الحرب السيبرانية من منظور القانون الدولي الإنساني

Cyber warfare from the perspective of international humanitarian law

نسيب نجيب[1]*،

[1] **كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو**

تاريخ الاستلام: 2021/08/29 تاريخ القبول للنشر: 2021/09/14 تاريخ النشر: 2021/12/31

الملخص

يعد تكييف الهجمات السيبرانية في وقتنا الراهن من أهم التحديات التي يواجهها المختصون في القانون الدولي، وذلك لصعوبة تحديد طبيعتها وعناصرها، وما يترتب عن هذه الهجمات من تبعات المسؤولية الجنائية أو المدنية الدولية، خاصة وأن تلك الهجمات قد تلجأ إليها بعض الدول لأجل تحقيق مكاسب معينة، كالهيمنة على واقع النزاع المسلح، إذ أصبحت التكنولوجيا الحديثة جزء مهم من وسائل الحرب المعاصرة والتي تتم في الفضاء السيبراني وهو ما اصطلح على تسميته بالحرب السيبرانية.

تهدف هذه الدراسة إلى تسليط الضوء على مفهوم الحرب السيبرانية التي أصبحت تهدد السلم والأمن الدوليين، وكذا دراسة إمكانية تطبيق أحكام القانون الدولي الإنساني عليها، من خلال التطرق إلى عرض وجهات النظر الفقهية المختلفة حول هده المسألة، والإشكاليات العملية لتطبيق مبادئ سلوكيات الحرب (Jus ad bello) على الحروب السيبرانية.

الكلمات المفتاحية: الهجمات السيبرانية، الحرب السيبرانية، الأسلحة السيبرانية، القانون الدولي الإنساني، مبادئ سلوكيات الحرب.

Abstract

The cyber attacks, at present, are adapted, qualified and considered as one of the most significant challenges faced by the international law specialists, since it's difficult to pin down it's nature, innate characteristics and elements, and the after comes of these attacks for international criminal or civil liability, especially that such attacks could be a resort for some states in order to achieve certain gains such as dominating the reality of the armed conflict, modern technology became an essential part of current means of war, which is done in cyberspace, called cyber warfare.

The purpose of this study is to highlight the concept of cyber warfare which threats the international peace and security, the study examines as well the possibility

* **المؤلف المراسل: nacibnadjib@gmail.com**

of applying the International humanitarian law, by suggesting the different legal theories perspectives about this issue, and the effective problems of applying the principles of war behavior (jus ad bello) on cyber warfares.

Keywords: cyber attacks, cyber warfare, cyber weapons, International humanitarian law, principles of war behavior.

* المؤلف المراسل: nacibnadjib@gmail.com

المقدمة

أدى ظهور الحاسب الآلي والتوسع في استخدام شبكة الإنترنت في مجالات الحياة المختلفة ظهور بعض الآثار السلبية والمخاطر المترتبة على هذا التوسع الكبير؛ إذ كلما زاد الاعتماد على هذه التقنيات في التنمية زادت المخاطر الناتجة عنها.

وبالتزامن مع هذا التطور الكبير في تكنولوجيا المعلومات والاتصالات وزيادة الاعتماد عليها، ظهر ما يسمى بالهجمات السيبرانية التي تتم في الفضاء السيبراني، والتي يقوم بها مخترقي الشبكات سواء كانوا دولا أو أشخاصا يمتلكون خبرة كبيرة في ميدان تقنيات المعلومات والحواسيب، ولديهم القدرة على الدخول إلى المواقع المحظورة في نظم شبكات الحواسيب بمختلف أشكالها، ويستهدف نشاطهم المواقع الإلكترونية المهمة مثل المواقع العسكرية، حيث يقومون باختراقها بقصد الحصول على أسرار، أو وثائق أو نشر رسائل احتجاجية، أو حتى لجمع المال.

وأصبحت الهجمات السيبرانية من أهم التحديات التي يواجهها المختصون في القانون الدولي العام؛ وذلك لصعوبة تحديد طبيعتها وعناصرها، وما يترتب على هذه الهجمات من تبعات المسؤولية الجنائية أو المدنية الدولية، خاصة وأن تلك الهجمات قد تلجأ إليها بعض الدول لأجل تحقيق مكاسب معينة، كالهيمنة على واقع النزاع المسلح، إذ أصبحت التكنولوجيا الحديثة جزء مهم من وسائل الحرب المعاصرة والتي تتم في الفضاء السيبراني وهو ما اصطلح على تسميته بالحرب السيبرانية.

ورغم أن المعالم الدقيقة لأي حرب سيبرانية لا تزال غير محددة، إلا أن الهجمات السيبرانية الكثيرة ضد البني التحتية للمعلومات وخدمات الإنترنت التي تعرضت لها العديد من الدول في وقتنا الراهن شكلت تهديدا خطيرا للأمن الداخلي للدول حيث تغيرت مفاهيم القوة والصراع والحرب، وارتبطت طبيعتها بالفضاء السيبراني.

وقد زاد لجوء الدول إلى استخدام الهجمات السيبرانية نظرا لما توفره هذه الأخيرة من جهد ومال، كالتقليل من تكلفة الحروب والنزاعات المسلحة، نتيجة سهولة استخدام الأسلحة السيبرانية مثل الفيروسات وبرامج التجسس، وقرصنة المعلومات العسكرية والإستراتيجية، فضلا على تحقيق الأهداف المسطرة في ظرف وجيز، وكذا حجم الدمار الهائل الذي يمكن أن تسببه تلك الأسلحة، حيث يرى البعض أن حجم الدمار الذي تلحقه الأسلحة السيبرانية يضاهي الدمار الذي تحدثه أسلحة الدمار الشامل المعروفة، عن طريق استهداف المنشآت الحيوية للدول، وشل كل مظاهر الحياة فيها، كمحطات الكهرباء والسدود والبنوك... الخ[1].

[1]– سعيد درويش، "ماهية الحرب الإلكترونية في ضوء قواعد القانون الدولي"، حوليات جامعة الجزائر 1، المجلد 29، العدد 2، 2016، ص 118.

وقد أدت الخطورة المتنامية لاستعمال الأسلحة السيبرانية في النزاعات المسلحة بفقهاء القانون الدولي إلى دراسة مفهوم الحرب السيبرانية، من خلال مقاربة هذه الحرب مع القواعد القابلة للتطبيق في النزاعات المسلحة التقليدية، وموقف القانون الدولي الإنساني منها.

بناء على ما تقدم، تتمحور إشكالية دراستنا حول مدى **ملائمة القواعد القانونية التقليدية الخاصة بالنزاعات المسلحة المنظمة بموجب القانون الدولي الإنساني واستيعابها لفكرة الحرب السيبرانية؟**

وللإجابة على الإشكالية المطروحة قسمنا موضوع الدراسة إلى مبحثين تناولنا في المبحث الأول دراسة مفهوم الحرب السيبرانية، وتطرقنا في المبحث الثاني إلى تكييف الحرب السيبرانية وفقا للقانون الدولي الإنساني.

المبحث الأول

مفهوم الحرب السيبرانية

ارتبط مسار الحروب عبر تاريخها الطويل، بالتطورات التقنية التي عرفتها الجماعات البشرية، وسخرتها في سبيل تطوير قدراتها القتالية، وصولا لتحقيق أهدافها، وتأمين مصالحها الحيوية المنشودة من خوض النزاع المسلح. ومع ولوج الحضارة الإنسانية عصر المعلومات والتقنيات الحديثة شهدت ساحات الحروب ظهور جيل جديد من المنظومات القتالية التي اعتمدت على الفضاء السيبراني في إدارة المعارك والتي صارت تعرف بالحرب السيبرانية. ومما تقدم أضحى من الضروري الوقوف على تعريف الحرب السيبرانية (المطلب الأول) والتطرق إلى بعض النماذج للحروب السيبرانية (المطلب الثاني).

المطلب الأول: تعريف الحرب السيبرانية

ليس هناك إجماع واسع على تعريف محدد ودقيق لمفهوم الحرب السيبرانية حتى الآن، وتكمن المشكلة الأساسية في غياب هذا التعريف إلى الطبيعة القانونية المتغيرة لمصطلحات متطورة ظهرت في الآونة الأخيرة في سياق النزاعات المسلحة، مثل الهجمات السيبرانية عن طريق الشبكة العنكبوتية من جهة، وحداثة الهجمات على شبكات الحواسيب التي تعد ظاهرة حديثة من جهة أخرى[2].

وعلى الرغم من غياب إجماع واسع على تعريف محدد ودقيق لمفهوم الحرب السيبرانية، إلا أن ذلك لم يمنع الفقهاء كل في تخصصه من تقديم تعاريف للإحاطة بهذا المفهوم، ومن تلك التعاريف ما ذهب إليها خبراء ومختصين في القانون الدولي الإنساني، وأولهم الأستاذ (SHIN) الذي عرف الحرب السيبرانية بأنها: "استخدام

[2]– أسامة صبري محمد، "الحرب الالكترونية ومبدأ التمييز في القانون الدولي الإنساني"، مجلة القانون للدراسات و البحوث القانونية، العدد 7، 2013، ص 5.

الطيف الالكتروني أو الكهرومغناطيسي لتخزين وتعديل وتبادل البيانات وجها لوجه مع أنظمة تحكم في بنى تحتية مرتبطة بها"[3].

وعرّف الأستاذ (Michael N. Schmitt) الحرب السيبرانية بأنها: "مجموعة من الإجراءات التي تتخذها الدولة للهجوم على نظم المعلومات المعادية بهدف التأثير والإضرار بها، وفي الوقت نفسه للدفاع عن نظم المعلومات الخاصة بالدولة المهاجمة"[4].

كما عرّفها كل من الأستاذ "ريتشارد كلارك" و الأستاذ "روبرت كناكي" على أنها: " أعمال تقوم بها دولة تحاول من خلالها اختراق أجهزة الكمبيوتر والشبكات التابعة لدولة أخرى بهدف تحقيق أضرار بالغة أو تعطيلها"[5].

وعرفها الأستاذ (Marco Roscini) بأنها: "تطويع الإمكانيات الالكترونية العسكرية لأجل التأثير في مواقع الكترونية أخرى وتعطيلها أو تدميرها سواء أكانت تقدم خدمات مدنية أو عسكرية"[6].

ويعتبر آخرون أن الحرب السيبرانية هي:" امتداد للحروب التقليدية والمادية، إذ يتألف جندها من المدنيين والعسكريين في آن واحد، كما أنها حرب أدمغة بالدرجة الأولى، كونها تستهدف في المقام الأول تدمير البنية العلمية والمعلوماتية للهدف، وتأخذ أشكالا عدة، كشكل الاتصالات بين الجيوش وقياداتها، وإضعاف شبكات النقل والإمدادات اللوجستية، وضرب المعلومات الاقتصادية، والعبث بالمحتوى التقني والرقمي وغيرها"[7].

وهناك من يربط مفهوم الحرب السيبرانية ببيئة الإنترنت فقط، كونها ساعدت على انتشار المعلومات في مختلف أرجاء المعمورة وسهلت الوصول إليها بشكل سريع. ويتم تعريف الحرب السيبرانية بناء على ذلك بأنها: "الحرب التي تستهدف المعلومات. وهي تعبير عن الاعتداءات التي تطال مواقع البيانات الموجودة على

---

[3]– نقلا عن: أحمد عبيس نعمة الفتلاوي، "الهجمات السيبرانية: مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر"، مجلة المحقق الحلي للعلوم القانونية والسياسية، العدد 4، السنة 8، 2016، ص 616.

[4]– نقلا عن: يحيى ياسين سعود، "الحرب السيبرانية في ضوء قواعد القانون الدولي الإنساني"، المجلد 4، العدد 4، 2018، ص 84.

[5]– نقلا عن: يحيى مفرح الزهراني، "الأبعاد الإستراتيجية والقانونية للحرب السيبرانية"، مجلة البحوث والدراسات، العدد 23، السنة 14، 2017، ص 235.

[6]– نقلا عن: أحمد عبيس نعمة الفتلاوي، المرجع السابق، ص 616.

[7]– حكيم غريب، صبرينة شرقي، "تداعيات الحرب الإلكترونية على العلاقات الدولية: دراسة في الهجوم الإلكتروني على إيران (فيروس ستكنست") ، دفاتر السياسة والقانون، المجلد 12، العدد 2، 2020، ص 96.

الإنترنيت، وتحاول الاستيلاء على معطياتها، بين أطراف متناقضة الأهداف، ومتعارضة المصالح، ومختلفة المواقف"[8].

ويرى بعض القانونيين أن أساليب عمل الحروب السيبرانية تتقارب من ناحية قانونية مع إشاعة الرعب والإرهاب، لذلك يمكن تعريف الحروب السيبرانية استنادا لهذه النظرة القانونية بأنها: " نظام قائم على الرعب المنتشر في شبكة الإنترنت، والتي تهدف إلى تنفيذ العديد من الأعمال لترويع أمن الأفراد والجماعات والمؤسسات والدول، وإدخالهم في أزمات نفسية واقتصادية وسياسية واجتماعية ناتجة عما يعرف بالإرهاب الصامت"[9].

ومن التعاريف الحديثة للحرب السيبرانية نذكر تعريف مجموعة الخبراء التابعين للناتو الوارد في القاعدة 30من دليل تالين المتعلق بتطبيقات القانون الدولي في مجالات الصراع والحروب السيبرانية[10]، تنص على أنها:" كل العمليات السيبرانية سواء كانت دفاعية أو هجومية، والتي يعتقد أنها قد تسبب إصابات أو وفيات للبشر، أو تلف وضرر للأشياء المادية"[11].

المطلب الثاني: نماذج عن الحروب السيبرانية

تعرضت العديد من الدول في السنوات الأخيرة الماضية إلى عدة هجمات سيبرانية، وتتنوع هذه الهجمات الخطيرة ما بين تدمير أنظمة إلكترونية لمنشآت حيوية عسكرية أو مدنية . وتعطيل أو إتلاف شبكات الدفاع العسكرية عن بعد، واختراق أو تعطيل أو تدمير شبكات القطاع العام والخاص، وتعطيل البنية التحتية للدول. ومن بين أكثر الهجمات التي وقعت على المستوى الدولي والتي يمكن إدراجها في سياق الحروب السيبرانية،

---

[8]– وليد غسان سعيد جلعود، دور الحرب الإلكترونية في الصراع العربي الإسرائيلي، مذكرة ماجستير في التخطيط والتنمية السياسية، كلية الدراسات العليا، جامعة النجاح الوطنية نابلس، فلسطين، 2013، ص 82.

[9]– حكيم غريب، صبرينة شرقي، المرجع السابق، ص 96.

[10] - Une vingtaine d'experts juristes internationaux dont les nationalités sont représentatives des nations membres de l'Otan a tenté une première analyse de l'interprétation des normes de droit international aux attaques cybernétiques. En s'appuyant ainsi sur le droit international préexistant notamment dans le domaine des conflits armés, du droit de l'espace, de la mer et de l'air, certaines règles applicables ont été étendues aux activités cyber. Cette première analyse constitue ainsi le socle futur de potentielles nouvelles normes juridiques internationales du cyberespace. Cette initiative, lancée au sein du Centre de cyberdéfense de l'Otan (CCD-CoE) situé à Tallinn en Estonie, est tout à fait innovante. Pendant trois ans, les experts ont travaillé sous la direction du professeur Michael Schmitt de l'US Naval War College à la création d'un manuel de droit applicable à la cyberguerre, appelé communément *Manuel de Tallinn (2013)*. Voir, Oriane BARAT- GINIES, "Existe-t-il un droit international du cyberespace ? ", La Découverte, n° 152-153, 2014/1, p. 202.

[11]– نقلا عن سعيد درويش، "الحروب السيبرانية وأثرها على حقوق الإنسان: دراسة على ضوء أحكام دليل " تالين""، المجلة الجزائرية للعلوم القانونية والاقتصادية والسياسية، المجلد 54، العدد 5، 2017، ص 181.

نذكر الهجمات التي استهدفت إستونيا عام 2007 (الفرع الأول)، وكذا استهداف المواقع النووية الإيرانية بهدف تعطيلها عام 2010 (الفرع الثاني).

الفرع الأول: الهجوم السيبراني على إستونيا

قامت الحكومة الاستونية بتاريخ 26 أفريل 2007 بنقل نصب تذكاري يعود للحرب العالمية الثانية، مخصصا لتخليد الجيش الأحمر الروسي من وسط عاصمة استونيا "تالين" إلى مقبرة عسكرية خارجها، مما أدى إلى حدوث مظاهرات شعبية من قبل المجتمع الإستوني الناطق بالروسية، والذي يمثل ما يقارب 30 % من السكان، كما أدانت روسيا الرسمية هذا القرار.

وردا على هذا القرار تعرضت إستونيا وعلى مدار ثلاثة أسابيع إلى سلسلة من الهجمات السيبرانية التي طالت العديد من المواقع الحكومية والعسكرية والخاصة الاستونية وأصابتها بالشلل التام، بما في ذلك مواقع الإعلام والبنوك ومشغلي الهاتف المحمول وخدمات الطوارئ، مما أدى إلى حرمان العديد من السكان من الوصول إلى خدمات أساسية عبر الانترنيت[12].

ووجهت إستونيا اتهاما رسميا لروسيا في ارتكابها هذه الهجمات السيبرانية، إذ اعتبرتها إستونيا بمثابة أعمال انتقامية بسبب قيامها بنقل النصب التذكاري المخلد للجيش الروسي خارج العاصمة تالين، وهو ما نفته روسيا[13].

وقد اعتبر العديد من الخبراء أن الحديث عن حرب سيبرانية ظل حديثا نظريا حتى تاريخ هذه الهجمات التي تعرضت لها إستونيا في 2007، والتي تعد أول حرب سيبرانية تم استخدام الفضاء السيبراني فيها لتدمير أهداف حيوية للعدو[14].

الفرع الثاني: الهجوم السيبراني على المواقع النووية الإيرانية

تم استهداف المفاعلات النووية الإيرانية بفيروس (Stuxnet)[15] ، الذي تم اكتشافه لأول مرة في جوان 2010، والذي يعد الأخطر على صعيد الهجمات السيبرانية لمنشآت مدنية أو عسكرية على الإطلاق، إذ تعرضت المواقع النووية الإيرانية إلى أسلوب ومنهج يقوم على شقين: الأول باستهداف أجهزة الطرد المركزية

---

[12] - Evelyne AKOTO, "Les cyberattaques étatiques constituent-elles des actes d'agression en vertu du droit international public ?" : Première partie, Revue de droit d'Ottawa, Volume 46, n° 1, 2014-2015, p. 13, Voir également : Jean-Loup SAMAAN, "Les cyber-conflits, une révolution géopolitique?", AFRI, Volume XI, 2010, p. 993.

[13] - Evelyne AKOTO, Op.Cit, p. 14.

[14]– إيهاب خليفة، كيف يمكن أن تدير الدول شؤونها في عصر الإنترنت، العربي للنشر والتوزيع، القاهرة، 2017، ص 21.

[15] - Stuxnet est un ver qui ferait partie d'un programme secret américain intitulé *Olympic Games*104. Autorisé en 2006 par le président Georges Bush et poursuivi par le président Barack Obama après sa prise de pouvoir en 2009, *Olympic Games* a pour objectif le sabotage du programme nucléaire iranien. Voir : Evelyne AKOTO, Op.Cit, p. 17.

وخروجها عن السيطرة من جهة، أما الثاني فبالتحايل على أجهزة التحكم والإيحاء لها، أن عمليات تشغيل المنشأة النووية تعمل بصورة طبيعية، إلا أنها في الواقع معطلة[16].

وأعلنت السلطات الإيرانية أن الفيروس قد أصاب حوالي 16000 جهاز كمبيوتر وذلك بعد تعرضهم لهجوم في أكتوبر 2010، وآخر في أفريل 2011، وتسبب في تعطيل حوالي 1000 من أجهزة الطرد المركزي في المفاعل النووي الإيراني في مدينة " ناتانز"، فضلا على تعطيل البرنامج النووي الإيراني لتخصيب اليورانيوم لمدة سنتين. واتهمت إيران الولايات المتحدة الأمريكية وإسرائيل بالوقوف وراء هذا الهجوم[17].

وقد شكل استعمال هذا الفيروس نقلة نوعية في خطورة الحروب السيبرانية التي انتقلت من تدمير البيانات وسرقتها إلى تدمير المكونات المادية نفسها ونظم التشغيل لقطاعات حيوية مثل الطاقة النووية[18]. وهو ما يفتح الباب أمام الكثير من التكهنات بأن مثل هذه الأسلحة المتطورة يمكن أن تصبح أمرا شائعا في المستقبل[19].

المبحث الثاني

تكييف الحرب السيبرانية وفقا للقانون الدولي الإنساني

تطرق العديد من فقهاء القانون الدولي إلى موضوع الحروب السيبرانية، فطرحوا عددا من الإشكاليات القانونية المتمحورة حول القانون الواجب التطبيق عليها . وإن كان غالبية الفقهاء يؤكدون إمكانية تطبيق قواعد القانون الدولي الإنساني على هذه الحروب، غير أن جانب آخر من الفقه رفض هذا الطرح وأقروا بوجود فراغ قانوني في هذه المسألة (المطلب الأول). ومع التسليم بانطباق القانون الدولي الإنساني على الحروب السيبرانية، إلا أن ذلك لا يعني إنكار حقيقة وجود العديد من الإشكالات العملية لتطبيق مبادئ القانون الدولي الإنساني على الحروب السيبرانية، وتظهر هذه الإشكالات خاصة عند تطبيق مبادئ سلوكيات الحرب (المطلب الثاني).

المطلب الأول: جدلية انطباق القانون الدولي الإنساني على الحروب السيبرانية

اختلف الفقه حول انطباق القانون الدولي الإنساني على الحروب السيبرانية من عدمه، فهناك من يرى أنه لا يمكن أن يطبق القانون الدولي الإنساني على تلك الحروب التي تحمل طبيعة خاصة، وتحتاج إلى نموذج

---

[16] – أحمد عبيس نعمة الفتلاوي، المرجع السابق، ص 626. وانظر أيضا:

– Barbara Louis-SIDNEY, "La dimension juridique du cyberespace", Revue internationale et stratégique, n° 87, 2012/3, p. 82.

[17]– إيهاب خليفة، كيف يمكن أن تدير الدول شؤونها في عصر الإنترنت، المرجع السابق، ص 205.

[18]– إيهاب خليفة، الحرب السيبرانية، الاستعداد لقيادة المعارك العسكرية في الميدان الخامس، العربي للنشر والتوزيع، القاهرة، 2021، ص 91.

[19]– حكيم غريب، صبرينة شرقي، المرجع السابق، ص 101.

قانوني جديد يتعامل معها وينظم استخدامها (الفرع الأول)، وهناك من يرى أنه يمكن تطبيق القانون الدولي الإنساني على الحروب السيبرانية عن طريق القياس والاجتهاد في المقارنة (الفرع الثاني).

الفرع الأول: استحالة تطبيق القانون الدولي الإنساني على الحروب السيبرانية

تكمن خصوصية الفضاء الإلكتروني في عدم وجود دولة بإمكانها فرض سيطرتها وسيادتها الأحادية عليه، وهذا يؤدي إلى استخدامه بشكل قد يضر الإنسانية. وعلى هذا الأساس ظهر اتجاه فقهي سمي بالاتجاه الحر يرفض التعامل القانوني مع الإنترنت ويقضي بأن الإنترنت منطقة بلا قانون.

ويعتبر أنصار هذا الاتجاه الذي يتزعمه بعض السياسيين الأمريكيين وعلماء التقنية، وتساندهم فئة قليلة من فقهاء القانون الدولي، أن الإنترنت مكان أو قارة أو فضاء مستقل في حد ذاته عن كل الفضاءات الأخرى بما فيها فضاؤنا المادي الملموس. وبالتالي لا يمكن إخضاعه حتى للقانون الدولي العام التقليدي، فهذا القانون لم ينجح لحد الآن بحكم الفضاء البحري أو الجوي الخارجيين[20].

ويستند أنصار هذا الاتجاه على حجة أن الإنترنت عالم جديد لا يتفق والواقع المادي التقليدي. وعلى أساس ذلك، طرحوا سؤالا وجيها، هو إن سلمنا بضرورة إخضاع الإنترنت للقانون، فأي سلطة يكون بإمكانها السهر على فرض أحكامه في ظل استقلالية الشبكة وانفلاتها من مفهوم الخضوع؟ وأجابوا بانعدام السلطة القادرة على ذلك. وحتى إن وجد مثل هذا القانون، فإنها تبقى منطقة بلا قانون، لاستحالة إخضاعها للتدخل التنظيمي التقليدي للدول، كونها تتسم بطابع عالمي مفتوح، ويتعذر إخضاعها لقانون واحد لاشتراك كل الدول فيها[21].

وفيما يتعلق بتطبيق أحكام القانون الدولي الإنساني على الحرب السيبرانية، فابتداء لا توجد أي قواعد قانونية في اتفاقيات القانون الدولي الإنساني تتعامل بشكل مباشر مع الهجمات السيبرانية، فهي غير منظمة في النزاعات المسلحة، إضافة إلى أن تطوير الهجمات السيبرانية حصل في فترة لاحقة على إعداد صكوك القانون الدولي الإنساني، كما أن القانون الدولي الإنساني وضعت قواعده لتنظيم وسائل وأساليب القتال ذات الطبيعة المتحركة التي تنتج عنها آثار مادية غير متوفرة في الهجمات السيبرانية، وبالتالي تكون هذه الأخيرة خارج نطاق القانون الدولي الإنساني لأنها ليست هجمات مسلحة[22].

ويبين أصحاب هذا الاتجاه أنه وعلى الرغم من أن مسمى الحرب يطلق على هجمات الكمبيوتر، فهو أيضا بحاجة إلى نظر، كون أن الحرب مفهوم يرتكز بالأساس على استخدام الجيوش النظامية، وكان يسبقها إعلان واضح لحالة الحرب وميدان قتال محدد. أما في هجمات الفضاء السيبراني، فإنها غير محددة المجال أو الأهداف كونها تنفذ عبر شبكات المعلومات والاتصال المتعدية للحدود الدولية، أو اعتمادها على أسلحة

---

[20]– طالب حسن موسى، عمر محمود أعمر، "الإنترنت قانونا"، مجلة الشريعة والقانون، العدد 37، 2016، ص ص 7-8.

[21]– المرجع نفسه، ص 8.

[22]– أسامة صبري محمد، المرجع السابق، ص 8.

الكترونية جديدة تلاءم 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 السيبراني تبدو غير واقعية، لأن وسائل وأساليب الحرب السيبرانية غير واضحة ومفهومة بشكل كاف، ولأنها تتم في سرية تامة.

وتتسم كذلك هجمات الفضاء السيبراني بأنها استباقية ومن دون سابق إنذار، وأنها غير محددة المجال أو المدى، وتكون أهدافها غير محددة بخلاف الحرب التقليدية التي تكون أهدافها ومكانها محددين وتكون قوات الحرب السيبرانية غير معروفه وليست محددة في دولة سواء أكانت هدفا للحرب أو مشاركة فيها، حيث لا تصبح بالضرورة الدولة هي الهدف، وتكون الحرب السيبرانية 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].

الفرع الثاني: خضوع الحروب السيبرانية للقانون الدولي الإنساني

يرى أنصار هذا الاتجاه عدم وجود فراغ قانوني في الفضاء السيبراني، واعتبار القواعد القانونية القائمة كافية وكفيلة لتنظيمه، والذي تشكل الإنترنت أحد وسائله الرئيسية، خاصة إذا علمنا أنه سبق تنظيم وسائل اتصال تشبهها مثل الهاتف والفاكس وغيرها من الوسائل الالكترونية.

وعليه ينطبق القانون الدولي الإنساني بمبادئه وقواعده بصفة عامة على أي نزاع مسلح بما فيها الحروب السيبرانية، فإذا كنا نتفق بأن اتفاقيات القانون الدولي الإنساني لم تشر على وجه الخصوص للهجمات السيبرانية إلا أن هذه الحجة ليس لها أهمية تذكر، لأن شرط مارتينز وهو من المبادئ الراسخة في القانون الدولي الإنساني ينص صراحة على أنه عند وجود حالة لا تغطيها اتفاقية دولية "يظل المدنيون والمقاتلون تحت حماية وسلطة مبادئ القانون الدولي المستمد من التقاليد الراسخة، ومن مبادئ الإنسانية، وما يمليه الضمير العام"[25].

---

[23]– عمر محمود أعمر، "الحرب الإلكترونية في القانون الدولي الإنساني"، الشريعة والقانون، المجلد 46، العدد 3، 2019، ص 137.

[24]– المرجع نفسه، ص 137.

[25] - مايكل ن. شميت، "الحرب بواسطة شبكات الاتصال: الهجوم على شبكات الكمبيوتر (الحاسوب) والقانون في الحرب"، المجلة الدولية للصليب الأحمر، مختارات من أعداد 2002، ص 90.

وعلى هذا الأساس فإن كل ما يقع أثناء النزاع المسلح يخضع لمبادئ القانون الدولي الإنساني، وعليه لا وجود لفراغ قانوني بالنسبة للهجمات السيبرانية. كما أن قبول العرف الدولي كمصدر للقانون الدولي والمنصوص عليه في المادة 38 من النظام الأساسي لمحكمة العدل الدولية يؤكد أيضا المغالطة التي وقع فيها من يرفضون انطباق القانون الدولي الإنساني على الهجمات السيبرانية اعتمادا على غياب نص قانوني معين[26].

أما بالنسبة للحجة التي ترتكز على حقيقة أن الهجمات السيبرانية يرجع تاريخها إلى ما بعد اعتماد المواثيق الدولية المشكلة للقانون الدولي الإنساني فإنها تنطوي على مغالطة أيضا، ذلك أن مثل هذا التبرير كان قد قدم إلى محكمة العدل الدولية في مسألة مدى مشروعية التهديد بالأسلحة النووية أو استخدامها سنة 1996، ورفضت المحكمة في رأيها الاستشاري الاتجاه القائل بأنه نظرا لأن المبادئ والقواعد الإنسانية قد وضعت قبل اختراع الأسلحة النووية، فإن القانون الدولي الإنساني يكون غير منطبق عليها، واعتبرته رأيا تمثله أقلية بسيطة. بينما أكدت أن رأي الغالبية العظمى من الدول والفقه وبدون أي شك، هو انطباق القانون الدولي الإنساني على الأسلحة النووية[27].

ولأنه ليس هناك ما يدعو للتمييز بين الأسلحة النووية وأسلحة الحاسوب على الأقل من حيث التوقيت الذي استحدثت فيه بالنسبة لدخول المعايير الإنسانية ذات الصلة حيز التنفيذ، فإن نفس النتيجة تنطبق على الهجمات على شبكات الحاسوب أي التي تتم عبر الفضاء السيبراني[28].

وفي نفس السياق أشارت المادة 36 من البروتوكول الإضافي الأول الملحق باتفاقيات جنيف لعام 1949 المتعلق بحماية ضحايا النزاعات المسلحة الدولية لعام 1977 على ما يلي: "**يلتزم أي طرف سام متعاقد، عند دراسة أو تطوير أو اقتناء سلاح جديد أو أداة للحرب أو إتباع أسلوب للحرب، بأن يتحقق مما إذا كان ذلك محظورا في جميع الأحوال أو في بعضها بمقتضى هذا الملحق " البروتوكول " أو أية قاعدة أخرى من قواعد القانون الدولي التي يلتزم بها الطرف السامي المتعاقد**".

---

[26]– مايكل ن. شميت، مرجع سابق، ص 90.

[27] - CIJ, avis consultatif du 8 juillet 1996, Licéité de la menace ou de l'emploi d'armes nucléaires, « … La question de l'applicabilité des principes et règles du droit humanitaire à la menace ou à l'emploi éventuels d'armes nucléaires, la Cour note que des doutes ont parfois été exprimés sur ce point, au motif que les principes et règles en question se sont développés avant l'invention des armes nucléaires et que les conférences de Genève de 1949 et de 1974-1977, qui ont adopté, respectivement, les quatre conventions de Genève de 1949 et les deux roto col es additionnels v relatifs, n'ont pas spécifiquement traité des armes nucléaires. Ce point de vue est toutefois très minoritaire. De l'avis de la grande majorité des Etats et de la doctrine, il ne fait aucun doute que le droit humanitaire s'applique aux armes nucléaires. Paragraphe 85, CIJ Recueil 1996, p.37, in : https://www.icj-cij.org/public/files/case-related/95/095-19960708-ADV-01-00-FR.pdf

[28]– هاجر ختال، "الوضع القانوني للحرب السيبرانية على ضوء قواعد القانون الدولي"، مجلة التواصل في الاقتصاد والإدارة والقانون، المجلد 25، العدد 3، 2019، ص 167.

فوفقا لهذا النص إذا كيفنا الهجمات السيبرانية بأنها سلاح أو أسلوب من أساليب الحرب، فعلى الدول التحقق من مدى مشروعية استخدامها وفقا لقواعد هذا البروتوكول أو أية قاعدة أخرى من قواعد القانون الدولي، وهو ما يؤكد انطباق أحكام القانون الدولي الإنساني على الحرب السيبرانية.

وهو ما سارت علية محكمة العدل الدولية في مسألة مدى مشروعية التهديد بالأسلحة النووية أو استخدامها، إذ أكدت في رأيها الاستشاري أن القانون الدولي الإنساني قد تطور ليأخذ بعين الاعتبار تغير الظروف، ولا يقتصر تطبيقه على أسلحة الماضي، وإنما ينطبق أيضا على استعمال الأسلحة الجديدة[29].

وفيما يتعلق بحجة اعتبار أن الهجوم على شبكات الحاسوب ليس نزاعا مسلحا لغياب الأعمال العدائية التقليدية، ولأن وجود النزاع المسلح هو شرط لتطبيق القانون الدولي الإنساني، قد أصبحت مسألة نسبية في وقتنا الراهن، فنظرا للتقدم في وسائل وطرق الحرب، ولا سيما حرب المعلومات، فلا يكفي لتطبيق القانون الدولي الإنساني الاعتماد على معيار الفاعل فقط، بل يجب الاعتماد بدرجة أكبر على معيار آثار العمل. فلا أحد ينكر على سبيل المثال أن الحرب البيولوجية أو الكيميائية تخضع للقانون الدولي الإنساني على الرغم من أنها لا تتضمن استعمال أسلحة حركية.

وعلى هذا الأساس فإن مبادئ القانون الدولي الإنساني تنطبق أينما تمت هجمات سيبرانية على دولة بشكل مكثف، فلا يمكن القبول بفرضية أن كل تصرف سيبراني ينشأ عنه قرصنة أو اختراق لبيانات الكترونية هو بمثابة أعمال عنف مسلح. كما يجب أن تهدف هذه الهجمات إلى إلحاق الأذى أو الوفاة للأفراد المدنيين أو إحداث أضرار بالبنى التحتية للدولة المستهدفة. وبهذا المقياس فالهجوم مثلا على شبكات الحاسوب الخاصة بنظام التحكم في مطار تابع لدولة معينة من قبل عملاء دولة أخرى يقتضي بداهة تطبيق أحكام القانون الدولي الإنساني على الرغم من عدم استخدام القوات المسلحة التقليدية [30].

المطلب الثاني: الإشكالات العملية لتطبيق مبادئ سلوكيات الحرب (Jus ad bello) على الحروب السيبرانية

إذا سلمنا بانطباق القانون الدولي الإنساني على الحروب السيبرانية، إلا أن ذلك لا يعني إنكار حقيقة الثغرات التي شهدتها طبيعة الحروب منذ اعتماد اتفاقيات جنيف لعام 1949، حيث أصبحت وسائل وأساليب

---

[29] - CIJ, avis consultatif du 8 juillet 1996, Licéité de la menace ou de l'emploi d'armes nucléaires, « … Il est significatif à cet égard que la thèse selon laquelle les règles du droit humanitaire ne s'appliqueraient pas aux armes nouvelles, en raison même de leur nouveauté, n'ait pas été invoquée en l'espèce. Tout au contraire, l'argument suivant lequel ces armes échapperaient par leur nouveauté au droit international humanitaire a été expressément rejeté en ces termes :
-De manière générale, le droit international humanitaire s'applique à la menace ou à l'emploi d'armes nucléaires comme il s'applique à d'autres armes.
- Le droit international humanitaire a évolué pour tenir compte des circonstances et son application ne se limite pas aux armements du passé... ». Paragraphe 85, CIJ Recueil 1996 ,Op.Cit., pp.37- 38.

[30] – مايكل ن. شميت، المرجع السابق، ص 94.

الحروب متطورة إلى درجة لم يكن يتصورها واضعي تلك الاتفاقيات، مما يؤدي إلى صعوبات عملية في إمكانية تطبيق مبادئ وقواعد القانون الدولي الإنساني على الحروب السيبرانية، وتظهر هذه الإشكالات خاصة عند تطبيق مبادئ سلوكيات الحرب (Jus ad bello) المتمثلة أساسا في مبدأ الضرورة العسكرية (الفرع الأول)، ومبدأ التناسب (الفرع الثاني) ، ومبدأ التمييز (الفرع الثالث).

الفرع الأول: مبدأ الضرورة العسكرية

يعد هذا المبدأ من أهم المبادئ الأساسية التي قام عليها القانون الدولي الإنساني، ويقصد بمبدأ الضرورة العسكرية بشكل عام التزام أطراف النزاع المسلح باستخدام القوة الضرورية لتحقيق هدف القتال الذي يتمثل في إخضاع العدو وتحقيق النصر عليه، فلا يمكن أن نتصور قيام حرب دون أن تكون هزيمة العدو والنصر عليه ضرورة عسكرية لدى قادة وجيوش الدولة الطرف في النزاع . ومن هنا نقول أن الهدف من الضرورة العسكرية هو كسب الحرب في حد ذاتها، ولكن وفق للقوانين المنظمة لها. ومن ثم فإن كل استخدام للقوة المسلحة يتجاوز تحقيق الهدف من القتال يصبح دون مسوغ من مسوغات الضرورة العسكرية يدخل في خانة العمل غير المشروع[31].

وقد أخذت اتفاقيات جنيف لعام 1949 بفكرة الضرورة العسكرية التي قد تمليها ظروف القتال، وجعلت منها مسوغا لبعض الانتهاكات الجسيمة لأحكامها، حيث أشارت هذه الاتفاقيات إلى أن تدمير الممتلكات أو الاستيلاء عليها على نطاق واسع يعد انتهاكا جسيما لهذه الاتفاقيات ما لم تبرره الضرورات الحربية[32].

كما أخذ البروتوكول الإضافي الثاني الملحق باتفاقيات جنيف لعام 1949 المتعلق بحماية ضحايا النزاعات المسلحة غير الدولية لعام 1977 بمبدأ الضرورة العسكرية، فقد أشارت المادة 15 منه إلى حظر مهاجمة المنشآت المحتوية على قوى خطرة حتى لو كانت أهدافا عسكرية، إذا كان من شأن ذلك أن يلحق خسائر فادحة بالسكان المدنيين، كما حظرت المادة 17 من البروتوكول ذاته الترحيل القسري للمدنيين ما لم تبرره الضرورات العسكرية الملحة.

وتظهر إشكاليات تطبيق هذا المبدأ على الهجمات السيبرانية في صعوبة التمييز بين الأهداف العسكرية والمدنية والتي من الممكن أن تستهدف منشآت تقدم خدمة للقطاع العسكري وفي الوقت نفسه للمدنيين. كما أن الضرورات العملية في تطبيق مبدأ الضرورة العسكرية يصعب تطبيقها على الهجمات السيبرانية، فعلى سبيل المثال يمكن تحقيق الأهداف بأسر المقاتلين فقط دون قتلهم، فوجود المقاتل في ساحة القتال أفضل دائما في اتخاذ هكذا قرار والقدرة على التميز بين من يدعي الإصابة والذي قد يمثل تهديدا، وبالتالي يمكن استهدافه وقتله

[31]– خالد روشو، الضرورة العسكرية في نطاق القانون الدولي الإنساني، رسالة دكتوراه في القانون العام، كلية الحقوق والعلوم السياسية، جامعة أبي بكر بلقايد، تلمسان، 2012-2013، ص 83.

[32]– راجع المواد 50، 51، 17 من اتفاقيات جنيف الأولى والثانية والثالثة لعام 1949على التوالي.

وفقا لمبدأ الضرورة العسكرية، وبين من جرح جرحا بالغا حتى أنه لم يعد يمثل تهديدا، ذلك أن مبدأ الضرورة العسكرية يستلزم أن تكون القوة المستخدمة لا تتضمن عمليات الثأر، بالإضافة إلى عدم وجود بديل آخر للإجراءات أو التدابير المقرر استخدامها استنادا لمبدأ الضرورة[33].

الفرع الثاني: مبدأ التناسب

يعد مبدأ التناسب أحد المبادئ الجوهرية التي يجب تطبيقها أثناء النزاعات المسلحة سواء كانت دولية أم غير دولية لأنه يهدف إلى الحد أو التقليل من الخسائر وأوجه المعاناة المترتبة على العمليات العسكرية سواء بالنسبة للأشخاص أو الأشياء.

ويعد هذا المبدأ من المسائل الدقيقة التي يصعب تحقيقها في بعض الأحيان أثناء القتال وإدارة العمليات الحربية، إذ يحظر القانون الدولي الإنساني الهجمات غير المتناسبة من أجل إنقاذ المدنيين والأعيان المدنية من آثار الحرب بقدر الإمكان[34].

ويعتمد مبدأ التناسب على تحقيق التوازن بين أمرين جوهريين، هما الميزة العسكرية المتوقعة من أعمال القتال من جانب والخسائر التي تلحقها هذه العمليات بالمدنيين والأعيان المدنية من جانب آخر، ويشترط في الميزة العسكرية أن تكون متوقعة وتتحقق عادة من خلال السيطرة على جزء من الإقليم أو تدمير القوات العسكرية للعدو أو إضعافها، كما يشترط فيها أن تكون ملموسة ومباشرة[35].

وتظهر إشكاليات تطبيق هذا المبدأ على الهجمات السيبرانية في أن برمجة تلك العمليات الالكترونية لا يمكن في مقدورها تطبيق مبدأ التناسب، لاسيما إذا ما علمنا أن معادلة التناسب تعد معادلة صعبة ودقيقة حتى أثناء وإدارة العمليات الحربية التقليدية، فتحقيق المهمة القتالية وإحراز النصر هدف أساسي للقوات العسكرية، وتنفيذ القوانين وضبط التدمير وعدم إلحاق أضرار مفرطة بالخصم التزام قانوني واجب النفاذ، وبالتالي يحتاج إلى قائد عسكري متمكن يسوي ميزان هذه المعادلة، والأمر بدون شك يزداد تعقيدا إذا ما تعلق الأمر بالهجمات السيبرانية[36].

---

[33]– يحيى ياسين سعود، المرجع السابق، ص 96.

[34]– يقصد بالهجوم غير المتناسب حسب المادة (51/5/ب) من البروتوكول الإضافي الأول الملحق باتفاقيات جنيف لعام 1949 المتعلق بحماية ضحايا النزاعات المسلحة الدولية لعام 1977 بأنه: "**الهجوم الذي يمكن أن يتوقع منه أن يسبب خسائر في أرواح المدنيين أو إصابة بهم أو أضرارا بالأعيان المدنية، أو أن يحدث خلطا بين هذه الخسائر والأضرار بشكل يفرط في تجاوز ما ينتظر أن يسفر عنه ذلك الهجوم من ميزة عسكرية ملموسة ومباشرة**".

[35]– مصعب التجاني، "القانون الدولي الإنساني وحماية المدنيين خلال النزاعات المسلحة " نموذج الحالة السورية""، المركز الديمقراطي العربي للدراسات الإستراتيجية والسياسية والاقتصادية، برلين، ألمانيا، 2019، ص ص 69-70.

[36]– يحيى ياسين سعود، المرجع السابق، ص ص 96-97.

وهو ما أكده فقهاء القانون الدولي إذ يرى الأستاذ (Shin) أن مبدأ التناسب في استخدام القوة السيبرانية لا يزال غامضا ويحتاج إلى أجوبة أهمها كيف يمكن ضمان مبدأ التناسب في الرد على الهجمات السيبرانية.

ويتفق الأستاذ (Rex) مع ما ذهب إليه الأستاذ (Shin) بقوله: " إذا تم توجيه هجمات سيبرانية ضد بنى تحتية ثنائية الاستعمال (مدنية وعسكرية) وعن بعد، فلا يبدو أن المنفعة العسكرية ستكون واضحة، ما يجعل تطبيق مبدأ التناسب أثناء الهجمات السيبرانية أمرا في غاية الصعوبة"[37].

الفرع الثالث: مبدأ التمييز

يعتبر مبدأ التمييز من أهم المبادئ التي جاء بها القانون الدولي الإنساني لضبط العمليات الحربية، ويتضمن هذا المبدأ تطبيقين أساسيين هما :ضرورة التمييز بين المقاتلين وغير المقاتلين في جميع الأوقات، وأن يتمتع المدنيين بالحصانة ضد الهجمات التي توجه إلى الأهداف العسكرية. وضرورة التمييز بين الأعيان المدنية والأعيان العسكرية، وأنه لا يجوز مهاجمة الأعيان المدنية بأي حال من الأحوال[38].

وقد تم التطرق إلى مبدأ التمييز بصورة واضحة في المادة 48 من البروتوكول الإضافي الأول الملحق باتفاقيات جنيف لعام 1949 المتعلق بحماية ضحايا النزاعات المسلحة الدولية لعام 1977 التي نصت على ما يلي: " **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**".

ويعد تطبيق مبدأ وجوب التمييز بين المقاتلين والمدنيين على الهجمات السيبرانية مسألة في غاية التعقيد –على عكس الهجمات التقليدية–إذ سيكون المهاجم في الأغلب بعيدا عن المكان المستهدف من الهجوم ولمسافة قد تتجاوز المئات من الكيلومترات، ما يعني أن التمييز بين المقاتلين والمدنيين هو أمر صعب إذا لم يكن مستحيلا[39].

كما تصبح مسألة التمييز بين الأهداف المدنية والعسكرية في الهجمات السيبرانية صعبة، خاصة أن نظم الحواسيب العسكرية غالب ما تتصل بالنظم التجارية والمدنية وتعتمد عليها كليا أو جزئيا، بل وقد يكون هناك تداخل بين الاستخدامات المدنية والعسكرية بارتباطهما بشبكة واحدة ووسيط واحد هو الفضاء السيبراني، ومن ثم يكون من المستحيل شن هجوم سيبراني على بنى تحتية عسكرية وجعل آثارها تقتصر على هدف عسكري

---

[37]– أحمد عبيس نعمة الفتلاوي، المرجع السابق، ص 638.

[38]– ساهم مبدأ التمييز إلى حد كبير في حماية غير المقاتلين من الفئات التي تتمتع بالحماية من :جرحى ومرضى وغرقى، وأسرى حرب، ومدنيين، والقائمين بالخدمات الإنسانية، وبالتالي كفل لهم حماية شرفهم وعقائدهم، وعاداتهم، ومعاملتهم بإنسانية وخصوصا الحماية ضد أشكال العنف أو التهديد وغيرها، كما ضمن مبدأ التمييز الحماية للأعيان غير العسكرية والمتمثلة في :الأعيان المدنية، والثقافية، والبيئية الطبيعية، والأشياء اللازمة لحماية السكان المدنيين. راجع: خالد روشو، المرجع السابق، ص 142.

[39]– أحمد عبيس نعمة الفتلاوي، المرجع السابق، ص 636.

وحسب ودون الإضرار بالمدنيين والمنشآت المدنية[40]. فعلى سبيل المثال عندما تتعرض الحواسيب أو الشبكات المعلوماتية التابعة لقوات عسكرية لدولة ما لهجمات سيبرانية، قد تجعل المدنيين عرضة لخطر الحرمان من الاحتياجات الأساسية مثل مياه الشرب والرعاية الطبية والكهرباء نظرا لاعتمادها على نفس الشبكات التي تم استهدافها.

الخاتمة

فرضت خطورة الحروب السيبرانية على الدول والعديد من المنظمات الدولية إعادة التفكير في مفهوم الأمن الدولي، الذي يتيح للدول من أن تصبح في مأمن من المخاطر التي يمكن أن تتعرض لها سواء في سلامة أراضيها أو استقلالها السياسي أو حماية البنى التحتية لمنشأتها الحيوية ومن كافة أوجه الاستخدام غير المشروع لتكنولوجيا الاتصال والمعلومات. ومن أهم الإشكاليات التي تواجه المجتمع الدولي هو ما يتعلق بالجدل حول مدى اعتبار الأسلحة السيبرانية كالأسلحة غير التقليدية وإمكانية إخضاعها لقيود الاتفاقيات الدولية المكونة للقانون الدولي الإنساني.

وخلصنا أن فقه القانون الدولي يدعم اعتبار الأسلحة السيبرانية مثلها مثل الأسلحة الأخرى (التقليدية والمتطورة)، التي يتم استعمالها في النزاعات المسلحة، والمنظمة بموجب قواعد ومبادئ القانون الدولي الإنساني، كما اعتبر الحرب السيبرانية بمثابة حرب حقيقية نظرا لما تلحقه من آثار قد تضاهي في جسامتها أضرار الحروب التقليدية.

وبالرغم من ذلك تبقى مسألة تطبيق مبادئ وقواعد القانون الدولي الإنساني على الحرب السيبرانية غير عملية في وقتنا الراهن، وذلك بسبب الفوارق الجوهرية بين الهجوم المسلح المادي والهجوم السيبراني، وكذا عدم إمكانية إسقاط بعض مبادئ القانون الدولي الإنساني على الهجمات التي تتم في الفضاء السيبراني.

ولتطبيق أمثل لقواعد ومبادئ القانون الدولي على الحروب السيبرانية نقترح مجموعة من التوصيات المتمثلة فيما يلي:

– وضع تعريف دقيق لمصطلح الحرب السيبرانية من خلال عقد مؤتمر عالمي تحت رعاية منظّمة الأمم المتّحدة، وضمن اتفاقية شاملة وعامة لتنظيم الفضاء السيبراني وفق مبدأ حظر استخدام القوة في العلاقات الدولية.

[40]– بلقاسم بن صابر، محمد حيدرة، "الهجمات السيبرانية ومواجهتها في ضوء القانون الدولي المعاصر"، مجلة حقوق الإنسان والحريات العامة، العدد 4، 2017، ص 202. وانظر أيضا: عادل عبد الصادق، أسلحة الفضاء الإلكتروني في ضوء القانون الدولي الإنساني، مكتبة الإسكندرية، وحدة الدراسات المستقبلية، مصر، 2016، ص 96.

– الدعوة إلى اتفاقية دولية للحد من التسلح داخل الفضاء السيبراني مثل تلك الاتفاقيات التي تم إبرامها سابقا بشأن حظر الانتشار النووي والكيماوي والبيولوجي، حيث يمكن أن تسهم مثل هذه الاتفاقية في حال تطبيقها على الفضاء السيبراني وضع قيود على استخدام الأسلحة السيبرانية وانتشارها وتطويرها.

– إعطاء تفسير أوسع لمبادئ وقواعد القانون الدولي الإنساني، ومنها على سبيل المثال ما يعرف بشرط مارتنز لتشمل جميع الظروف المتغيرة، لاسيما تلك المتعلقة بوسائل وأساليب القتال الحديثة.

– تعديل اتفاقيات جنيف الأربعة لعام 1949 التي تشكل حجر الأساس للقانون الدولي الإنساني، بغرض تجريم الهجمات السيبرانية التي تستهدف البنى التحتية للدول مثل محطات الكهرباء والمياه التي تعد ضرورية لبقاء السكان المدنيين أحياء.

– إقرار مسؤولية الدولة على جميع التصرفات التي تقوم بهدف تطوير الأسلحة السيبرانية لاستعمالها بهدف الإضرار بمصالح الدول الأخرى، واعتبار ذلك بمثابة خرق لالتزام دولي يخضع إلى القانون الدولي الجنائي.

قائمة المراجع

أولا: المراجع باللغة العربية

الكتب

1- إيهاب خليفة ، كيف يمكن أن تدير الدول شؤونها في عصر الإنترنت، العربي للنشر والتوزيع، القاهرة ، 2017.

2- إيهاب خليفة، الحرب السيبرانية، الاستعداد لقيادة المعارك العسكرية في الميدان الخامس، العربي للنشر والتوزيع، القاهرة، 2021.

3- عادل عبد الصادق، أسلحة الفضاء الإلكتروني في ضوء القانون الدولي الإنساني، مكتبة الإسكندرية، وحدة الدراسات المستقبلية، مصر، 2016.

4- مصعب التجاني، القانون الدولي الإنساني وحماية المدنيين خلال النزاعات المسلحة " نموذج الحالة السورية"، المركز الديمقراطي العربي للدراسات الإستراتيجية والسياسية والاقتصادية، برلين، ألمانيا، 2019.

الرسائل والمذكرات الجامعية

1- خالد روشو، الضرورة العسكرية في نطاق القانون الدولي الإنساني، رسالة دكتوراه في القانون العام، كلية الحقوق والعلوم السياسية، جامعة أبي بكر بلقايد، تلمسان، 2012-2013

2- وليد غسان سعيد جلعود، دور الحرب الإلكترونية في الصراع العربي الإسرائيلي، مذكرة ماجستير في التخطيط والتنمية السياسية، كلية الدراسات العليا، جامعة النجاح الوطنية نابلس، فلسطين، 2013.

المقالات

1- أحمد عبيس نهعمة الفتلاوي، "الهجمات السيبرانية: مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر"، مجلة المحقق الحلي للعلوم القانونية والسياسية، العدد 4، السنة الثامنة، 2016.

2- أسامة صبري محمد، "الحرب الالكترونية و مبدأ التمييز في القانون الدولي الإنساني"، مجلة القانون للدراسات و البحوث القانونية، العدد 7، 2013.

3- بلقاسم بن صابر، محمد حيدرة، "الهجمات السيبرانية ومواجهتها في ضوء القانون الدولي المعاصر"، مجلة حقوق الإنسان والحريات العامة، العدد 4، 2017.

4- حكيم غريب، صبرينة شرقي،" تداعيات الحرب الإلكترونية على العلاقات الدولية: دراسة في الهجوم الإلكتروني على إيران (فيروس ستكنست)"، دفاتر السياسة والقانون، المجلد 12، العدد 2، 2020.

5- سعيد درويش، "الحروب السيبرانية وأثرها على حقوق الإنسان: دراسة على ضوء أحكام دليل " تالين "، المجلة الجزائرية للعلوم القانونية والاقتصادية والسياسية، المجلد 45، العدد 5، 2017.

6- سعيد درويش، "ماهية الحرب الإلكترونية في ضوء قواعد القانون الدولي"، حوليات جامعة الجزائر 1، المجلد 29، العدد 2، 2016.

7- طالب حسن موسى، عمر محمود أعمر، "الإنترنت قانونا"، مجلة الشريعة والقانون، العدد 37، 2016.

8- عمر محمود أعمر، "الحرب الإلكترونية في القانون الدولي الإنساني"، الشريعة والقانون، المجلد 46، العدد 3، 2019.

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

10- هاجر ختال، "الوضع القانوني للحرب السيبرانية على ضوء قواعد القانون الدولي"، مجلة التواصل في الاقتصاد والإدارة والقانون، المجلد 25، العدد 3، 2019.

11- يحيى مفرح الزهراني، "الأبعاد الإستراتيجية والقانونية للحرب السيبرانية"، مجلة البحوث والدراسات، العدد 23، السنة 14، 2017.

12- يحيى ياسين سعود،" الحرب السيبرانية في ضوء قواعد القانون الدولي الإنساني"، المجلد 4، العدد 4، 2018.

الاتفاقيات الدولية

1- اتفاقية جنيف الأولى لتحسين حال الجرحى والمرضى بالقوات المسلحة في الميدان، لسنة 1949.

2- اتفاقية جنيف الثانية لتحسين حال جرحى ومرضى وغرقى القوات المسلحة في البحار، لسنة 1949.

3- اتفاقية جنيف الثالثة بشأن معاملة أسرى الحرب، لسنة 1949.

4- البرتوكول الإضافي الأول الملحق باتفاقات جنيف لعام 1949 المتعلق بحماية ضحايا المنازعات الدولية المسلحة، لسنة 1977.

5- البرتوكول الإضافي الثاني الملحق باتفاقات جنيف لعام 1949 المتعلق بحماية ضحايا المنازعات المسلحة غير الدولية، لسنة 1977.

ثانيا: المراجع باللغة الفرنسية

Articles

1- Barbara Louis-SIDNEY, La dimension juridique du cyberespace, Revue internationale et stratégique, n° 87, 2012/3.

2- Jean-Loup SAMAAN, Les cyber-conflits, une révolution géopolitique?, AFRI, Volume XI, 2010.

3- Oriane BARAT- GINIES, Existe-t-il un droit international du cyberespace ? , La Découverte, n° 152-153, 2014.

4-Evelyne AKOTO, Les cyberattaques étatiques constituent-elles des actes d'agression en vertu du droit international public ? : Première partie, Revue de droit d'Ottawa, Volume 46, n° 1, 2014- 2015.

Jurisprudence

- CIJ, avis consultatif du 8 juillet 1996, Licéité de la menace ou de l'emploi d'armes nucléaires, Recueil de la CIJ 1996, in : https://www.icj-cij.org/public/files/case-related/95/095-19960708-ADV-01-00-FR.pdf