف التي يعتبرها القانون الدولي الإنساني قاعدة للهجوم، فإن غياب القواعد في القانون الدولي الإنساني المنطبقة على الحرب الإلكترونية، لا يجرد هذه

(1) : عبد الغني عبد الحميد محمود ، حماية ضحايا النزاعات المسلحة في القانون الدولي الإنساني والشرعية الإسلامية ، بعثة اللجنة الدولية للصليب

الأحمر القاهرة ، ط 04 ، 2009 ، ص 54.

الحرب من القيود القانونية فيمكن أن تخضع لشرط مارتنز ولقواعد حقوق الإنسان في نفس الوقت، وغياب هذه القواعد يمكن أن يكون حافزا للدول على إعداد اتفاقية خاصة بتنظيم وتقييد الحرب الإلكترونية.

ثالثا : إن الحرب الإلكترونية وسيلة من وسائل القتال المعاصرة، بدأت الدول تلجأ إليها في النزاعات الحديثة، وبالتالي تخضع للمادة 36 من البرتوكول الإضافي الأول، وعليه فإن الدول ملزمة بمراجعة قانونية لمثل هذه الوسائل، ومدى مطابقتها لمعايير القانون الدولي الإنساني، ولا يجوز الدفع بأن الوسائل المستخدمة في الحرب الإلكترونية غير خاضعة لتلك المعايير، بحجة غياب القواعد المنظمة للحرب الإلكترونية، فذلك الغياب لا يبرر عدم مراجعة تلك الوسائل.

ثالثا: الأشخاص الذين يساهمون في الحرب الإلكترونية يعدون مدنيين فاقدون للحماية طيلة مشاركتهم في تلك الهجمات، بشرط استيفائهم لمتطلبات المشاركة المباشرة، ولا يجوز للدول ضمهم إلى القوات المسلحة.

رابعا: تبقى الهجمات الإلكترونية مقيدة بعدم توجيهها إلا إلى الأهداف العسكرية، وحظر توجيهها إلى الأهداف المدنية، وحظر توجيه الهجمات إلى المنشآت ذات الاستخدام المزدوج، إلا في حالة تحقيق ميزة عسكرية، كما أن الحرب الإلكترونية مقيدة بعدم توجيهها عشوائيا.

خامسا: يجب على الدولة المهاجمة والمدافعة في الحرب الإلكترونية على حد سواء، اتخاذ الاحتياطات اللازمة التي وردت في المادة 5 والمادة 58 من البرتوكول الإضافي الأول، فعلى المهاجم اتخاذ جميع الاحتياطات الممكنة عند اختياره لوسائل وأساليب الهجوم من أجل تفادي الخسائر والأضرار المدنية العرضية والحد منها في جميع الأحوال . وقد تكون الخسائر والأضرار المدنية العرضية الناجمة عن العمليات الإلكترونية في بعض الحالات أقل من الخسائر في الحرب التقليدية.

سادسا: تبقى الحرب الإلكترونية مفتوحة لكثير من المناقشات القانونية، فالدول التي تستخدم مثل هذه الوسائل تدافع عن استخدامها بأنها تستجيب لمتطلبات القانون الدولي الإنساني، وبصفة خاصة مبدأ التمييز، وتدفع الدول المتضررة بأن تلك الأسلحة لا تراعي مبدأ التمييز.

وخلاصة القول من هذا البحث أن الحرب الإلكترونية، بوسائلها المتعددة لا تستوفي مبدأ التمييز بل تنطوي الهجمات الإلكترونية في أغلب الأحيان على الهجمات العشوائية، وتبقى الدول التي لا تملك القدرات الإلكترونية في وضع سيئ ، كما أن المهاجم الإلكتروني شخص لا يمكن الوصول إليه في أغلب الأحيان، مما يجعله مهاجم يلجأ إلى الغدر واقتناص الفرص كوسيلة قتالية، وهو محظور في القانون الدولي الإنساني. كما أن الحرب الإلكترونية تتأججها أكبر من نتائج الحرب التقليدية، مما يتطلب قواعد عالمية تحظر أو تقييد اللجوء إلى الحرب الإلكترونية.

قائمة المراجع:

1- الكتب:

- 1) إيزابيل داوست، حروب جديدة ، أسلحة جديدة؟ التزام الدول بتقييم شرعية وسائل وأساليب الحرب، مراجعة الصليب الأحمر الدولي، المجلد 84 ، العدد 846، حزيران 2002.

- (2) كاتلين لاواند، مراجعة شرعية الأسلحة الجديدة، البشر وأساليب الحرب، المراجعة الدولية للصليب الأحمر، المجلد 88 ، العدد 864 ديسمبر 2006 .
- (3) عبد الغني عبد الحميد محمود ، حماية ضحايا النزاعات المسلحة في القانون الدولي الإنساني والشريعة الإسلامية ، بعثة اللجنة الدولية للصليب الأحمر القاهرة ، ط04. 2009.
- (4) كنوت دورمان، قابلية تطبيق البروتوكولات الإضافية لهجمات شبكات الكمبيوتر ، 2004 .
- (5) مارتين سي لبيكي، الردع الإلكتروني والحرب الإلكترونية ، راند ، 2009
- 6) Max Blumenthal , international humanitarian law for cyber-warfare ,School of international Service the American university ,2011,p2.
- 7) Myriam Dunn Cavelty, Cyberwar: Concept, Status. Quo, And Limitations, CSS Analysis In Security Policy, CSS ETH Zurich, No.71, April 2010, At This Link: www.Sta.Ethz.Ch/Content/Download/906/6864/Version/1/File/CSS_Analysis_71.Pdf
- 8) Richard A. Clarke & Robert knake, Cyber War, HarperCollins (2010), p:6.
- 9) Dieter Fleck , technological challenges in armed conflicts and areas of regulation ,p5.
- 10) Marco Roscint , World Wide Warfare – Jus ad bellum and the use of cyber Force , Max Planck Yearbook of United Nations Law , VOL.14,2010,p95.
- 1) William J. Lynn III, Defending a New Domain: The Pentagon's Cyberstrategie, Foreign Affairs, September-October 2010, p:98.

2- القوانين والاتفاقيات.

- (1) اتفاقية لاهاي لعام 1907 واتفاقية حظر استحداث وانتاج وتخزين الاسلحة البكتريولوجية وتدمير تلك الاسلحة 1972.
- (2) اتفاقية حظر استخدام تقنيات التغيير في البيئة لأغراض عسكرية أو لأية أغراض عدائية أخرى 1976.
- (3) اتفاقية حظر أو تقييد استعمال أسلحة تقليدية معينة يمكن اعتبارها مفرطة الضرر أو عشوائية الأثر والبروتوكول الخامس الملحق باتفاقية حظر أو تقييد استعمال أسلحة تقليدية معينة يمكن اعتبارها مفرطة الضرر أو عشوائية الأثر. 2003.
- (4) القانون الدولي الإنساني وتحديات النزاعات المسلحة المعاصرة، التقرير الحادي، والثلاثين، 2011 لاتفاقية هي أول معاهدة دولية بشأن الجرائم التي ترتكب عبر شبكة الانترنت وشبكات الكمبيوتر الأخرى، والتعامل بشكل خاص مع التعدي على حق المؤلف، ذات الصلة بالحاسوب الاحتيال، و المواد الإباحية، جرائم الكراهية وانتهاكات أمن الشبكة. نقلا عن : Michael Geraiss,cyber attacks and the law of war, yale university law school ,October 1,2011,p7

3-المجلات:

- (1) جان بيكتيه، تعليق على البروتوكولات الإضافية المؤرخة 08 / 06 / 1977 لاتفاقيات جنيف المؤرخة 12 / 07 / 1949 اللجنة الدولية للصليب الأحمر، جنيف 1987 .

(2) دليل قانون الأسلحة والوسائل والأساليب الجديدة للحرب؛ تدابير تنفيذ المادة 36 من البروتوكول الإضافي لعام 1977 ، اللجنة الدولية للصليب الأحمر، جنيف، يناير 2006، تقارير ووثائق، المراجعة الدولية للصليب الأحمر، المجلد 88 ، العدد 864 ديسمبر 2008.

(3) اللجنة الدولية للصليب الأحمر، الأسلحة الحديثة، منشور قسم الخدمات الإستشارية للقانون الدولي الإنساني. نقلا عن: Jean Pictet, op.cit, p426-427 30. المجلة الدولية للصليب الأحمر ، العدد 85، لسنة 2003.

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

4-الملتقيات:

(1) يوهان ChrstophWoltag - ، عمليات شبكات الكمبيوتر تحت مستوى القوة المسلحة ، الجمعية الأوروبية للقانون الدولي ، سلسلة أوراق المؤتمرات ، ورقة المؤتمر رقم 2011/1 ، 2011 .

5-المواقع الإلكترونية:

(1) أسامة صبري محمد، الحرب الإلكترونية ومبدأ التمييز في القانون الدولي الإنساني، مقال منشور على شبكة النت، 10.10.2021 ، www.assrn.com/abstract=3265966

(2) جريج برونو ، The Evolution of Cyber Warfare ، مجلس العلاقات الخارجية ، 27 فبراير 2008 ، نقلا عن: www.cfr.org/2022/10/03/evolution_of_cyber_warfare.html/15577/

(3) سايمون تيسدال ، الحرب الإلكترونية "تهديد متزايد" ، صحيفة الجارديان ، 3 فبراير 2010 ، نقلا عن: www.guardian.co.uk/technology/2010/feb/03/cyber-warfare-growing-threat

4) Attack and jus in bello, irrcline, Vol.84 ,N.846,2002p,368.Michael N.Schmit , wired warfare computernetwork-No Legal Vacuum In Cyber Space , 2011, WWW.ICRC.ORG.2022/10/08 تاريخ الإطلاع: John Richardson , Stuxnet as cyberwarfare : Applying the law of war to the Virtual attlefield ,JMR Portfolio Intelligence,2011,p9. Available at www.assrn.com/abstract=1892888.2022/10/08 تاريخ الإطلاع:

5) <https://snaccooperative.org/ark:/99166/w69g8nr62022/11/01> .تاريخ